Version:1.10.0.3

Hash:HlOvZs2kwNUf/TwjCwA3pAMsBx0=



Data Protection Manual

For Police Data Protection Professionals

Version 1.2

22nd March 2021

Updated to be in accord with:

General Data Protection Regulation

Data Protection Act 2018

The Data Protection (Charges and Information) Regulations 2018 (SI No. 480)

The Data Protection Act 2018 (Commencement No. 1 and Transitional and Saving Provisions) Regulations 2018 (SI. 625)

Note: This Manual has not been updated to reflect the legislative changes arising from [The Data Protection, Privacy and Electronic Communications (Amendments etc)(EU Exit) Regulations 2019](https://www.legislation.gov.uk/ukdsi/2019/9780111177594/contents) as amended by [The Data Protection, Privacy and Electronic Communications (Amendments etc)(EU Exit) Regulations 2020](https://www.legislation.gov.uk/ukdsi/2020/9780348213522).

This manual has been produced by the National Police Chiefs’ Council (NPCC) Data Protection, Freedom of Information, information Sharing and Disclosure Portfolio Group on behalf of the NPCC. It is updated and adapted to reflect decisions made by the NPCC, views of the Information Commissioner’s Office (ICO) (where appropriate) and the evolution of the legislation as it is interpreted, challenged or reviewed. All modifications to this manual will be the responsibility of the NPCC Data Protection, Freedom of Information, information Sharing and Disclosure Portfolio Group.

All enquiries about this manual should be addressed to the Secretary of the NPCC Data Protection, Freedom of Information, information Sharing and Disclosure Portfolio Group c/o ACRO, PO Box 481, Fareham, PO14 9FS.

Acknowledgement: The NPCC would like to express its thanks to Andy Begent, Essex Police, and colleagues who have assisted in the creation of this Manual.

© National Police Chiefs’ Council (2018 2019 2020)

NPCC, 1st Floor, 10 Victoria Street, London SW1H 0NN

Enquiries regarding this Manual should be directed to [dataprotection@npcc.pnn.police.uk](mailto:dataprotection@npcc.pnn.police.uk)

All rights reserved. Outside of the police service no part of this publication may be reproduced, modified, amended, stored in any retrieval system or transmitted, in any form or by any means, without the prior written permission of NPCC or their duly authorised representative.

# Contents

[Contents 3](#_Toc67323832)

[1 Introduction 9](#_Toc67323833)

[1.1 Foreword by NPCC Information Management Lead 9](#_Toc67323834)

[1.2 Terminology Used, Manual Structure and Standards (Appendix J) 9](#_Toc67323835)

[1.3 Overview of Legislation 10](#_Toc67323836)

[1.4 GDPR and DPA elements not covered 11](#_Toc67323837)

[1.5 Territorial Extent, Commencement, and Transitional Provisions of Act 13](#_Toc67323838)

[1.5.1 Territorial Extent (DPA Part 7 Section 207) 13](#_Toc67323839)

[1.5.2 Transitional provisions (DPA Part 7 Section 213 & Schedule 20) 15](#_Toc67323840)

[1.5.3 Commencement (DPA Part 7 Section 212) 16](#_Toc67323841)

[2 Governance & Responsibilities 17](#_Toc67323842)

[2.1 Overview 17](#_Toc67323843)

[2.2 National Police Chiefs’ Council (NPCC) and its Information Management Operational Requirements Coordinating Committee (IMORCC) 17](#_Toc67323844)

[2.3 Chief Officer (Chief Constable or Commissioner) 17](#_Toc67323845)

[2.4 Senior Information Risk Owner 17](#_Toc67323846)

[2.5 Information Asset Owner 18](#_Toc67323847)

[2.6 Data Protection Officer (DPO) (Appendix A & Appendix B) 18](#_Toc67323848)

[2.6.1 Overview 18](#_Toc67323849)

[2.6.2 Designation 19](#_Toc67323850)

[2.6.3 Position 20](#_Toc67323851)

[2.6.4 Tasks 20](#_Toc67323852)

[2.6.5 NPCC Data Protection Officer 21](#_Toc67323853)

[2.7 Records Manager 21](#_Toc67323854)

[2.8 Information Security Officer 21](#_Toc67323855)

[2.9 All staff 22](#_Toc67323856)

[2.10 Structure 22](#_Toc67323857)

[2.11 Information Commissioner/Commissioner 22](#_Toc67323858)

[2.12 Data protection training, awareness and guidance 22](#_Toc67323859)

[2.13 Data Protection Compliance Auditing, Data Quality Auditing and Monitoring 23](#_Toc67323860)

[2.14 National Police Information Systems 23](#_Toc67323861)

[2.15 Data Protection Fee (Data Protection (Charges and Information) Regulations 2018) 23](#_Toc67323862)

[3 Definitions 25](#_Toc67323863)

[3.1 Introduction 25](#_Toc67323864)

[3.2 Key Definitions Applicable to General Processing (GDPR/DPA Part 2) 25](#_Toc67323865)

[3.3 Key Definitions Applicable to Law Enforcement Processing 26](#_Toc67323866)

[3.4 Personal Data and Data Subject (GDPR Article 4 DPA Part 1 Section 3) 27](#_Toc67323867)

[3.5 Special Category Data (Special Categories of Personal Data) and Sensitive Processing (GDPR Article 9 DPA Part 3 Section 35) 28](#_Toc67323868)

[3.6 Processing (GDPR Article 4 DPA Part 1 Section 3) 28](#_Toc67323869)

[3.7 Restriction of Processing (GDPR Article 4 DPA Part 3 Section 33) 29](#_Toc67323870)

[3.8 Profiling (GDPR Article 4 DPA Part 3 Section 33) 30](#_Toc67323871)

[3.9 Pseudonymisation (GDPR Article 4) 30](#_Toc67323872)

[3.10 Filing System (GDPR Article 4 DPA Part 1 Section 3) 30](#_Toc67323873)

[3.11 Controller (GDPR Article 4, DPA Part 1 Section 3) 30](#_Toc67323874)

[3.12 Processor (GDPR Article 4 DPA Part 3 Section 32) 32](#_Toc67323875)

[3.13 Recipient (GDPR Article 4 DPA Part 3 Section 33) 32](#_Toc67323876)

[3.14 Third Party (GDPR Article 4) 33](#_Toc67323877)

[3.15 Consent (GDPR Article 4) 33](#_Toc67323878)

[3.16 Personal Data Breach (GDPR Article 4 DPA Part 3 Section 33) 33](#_Toc67323879)

[3.17 Genetic Data (GDPR Article 4 DPA Part 7 Section 205) 34](#_Toc67323880)

[3.18 Biometric Data (GDPR Article 4 DPA Part 7 Section 205) 34](#_Toc67323881)

[3.19 Data Concerning Health & Health Record (GDPR Article 4, DPA Part 7 Section 205) 34](#_Toc67323882)

[3.20 Public Authority and Public Body (DPA Part 2 Section 7) 35](#_Toc67323883)

[3.21 GDPR (DPA Part 1 Section 3) 36](#_Toc67323884)

[3.22 Applied GDPR (DPA Part 1 Section 3) 36](#_Toc67323885)

[3.23 Law Enforcement Directive (DPA Part 1 Section 3) 36](#_Toc67323886)

[3.24 Competent Authority (DPA Part 3 Section 30, Schedule 7) 36](#_Toc67323887)

[3.25 Law Enforcement Purposes (DPA Part 3 Section 31) 38](#_Toc67323888)

[3.26 Employee (DPA Part 3 Section 33) 39](#_Toc67323889)

[3.27 Third Country (DPA Part 3 Section 33) 39](#_Toc67323890)

[3.28 Health Professional & Social Work Professional (DPA Part 7 Section 204) 39](#_Toc67323891)

[3.29 Criminal Offence Data (GDPR Article 10, DPA Part 2 Section 11) 40](#_Toc67323892)

[4 General Processing (GDPR & DPA Part 2) 42](#_Toc67323893)

[4.1 Scope: General Processing, GDPR and Applied GDPR Scheme 42](#_Toc67323894)

[4.1.1 Examples of Police General Processing 42](#_Toc67323895)

[4.1.2 Examples of Exclusions from Police General Processing 43](#_Toc67323896)

[4.1.3 Processing which does not require identification (GDPR Article 11) 43](#_Toc67323897)

[4.2 General Processing Data Protection Principles (GDPR & DPA Part 2) 44](#_Toc67323898)

[4.2.1 Overview of General Processing Principles (GDPR Article 5) 44](#_Toc67323899)

[4.2.2 General Processing; First Principle – Lawfulness, Fairness & Transparency (GDPR Article 5) 46](#_Toc67323900)

[4.2.3 General Processing; Second Principle – Purpose Limitation (GDPR Article 5) 57](#_Toc67323901)

[4.2.4 General Processing; Third Principle – Data Minimisation (GDPA Article 5) 58](#_Toc67323902)

[4.2.5 General Processing; Fourth Principle – Accuracy (GDPR Article 5) 60](#_Toc67323903)

[4.2.6 General Processing: Fifth Principle – Storage Limitation (GDPA Article 5) 61](#_Toc67323904)

[4.2.7 General Processing: Sixth Principle – Integrity & Confidentiality (GDPR Article 5) 63](#_Toc67323905)

[4.2.8 General Processing; Accountability Requirement 67](#_Toc67323906)

[4.2.9 Police Approach to Data Quality on Major IT Systems 67](#_Toc67323907)

[4.3 General Data Processing Exemptions/Restrictions to Data Subject Rights (DPA Part 2 Section 15) 69](#_Toc67323908)

[4.3.1 Overview 69](#_Toc67323909)

[4.3.2 DPA Schedule 2 Part 1 Exemptions etc. from the GDPR 70](#_Toc67323910)

[4.3.3 DPA Schedule 2 Part 2 Exemptions etc. from the GDPR 72](#_Toc67323911)

[4.3.4 DPA Schedule 2 Part 3 Exemptions etc. from the GDPR 73](#_Toc67323912)

[4.3.5 DPA Schedule 2 Part 4 Exemptions etc. from the GDPR 75](#_Toc67323913)

[4.3.6 DPA Schedule 2 Part 5 Exemptions etc. from the GDPR 77](#_Toc67323914)

[4.3.7 DPA Schedule 2 Part 6 Exemptions etc. from the GDPR 79](#_Toc67323915)

[4.3.8 DPA Schedule 3 Exemptions etc. from the GDPR: health, social work, education and child abuse 82](#_Toc67323916)

[4.3.9 DPA Schedule 4 Exemptions etc. from the GDPR: disclosure prohibited or restricted by an enactment 82](#_Toc67323917)

[4.4 General Processing Rights 82](#_Toc67323918)

[4.4.1 Overview of General Processing Rights 82](#_Toc67323919)

[4.4.2 Transparent information, communication and modalities for the exercise of the rights of the data subject (GDPR Article 12) 83](#_Toc67323920)

[4.4.3 Right to be Informed (Transparency & Privacy Notice) (GDPR Articles 13 & 14) 85](#_Toc67323921)

[4.4.4 Right of Access by the Data Subject (GDPR Article 15, DPA Part 2 Section 12) 89](#_Toc67323922)

[4.4.5 Right to Rectification (GDPR Article 16) 95](#_Toc67323923)

[4.4.6 Right to Erasure (“Right to be Forgotten”) (GDPR Article 17) 97](#_Toc67323924)

[4.4.7 Right to Restriction of Processing (GDPR Article 18) 100](#_Toc67323925)

[4.4.8 Notification obligation regarding rectification or erasure of personal data or restriction of processing (GDPR Article 19) 102](#_Toc67323926)

[4.4.9 Right to Data Portability (GDPR Article 20) 103](#_Toc67323927)

[4.4.10 Right to Object (GDPR Article 21) 104](#_Toc67323928)

[4.4.11 Automated individual decision-making, including profiling (GDPR Article 22) 106](#_Toc67323929)

[4.4.12 Data subject’s rights and other prohibitions and restrictions (Part 7 Section 186) 109](#_Toc67323930)

[4.4.13 Summary table of exemptions and restrictions from General Processing Rights 109](#_Toc67323931)

[4.5 General Processing Controller & Processor Obligations 110](#_Toc67323932)

[4.5.1 Overview & Scope (GDPR Article 24) 110](#_Toc67323933)

[4.5.2 Data Protection by Design & Default (GDPR Article 25) 112](#_Toc67323934)

[4.5.3 Joint Controllers (GDPR Article 26) 117](#_Toc67323935)

[4.5.4 Obligations on Processors (GDPR Article 28 and GDPR Article 29) 119](#_Toc67323936)

[4.5.5 Records of Processing Activities (RoPA) (GDPR Article 30) 122](#_Toc67323937)

[4.5.6 General Data Processing & Procurement 123](#_Toc67323938)

[4.5.7 HR Processing 123](#_Toc67323939)

[4.6 Transfers to Third Countries or International Organisations (GDPR Articles 44 to 49) 123](#_Toc67323940)

[4.7 Processing for archiving, research and statistical purposes (GDPR Article 89) 132](#_Toc67323941)

[4.8 Re-use of Data Collected for General Processing for Law Enforcement Processing 133](#_Toc67323942)

[4.9 Information Sharing Under the GDPR Guidance & Template (Appendix M) 134](#_Toc67323943)

[5 Comparison between General Processing and Law Enforcement obligations 135](#_Toc67323944)

[5.1 Overview 135](#_Toc67323945)

[5.2 Data Protection Principles Comparison 135](#_Toc67323946)

[5.3 Fair Processing Comparison 135](#_Toc67323947)

[5.4 Data Subject Rights Comparison 135](#_Toc67323948)

[5.5 Data Subject Rights Requirements Comparison 137](#_Toc67323949)

[5.6 Information to be supplied under the Right of Access Comparison 137](#_Toc67323950)

[5.7 Data Controller and Data Processor Obligations Comparison 137](#_Toc67323951)

[5.8 Exemptions/Restrictions Comparison 137](#_Toc67323952)

[6 Law Enforcement Processing (Part 3 of DPA) 138](#_Toc67323953)

[6.1 Scope: Competent Authorities & Law Enforcement Purposes (DPA Part 3 Section 29, Section 30, Section 31) 138](#_Toc67323954)

[6.1.1 Examples of Police Law Enforcement Processing 139](#_Toc67323955)

[6.2 Law Enforcement Principles 139](#_Toc67323956)

[6.2.1 Overview and general duty of Controller (DPA Part 3 Section 34) 139](#_Toc67323957)

[6.2.2 First Law Enforcement Principle – Lawful & Fair Processing (DPA Part 3 Section 35) 140](#_Toc67323958)

[6.2.3 Second Law Enforcement Principle – Specific, explicit & legitimate purpose (DPA Part 3 Section 36) 143](#_Toc67323959)

[6.2.4 Third Law Enforcement Principle – Adequate, relevant & not excessive (DPA Part 3 Section 37) 144](#_Toc67323960)

[6.2.5 Fourth Law Enforcement Principle – Accurate & kept-up-to-date where necessary (DPA Part 3 Section 38) 145](#_Toc67323961)

[6.2.6 Fifth Law Enforcement Principle – Kept no longer than is necessary (DPA Part 3 Section 39) 148](#_Toc67323962)

[6.2.7 Sixth Law Enforcement Principle – Processed securely (DPA Part 3 Section 40, Section 66) 149](#_Toc67323963)

[6.3 Law Enforcement Processing Rights 152](#_Toc67323964)

[6.3.1 Overview 152](#_Toc67323965)

[6.3.2 Law Enforcement Processing Rights: Overview & Scope (DPA Part 3 Section 43) 152](#_Toc67323966)

[6.3.3 Information for Data Subjects (DPA Part 3 Section 44) (Appendix G & Appendix N) 153](#_Toc67323967)

[6.3.4 Right of Access (DPA Part 3 Section 45) 155](#_Toc67323968)

[6.3.5 Rights to Rectification, Erasure or Restriction (DPA Part 3 Section 46 & Section 47) 160](#_Toc67323969)

[6.3.6 Rights re Automated Decision-Making (DPA Part 3 Section 49 & Section 50) 165](#_Toc67323970)

[6.3.7 Subject Rights: Supplementary (DPA Part 3 Section 51) 167](#_Toc67323971)

[6.3.8 Form of Provision of Information (DPA Part 3 Section 52) 167](#_Toc67323972)

[6.3.9 Data subject’s rights and other prohibitions and restrictions (DPA Part 7 Section 186) 170](#_Toc67323973)

[6.3.10 Summary table of exemptions and restrictions from Law Enforcement Rights 170](#_Toc67323974)

[6.4 Law Enforcement Controller & Processor Obligations 172](#_Toc67323975)

[6.4.1 Overview & Scope (DPA Part 3 Section 55) 172](#_Toc67323976)

[6.4.2 Obligation to Ensure Compliance (DPA Part 3 Section 56 & Section 57) 173](#_Toc67323977)

[6.4.3 Joint Controller Clarity of Responsibilities (DPA Part 3 Section 58) (Appendix F) 174](#_Toc67323978)

[6.4.4 Obligations on Processors (DPA Part 3 Section 59 & Section 60) 176](#_Toc67323979)

[6.4.5 Records of Processing Activities (RoPA) (DPA Part 3 Section 61) 177](#_Toc67323980)

[6.4.6 Logging Requirements (DPA Part 3 Section 62) 179](#_Toc67323981)

[6.4.7 Data Protection Impact Assessments (DPIA’s) (DPA Part 3 Section 64 & Section 65) 180](#_Toc67323982)

[6.5 Transfers to Third Countries (DPA Part 3 Section 72, Section 73, Section 74, Section 75, Section 76, Section 77, and Section 78) 182](#_Toc67323983)

[6.6 Safeguards: Archiving (DPA Part 3 Section 41) 187](#_Toc67323984)

[6.7 Safeguards: Sensitive Processing (Appropriate Policy Document) (DPA Part 3 Section 42) (Appendix D) 187](#_Toc67323985)

[6.8 Re-use of Data Collected for Law Enforcement Processing for General Processing 189](#_Toc67323986)

[6.9 Request to external organisation for the disclosure of personal data to the police (Appendix E) 189](#_Toc67323987)

[7 Intelligence Service Processing (Part 4 of the Act) 190](#_Toc67323988)

[7.1 Overview: 190](#_Toc67323989)

[8 Assessing Data Protection Compliance 191](#_Toc67323990)

[8.1 Audit 191](#_Toc67323991)

[8.2 Consensual Audit by the Commissioner (DPA Part 5 Section 129) 191](#_Toc67323992)

[8.3 Aide Memoire for a model approach to assessing data protection compliance 191](#_Toc67323993)

[9 The Commissioner, Enforcement & Offences (Part 5, 6 & 7 of Act) 199](#_Toc67323994)

[9.1 Co-operation with the Commissioner & their Powers 199](#_Toc67323995)

[9.1.1 Co-operation with the Commissioner (GDPR Article 31, DPA Part 5 Section 63) 199](#_Toc67323996)

[9.1.2 Disclosure of information to the Commissioner (DPA Part 5 Section 131) 199](#_Toc67323997)

[9.1.3 Offence regarding breach of confidentiality by the Commissioner (DPA Part 5 Section 132) 200](#_Toc67323998)

[9.1.4 Information Notices (DPA Part 6 Section 142, Section 143, Section 144) 200](#_Toc67323999)

[9.1.5 Information Orders (DPA Part 6 Section 145) 203](#_Toc67324000)

[9.1.6 Assessment Notices (DPA Part 6 Section 146 & Section 147) 203](#_Toc67324001)

[9.1.7 Destroying or falsifying information and documents etc. (DPA Part 6 Section 148) 206](#_Toc67324002)

[9.1.8 Enforcement Notices (DPA Part 6 Section 149, Section 150, Section 151, Section 152, Section 153) 207](#_Toc67324003)

[9.1.9 Powers of Entry & Inspection (DPA Part 6 Section 154 & Schedule 15) 210](#_Toc67324004)

[9.1.10 Penalty Notices (DPA Part 6 Section 155, Section 156, Section 157, Section 158, Section 159, Schedule 16) 210](#_Toc67324005)

[9.1.11 Appeals (DPA Part 6 Section 162, Section 163, Section 164) 216](#_Toc67324006)

[9.2 Commissioner’s Codes of Practice 217](#_Toc67324007)

[9.2.1 Overview 217](#_Toc67324008)

[9.3 Handling allegations of criminal offences under the Act 220](#_Toc67324009)

[9.3.1 Offence not connected to the force 220](#_Toc67324010)

[9.3.2 Offence or misconduct identified by or reported to the police relating to police-held personal data 221](#_Toc67324011)

[9.3.3 Offence identified or reported to the Information Commissioner relating to police-held personal data 222](#_Toc67324012)

[9.3.4 Victim care 222](#_Toc67324013)

[9.4 Offences 222](#_Toc67324014)

[9.4.1 Offence: Unlawful obtaining etc of personal data (DPA Part 6 Section 170) 222](#_Toc67324015)

[9.4.2 Offence: Re-identification of de-identified personal data (DPA Part 6 Section 171) 223](#_Toc67324016)

[9.4.3 Offence: Alteration etc of personal data to prevent disclosure to data subject (DPA Part 6 Section 173) 225](#_Toc67324017)

[9.4.4 Offence; Prohibition of requirement to produce relevant records (Enforced Right of Access) (DPA Part 7 Section 184) 226](#_Toc67324018)

[9.4.5 Offence: Breach of confidentiality by Commissioner (DPA Part 5 Section 132) 227](#_Toc67324019)

[9.4.6 Offence: False statements made in response to an Information Notice (DPA Part 6 Section 144) 227](#_Toc67324020)

[9.4.7 Destroying or falsifying information and documents etc. (DPA Part 6 Section 148) 227](#_Toc67324021)

[9.4.8 Penalties for Offences (DPA Part 7 Section 196) 228](#_Toc67324022)

[9.4.9 Prosecution (DPA Part 7 Section 197) 228](#_Toc67324023)

[9.4.10 Liability of Directors etc (DPA Part 7 Section 198) 229](#_Toc67324024)

[9.4.11 Recordable Offences (DPA Part 7 Section 199) 230](#_Toc67324025)

[10 Case Studies 231](#_Toc67324026)

[10.1 Under development – to be included in a future edition of this Manual. 231](#_Toc67324027)

[11 Appendices 232](#_Toc67324028)

[11.1 Appendix A: Role & Position of DPO Letter (see 2.6) 232](#_Toc67324029)

[11.2 Appendix B: Role & Position of DPO Report (see 2.6) 232](#_Toc67324030)

[11.3 Appendix C: Personal Data Breaches (see 4.2.7.2 and 6.2.7.1) 232](#_Toc67324031)

[11.4 Appendix D: Appropriate Policy Template (see 4.2.2.7 and 6.7) 232](#_Toc67324032)

[11.5 Appendix E: Request to external organisation for the disclosure of personal data to the Police (Version 1.1.3) (see 6.9) 232](#_Toc67324033)

[11.6 Appendix F: Joint Controllers Definitions & Arrangements (see 4.5.3 & 6.4.3) 232](#_Toc67324034)

[11.7 Appendix G: High-Level Privacy Notice [see 4.4.3.1] 233](#_Toc67324035)

[11.8 Appendix H: Lower-Level Specific Privacy Notice for GDPR (see 4.4.3.2) 233](#_Toc67324036)

[11.9 Appendix I: Information Management IT System Requirements (see 4.5.2) 233](#_Toc67324037)

[11.10 Appendix J: Standards (see 1.2) 233](#_Toc67324038)

[11.11 Appendix K: DPIA ICO Derived Template (see 4.5.2.1) 233](#_Toc67324039)

[11.12 Appendix L: National Data Processing Contract Template (see 4.5.4) 233](#_Toc67324040)

[11.13 Appendix M: Information Sharing Under the GDPR Guidance & Template (see 4.9) 233](#_Toc67324041)

[ 233](#_Toc67324042)

[11.14 Appendix N: Lower-Level Specific Privacy Notice for Law Enforcement Processing (see 6.3.3) 234](#_Toc67324043)

[ 234](#_Toc67324044)

[11.15 Appendix O: Collaborative Units - Project management-based approach to deliver Data Protection compliance (see 4.5.3.1) 234](#_Toc67324045)

[ 234](#_Toc67324046)

[12 Version Control 235](#_Toc67324047)

[12.1 Significant changes to previous version 235](#_Toc67324048)

# Introduction

## Foreword by NPCC Information Management Lead

The NPCC Data Protection Manual of Guidance has been produced by the National Police Chiefs’ Council’s Information Management & Operational Requirements Coordination Committee to assist police forces in their statutory responsibility to comply with the Data Protection Act 2018 and the General Data Protection Regulation.

This Manual is the latest in a series of guidance materials created by the police service in support of our continuing commitment to data protection, complying with legislation for more than thirty years since the 1984 and 1998 Acts[[1]](#footnote-1).

Over that period the way in which personal data is used by society in general and the police in particular has changed significantly with the digital revolution. The one thing which has remained constant is the requirement for the police to retain the public’s confidence in the way we obtain and use their personal information.

The underlying philosophy of the Manual is simple – data protection compliance is not merely a regulatory necessity, but is a core requirement to support effective policing. The Manual identifies the structures, responsibilities, policies and processes that must be in place to ensure consistency in the way the Act is applied within the police service. This is supported by baseline standards that can be found throughout the document.

The primary target audience for this Manual are Police Data Protection Professionals, though it is of relevance also to Information Asset Owners, Chief Constables or Commissioners (in their capacity as ‘Controllers’ under the Act) and Senior Information Risk Owners (SIROs).

This Manual has been used to develop the Data Protection Authorised Professional Practice, which has been designed to provide necessary general data protection learning for police officers, staff and others working for the police.

The Manual should be regarded as a document that both helps to create an environment across the police service in which compliance can be achieved, and as a means of providing guidance in areas of police business where the Act is regularly applied.

Commissioner Ian Dyson QPM.

Chair of the National Police Chiefs’ Council (NPCC) Information Management Operational Requirements Coordinating Committee (IMORCC).

## Terminology Used, Manual Structure and Standards (Appendix J)

To avoid potential confusion between items within the GDPR and the Act this Manual prefaces references with either GDPR or DPA e.g. GDPR Article 10, GDPR Recital 22, DPA Part 2, DPA Section 2 etc.

Within the parts of this manual which detail the legislation relevant extracts of the GDPR Articles and the DPA appear in italic form as do extracts from ICO guidance. Sub sections starting with **Commentary** – are intended to show how the legislation applies to policing and sections that look like this identify standards police forces must adopt. Sections that look like this indicate links to the ICO guidance or content provided by the ICO. For ease of reference all standards have been included in this manual at 11.10 Appendix J.

Hyperlinks have been added throughout this document to link to the relevant sections of the DPA officially published on the legislation.gov.uk website. The GDPR has been officially published [here](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN), but this document includes links to the [gdpr-info.eu](https://gdpr-info.eu/) website where each of the GDPR articles and recitals are helpfully separated into individual pages.

## Overview of Legislation

[DPA Section 2 Protection of personal data](http://www.legislation.gov.uk/ukpga/2018/12/section/2) succinctly describes the underlying intent to protect personal data. It states:

*(1) The GDPR, the applied GDPR and this Act protect individuals with regard to the processing of personal data, in particular by—*

*(a) requiring personal data to be processed lawfully and fairly, on the basis of the data subject’s consent or another specified basis,*

*(b) conferring rights on the data subject to obtain information about the processing of personal data and to require inaccurate personal data to be rectified, and*

*(c) conferring functions on the Commissioner, giving the holder of that office responsibility for monitoring and enforcing their provisions.*

*(2) When carrying out functions under the GDPR, the applied GDPR and this Act, the Commissioner must have regard to the importance of securing an appropriate level of protection for personal data, taking account of the interests of data subjects, controllers and others and matters of general public interest.*

**Commentary** - The Act replaced the UK’s Data Protection Act 1998 (“the 1998 Act”) in May 2018 to keep the law up-to-date for the digital age in which ever increasing amounts of personal data – information relating to identifiable living individuals - are being processed. It set new standards for protecting personal data, in accordance with recent EU data protection laws, giving people more control over use of their data.

The four main matters provided for in the Act are general data processing, law enforcement data processing, data processing for national security purposes including processing by the intelligence services, and regulatory oversight and enforcement.

The 1998 Act implemented the European Data Protection Directive (Directive 95/46/EC). On 25th May 2018 had the Directive was replaced by the [General Data Protection Regulation (EU) 2016/679)](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN) (“the GDPR”).

The Act is structured in seven parts.

* Part 1 contains preliminary matters.
* Part 2 contains provision extending the GDPR standards to areas outside EU competence (the “Applied GDPR” scheme), with the exception of law enforcement and processing by the intelligence services. The Act and the GDPR apply substantively the same standards to the majority of data processing in the UK, in order to create a clear and coherent data protection regime. It also sets out certain derogations that provide exemptions from the GDPR.
* Part 3 contains provision for law enforcement data processing and any interpretation of the provisions of Part 3 should consider the relevant recitals of the Law Enforcement Directive which it is intended to implement.
* Part 4 provides likewise for data processing by the intelligence services.
* The remaining parts provide for the continuance of the Information Commissioner (the “Commissioner”), enforcement and offences, and supplementary provisions.

Processing by the police splits into General Processing (covered by DPA Part 2) and Law Enforcement Processing (covered by DPA Part 3). General Processing includes all processing directly within the scope of the GDPR plus the Applied GDPR where equivalent provisions to the GDPR are applied to other general processing.

Although an item personal data may be concurrently subject to both General Processing and Law Enforcement Processing any individual processing operation by the police has to be either General Processing or Law Enforcement Processing – both cannot apply at the same time to a particular processing operation.



## GDPR and DPA elements not covered

The following elements of the GDPR are not covered by this Manual:

Article 1 Subject-matter and objectives

Article 2 Material scope

Article 3 Territorial scope

Article 8 Conditions applicable to child's consent in relation to information society services

Article 27 Representatives of controllers or processors not established in the Union

Article 40 Codes of conduct

Article 41 Monitoring of approved codes of conduct

Article 42 Certification

Article 43 Certification bodies

Article 50 International cooperation for the protection of personal data

Chapter VI Entirety (Articles 51 to 59 inclusive)

Chapter VII Entirety (Articles 60 to 76 inclusive)

Chapter VIII Entirety (Articles 77 to 84 inclusive)

Article 85 Processing and freedom of expression and information

Article 86 Processing and public access to official documents

Article 87 Processing of the national identification number

Article 88 Processing in the context of employment

Article 90 Obligations of secrecy

Article 91 Existing data protection rules of churches and religious associations

Chapter X Entirety

Chapter XI Entirety

The following elements of the DPA are not covered by this Manual:

Part 1 Section 1 Overview

Part 2 Section 9 Child’s consent in relation to information society services

Part 2 Section 13 Obligations of credit reference agencies

Part 2 Section 16 Power to make further exemption etc by regulation

Part 2 Section 17 Accreditation of certification providers

Part 2 Section 18 Transfers of personal data to third countries etc

Part 2 Section 20 Meaning of court

Part 2 Section 21 Processing to which this Chapter applies\*

Part 2 Section 22 Application of the GDPR to processing to which this Chapter applies\*

Part 2 Section 23 Power to make provision in consequence of regulations related to the GDPR\*

Part 2 Section 24 Manual unstructured data held by FOI public authorities\*

Part 2 Section 25 Manual unstructured data used in longstanding historical research\*

Part 2 Section 26 National security and defence exemption\*

Part 2 Section 27 National security: certificate\*

Part 2 Section 28 National security and defence: modifications to Articles 9 and 32 of the applied GDPR\*

(\*see footnote 6)

Part 3 Section 79 National security: certificates by the Minister

Part 3 Section 80 Special processing restrictions

Part 3 Section 81 Reporting of infringements

Part 4 All content

Part 5 Section 114 The Information Commissioner

Part 5 Section 115 General functions under the GDPR and safeguards

Part 5 Section 116 Other general functions

Part 5 Section 117 Competence in relation to courts etc.

Part 5 Section 118 Co-operation and mutual assistance (Schedule 14)

Part 5 Section 119 Inspection of personal data in accordance with international obligations

Part 5 Section 120 Further international role

Part 5 Section 130 Records of national security certificates

Part 5 Section 133 Guidance about privileged communications

Part 5 Section 134 Fees for services

Part 5 Section 135 Manifestly unfounded or excessive requests by data subjects etc.

Part 5 Section 136 Guidance about fees

Part 5 Section 138 Regulations under section 137: supplementary

Part 5 Section 139 Reporting to Parliament

Part 5 Section 140 Publication by the Commissioner

Part 5 Section 141 Notices from the Commissioner

Part 6 Section 160 Guidance about regulatory action

Part 6 Section 161 Approval of first guidance about regulatory action

Part 6 Section 165 Complaints by data subjects

Part 6 Section 166 Orders to progress complaints

Part 6 Section 167 Compliance orders

Part 6 Section 168 Compensation for contravention of the GDPR

Part 6 Section 169 Compensation for contravention of other data protection legislation

Part 6 Section 174 The special purposes

Part 6 Section 175 Provision of assistance in special purposes proceedings

Part 6 Section 176 Staying special purposes proceedings

Part 6 Section 177 Guidance about how to seek redress against media organisations

Part 6 Section 178 Review of processing of personal data for the purposes of journalism

Part 6 Section 179 Effectiveness of the media’s dispute resolution procedures

Part 6 Section 180 Jurisdiction

Part 6 Section 181 Interpretation of Part 6 (Schedule 16)

Part 7 Section 182 Regulations and consultation (Schedule 2)

Part 7 Section 183 Power to reflect changes to the Data Protection Convention

Part 7 Section 185 Avoidance of certain contractual terms relating to health records

Part 7 Section 187 Representation of data subjects with their authority

Part 7 Section 188 Representation of data subjects with their authority: collective proceedings

Part 7 Section 189 Duty to review provision for representation of data subjects

Part 7 Section 190 Post-review powers to make provision about representation of data subjects

Part 7 Section 191 Framework for Data Processing by Government

Part 7 Section 192 Approval of the Framework

Part 7 Section 193 Publication & Review of the Framework

Part 7 Section 194 Effect of the Framework

Part 7 Section 195 Reserve forces: data-sharing by HMRC

Part 7 Section 200 Guidance about PACE codes of practice

Part 7 Section 201 Disclosure of information to the Tribunal

Part 7 Section 202 Proceedings in the First-tier Tribunal: contempt

Part 7 Section 203 Tribunal Procedure Rules

Part 7 Section 206 Index of defined expressions

Part 7 Section 209 Application to the Crown

Part 7 Section 210 Application to Parliament

Part 7 Section 211 Minor and consequential provision

Part 7 Section 215 Short title

Schedule 3 – Exemptions etc. from the GDPR: Health, Social Work, Education & Child Abuse Data

Schedule 4 – Exemptions etc. from the GDPR: Disclosure Prohibited or Restricted by an Enactment

Schedule 5 — Accreditation of certification providers: reviews and appeals

Schedule 9 — Conditions for processing under Part 4

Schedule 10 — Conditions for sensitive processing under Part 4

Schedule 11 — Other exemptions under Part 4

Schedule 12 — The Information Commissioner

Schedule 13 — Other general functions of the Commissioner

Schedule 14 — Co-operation and mutual assistance

## Territorial Extent, Commencement, and Transitional Provisions of Act

### Territorial Extent (DPA Part 7 Section 207)

[DPA Part 7 Section 207 Territorial application of this Act](http://www.legislation.gov.uk/ukpga/2018/12/section/207) states:

*(1) This Act applies only to processing of personal data described in subsections (2) and (3).*

*(2) It applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the United Kingdom, whether or not the processing takes place in the United Kingdom.*

*(3) It also applies to the processing of personal data to which Chapter 2 of Part 2 (the GDPR) applies where—*

*(a) the processing is carried out in the context of the activities of an establishment of a controller or processor in a country or territory that is not a member State, whether or not the processing takes place in such a country or territory,*

*(b) the personal data relates to a data subject who is in the United Kingdom when the processing takes place, and*

*(c) the processing activities are related to—*

*(i) the offering of goods or services to data subjects in the United Kingdom, whether or not for payment, or*

*(ii) the monitoring of data subjects’ behaviour in the United Kingdom.*

*(4) Subsections (1) to (3) have effect subject to any provision in or made under section 120 providing for the Commissioner to carry out functions in relation to other processing of personal data.*

*(5) Section 3(14)(c) does not apply to the reference to the processing of personal data in subsection (2).*

*(6) The reference in subsection (3) to Chapter 2 of Part 2 (the GDPR) does not include that Chapter as applied by Chapter 3 of Part 2 (the applied GDPR).*

*(7) In this section, references to a person who has an establishment in the United Kingdom include the following—*

*(a) an individual who is ordinarily resident in the United Kingdom,*

*(b) a body incorporated under the law of the United Kingdom or a part of the United Kingdom,*

*(c) a partnership or other unincorporated association formed under the law of the United Kingdom or a part of the United Kingdom, and*

*(d) a person not within paragraph (a), (b) or (c) who maintains, and carries on activities through, an office, branch or agency or other stable arrangements in the United Kingdom,*

*and references to a person who has an establishment in another country or territory have a corresponding meaning.*

[DPA Part 7 Section 214 Extent](http://www.legislation.gov.uk/ukpga/2018/12/section/214) states:

*(1) This Act extends to England and Wales, Scotland and Northern Ireland, subject to—*

*(a) subsections (2) to (5), and*

*(b) paragraph 12 of Schedule 12.*

*(2) Section 199 extends to England and Wales only.*

*(3) Sections 188, 189 and 190 extend to England and Wales and Northern Ireland only.*

*(4) An amendment, repeal or revocation made by this Act has the same extent in the United Kingdom as the enactment amended, repealed or revoked.*

*(5) This subsection and the following provisions also extend to the Isle of Man—*

*(a) paragraphs 332 and 434 of Schedule 19;*

*(b) sections 211(1), 212(1) and 213(2), so far as relating to those paragraphs.*

*(6) Where there is a power to extend a part of an Act by Order in Council to any of the Channel Islands, the Isle of Man or any of the British overseas territories, the power may be exercised in relation to an amendment or repeal of that part which is made by or under this Act.*

**Commentary** – [DPA Part 7 Section 207 Territorial Extent](http://www.legislation.gov.uk/ukpga/2018/12/section/207) sets out the territorial application of the Act. Its application to controllers and processors depends on the place of establishment and the context of the activities of the establishment in which the personal data is processed. Subsection (2) means the Act applies to processing in the context of the activities of an establishment of a controller or processor in the UK. Subsection (3) means that, in certain circumstances, the Act also applies to processing to which the GDPR applies which is carried out in the context of activities of an establishment of a controller or processor in a country or territory that is not part of the EU. Subsection (3) does not apply for the applied GDPR or for Parts 3 or 4 of the Act. This section also defines a ‘person who has an establishment in the United Kingdom’. This includes an individual who is ordinarily resident in the UK, a body incorporated under UK law, a partnership or other unincorporated association formed under UK law, or a person who maintains in the UK an office, branch or agency through which they carry out an activities or other stable arrangements.

The Act extends and applies to the whole of the UK and therefore to all UK police forces subject to the minor exceptions outlined in [DPA Part 7 Section 214 Extent](http://www.legislation.gov.uk/ukpga/2018/12/section/214) which mean:

[Part 7 Section 188 Representation of data subjects with their authority: collective proceedings](http://www.legislation.gov.uk/ukpga/2018/12/section/188) applies to England & Wales and Northern Ireland, but does not apply to Scotland.

[Part 7 Section 189 Duty to review provision for representation of data subjects](http://www.legislation.gov.uk/ukpga/2018/12/section/189) applies to England & Wales and Northern Ireland, but does not apply to Scotland.

[Part 7 Section 190 Post-review powers to make provision about representation of data subjects](http://www.legislation.gov.uk/ukpga/2018/12/section/190) applies to England & Wales and Northern Ireland, but does not apply to Scotland.

[DPA Part 7 Section 196 Penalties for Offences](http://www.legislation.gov.uk/ukpga/2018/12/section/196) applies to all of the UK but its sub-sections provide differing regimes for England & Wales, Scotland, and Northern Ireland.

[DPA Part 7 Section 197 Prosecution](http://www.legislation.gov.uk/ukpga/2018/12/section/197) applies to all of the UK but its sub-sections provide differing regimes for England & Wales, Scotland, and Northern Ireland.

[DPA Part 7 Sections 199 Recordable Offences](http://www.legislation.gov.uk/ukpga/2018/12/section/199) applies to England and Wales but does not apply to Scotland or Northern Ireland.

[DPA Schedule 12 The Information Commissioner](http://www.legislation.gov.uk/ukpga/2018/12/schedule/12) applies to England, Wales and Northern Ireland but its paragraphs 7 & 8 do not apply to Scotland.

[Part 7 Section 208 Children in Scotland](http://www.legislation.gov.uk/ukpga/2018/12/section/208) states:

*(1) Subsections (2) and (3) apply where a question falls to be determined in Scotland as to the legal capacity of a person aged under 16 to—*

*(a) exercise a right conferred by the data protection legislation, or*

*(b) give consent for the purposes of the data protection legislation.*

*(2) The person is to be taken to have that capacity where the person has a general understanding of what it means to exercise the right or give such consent.*

*(3) A person aged 12 or over is to be presumed to be of sufficient age and maturity to have such understanding, unless the contrary is shown.*

**Commentary** – This provision sets out the parameters to be used in Scotland to determine whether a child (a person aged under 16) has the legal capacity to exercise one of their rights or provide consent under either the GDPR or the Act. No equivalent provision exists in the Act for other parts of the United Kingdom.

### Transitional provisions (DPA Part 7 Section 213 & Schedule 20)

[DPA Part 7 Section 7 Transitional provision](http://www.legislation.gov.uk/ukpga/2018/12/section/213) states:

*(1) Schedule 20 contains transitional, transitory and saving provision.*

*(2) The Secretary of State may by regulations make transitional, transitory or saving provision in connection with the coming into force of any provision of this Act or with the GDPR beginning to apply, including provision amending or repealing a provision of Schedule 20.*

*(3) Regulations under this section that amend or repeal a provision of Schedule 20 are subject to the negative resolution procedure.*

**Commentary** – [DPA Part 7 Section Transitional provision](http://www.legislation.gov.uk/ukpga/2018/12/section/213) introduced [DPA Schedule 20](http://www.legislation.gov.uk/ukpga/2018/12/schedule/20) which makes necessary transitional provision. Subsection (2) provided a power for the Secretary of State to make regulations making further necessary transitional, transitory or saving provision in connection with the coming into force of any provision of the Act.

Regulations were published on 24th May 2018 under subsection (2): [The Data Protection Act 2018 (Commencement No. 1 and Transitional and Saving Provisions) Regulations 2018](http://www.legislation.gov.uk/uksi/2018/625/made). These have been considered in the writing of commentaries in this manual where applicable.

### Commencement (DPA Part 7 Section 212)

[DPA Part 7 Section 212 Commencement](http://www.legislation.gov.uk/ukpga/2018/12/section/212) states:

*(1) Except as provided by subsections (2) and (3), this Act comes into force on such day as the Secretary of State may by regulations appoint.*

*(2) This section and the following provisions come into force on the day on which this Act is passed—*

*(a)sections 1 and 3;*

*(b) section 182;*

*(c) sections 204, 205 and 206;*

*(d) sections 209 and 210;*

*(e) sections 213(2), 214 and 215;*

*(f) any other provision of this Act so far as it confers power to make regulations or Tribunal Procedure Rules or is otherwise necessary for enabling the exercise of such a power on or after the day on which this Act is passed.*

*(3) The following provisions come into force at the end of the period of 2 months beginning when this Act is passed—*

*(a) section 124;*

*(b) sections 125, 126 and 127, so far as they relate to a code prepared under section 124;*

*(c) section 177;*

*(d) section 178 and Schedule 17;*

*(e) section 179.*

*(4) Regulations under this section may make different provision for different areas.*

**Commentary** – [DPA Part 7 Section 212 Commencement](http://www.legislation.gov.uk/ukpga/2018/12/section/212) gave the Secretary of State the power to make regulations bringing the Act into force, including making different provision for different areas. Certain provisions listed in subsection (2) came into force on the date of Royal Assent. Other provisions listed in

subsection (3) came into force at the end of the period of 2 months beginning on the date of Royal Assent.

Consequently all provisions in the Act are now in force.

# Governance & Responsibilities

## Overview

**Commentary** - Each Chief Officer as “Controller” has a legal obligation to ensure that all processing of personal data, by or on behalf of their police force is in accordance with the Act.

Therefore, they must establish certain governance measures to help ensure compliance with the law. This chapter describes these measures in detail. They include:

* the allocation of specific compliance responsibilities to certain staff
* the establishment of effective reporting lines
* the implementation of data protection awareness training for all staff
* the publication of data protection guidance for all staff outlining the key elements of the Act
* the undertaking of data protection compliance auditing, data quality auditing and monitoring

At a national level Chief Officers support the activities of a Data Protection, Freedom of Information, Information Sharing & Disclosure Portfolio Group reporting to the National Police Chiefs’ Council (NPCC) via its Information Management Operational Requirements Coordinating Committee (IMORCC).

## National Police Chiefs’ Council (NPCC) and its Information Management Operational Requirements Coordinating Committee (IMORCC)

**Commentary** - The NPCC via one of its subsidiary groups, IMORCC, has identified one or more officers of NPCC rank to ensure that an effective, consistent and coordinated approach to ensuring compliance with the Act is adopted across all police forces.

The lead(s) are the primary point(s) of contact between the police service and the ICO and Government on data protection matters.

## Chief Officer (Chief Constable or Commissioner)

**Commentary** - The Chief Officer (meaning Chief Constable or Commissioner in the cases of the Metropolitan Police and City of London Police) is legally responsible for their force’s compliance with the Data Protection Act. They cannot delegate this legal responsibility.

Where a police force is involved in partnership working in which both the police force and the partner(s) determine the purpose and manner in which personal data is processed, then the police force and its partner(s) will both be responsible as ‘controllers.’

The Controller must ensure that effective lines of communication exist between them, their Senior Information Risk Owner and their police force’s Data Protection Officer.

## Senior Information Risk Owner

**Commentary** - The Chief Officer must formally designate an officer of executive (NPCC) rank or police staff equivalent to both support and oversee the management of data protection matters, ensuring that relevant police force policies, procedures and guidelines reflect the requirements of this manual. Ideally that individual will also be designated as the force Senior Information Risk Owner (SIRO).

Although the role of SIRO has its genesis within information assurance it is also significant in achieving compliance with the Act as most information used by the police is personal data.

By designating a SIRO, a police force demonstrates that there is a mechanism and decision-making process in place, at senior level, that considers appropriate technical and/or organisational measures for the type of information (including personal data), together with any risks to information and the business.

The SIRO is required to understand how the strategic business goals of the police force may be impacted upon by information system failures. The SIRO also ensures that management of information risks are weighed alongside the management of other risks facing the organisation such as financial, legal and operational risks.

In December 2018 the NPCC issued its Senior Risk Owner’s Handbook which can be found [here](http://library.college.police.uk/docs/appref/Senior-Information-Risk-Owner-SIRO-handbook-final-Dec-2018.pdf).

## Information Asset Owner

**Commentary** – The role of the Information Asset Owner (IAO) was created to provide a senior role responsible for ensuring specific information assets are handled and managed appropriately. An IAO is appointed by and reports to, the Senior Information Risk Owner (SIRO).

The IAO will, on behalf of their relevant SIRO and their end users, be able to understand and address risks to the information and ensure it is fully used within the law.

Each separate information asset (often but not always a computer system) should have a designated IAO. This is a senior role commonly at Chief Superintendent or equivalent level. The IAO will support their relevant SIRO to ensure that information risks are treated as a priority for business outcomes and that information is utilised in the most effective way. By treating information as a business priority and not as an ICT or technical issue, we can ensure that risks are addressed, managed and capitalised upon. This in turn leads to improved decision making and policy development.

The IAO role is an integral part of any information governance framework and so it is important for the IAO to support their relevant SIRO to set up and/or maintain a strong information governance structure appropriate to their operating environment.

In December 2018 the NPCC issued its Information Asset Owner’s Handbook which can be found [here](http://library.college.police.uk/docs/appref/Information-Asset-Owner-IAO-Final-Dec-2018.pdf).

## Data Protection Officer (DPO) ([Appendix A](#_Appendix_A:_Role) & [Appendix B](#_Appendix_B:_Role))

### Overview

**Commentary** - Police Forces are required to designate a DPO for General Processing as police forces are ‘[Public Authorities’](#_Public_Authority_and) and the same for Law Enforcement Processing as they are ‘[Competent Authorities’](#_Competent_Authority_(clause).

The requirements in terms of designation, position and tasks, for a DPO for General Processing are set out in the GDPR Article 37 Article 38 & Article 39 and GDPR Recital 97. The most relevant parts of that recital are:

*Where the processing is carried out by a public authority……a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation….The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.*

The DPA Part 2 contains no references to the DPO role.

The requirements in terms of designation, position and tasks, for a DPO for Law Enforcement Processing are set out in [DPA Part 3 Section 69](http://www.legislation.gov.uk/ukpga/2018/12/section/69), [Section 70](http://www.legislation.gov.uk/ukpga/2018/12/section/70) & [Section 71](http://www.legislation.gov.uk/ukpga/2018/12/section/71).

On 21st December 2017 Commissioner Ian Dyson, in his role as Chair of the NPCC’s Information Management & Operational Requirements Coordination Committee (IMORCC), wrote to Chief Officers asking for their attention to a paper produced by the NPCC’s Data Protection Reform Working Group concerning the role and position of Data Protection Officers in police forces. His letter and the report can be found at the rear of this manual as [Appendix A](#_Appendix_A:_Role) and [Appendix B](#_Appendix_B:_Role).

The College of Policing has issued a role profile for a Data Protection Officer which can be found on the college’s [Professional Development Platform](https://profdev.college.police.uk/professional-profile/data-protection-officer/).

The ICO has published guidance on the GDPR requirements for role of Data Protection Officer which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/), and for DPA Part 3 [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/accountability-and-governance/data-protection-officers/).

The police force must ensure it has nominated a Data Protection Officer to undertake, as a minimum, the tasks identified in data protection legislation. They must also ensure that all of the legislative requirements around the designation, position and tasks of the role are met.

### Designation

[GDPR Article 37](https://gdpr-info.eu/art-37-gdpr/) states:

*1.The controller and the processor shall designate a data protection officer in any case where:*

*(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;*

*(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or*

*(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.*

*2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.*

*3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.*

*4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.*

*5 .The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.*

*6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.*

*7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.*

[DPA Part 3 Section 69 Designation of a data protection officer](http://www.legislation.gov.uk/ukpga/2018/12/section/69) states:

*(1) The controller must designate a data protection officer, unless the controller is a court, or other judicial authority, acting in its judicial capacity.*

*(2) When designating a data protection officer, the controller must have regard to the professional qualities of the proposed officer, in particular—*

*(a) the proposed officer’s expert knowledge of data protection law and*

*practice, and*

*(b) the ability of the proposed officer to perform the tasks mentioned in*

*section 71.*

*(3) The same person may be designated as a data protection officer by several controllers, taking account of their organisational structure and size.*

*(4) The controller must publish the contact details of the data protection officer and communicate these to the Commissioner*.

### Position

[GDPR Article 38](https://gdpr-info.eu/art-38-gdpr/) states:

*1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.*

*2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.*

*3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.*

*4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.*

*5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.*

*6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.*

[DPA Part 3 Section 70 Position of data protection officer](http://www.legislation.gov.uk/ukpga/2018/12/section/70) states:

*(1) The controller must ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.*

*(2) The controller must provide the data protection officer with the necessary resources and access to personal data and processing operations to enable the data protection officer to—*

*(a) perform the tasks mentioned in section 71, and*

*(b) maintain his or her expert knowledge of data protection law and practice.*

*(3) The controller—*

*(a) must ensure that the data protection officer does not receive any instructions regarding the performance of the tasks mentioned in section 71;*

*(b) must ensure that the data protection officer does not perform a task or fulfil a duty other than those mentioned in this Part where such task or duty would result in a conflict of interests;*

*(c) must not dismiss or penalise the data protection officer for performing the tasks mentioned in section 71.*

*(4) A data subject may contact the data protection officer with regard to all issues relating to—*

*(a) the processing of that data subject’s personal data, or*

*(b) the exercise of that data subject’s rights under this Part.*

*(5) The data protection officer, in the performance of this role, must report to the highest management level of the controller.*

### Tasks

[GDPR Article 39](https://gdpr-info.eu/art-39-gdpr/) states:

*1. The data protection officer shall have at least the following tasks:*

*(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;*

*(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;*

*(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;*

*(d) to cooperate with the supervisory authority;*

*(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.*

*2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing*.

[DPA Part 3 Section 71 Tasks of data protection](http://www.legislation.gov.uk/ukpga/2018/12/section/71) officer states:

*(1) The controller must entrust the data protection officer with at least the following tasks—*

*(a) informing and advising the controller, any processor engaged by the controller, and any employee of the controller who carries out processing of personal data, of that person’s obligations under this Part,*

*(b) providing advice on the carrying out of a data protection impact assessment under section 64 and monitoring compliance with that section,*

*(c) co-operating with the Commissioner,*

*(d) acting as the contact point for the Commissioner on issues relating to processing, including in relation to the consultation mentioned in section 65, and consulting with the Commissioner, where appropriate, in relation to any other matter,*

*(e) monitoring compliance with policies of the controller in relation to the protection of personal data, and*

*(f) monitoring compliance by the controller with this Part.*

*(2) In relation to the policies mentioned in subsection (1)(e), the data protection officer’s tasks include—*

*(a) assigning responsibilities under those policies,*

*(b) raising awareness of those policies,*

*(c) training staff involved in processing operations, and*

*(d) conducting audits required under those policies.*

*(3) In performing the tasks set out in subsections (1) and (2), the data protection officer must have regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.*

### NPCC Data Protection Officer

**Commentary** - The NPCC has appointed a Data Protection Officer to assist police forces and the NPCC in meeting their obligations under arising from the GDPR and Data Protection Act 2018.

## Records Manager

**Commentary** - A police force’s records manager helps their force meet obligations arising from the GDPR and Data Protection Act 2018, particularly the fifth principle and records of processing activities.

## Information Security Officer

**Commentary** – A police force’s information security officer helps their force meet obligations arising from the GDPR and Data Protection Act 2018, particularly the sixth principle.

## All staff

**Commentary** – The term ‘all staff’ encompasses every police officer, member of police staff, police community support officer, special constable, volunteer, processor, contractor and approved persons working for or on behalf of the police.

The police force must ensure that all staff having access to personal data are made aware of the requirement to comply with data protection legislation and any supporting local policy, procedure , or other measure designed to help achieve compliance.

## Structure

**Commentary** - Each police force must have in place a management structure that will allow an effective dialogue on data protection issues between chief officers, the data protection officer and other staff.

The police force must ensure that appropriate measures are established so that any concerns regarding data protection compliance within their organisation are directed to the Data Protection Officer in a timely manner.

## Information Commissioner/Commissioner

**Commentary** - The Information Commissioner undertakes the [GDPR Article 51](https://gdpr-info.eu/art-51-gdpr/) role of ‘supervisory authority’ for the UK. [DPA Part 1 Section 3(8)](http://www.legislation.gov.uk/ukpga/2018/12/section/3) confirms that ‘Commissioner’ within the DPA means the Information Commissioner. DPA Part 5 sets out the role and function of the Information Commissioner, and further detail on that can be found in Chapter 9 of this document. For the purposes of the commentaries in this document the term ‘ICO’ meaning Information Commissioner’s Office is used to refer to the Commissioner/Information Commissioner and their office.

## Data protection training, awareness and guidance

**Commentary** - Training strategies must be designed to ensure that all staff receive, as a minimum, baseline awareness training, with further specialist training supplied as required dependent on role and circumstances.

Police forces must ensure that records are maintained for all staff receiving training. The records should evidence what training has been provided to whom and when, in order to enable subsequent analysis by the data protection officer and other staff as required. Such records are likely to assist as evidence in misuse enquiries and help police forces meet their obligations under the Act.

Police forces will provide their staff involved in the processing of personal data with guidance designed to make them aware of the requirements the Act places upon them. The guidance may take the form of a high-level force policy explaining the key elements of the Act such as the principles, exemptions and offences, plus more specific guidance to cover particular areas of interest, such as the handling of right of subject access requests, disclosure, and data processing contracts.

The Data Protection Officer must make arrangements with those developing policy to ensure that where necessary, data protection requirements are considered .

Other guidance may also be produced for the benefit of external audiences. For example, advice to the public as how to exercise their rights under the Act.

The police force must ensure that Data Protection training should be refreshed or repeated as required on at least an annual basis and records of training maintained as they could be subject of inspection by the ICO.

The College of Policing has developed a suite of data protection-related training products for police officers, staff and others to undertake:

* MLE E-learning ‘Managing Information’ (Operational & Non Operational);
* Foundation E-learning for Data Protection police professionals;

With reference to the MLE E-learning ‘Managing Information’ the NPCC has recommended[[2]](#footnote-2) that ‘all officers and staff are required to complete the training in a defined timescale.’

Intermediate Data Protection classroom training for Police Data Protection Professionals is being developed and Advanced classroom training for Police Data Protection Professionals is being considered. The College of Policing will also develop annual refresher training and has introduced related E-Learning modules: Government Security Classification (GSC) and Freedom of Information.

The College of Policing is currently developing a Data Protection Authorised Professional Pra0ctice (APP) and has produced other APP which are related to the Data Protection APP: Managing Police Information, Sharing Police Information, and Information Assurance (Security).

The NPCC Data Protection Manual of Guidance contains detailed guidance, primarily for Police Data Protection Professionals. The ICO’s website includes considerable guidance on data protection matters.

The police force must develop and implement training strategies that incorporate data protection aspects, and are designed to ensure that all police officers, police staff, volunteers and others involved in the processing of personal data are aware of the requirements that the Act places upon them.

## Data Protection Compliance Auditing, Data Quality Auditing and Monitoring

**Commentary** - In order to help achieve compliance with the Act police forces will be expected to undertake data protection compliance audits, inspections and monitoring (see 8.1 below).

## National Police Information Systems

**Commentary** – In all cases where the police develop information systems for use across multiple police forces any project overseeing that development must ensure that a Data Protection Impact Assessment is conducted for the information system in accordance with the ICO’s guidance (see [4.5.2](#_Data_Protection_by) and [6.4.8](#_Privacy_by_Default)).

## Data Protection Fee (Data Protection (Charges and Information) Regulations 2018)

**Commentary** – Section 108 of the Digital Economy Act 2017 (later duplicated as [DPA Part 5 Section 137](http://www.legislation.gov.uk/ukpga/2018/12/section/137)) gave the Secretary of State the power to introduce regulations to replace the requirement to ‘notify’ (or register) with the ICO, as was required by the 1998 Act). Under that power the [Data Protection (Charges and Information) Regulations 2018](http://www.legislation.gov.uk/ukdsi/2018/9780111165782/pdfs/ukdsi_9780111165782_en.pdf) introduced the new data protection fee.

Police forces fall under Tier 3 (as they each have more than 250 employees), which requires the payment of an annual data protection fee to the ICO of £2,900.

The ICO has the power under [DPA Part 5 Section 137](http://www.legislation.gov.uk/ukpga/2018/12/section/137) to enforce the [Data Protection (Charges and Information) Regulations 2018](http://www.legislation.gov.uk/ukdsi/2018/9780111165782/pdfs/ukdsi_9780111165782_en.pdf) and to serve monetary Penalty Notices on those who refuse to pay their data protection fee.

The Data Protection Officer must ensure appropriate measures are in place to make certain their force’s Data Protection Fee is paid in full and on time.

The ICO has published guidance on the fee which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-fee/).

# Definitions

## Introduction

**Commentary** – The GDPR contains definitions of key terms and these are supplemented by others within the Act that either apply to all processing, or to general processing or law enforcement processing.

For General Processing (processing covered by the GDPR and DPA Part 2) the definitions are either those within [GDPR Article 4](https://gdpr-info.eu/art-4-gdpr/) and [GDPR Article 9](https://gdpr-info.eu/art-9-gdpr/) or within the GDPR as supplemented by further provisions in the Act, including those at [DPA Part 1 Section 3](http://www.legislation.gov.uk/ukpga/2018/12/section/3), [DPA Part 2 Section 7](http://www.legislation.gov.uk/ukpga/2018/12/section/7), [Section 21](http://www.legislation.gov.uk/ukpga/2018/12/section/21), [Section 22](http://www.legislation.gov.uk/ukpga/2018/12/section/22), DPA Part 6 [Section 174](http://www.legislation.gov.uk/ukpga/2018/12/section/174) and [Section 181](http://www.legislation.gov.uk/ukpga/2018/12/section/181), and [DPA Part 7 Section 187](http://www.legislation.gov.uk/ukpga/2018/12/section/187), [Section 204](http://www.legislation.gov.uk/ukpga/2018/12/section/204) and [Section 205](http://www.legislation.gov.uk/ukpga/2018/12/section/205).

For Law Enforcement Processing (processing covered by DPA Part 3) the definitions are solely those contained within the Act, including those at [DPA Part 1 Section 3](http://www.legislation.gov.uk/ukpga/2018/12/section/3), [DPA Part 3 Section 30](http://www.legislation.gov.uk/ukpga/2018/12/section/30), [Section 31](http://www.legislation.gov.uk/ukpga/2018/12/section/31), [Section 32](http://www.legislation.gov.uk/ukpga/2018/12/section/32), and [Section 33](http://www.legislation.gov.uk/ukpga/2018/12/section/33).

Although there are some differences between some of the definitions relevant to the two types of processing those differences tend to be minor in nature.

The tables below provide an index of defined terms of most relevance to policing in the Act and GDPR. [DPA Part 7 Section 206](http://www.legislation.gov.uk/ukpga/2018/12/section/206) contains an index to definitions within the Act.

The definitions are explored in more detail after the tables below.

The ICO has published its guidance on Key Definitions under the GDPR [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/) and for DPA Part 3 [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/scope-and-key-definitions/).

## Key Definitions Applicable to General Processing (GDPR/DPA Part 2)

|  |  |  |
| --- | --- | --- |
| **Term** | **DPA Definition relevant to General Processing** | **GDPR Definition** |
| Personal Data | Part 1 Preliminary – Section 3(2) | Article 4(1) |
| Processing | Part 1 Preliminary – Section 3(4) | Article 4(2) |
| Restriction of Processing | - | Article 4(3) |
| Profiling | - | Article 4(4) |
| Pseudonymisation | - | Article 4(5) |
| Filing System | Part 1 Preliminary – Section 3(7) | Article 4(6) |
| Controller | Part 1 Preliminary – Section 3(6) Part 2 General Processing – Section 6(1) | Article 4(7) |
| Processor | Part 1 Preliminary – Section 3(6) | Article 4(8) |
| Recipient | - | Article 4(9) |
| Third Party | - | Article 4(10) |
| Consent | - | Article 4(11) |
| Personal Data Breach | - | Article 4(12) |
| Genetic Data | Part 7 Supplementary - Section 205(1) | Article 4(13) |
| Biometric Data | Part 7 Supplementary - Section 205(1) | Article 4(14) |
| Data Concerning Health | - | Article 4(15) |
| ‘Special Category Data’ | - | Article 9(1) |
| The Commissioner | Part 1 Preliminary - Section 3(8) | - |
| Data Subject | Part 1 Preliminary – Section 3(5) | - |
| GDPR | Part 1 Preliminary – Section 3(10) | - |
| Applied GDPR | Part 1 Preliminary - Section 3(11) | - |
| Public authority | Part 2 General Processing (GDPR) – Section 7 | - |
| Public body | Part 2 General Processing (GDPR) – Section 7 | - |
| FOI public authority | Part 2 General Processing (other General Processing) – Section 21(5) | - |
| Applied Chapter 2 | Part 2 General Processing (other General Processing) – Section 22(3) | - |
| Special Purposes | Part 6 Enforcement - Section 174 | - |
| Special Purposes Proceedings | Part 6 Enforcement - Section 174 | - |
| Assessment Notice | Part 6 Enforcement - Section 181 | - |
| Certification Provider | Part 6 Enforcement - Section 181 | - |
| Enforcement Notice | Part 6 Enforcement - Section 181 | - |
| Information Notice | Part 6 Enforcement - Section 181 | - |
| Penalty Notice | Part 6 Enforcement - Section 181 | - |
| Penalty Variation Notice | Part 6 Enforcement - Section 181 | - |
| Representative | Part 6 Enforcement - Section 181 | Article 4(17) |
| Representative Body (in relation to a right of a data subject) | Part 7 Supplementary - Section 187 | - |
| Health Professional | Part 7 Supplementary - Section 204 | - |
| Social Work Professional | Part 7 Supplementary - Section 204 | - |
| Health Record | Part 7 Supplementary - Section 205(1) | - |
| Inaccurate | Part 7 Supplementary - Section 205(1) | - |
| Publish | Part 7 Supplementary - Section 205(1) | - |

## Key Definitions Applicable to Law Enforcement Processing

|  |  |
| --- | --- |
| **Term** | **DPA Definition relevant to Law Enforcement Processing** |
| Personal Data | Part 1 Preliminary – Section 3(2) |
| Processing | Part 1 Preliminary – Section 3(4) |
| Data Subject | Part 1 Preliminary – Section 3(5) |
| Controller | Part 1 Preliminary – Section 3(6) |
| Processor | Part 1 Preliminary – Section 3(6) |
| Filing System | Part 1 Preliminary – Section 3(7) |
| Commissioner | Part 1 Preliminary - Section 3(8) |
| Special Purposes | Part 6 Enforcement - Section 174 |
| Special Purposes Proceedings | Part 6 Enforcement - Section 174 |
| Assessment Notice | Part 6 Enforcement - Section 181 |
| Certification provider | Part 6 Enforcement - Section 181 |
| Enforcement notice | Part 6 Enforcement - Section 181 |
| Information notice | Part 6 Enforcement - Section 181 |
| Penalty notice | Part 6 Enforcement - Section 181 |
| Penalty Variation Notice | Part 6 Enforcement - Section 181 |
| Representative | Part 6 Enforcement - Section 181 |
| Representative Body (in relation to a right of a data subject) | Part 7 Supplementary - Section 187 |
| Health Professional | Part 7 Supplementary - Section 204 |
| Social Work Professional | Part 7 Supplementary - Section 204 |
| Genetic Data | Part 7 Supplementary - Section 205(1) |
| Biometric Data | Part 7 Supplementary - Section 205(1) |
| Health Record | Part 7 Supplementary - Section 205(1) |
| Inaccurate | Part 7 Supplementary - Section 205(1) |
| Publish | Part 7 Supplementary - Section 205(1) |

**Commentary** - The remainder of this chapter includes the definitions of greatest relevance to policing,

## Personal Data and Data Subject (GDPR Article 4 DPA Part 1 Section 3)

[GDPR Article 4(1)](https://gdpr-info.eu/art-4-gdpr/) states:

*‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

[DPA Part 1 Section 3(2)](http://www.legislation.gov.uk/ukpga/2018/12/section/3) states:

*“Personal data” means any information relating to an identified or identifiable living individual (subject to subsection (14)(c)).*

[DPA Part 1 Section 3(14)](http://www.legislation.gov.uk/ukpga/2018/12/section/3) states:

*In Parts 5 to 7, except where otherwise provided—*

*(a) references to the GDPR are to the GDPR read with Chapter 2 of Part 2 and include the applied GDPR read with Chapter 3 of Part 2;*

*(b) references to Chapter 2 of Part 2, or to a provision of that Chapter, include that Chapter or that provision as applied by Chapter 3 of Part 2;*

*(c) references to personal data, and the processing of personal data, are to personal data and processing to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies;*

*(d) references to a controller or processor are to a controller or processor in relation to the processing of personal data to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies.*

**Commentary** - Effectively DPA Part 1 Section 3(2) extends the GDPR definition of Personal Data to apply across the whole Act.

Further clarity on Data Subject is provided at [DPA Part 1 Section 3(5)](http://www.legislation.gov.uk/ukpga/2018/12/section/3) which states:

*“Data subject” means the identified or identifiable living individual to whom personal data relates.*

and at [DPA Part 1 Section 3(3](http://www.legislation.gov.uk/ukpga/2018/12/section/3)) which states:

*“Identifiable living individual” means a living individual who can be identified, directly or indirectly, in particular by reference to—*

*(a) an identifier such as a name, an identification number, location data or an online identifier, or*

*(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.*

**Commentary** - The GDPR’s definition of Personal Data is more detailed than that in the 1998 Act and makes it clear that information such as an online identifier, for example a computer’s IP address, can be personal data. The more expansive definition expressly provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people. Also, personal data that has been pseudonymised, for example key-coded data, can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

The ICO has published guidance on the definition of Personal Data which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/) (GDPR) and [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/scope-and-key-definitions/#6) (DPA Part 3).

## Special Category Data (Special Categories of Personal Data) and Sensitive Processing (GDPR Article 9 DPA Part 3 Section 35)

[GDPR Article 9](https://gdpr-info.eu/art-9-gdpr/) (Processing of special categories of personal data) provides a definition through its opening paragraph which states:

*1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*

• Reveals racial or ethnic origin

• Reveals political opinions

• Reveals religious or philosophical beliefs

• Reveals trade union membership

• Is genetic data or biometric data used to uniquely identify a person

• Concerns health

• Concerns a person’s sex life or sexual orientation

[DPA Part 3 Section 35(8)](http://www.legislation.gov.uk/ukpga/2018/12/section/35) states:

*In this section, “sensitive processing” means—*

*(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;*

*(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;*

*(c) the processing of data concerning health;*

*(d) the processing of data concerning an individual’s sex life or sexual orientation.*

**Commentary** – The terms Special Categories of Personal Data and Sensitive Processing are defined respectively under the GDPR for General Processing and the DPA for Law Enforcement Processing and are similar in content.

The ICO has published guidance on the definition of Special Category Data which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/).

The ICO has published guidance on the definition of Sensitive Processing which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/scope-and-key-definitions/#8).

## Processing (GDPR Article 4 DPA Part 1 Section 3)

[GDPR Article 4(2)](https://gdpr-info.eu/art-4-gdpr/) states:

*‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

[DPA Part 1 Section 3(4)](http://www.legislation.gov.uk/ukpga/2018/12/section/3) states:

*“Processing”, in relation to personal data, means an operation or set of operations which is performed on personal data, or on sets of personal data, such as—*

*(a) collection, recording, organisation, structuring or storage,*

*(b) adaptation or alteration,*

*(c) retrieval, consultation or use,*

*(d) disclosure by transmission, dissemination or otherwise making available,*

*(e) alignment or combination, or*

*(f) restriction, erasure or destruction,*

*(subject to subsection (14)(c) and sections 5(7), 29(2) and 82(3), which make provision about references to processing in the different Parts of this Act).*

[DPA Part 1 Section 3(14)(c)](http://www.legislation.gov.uk/ukpga/2018/12/section/3) states:

*In Parts 5 to 7, except where otherwise provided—*

*(c) references to personal data, and the processing of personal data, are to personal data and processing to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies;*

[DPA Part 2 Section 5(7)](http://www.legislation.gov.uk/ukpga/2018/12/section/5) states:

*(7) A reference in Chapter 2 or Chapter 3 of this Part to the processing of personal data is to processing to which the Chapter applies.*

[DPA Part 3 Section 29(2)](http://www.legislation.gov.uk/ukpga/2018/12/section/29) states:

*(2) Any reference in this Part to the processing of personal data is to processing to which this Part applies.*

**Commentary** – This term is similarly defined under the GDPR for General Processing and DPA for Law Enforcement Processing. The final sentence of the DPA definition means that additional provisions concerning the term ‘processing’ have to be considered depending upon which part of the Act is being applied:

DPA Part 1 Section 3(14)(c) means that except where specified otherwise within DPA Part 5 The Information Commissioner, DPA Part 6 Enforcement and DPA Part 7 Supplementary and final provision any references to ‘processing’ relate to processing covered by DPA Part 2 Sections to 28 (General Processing), and DPA Part 3 (Law Enforcement Processing). DPA Part 4 which is mentioned in the clause is not relevant to policing as it only applies to processing by any of the three intelligence services.

DPA Part 2 Section 5(7) means that any reference to ‘processing’ within DPA Part 2 Sections 6 to 28 refers to processing covered by the GDPR and Applied GDPR covered by DPA Part 2.

DPA Part 3 Section 29(2) means that any reference to ‘processing’ within DPA Part 3 refers to processing covered by DPA Part 3 (law enforcement processing).

DPA Part 4 Section 82(3) is not relevant to policing as it only applies to processing by any of the three intelligence services.

## Restriction of Processing (GDPR Article 4 DPA Part 3 Section 33)

[GDPR Article 4(3)](https://gdpr-info.eu/art-4-gdpr/) states:

*‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future.*

[DPA Part 3 Section 33(6](http://www.legislation.gov.uk/ukpga/2018/12/section/33)) states:

*“Restriction of processing” means the marking of stored personal data with the aim of limiting its processing for the future.*

**Commentary** – This term is almost identically defined in the GDPR for General Processing, and in the DPA Part 3 for Law Enforcement Processing.

## Profiling (GDPR Article 4 DPA Part 3 Section 33)

[GDPR Article 4(4)](https://gdpr-info.eu/art-4-gdpr/) and the [DPA Part 3 Section 33(4](http://www.legislation.gov.uk/ukpga/2018/12/section/33)), state:

*‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.*

**Commentary** – This term is identically defined under the GDPR and DPA for General Processing and Law Enforcement Processing respectively.

## Pseudonymisation (GDPR Article 4)

[GDPR Article 4(5)](https://gdpr-info.eu/art-4-gdpr/) states:

*‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*

**Commentary** – This term does not appear in the Act, but is defined for General Processing by the GDPR.

## Filing System (GDPR Article 4 DPA Part 1 Section 3)

[GDPR Article 4(6)](https://gdpr-info.eu/art-4-gdpr/) states:

*‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.*

[DPA Part 1 Section 3(7)](http://www.legislation.gov.uk/ukpga/2018/12/section/3) states:

*“Filing system” means any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis.*

**Commentary** – This term is defined in the GDPR and that definition is effectively extended by the DPA across all processing.

## Controller (GDPR Article 4, DPA Part 1 Section 3)

[GDPR Article 4(7)](https://gdpr-info.eu/art-4-gdpr/) states:

*‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*

[DPA Part 2 Section 5 Definitions](http://www.legislation.gov.uk/ukpga/2018/12/section/5) includes:

*(1) Terms used in Chapter 2 of this Part and in the GDPR have the same meaning in Chapter 2 as they have in the GDPR.*

*(2) In subsection (1), the reference to a term's meaning in the GDPR is to its meaning in the GDPR read with any provision of Chapter 2 which modifies the term's meaning for the purposes of the GDPR.*

*(3) Subsection (1) is subject to any provision in Chapter 2 which provides expressly for the term to have a different meaning and to section 204.*

*(4) Terms used in Chapter 3 of this Part and in the applied GDPR have the same meaning in Chapter 3 as they have in the applied GDPR.*

*(5) In subsection (4), the reference to a term's meaning in the applied GDPR is to its meaning in the GDPR read with any provision of Chapter 2 (as applied by Chapter 3) or Chapter 3 which modifies the term's meaning for the purposes of the applied GDPR.*

*(6) Subsection (4) is subject to any provision in Chapter 2 (as applied by Chapter 3) or Chapter 3 which provides expressly for the term to have a different meaning.*

*(7) A reference in Chapter 2 or Chapter 3 of this Part to the processing of personal data is to processing to which the Chapter applies.*

[DPA Part 2 Section 6 Meaning of controller](http://www.legislation.gov.uk/ukpga/2018/12/section/6) states:

*(1) The definition of “controller” in Article 4(7) of the GDPR has effect subject to—*

*(a) subsection (2),*

*(b) section 209, and*

*(c) section 210.*

*(2) For the purposes of the GDPR, where personal data is processed only—*

*(a )for purposes for which it is required by an enactment to be processed, and*

*(b) by means by which it is required by an enactment to be processed,*

*the person on whom the obligation to process the data is imposed by the enactment (or, if different, one of the enactments) is the controller.*

[DPA Part 1 Section 3 Terms relating to the processing of personal data](http://www.legislation.gov.uk/ukpga/2018/12/section/3) includes:

*(6) “Controller” and “processor”, in relation to the processing of personal data to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies, have the same meaning as in that Chapter or Part (see sections 5, 6, 32 and 83 and see also subsection (14)(c))*.

And

*(14) In Parts 5 to 7, except where otherwise provided—…*

*(c) references to personal data, and the processing of personal data, are to personal data and processing to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies;*

[DPA Part 3 Section 32](http://www.legislation.gov.uk/ukpga/2018/12/section/32) includes:

*(1) In this Part, “controller” means the competent authority which, alone or jointly with others—*

*(a) determines the purposes and means of the processing of personal data,*

*or*

*(b) is the controller by virtue of subsection (2).*

*(2) Where personal data is processed only—*

*(a) for purposes for which it is required by an enactment to be processed,*

*and*

*(b) by means by which it is required by an enactment to be processed,*

*the competent authority on which the obligation to process the data is imposed by the enactment (or, if different, one of the enactments) is the controller.*

*(3) In this Part, “processor” means any person who processes personal data on behalf of the controller (other than a person who is an employee of the controller).*

[DPA Part 4 Section 83](http://www.legislation.gov.uk/ukpga/2018/12/section/83) only applies to processing by the three intelligence agencies.

**Commentary** – For General Processing – processing subject to the GDPR and DPA Part 2 - Controller is defined within the GDPR and this definition is supplemented by the definition arising from a combination of DPA Part 2 Section 5 and Section 6, and DPA Part Section 3(6) & (14), with DPA Part Section 3(6) also requiring consideration of DPA Part 3 Section 32. This rather cumbersome construct does not practically the GDPR definition which is the one which, for practical purposes, police forces should use.

For Law Enforcement Processing – processing subject to DPA Part 3 – Controller is succinctly defined under DPA Part 3 Section 32. As is the case with General Processing this simple definition supplemented by the technical provisions at DPA Part 1 Section 3(6) & (14), with DPA Part Section 3(6) also requiring consideration of DPA Part 3 Section 32. This rather cumbersome construct does not practically the DPA Part 3 Section 32 definition which is the one which, for practical purposes, police forces should use.

Where a police force independently determines the purpose and means of General Processing or Law Enforcement Processing the Controller will be the Chief Officer (Chief Constable or Commissioner in the cases of the City of London and Metropolitan Police). Where such activity is carried out jointly with one or more other person or organisation the Controller will be the Chief Officer and the other person or organisation.

Joint controllership for General Processing is often seen where police forces signed ‘Section 22a’ agreements and merged some of their support services such as Human Resources or Finance functions.

Examples of joint controllership for Law Enforcement Processing include the Police National Database, Police National Computer and the Athena Database.

The ICO has published guidance on Controllers and Processors which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/) (GDPR) and [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/scope-and-key-definitions/#7) (DPA Part 3).

Where the police force engages in joint controllership for either General Processing or Law Enforcement Processing it must ensure that the scope, boundaries, responsibilities and nature of that joint controllership are clearly documented and understood by all parties.

## Processor (GDPR Article 4 DPA Part 3 Section 32)

[GDPR Article 4(8)](https://gdpr-info.eu/art-4-gdpr/) states:

*‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

[DPA Part 3 Section 32(3)](http://www.legislation.gov.uk/ukpga/2018/12/section/32) states:

*In this Part, “processor” means any person who processes personal data on behalf of the controller (other than a person who is an employee of the controller).*

**Commentary** - The definition of processor for General Processing found within the GDPR and that for Law Enforcement Processing within the DPA are similar, the key distinction being that the GDPR definition does not explicitly exclude employees of the controller from being processors.

The NPCC position is that officers and staff working for a police force are not processors when their role requires them to process personal data on behalf of or under instruction of the Chief Officer.

The ICO has published guidance on Controllers and Processors which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/) (GDPR).

## Recipient (GDPR Article 4 DPA Part 3 Section 33)

[GDPR Article 4(9)](https://gdpr-info.eu/art-4-gdpr/) states:

*‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.*

[DPA Part 3 Section 33(5)](http://www.legislation.gov.uk/ukpga/2018/12/section/33) states:

*“Recipient”, in relation to any personal data, means any person to whom the data is disclosed, whether a third party or not, but it does not include a public authority to whom disclosure is or may be made in the framework of a particular inquiry in accordance with the law.*

**Commentary** - There are two slightly different definitions of recipient in the GDPR and DPA for General Processing and Law Enforcement Processing respectively.

## Third Party (GDPR Article 4)

[GDPR Article 4(10)](https://gdpr-info.eu/art-4-gdpr/) states:

*‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.*

**Commentary** - The only definition for this is provided by the GDPR in respect of General Processing. The Act provides a definition of third party in DPA Schedule 9(6)(3), but this is only relevant to Intelligence Services’ Processing (DPA Part 4).

## Consent (GDPR Article 4)

[GDPR Article 4(11)](https://gdpr-info.eu/art-4-gdpr/) states:

*‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

**Commentary** - The only definition for this is provided by the GDPR in respect of General Processing. The Act provides a definition of consent in DPA Part 4 Section 82(2), but this is only relevant to Intelligence Services’ Processing (DPA Part 4).

## Personal Data Breach (GDPR Article 4 DPA Part 3 Section 33)

[GDPR Article 4(12)](https://gdpr-info.eu/art-4-gdpr/) states:

*‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

[DPA Part 3 Section 33(3](http://www.legislation.gov.uk/ukpga/2018/12/section/33)) states:

*“Personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

**Commentary** – Both the GDPR and DPA define this term identically for General Processing and Law Enforcement Processing respectively. It is important to note that the definition is not simply related a breach of security leading to unauthorized disclosure of personal data but it also encompasses destruction, loss and alteration of personal data.

## Genetic Data (GDPR Article 4 DPA Part 7 Section 205)

[GDPR Article 4(13](https://gdpr-info.eu/art-4-gdpr/)) states:

*‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.*

[DPA Part 7 Section 205 General interpretation](http://www.legislation.gov.uk/ukpga/2018/12/section/205) states:

*“genetic data” means personal data relating to the inherited or acquired genetic characteristics of an individual which gives unique information about the physiology or the health of that individual and which results, in particular, from an analysis of a biological sample from the individual in question.*

**Commentary** – Almost identical definitions for this term appear in the GDPR and DPA for General Processing and all processing respectively.

## Biometric Data (GDPR Article 4 DPA Part 7 Section 205)

[GDPR Article 4(14)](https://gdpr-info.eu/art-4-gdpr/) states:

*‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.*

[DPA Part 7 Section 205 General interpretation](http://www.legislation.gov.uk/ukpga/2018/12/section/205) states:

*“biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data.*

**Commentary** – Almost identical definitions for this term appear in the GDPR and DPA for General Processing and all processing respectively.

The definitions cover DNA Profile Data, Fingerprint Data, and images capable of being used to recognize individuals. Conceivably the definitions may encompass some audio recordings.

## Data Concerning Health & Health Record (GDPR Article 4, DPA Part 7 Section 205)

[GDPR Article 4(15)](https://gdpr-info.eu/art-4-gdpr/) states:

*‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.*

[DPA Part 7 Section 205 General interpetation](http://www.legislation.gov.uk/ukpga/2018/12/section/205) states:

*(1) In this Act - ….*

*“data concerning health” means personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveals information about his or her health status.*

Although there is no GDPR definition of ‘health record’ [DPA Part 7 Section 205 General interpretation](http://www.legislation.gov.uk/ukpga/2018/12/section/205) does provide one:

*(1) In this Act - ….*

*“health record” means a record which—*

*(a) consists of data concerning health, and*

*(b) has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates.*

**Commentary** – Almost identical definitions for the term ‘data concerning health’ and ‘health record’ appear in the GDPR and DPA for General Processing and all processing respectively. The DPA definition references ‘health professional’ and that term is also defined in the Act.

Within policing these definitions cover information concerning the health of detained persons. They also encompass information concerning the health of officers and staff, such as Occupational Health records or absence recording records.

## Public Authority and Public Body (DPA Part 2 Section 7)

DPA Part 2 Section 7 states:

*(1) For the purposes of the GDPR, the following (and only the following) are “public authorities” and “public bodies” under the law of the United Kingdom—*

*(a) a public authority as defined by the Freedom of Information Act 2000, subject to subsection (2),*

*(b) a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002 (asp 13), subject to subsection (2), and*

*(c) an authority or a body specified by the Secretary of State in regulations*

*(2) An authority or body that falls within subsection (1) is only a “public authority” or “public body” for the purposes of the GDPR when performing a task carried out in the public interest or in the exercise of official authority vested in it.*

*(3) The references in subsection (1)(a) and (b) to public authorities and Scottish public authorities as defined by the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 (asp 13) do not include any of the following that fall within those definitions—*

*(a) a parish council in England;*

*(b) a community council in Wales;*

*(c) a community council in Scotland;*

*(d) a parish meeting constituted under section 13 of the Local Government Act 1972;*

*(e) a community meeting constituted under section 27 of that Act;*

*(f) charter trustees constituted—*

*(i) under section 246 of that Act,*

*(ii) under Part 1 of the Local Government and Public Involvement in Health Act 2007, or*

*(iii) by the Charter Trustees Regulations 1996 (S.I. 1996/263).*

*(4) The Secretary of State may by regulations provide that a person specified or described in the regulations that is a public authority described in subsection (1)(a) or (b) is not a “public authority” or “public body” for the purposes of the GDPR.*

*(5) Regulations under this section are subject to the affirmative resolution procedure.*

**Commentary** - The term ‘public authority’ and “public body” are not defined in the GDPR so for certainty the Act has adopted the definitions in the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002. Effectively DPA Part 2 Section 7(1) confirms that all Home Office funded police forces are public authorities.

## GDPR (DPA Part 1 Section 3)

[DPA Part 1 Section 3(10)](http://www.legislation.gov.uk/ukpga/2018/12/section/3) states:

*“The GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).*

**Commentary** – None required.

## Applied GDPR (DPA Part 1 Section 3)

[DPA Part 1 Section 3(11)](http://www.legislation.gov.uk/ukpga/2018/12/section/3) states:

*“The applied GDPR” means the GDPR as applied by Chapter 3 of Part 2* [of the DPA].

**Commentary** – None required.

## Law Enforcement Directive (DPA Part 1 Section 3)

[DPA Part 1 Section 3(12)](http://www.legislation.gov.uk/ukpga/2018/12/section/3) states:

*“The Law Enforcement Directive” means Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*.

**Commentary** – None required.

## Competent Authority (DPA Part 3 Section 30, Schedule 7)

The opening part of [DPA Part 3 Section 30](http://www.legislation.gov.uk/ukpga/2018/12/section/30) states:

*(1) In this Part, “competent authority” means—*

*(a) a person specified or described in* [*Schedule 7*](http://www.legislation.gov.uk/ukpga/2018/12/schedule/7)*, and*

*(b) any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes.*

*(2) But an intelligence service is not a competent authority within the meaning of this Part.*

[DPA Schedule 7 Competent Authorities](http://www.legislation.gov.uk/ukpga/2018/12/schedule/7) states:

*1 Any United Kingdom government department other than a non-ministerial government department.*

*2 The Scottish Ministers.*

*3 Any Northern Ireland department.*

*4 The Welsh Ministers.*

*Chief officers of police and other policing bodies*

*5 The chief constable of a police force maintained under section 2 of the Police Act 1996.*

*6 The Commissioner of Police of the Metropolis.*

*7 The Commissioner of Police for the City of London.*

*8 The Chief Constable of the Police Service of Northern Ireland.*

*9 The chief constable of the Police Service of Scotland.*

*10 The chief constable of the British Transport Police.*

*11 The chief constable of the Civil Nuclear Constabulary.*

*12 The chief constable of the Ministry of Defence Police.*

*13 The Provost Marshal of the Royal Navy Police.*

*14 The Provost Marshal of the Royal Military Police.*

*15 The Provost Marshal of the Royal Air Force Police.*

*16 The chief officer of—*

*(a) a body of constables appointed under provision incorporating section 79 of the Harbours, Docks, and Piers Clauses Act 1847;*

*(b) a body of constables appointed under an order made under section 14 of the Harbours Act 1964;*

*(c) the body of constables appointed under section 154 of the Port of London Act 1968 (c.xxxii).*

*17 A body established in accordance with a collaboration agreement under section 22A of the Police Act 1996.*

*18 The Director General of the Independent Office for Police Conduct.*

*19 The Police Investigations and Review Commissioner.*

*20 The Police Ombudsman for Northern Ireland.*

*Other authorities with investigatory functions*

*21 The Commissioners for Her Majesty's Revenue and Customs.*

*22 The Welsh Revenue Authority.*

*23 Revenue Scotland.*

*24 The Director General of the National Crime Agency.*

*25 The Director of the Serious Fraud Office.*

*26 The Director of Border Revenue.*

*27 The Financial Conduct Authority.*

*28 The Health and Safety Executive.*

*29 The Competition and Markets Authority.*

*30 The Gas and Electricity Markets Authority.*

*31 The Food Standards Agency.*

*32 Food Standards Scotland.*

*33 Her Majesty's Land Registry.*

*34 The Criminal Cases Review Commission.*

*35 The Scottish Criminal Cases Review Commission.*

*Authorities with functions relating to offender management*

*36 A provider of probation services (other than the Secretary of State), acting in pursuance of arrangements made under section 3(2) of the Offender Management Act 2007.*

*37 The Youth Justice Board for England and Wales.*

*38 The Parole Board for England and Wales.*

*39 The Parole Board for Scotland.*

*40 The Parole Commissioners for Northern Ireland.*

*41 The Probation Board for Northern Ireland.*

*42 The Prisoner Ombudsman for Northern Ireland.*

*43 A person who has entered into a contract for the running of, or part of—*

*(a) a prison or young offender institution under section 84 of the Criminal Justice Act 1991, or*

*(b) a secure training centre under section 7 of the Criminal Justice and Public Order Act 1994.*

*44 A person who has entered into a contract with the Secretary of State—*

*(a) under section 80 of the Criminal Justice Act 1991 for the purposes of prisoner escort arrangements, or*

*(b) under paragraph 1 of Schedule 1 to the Criminal Justice and Public Order Act 1994 for the purposes of escort arrangements.*

*45 A person who is, under or by virtue of any enactment, responsible for securing the electronic monitoring of an individual.*

*46 A youth offending team established under section 39 of the Crime and Disorder Act 1998.*

*Other authorities*

*47 The Director of Public Prosecutions.*

*48 The Director of Public Prosecutions for Northern Ireland.*

*49 The Lord Advocate.*

*50 A Procurator Fiscal.*

*51 The Director of Service Prosecutions.*

*52 The Information Commissioner.*

*53 The Scottish Information Commissioner*

*54 The Scottish Courts and Tribunal Service.*

*55 The Crown agent.*

*56 A court or tribunal.*

**Commentary** - This only applies to Law Enforcement Processing,excluding any of the three intelligence services (which are defined in paragraph (7)). Paragraphs (3) to (6) are not relevant to policing.

A competent authority may also be any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

This definition covers not only all police forces, prosecutors and other criminal justice agencies in the UK, but also other organisations with law enforcement functions, such as Her Majesty’s Revenue and Customs, the Health and Safety Executive and the ICO.

Police, Fire and Crime Commissioners are not competent authorities.

Non Home Office-funded police forces, such as the Port of Dover Police are competent authorities under DPA Section 30(1)(b).

Schedule 7 may be amended by regulations, published as a Statutory Instrument. To date none have been issued relating to Schedule 7.

The determination by a police force as to whether or not an organisation is a competent authority processing personal data for law enforcement purposes may be significant should the police force be considering disclosing operational data to that organisation.

Also see 6.1.

The ICO has published guidance on the definition of Competent Authority which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/scope-and-key-definitions/#2).

## Law Enforcement Purposes (DPA Part 3 Section 31)

[DPA Part 3 Section 31 The law enforcement purposes](http://www.legislation.gov.uk/ukpga/2018/12/section/31) states:

*For the purposes of this part “law enforcement purposes” are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.*

**Commentary** - This only applies to Law Enforcement Processing. This is inconsistent with definition of ‘policing purposes’, within the [MoPI Statutory Code of Practice](http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf), being somewhat narrower, and it remains to be seen what the practical consequences of that are.

The ICO has publish guidance on the definition of Law Enforcement Purposes which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/scope-and-key-definitions/#3).

## Employee (DPA Part 3 Section 33)

[DPA Part 3 Section 33(2)](http://www.legislation.gov.uk/ukpga/2018/12/section/33) states:

*“Employee”, in relation to any person, includes an individual who holds a position (whether paid or unpaid) under the direction and control of that person.*

**Commentary** - This term is not defined in the GDPR. It is currently unclear as to whether unpaid police volunteers should be considered employees. This is significant because DPA Part 3 Section 32(3) makes it clear that a processor does not include an employee of the controller.

## Third Country (DPA Part 3 Section 33)

[DPA Part 3 Section 33(7)](http://www.legislation.gov.uk/ukpga/2018/12/section/33) states:

*“Third country” means a country or territory other than a member State* [of the European Union]*.*

**Commentary** - This term is not defined in the GDPR despite being used extensively throughout the regulation. It is therefore assumed by the NPCC that it means any country or territory outside the [European Economic Area (EEA)](https://www.gov.uk/eu-eea) as per the DPA definition.

## Health Professional & Social Work Professional (DPA Part 7 Section 204)

[DPA Part 7 Section 204 Meaning of “health professional” and “social work professional”](http://www.legislation.gov.uk/ukpga/2018/12/section/204) states:

*(1) In this Act, “health professional” means any of the following—*

*(a) a registered medical practitioner;*

*(b) a registered nurse or midwife;*

*(c) a registered dentist within the meaning of the Dentists Act 1984 (see section 53 of that Act);*

*(d) a registered dispensing optician or a registered optometrist within the meaning of the Opticians Act 1989 (see section 36 of that Act);*

*(e) a registered osteopath with the meaning of the Osteopaths Act 1993 (see section 41 of that Act);*

*(f) a registered chiropractor within the meaning of the Chiropractors Act 1994 (see section 43 of that Act);*

*(g) a person registered as a member of a profession to which the Health and Social Work Professions Order 2001 (S.I. 2002/254) for the time being extends, other than the social work profession in England;*

*(h) a registered pharmacist or a registered pharmacy technician within the meaning of the Pharmacy Order 2010 (S.I. 2010/231) (see article 3 of that Order);*

*(i) a registered person within the meaning of the Pharmacy (Northern*

*Ireland) Order 1976 (S.I. 1976/1213 (N.I. 22)) (see Article 2 of that Order);*

*(j) a child psychotherapist;*

*(k) a scientist employed by a health service body as head of a department.*

*(2) In this Act, “social work professional” means any of the following—*

*(a) a person registered as a social worker in England in the register maintained under the Health and Social Work Professions Order 2001 (S.I. 2002/254);*

*(b) a person registered as a social worker in the register maintained by Social Care Wales under section 80 of the Regulation and Inspection of Social Care (Wales) Act 2016 (anaw 2);*

*(c) a person registered as a social worker in the register maintained by the Scottish Social Services Council under section 44 of the Regulation of Care (Scotland) Act 2001 (asp 8);*

*(d) a person registered as a social worker in the register maintained by the Northern Ireland Social Care Council under section 3 of the Health and Personal Social Services Act (Northern Ireland) 2001 (c. 3 (N.I.)).*

*(3) In subsection (1)(a) “registered medical practitioner” includes a person who is provisionally registered under section 15 or 21 of the Medical Act 1983 and is engaged in such employment as is mentioned in subsection (3) of that section.*

*(4) In subsection (1)(k) “health service body” means any of the following—*

*(a) the Secretary of State in relation to the exercise of functions under section 2A or 2B of, or paragraph 7C, 8 or 12 of Schedule 1 to, the National Health Service Act 2006;*

*(b) a local authority in relation to the exercise of functions under section 2B or 111 of, or any of paragraphs 1 to 7B or 13 of Schedule 1 to, the National Health Service Act 2006;*

*(c) a National Health Service trust first established under section 25 of the National Health Service Act 2006;*

*(d) a Special Health Authority established under section 28 of the National Health Service Act 2006;*

*(e) an NHS foundation trust;*

*(f) the National Institute for Health and Care Excellence;*

*(g) the Health and Social Care Information Centre;*

*(h) a National Health Service trust first established under section 5 of the National Health Service and Community Care Act 1990;*

*(i) a Local Health Board established under section 11 of the National Health Service (Wales) Act 2006;*

*(j) a National Health Service trust first established under section 18 of the National Health Service (Wales) Act 2006;*

*(k) a Special Health Authority established under section 22 of the National Health Service (Wales) Act 2006;*

*(l) a Health Board within the meaning of the National Health Service (Scotland) Act 1978;*

*(m) a Special Health Board within the meaning of the National Health Service (Scotland) Act 1978;*

*(n) a National Health Service trust first established under section 12A of the National Health Service (Scotland) Act 1978;*

*(o) the managers of a State Hospital provided under section 102 of the National Health Service (Scotland) Act 1978;*

*(p) the Regional Health and Social Care Board established under section 7 of the Health and Social Care (Reform) Act (Northern Ireland) 2009 (c. 1 (N.I));*

*(q) a special health and social care agency established under the Health and Personal Social Services (Special Agencies) (Northern Ireland) Order 1990 (S.I. 1990/247 (N.I. 3));*

*(r) a Health and Social Care trust established under Article 10 of the Health and Personal Social Services (Northern Ireland) Order 1991 (S.I. 1991/194 (N.I. 1)).*

**Commentary** - These terms are not defined in the GDPR. The DPA definitions are applicable to all processing.

## Criminal Offence Data (GDPR Article 10, DPA Part 2 Section 11)

[DPA Part 2 Section 11 Special categories of personal data etc: supplementary](http://www.legislation.gov.uk/ukpga/2018/12/section/11) includes:

*(2) In Article 10 of the GDPR and section 10, references to personal data relating to criminal convictions and offences or related security measures include personal data relating to—*

1. *the alleged commission of offences by the data subject, or*
2. *proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.*

[GDPR Article 10 Processing of personal data relating to criminal convictions and offences](https://gdpr-info.eu/art-10-gdpr/) states:

*Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.*

**Commentary** – The term is not fully defined in the Act but this provision contains a non-exhaustive definition of personal data relating to criminal convictions and offences or related security measures mentioned in GDPR Article 10. In other words what the article refers to The ICO refers to this information as ‘Criminal Offence Data’ but that helpful ‘label’ does not exist in the Act.

The ICO has published guidance on Criminal Offence Data which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/#ib2).

# General Processing (GDPR & DPA Part 2)

## Scope: General Processing, GDPR and Applied GDPR Scheme

**Commentary** - The GDPR applied directly in the United Kingdom from 25th May 2018.

The GDPR encompasses “General Processing” which, for ease of reference, may be defined from a policing perspective as any processing of personal data that does not fall under the scope of Law Enforcement Processing[[3]](#footnote-3) ([DPA Part 3](http://www.legislation.gov.uk/ukpga/2018/12/part/3)) or Intelligence Services Processing (DPA Part 4)[[4]](#footnote-4).



General Processing has to be compliant with both the GDPR and DPA Part 2.

This requirement to meet GDPR requirements, which are split into Articles and associated Recitals, and to also consider DPA Part 2 requirements, means that navigating data protection compliance for General Processing can be a complex task.

The scope of DPA Part 2 is set out in that part’s [Section 4](http://www.legislation.gov.uk/ukpga/2018/12/section/4), which explains that [DPA Part 2 Chapter 2](http://www.legislation.gov.uk/ukpga/2018/12/part/2/chapter/2) (i.e. DPA Part 2 Sections 6 to 20) applies to processing covered by the GDPR and that [DPA Part 2 Chapter 3](http://www.legislation.gov.uk/ukpga/2018/12/part/2/chapter/3) (the Applied GDPR Scheme – DPA Part 2 Sections 21 to 28) extends that scope to areas not covered by the GDPR. The scope the GDPR itself is provided by GDPR Article 2 together with GDPR Recitals 14-21.

It may be assumed by Police Data Protection Professionals that any processing by the police that falls outside the scope of [DPA Part 3](http://www.legislation.gov.uk/ukpga/2018/12/part/3) should be considered under the requirements of the GDPR and DPA Part 2.

Within Chapter 4 of this manual relevant extracts of the GDPR Articles and the DPA appear in italic form as do extracts from ICO guidance. Sub-sections starting with “**Commentary”** are intended to show how the legislation is likely to apply to policing. Where exemptions are applicable they can be found at the end of commentary sub-sections.

The ICO has published its Guide to the General Data Protection Regulation on its [website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/).

### Examples of Police General Processing

**Commentary** - Police General Processing encompasses, but is not limited to, processing of personal data for the following purposes:

* Administration of officers, staff, volunteers and others working for the police
* Occupational health and welfare
* Management of public relations, journalism, advertising and media
* Management of finance, internal review, accounting and auditing
* Training
* Property management
* Insurance management
* Vehicle and transport management
* Payroll and benefits management
* Management of complaints
* Vetting of officers, staff, volunteers and others working for the police
* Management of information technology systems
* Legal services including participation in civil proceedings
* Information provision
* Licensing and registration
* Pensioner administration
* Research including surveys
* Performance management
* Sports, social and recreation
* Procurement
* Planning
* System testing
* Security
* Health management
* Sale, provision or purchase of goods and services.

### Examples of Exclusions from Police General Processing

**Commentary** - There are a number of police processing operations which may be difficult to distinguish between General Processing and Law Enforcement Processing. To assist Police Data Protection Professionals the NPCC position is that the following (not exhaustive) are to be regarded as being Law Enforcement Processing rather than General Processing:

* DBS Vetting
* Some elements of Custody Records for detainees i.e. those concerning health and welfare

### Processing which does not require identification (GDPR Article 11)

GDPR Article 11 states:

*1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.*

*2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.*

The associated GDPR Recital 57 states:

*If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.*

**Commentary** - This Article and the associated GDPR Recital 57 mean that if the personal data processed by a police force does not permit it to identify the data subject there is no obligation on the police force to obtain additional information in order to identify the data subject for the sole reason of complying with any provision of the GDPR.

The GDPR Articles 15 to 20 mentioned in the second part of the Article refer to the rights of access by the data subject, right to rectification, right to erasure (“right to be forgotten”), right to restriction on processing, notification obligation regarding rectification or erasure of personal data or restriction of processing, and right to data portability.

The ICO is yet to publish guidance on Article 11.

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 11(2) (processing not requiring identification) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of Article 11(2) would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

## General Processing Data Protection Principles (GDPR & DPA Part 2)

### Overview of General Processing Principles (GDPR Article 5)

GDPR Article 5 states:

*1. Personal data shall be:*

*(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);*

*(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);*

*(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);*

*(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);*

*(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);*

*(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).*

*2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).*

GDPR Recital 39 provides further interpretation of the principles (paragraph breaks added for clarity):

*Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.*

*The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed.*

*Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.*

*The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum.*

*Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.*

*In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.*

*Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted.*

*Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.*

**Commentary** – The GDPR sets out six General Data Protection Principles and an additional requirement that the Controller (the Chief Officer of UK police forces) shall be responsible for, and be able to demonstrate compliance with the Principles, something which the GDPR refers to as ‘accountability’. The General Data Protection Principles, derived from the GDPR and extended by the DPA, apply to all General Processing.

The General Data Protection Principles are broadly consistent with those of the 1998 Act. The biggest differences are that there are no specific GDPR Principles for data subject rights or overseas transfers, and that there is now the ‘accountability’ requirement arising from GDPR Article 5(2).

The ICO has published guidance on the GDPR Principles which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/).

Exemptions from a requirement to comply in certain circumstances with elements of the General Data Protection Principles are available. These are mentioned briefly within the narrative of each of the principles under 4.2 and in more detail under 4.3.

**Exemption – Crime & Taxation.** [DPA Schedule 2 Part 1 Paragraph 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/2/enacted) disapplies GDPR Article 5 (General Data Protection Principles) so far as they correspond to the data subject rights and obligations under GDPR Article 13(1) to (3), GDPR Article 14(1) to (4), GDPR Article 15(1) to (3), GDPR Article 16, GDPR Article 17(1) & (2), GDPR Article 20(1) & (2), and GDPR Article 21(1) to the extent that the application of those provisions would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of a tax or an imposition of a similar nature. [See 4.3.2.1](#_Exemptions_-_Crime)

**Exemption – Disclosure Required by Law.** [DPA Schedule 2 Part 1 Paragraph 5](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/5/enacted) disapplies GDPR Article 5 (General Data Protection Principles) so far as they correspond to the data subject rights and obligations under GDPR Article 13(1) to (3), GDPR Article 14(1) to (4), GDPR Article 15(1) to (3), GDPR Article 16, GDPR Article 17(1) & (2), GDPR Article 20(1) & (2), and GDPR Article 21(1) to the extent that the application of those provisions would prevent the controller from:

1. complying with an obligation to make personal data available to the public, or
2. complying with an obligation to disclose personal data required by an enactment, rule of law or order of a court or tribunal, or
3. making a disclosure where necessary or in connection with legal proceedings (including prospective ones), or making a disclosure necessary for obtaining legal advice, or making a disclosure that is otherwise necessary for establishing, exercising or defending legal rights.

[See 4.3.2.2.](#_Exemption_-_Disclosure)

**Exemption – Functions designed to protect the public etc.** [DPA Schedule 2 Part 2 Paragraph 7](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/7/enacted) disapplies GDPR Article 5 (General Data Protection Principles) so far as they correspond to the data subject rights and obligations under GDPR Article 13(1) to (3), GDPR Article 14(1) to (4), GDPR Article 15(1) to (3), GDPR Article 16, GDPR Article 17(1) & (2), GDPR Article 18(1), GDPR Article 20(1) & (2), and GDPR Article 21(1) to the extent that the application of those provisions would prejudice the proper discharge of functions:

* designed to protect the public against dishonesty, malpractice, serious improper conduct, unfitness or incompetence by anyone whose activity brings them into contact with the public
* relating to health and safety and welfare at work.

[See 4.3.3.1](#_Exemption_–_Functions)

**Exemption – Legal Professional Privilege**. [DPA Schedule 2 Part 4 Paragraph 19](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/19/enacted) disapplies GDPR Article 5 (General Data Protection Principles) so far as they correspond to the data subject rights and obligations under GDPR Article 13(1) to (3), GDPR Article 14(1) to (4), and GDPR Article 15(1) to (3) in respect of personal data that is subject to Legal Professional Privilege or for Scotland Confidentiality of Communications. [See 4.3.5.1](#_Exemption_–_Legal)

**Exemption – Self Incrimination** – [DPA Schedule 2 Part 4 Paragraph 20](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/20/enacted) disapplies GDPR Article 5 (General Data Protection Principles) by a person so far as they correspond to the data subject rights and obligations under GDPR Article 13(1) to (3), GDPR Article 14(1) to (4), and GDPR Article 15(1) to (3) to the extent that the application of those provisions would, by revealing evidence of the of the commission of a non-DPA-related offence, expose the person to proceedings for that offence. [See 4.3.5.2](#_Exemption_–_Self)

**Exemption – Management Forecasts** – [DPA Schedule 2 Part 4 Paragraph 22](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/22/enacted) disapplies GDPR Article 5 (General Data Protection Principles) in relation to personal data processed for business management forecasting or planning activities so far as they correspond to the data subject rights and obligations under GDPR Article 13(1) to (3), GDPR Article 14(1) to (4), and GDPR Article 15(1) to (3) to the extent that the application of those provisions would be likely to prejudice the conduct of those activities. [See 4.3.5.4](#_Exemption_–_Management)

**Exemption – Negotiations** – [DPA Schedule 2 Part 4 Paragraph 23](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/23/enacted) disapplies GDPR Article 5 (General Data Protection Principles) in relation to personal data that consists of records of the intentions of the controller in relation to negotiations with the data subject as far as they correspond to the data subject rights and obligations under GDPR Article 13(1) to (3), GDPR Article 14(1) to (4), and GDPR Article 15(1) to (3) to the extent that the application of those provisions would be likely to prejudice those negotiations. [See 4.3.5.5](#_Exemption_–_Negotiations).

**Exemption – Confidential References** – [DPA Schedule 2 Part 4 Paragraph 24](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/24/enacted) disapplies GDPR Article 5 (General Data Protection Principles) in relation to personal data that consists of confidential references about the data subject as far as they correspond to the data subject rights and obligations under GDPR Article 13(1) to (3), GDPR Article 14(1) to (4), and GDPR Article 15(1) to (3). . [See 4.3.5.6.](#_Exemption_–_Confidential)

### General Processing; First Principle – Lawfulness, Fairness & Transparency (GDPR Article 5)

#### Overview of First General Processing Principle

GDPR Article 5(1)(a) states:

*Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.*

**Commentary** -- The First Principle is likely to be the most significant of the six Principles.

It requires there to be a lawful basis for general processing with at least one of five available conditions met, and for that processing to be both fair and transparent, and the police force must be able to demonstrate that a lawful basis applies.

If the purpose of the processing changes it requires further consideration to be made of five further factors to determine if the new processing would be lawful.

If the processing involves Special Category Data there is an additional requirement under GDPR Article 9 that at least one of the ten special processing conditions is met plus any associated DPA Part 2 Section 9 & Schedule 1 conditions.

If the processing involves Criminal Offence Data there is an additional requirement under GDPR Article 10 that the processing is occurring under official authority.

The ICO has published guidance on the First GDPR Principle which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/).

There are a number of exemptions relevant to the First General Principle which are set out below.

**Exemption – Crime & Taxation.** [DPA Schedule 2 Part 1 Paragraph 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/2/enacted) disapplies GDPR Articles 5(1)(a) & (b)[[5]](#footnote-5) as amended by the DPA to the extent that the application of those provisions would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of a tax or an imposition of a similar nature. [See 4.3.2.1](#_Exemptions_-_Crime)

**Exemption – Disclosure Required by Law.** [DPA Schedule 2 Part 1 Paragraph 5](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/5/enacted) disapplies GDPR Articles 5(1)(a) & (b)[[6]](#footnote-6) as amended by the DPA to the extent that the application of those provisions would prevent the controller from:

1. complying with an obligation to make personal data available to the public, or
2. complying with an obligation to disclose personal data required by an enactment, rule of law or order of a court or tribunal, or
3. making a disclosure where necessary or in connection with legal proceedings (including prospective ones), or making a disclosure necessary for obtaining legal advice, or making a disclosure that is otherwise necessary for establishing, exercising or defending legal rights.

[See 4.3.2.2.](#_Exemption_-_Disclosure)

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 5(1)(a) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of Article 5(1)(a) would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

#### Lawful Processing & Processing Conditions (GDPA Article 6, DPA Part 2 Section 8)

GDPR Article 6(1) (Lawfulness of Processing) states:

*Processing shall be lawful only if and to the extent that at least one of the following applies:*

***[Consent]***

*(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*

***[Contract]***

*(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*

***[Legal Obligation]***

*(c) processing is necessary for compliance with a legal obligation to which the controller is subject;*

***[Vital Interests]***

*(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;*

***[Public Task]***

*(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*

***[Legitimate Interests]***

*(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

*Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.*

GDPR Recitals 40, 41 and 43 are of relevance to GDPR Article 6(1). GDPR Recital 40 states:

*In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.*

GDPR Recital 41 states:

*Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the ‘Court of Justice’) and the European Court of Human Rights.*

GDPR Recital 43 states:

*Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.*

[DPA Part 2 Section 8 Lawfulness of processing: public interest etc](http://www.legislation.gov.uk/ukpga/2018/12/section/8) states:

*In Article 6(1) of the GDPR (lawfulness of processing), the reference in point (e) to processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller’s official authority includes processing of personal data that is necessary for—*

*(a) the administration of justice,*

*(b) the exercise of a function of either House of Parliament,*

*(c) the exercise of a function conferred on a person by an enactment or rule of law,*

*(d) the exercise of a function of the Crown, a Minister of the Crown or a government department, or*

*(e) an activity that supports or promotes democratic engagement.*

**Commentary** – GDPR Article 6(1) requires that general processing shall be lawful only if and to the extent that at least one of six processing conditions listed within that element of the GDPR are met. The **sixth processing condition at GDPR Article 6(1)(f)[[7]](#footnote-7) cannot be used by the police** as it is not available to public authorities which by definition includes the police. If an appropriate processing condition does not apply the processing is unlawful. [DPA Part 2 Section 8](http://www.legislation.gov.uk/ukpga/2018/12/section/8) provides a non-exhaustive list of examples of processing under Public Task which includes administration of justice.

All the conditions, with the exception of (a) [Consent], require that the processing is necessary and the ICO’s view is that if the purpose can reasonably be achieved without the processing then there is no lawful basis to process.

GDPR Article 6(2) and (3) are not directly relevant to policing.

If Special Category Data is being processed there is a further requirement to identify an additional condition for processing that type of data (see 4.2.2.5). Similar requirements apply to Criminal Offences and Convictions Data (see 4.2.2.6).

The ICO has published guidance on Lawful Basis for Processing which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/). It has also produced an interactive tool for determining law basis which can be found [here](https://ico.org.uk/for-organisations/gdpr-resources/#lawful) and other resources to assist understanding and identification of lawful bases for processing which can be found [here](https://ico.org.uk/for-organisations/gdpr-resources/#resources).

Within policing the following provide examples of where each particular condition is likely to be applicable:

**Consent** (a) (see 4.2.2.4)

* officers or staff agree to their names and other identifiers to be used for the purposes of the police force’s lottery
* officers or staff agree to their biographical information and photographs to be placed on the force intranet’s news pages
* victims of crime agree to their contact details and details of their crime to be provided to victim services
* recipients of police awards or commendations agree to their information being released to the media or via the force internet site
* applicants for jobs with the police agree to provide their information so that the recruitment process can progress

Note: NPCC’s position remains that police forces should, where possible, use a condition other that consent due to the complexity of obtaining valid consent and the risk of consent being withdrawn.

The ICO has published guidance on Consent which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

**Contract** (b)

* Contracts of employment with staff

The ICO has published guidance on Contract which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/).

**Legal Obligation** (c)

* officer or staff pay information is supplied to HMRC in order that tax may be collected
* officer or staff pay information is supplied to the National Fraud Initiative so that fraud may be detected

The ICO has published guidance on Legal Obligation which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/).

**Vital Interests** (d)

* police use of vital interests is likely to fall under Law Enforcement rather than GDPR & DPA Part 2 (General Processing). The ICO adopts a narrow interpretation of ‘vital interests’ as meaning ‘to protect someone’s life.’ The NPCC has a broader interpretation that ‘vital interests’ encompasses situations where processing of personal data is required in order to prevent harm to an individual.

The ICO has published guidance on Vital Interests which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/).

**Public Task** (e)

* administration of justice

The ICO has published guidance on Public Task which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/).

In addition, in correspondence with the NPCC the ICO has stated:

Where an organisation is relying upon the public task lawful basis for processing, they should document the lawful basis and be able to demonstrate a clear basis in either statute or common law for the relevant task, function or power for which you are using the personal data. Furthermore organisations should be able to demonstrate that there is no other reasonable and less intrusive means to achieve this purpose.

To help you meet your accountability and transparency obligations, you will need to:

• document your decision that the processing is necessary for you to perform a task in the public interest or exercise your official authority;

• identify the relevant task or authority and its basis in common law or statute; and

• include basic information about your purposes and lawful basis in your privacy notice.

The NPCC’s position is that any documenting of the lawful basis for processing should occur within the police force’s register of processing activities (RoPA) (see 4.5.5) and its privacy notice (see 4.2.2.7).

The lawful basis for processing must be recorded in forces’ Registers of Processing Activities.

As well as the necessity to meet one of the five processing conditions, the wider requirement to be lawful means that any processing must also not contravene the rule of law, including statute and Common Law. Unlawful processing may arise where the police processing of personal data is:

* beyond or in contravention of their statutory or Common Law powers (e.g., ultra vires), for example, the police sell the names and addresses of burglary victims to companies trying to sell double-glazing;
* in breach of an obligation of confidentiality, for example, the police publish the names and home addresses of all staff on the internet;
* in breach of any law or prohibitions, for example: the police obtain personal data in contravention of the Regulation of Investigatory Powers Act 2000; the police process personal data in a manner which breaches the Article 8 rights of the Human Rights Act 1998;
* in breach of an enforceable contractual agreement.

There is only one exemption from the lawfulness aspects of GDPR Article 6, which is unlikely to be used by the police, but is set out immediately below.

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 6 (lawfulness) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of Article 6 would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

#### Lawful Processing – Change of Purpose

GDPR Article 6(4) states:

*Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:*

*(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;*

*(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;*

*(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;*

*(d) the possible consequences of the intended further processing for data subjects;*

*(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.*

**Commentary** - In cases where the purpose of general processing changes from the initial purpose for which the personal data was collected and the processing is not based on consent or law GDPR Article 6(4) requires the police forces to consider five listed factors to determine whether the different purpose is compatible with the original purpose of the processing.

If the original lawful basis was consent then it is necessary to either seek specific consent for the new purpose or find a different lawful condition for processing, and satisfy the requirements of the remainder of the First Principle (fair and transparent).

There is an interdependency between change of purpose covered in this section and transparency requirements covered at 4.2.2.7.

The GDPR Article 89 recognises that further processing for archiving purposes in the public interest, scientific research purposes and statistical purposes is to be regarded as compatible (see [4.7](#_Processing_for_archiving,)).

The ICO guidance states:

*“As a general rule, if the new purpose is very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is unlikely to be compatible with your original purpose for collecting the data.”*

#### Lawful Processing - Consent

[GDPR Article 4(11)](https://gdpr-info.eu/art-4-gdpr/) defines consent of a data subject as:

*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

[GDPR Article 7 (Conditions for Consent)](https://gdpr-info.eu/art-7-gdpr/) states:

*1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*

*2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*

*3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*

*4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*

There are three GDPR Recitals relevant to consent in the policing context. The first, GDPR Recital 32 (“Conditions for Consent”) states:

*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.*

The second, GDPR Recital 42 (“Burden of proof and requirements for consent ”) states:

*Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC (1) a declaration of consent pre- formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.*

The third, GDPR Recital 43 (“Freely-given consent”) states:

*In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.*

**Commentary -** Consent is one of the five processing conditions available to the police for general processing of personal data. The NPCC’s position is that police forces should, where possible, use a processing condition other that consent. This is because consent can be withdrawn and because the nature and role of a police force, in particular its relative position of power over data subjects, means that it may be difficult to show that any consent is freely given and valid.

Withdrawal of consent does not make unlawful any processing previously undertaken which had used consent as the lawful basis for processing.

The ICO has produced guidance on consent which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

Where the police force uses consent as their legal basis for general processing they should ensure their usage is consistent with the ICO consent guidance.

There is one exemption to consent which may be relevant to police force’s media activities which is set out immediately below.

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 7 (conditions for consent) & Articles 8(1) & (2) (child’s consent) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of Article 7 or Article 8(1) or (2) would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

#### Lawful Processing - Special Category Data and Special Processing Conditions (GDPR Article 9(1), DPA Part 2 Section 10)

Special Category Data (or “Special Categories of personal data”) is defined under GDPR Article 9(1) and is personal data which:

* Reveals racial or ethnic origin
* Reveals political opinions
* Reveals religious or philosophical beliefs
* Reveals trade union membership
* Is genetic data or biometric data used to uniquely identify a person
* Is data concerning health
* Is data concerning a person’s sex life or sexual orientation

[DPA Part 2 Section 10 Special categories of personal data and criminal convictions etc data](http://www.legislation.gov.uk/ukpga/2018/12/section/10) states:

*(1) Subsections (2) and (3) make provision about the processing of personal data described in Article 9(1) of the GDPR (prohibition on processing of special categories of personal data) in reliance on an exception in one of the following points of Article 9(2)—*

*(a) point (b) (employment, social security and social protection);*

*(b) point (g) (substantial public interest);*

*(c) point (h) (health and social care);*

*(d) point (i) (public health);*

*(e) point (j) (archiving, research and statistics).*

*(2) The processing meets the requirement in point (b), (h), (i) or (j) of Article 9(2) of the GDPR for authorisation by, or a basis in, the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1 of Schedule 1.*

*(3) The processing meets the requirement in point (g) of Article 9(2) of the GDPR for a basis in the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 2 of Schedule 1.*

*(4) Subsection (5) makes provision about the processing of personal data relating to criminal convictions and offences or related security measures that is not carried out under the control of official authority.*

*(5) The processing meets the requirement in Article 10 of the GDPR for authorisation by the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1, 2 or 3 of Schedule 1.*

*(6) The Secretary of State may by regulations—*

*(a) amend Schedule 1—*

*(i) by adding or varying conditions or safeguards, and*

*(ii) by omitting conditions or safeguards added by regulations under this section, and*

*(b) consequentially amend this section.*

*(7) Regulations under this section are subject to the affirmative resolution procedure.*

**Commentary -** Police forces are most likely to generally process Special Category Data of the following types, primarily relating to their own prospective, existing and retired officers and staff and others who work for their organisation; personal data which:

* Reveals racial or ethnic origin
* Reveals trade union membership
* Is genetic data or biometric data used to uniquely identify a person
* Is data concerning health

Such Special Category Data is likely to be processed by police forces for the following purposes:

* Employment
* Defending Legal Claims
* Health & Welfare
* Archiving, Research or Statistics

Due to its increased sensitivity Special Category Data requires greater protection before it may be processed. Consequently Special Category Data cannot be processed unless one of the ten special processing conditions listed under GDPR Article 9(2) applies subject, where necessary, to meeting any associated condition provided under [DPA Part 2 Section 10](http://www.legislation.gov.uk/ukpga/2018/12/section/10) and DPA Schedule 1.

In addition, one of the processing conditions set out in GDPR Article 6 must also be met. The GDPR Article 6 processing condition does not dictate which GDPR Article 9(2) special processing condition is used, and vice-versa, though in all cases the most appropriate ones should be used.

[DPA Part 2 Section 10](http://www.legislation.gov.uk/ukpga/2018/12/section/10) and Schedule 1 provide further conditions required by five of the special processing conditions – those concerning employment, social security and protection (GDPR Article 9(2)(b)), substantial public interest (GDPR Article (2)(g)), health and social care (GDPR Article 9(2)(h)), public health (GDPR Article 9(2)(i)), and archiving, research and statistics (GDPR Article 9(2)(j)). Processing is not permitted under any of those five special conditions unless:

* in the case of substantial public interest (GDPR Article (2)(g)), it meets a condition in DPA Schedule 1 Part 2; or
* in the other four cases, it meets a condition in DPA Schedule 1 Part 1.

As with GDPR Article 6 processing conditions the Article 9(2) special processing conditions should be recorded within the police force’s register of processing activities (RoPA) (see 4.5.5) and its privacy notice (see 4.2.2.7). The special processing conditions listed under GDPR Schedule 9(2) most likely to be used by the police are as follows:

***Explicit Consent***

*(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;*

***Employment, Social Security and Social Protection***

*(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject (also requires compliance with a DPA Schedule 1 Part 1 condition);*

***Defence of Legal Claims***

*(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;*

***Health and Social Care***

*(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 (also requires compliance with a DPA Schedule 1 Part 1 condition, and DPA Part 2 Section 10(1));*

***Archiving, Research and Statistics***

*(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (also requires compliance with a DPA Schedule 1 Part 1 condition).*

The ICO has produced guidance on Special Category Data which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/).

There is one exemption to consent which may be relevant to police force’s media activities which is set out immediately below.

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 9 (processing of special categories of data) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of Article 6 would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

#### Lawful Processing – Criminal Offence Data

GDPR Article 10 states:

*Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.*

[DPA Part 2 Section 11 Special categories of personal data etc: supplementary](http://www.legislation.gov.uk/ukpga/2018/12/section/11) states:

*(1) For the purposes of Article 9(2)(h) of the GDPR (processing for health or social care purposes etc), the circumstances in which the processing of personal data is carried out subject to the conditions and safeguards referred to in Article 9(3) of the GDPR (obligation of secrecy) include circumstances in which it is carried out—*

*(a) by or under the responsibility of a health professional or a social work professional, or*

*(b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.*

*(2) In Article 10 of the GDPR and section 10, references to personal data relating to criminal convictions and offences or related security measures include personal data relating to—*

*(a) the alleged commission of offences by the data subject, or*

*(b) proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.*

**Commentary** - GDPR Article 10 requires any general *processing of personal data relating to criminal convictions and offences or related security measures* to occur under official authority or be authorised by law – the ICO refers to this as “Criminal Offence Data”. It also requires that *any comprehensive register of criminal convictions shall be kept only under the control of official authority.*

[DPA Part 2 Section 11(2)](http://www.legislation.gov.uk/ukpga/2018/12/section/11) provides additional non-exhaustive definitions of Criminal Offence Data stating that it includes personal data relating to: the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

[DPA Part 2 Section 10(4) and (5)](http://www.legislation.gov.uk/ukpga/2018/12/section/10) along with Schedule 1 set out very restrictive provisions that permit processing of Criminal Offence Data not under official authority. None of these are considered relevant to police forces as the police’s use of Criminal Offence Data is deemed as occurring ‘under official authority’.

The primary scenarios where GDPR Article 10 applies to a police force are where Criminal Offence Data is generally processed for the following purposes:

* for the vetting of police officers and staff and others working for or on behalf of the police force
* to investigate misconduct complaints
* journalism and public relations
* to defend legal claims against the police force

The NPCC’s position is that the necessary authority required by GDPR Article 10 exists in those scenarios.

As well as meeting the GDPR Article 10 requirements the processing must meet a GDPR Article 6(1) processing condition and a DPA Schedule 1 Part 1, 2 or 3 condition and an Appropriate Policy Document must be created in accordance with [DPA Schedule 1 Part 4](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/part/4).

The ICO has published guidance on Criminal Offence Data which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/).

There is one exemption to consent which may be relevant to police force’s media activities which is set out immediately below.

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 10 (data relating to criminal convictions etc.) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of Article 10 would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

#### Appropriate Policy Document (DPA Schedule 1 Part 4)

[DPA Schedule 1 Part 4 Appropriate policy document and additional safeguards](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/part/4) states:

***Application of this Part of this Schedule***

*38 This Part of this Schedule makes provision about the processing of personal data carried out in reliance on a condition in Part 1, 2 or 3 of this Schedule which requires the controller to have an appropriate policy document in place when the processing is carried out.*

***Requirement to have an appropriate policy document in place***

*39 The controller has an appropriate policy document in place in relation to the processing of personal data in reliance on a condition described in paragraph 38 if the controller has produced a document which—*

*(a) explains the controller's procedures for securing compliance with the principles in Article 5 of the GDPR (principles relating to processing of personal data) in connection with the processing of personal data in reliance on the condition in question, and*

*(b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the condition, giving an indication of how long such personal data is likely to be retained.*

***Additional safeguard: retention of appropriate policy document***

*40(1) Where personal data is processed in reliance on a condition described in paragraph 38, the controller must during the relevant period—*

*(a) retain the appropriate policy document,*

*(b) review and (if appropriate) update it from time to time, and*

*(c) make it available to the Commissioner, on request, without charge.*

*(2)“Relevant period”, in relation to the processing of personal data in reliance on a condition described in paragraph 38, means a period which—*

*(a) begins when the controller starts to carry out processing of personal data in reliance on that condition, and*

*(b) ends at the end of the period of 6 months beginning when the controller ceases to carry out such processing.*

***Additional safeguard: record of processing***

*41 A record maintained by the controller, or the controller's representative, under Article 30 of the GDPR in respect of the processing of personal data in reliance on a condition described in paragraph 38 must include the following information—*

*(a) which condition is relied on,*

*(b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing), and*

*(c) whether the personal data is retained and erased in accordance with the policies described in paragraph 39(b) and, if it is not, the reasons for not following those policies.*

**Commentary** – DPA Schedule 1 Part 4, which requires the creation and management of an Appropriate Policy Document applies when processing of Special Category Data relies upon a DPA Schedule 1 Part 1 or Part 2 Special Processing Condition or when processing of Criminal Offence Data occurs.

This appropriate policy documentation must:

* explain how the controller complies with the data protection principles set out in Article 5 of the GDPR;
* explain the controller’s policies for the retention and erasure of personal data processed under the relevant condition; and
* be retained, reviewed and (if appropriate) updated by the controller and (if requested) made available to the Information Commissioner, until six months after the controller ceases carrying out the processing.

Where appropriate policy documentation is required, the controller’s records of processing activities (under Article 30 of the GDPR) must include:

* details of the relevant condition relied on;
* how processing satisfies Article 6 of the GDPR (lawfulness of processing); and
* details of whether the personal data is retained and erased in accordance with the appropriate policy documentation (and if not the reasons why not).

A similar requirement for an Appropriate Policy Document arises for Law Enforcement processing via DPA Part 3 Section 42.

[Appendix D](#_Appendix_D:_Appropriate) contains a template for an Appropriate Policy Document.

#### Fairness and Transparency (GDPR Articles 13 & 14)

**Commentary** - The fairness and transparency elements of the First General Processing Principle are usually satisfied through compliance with GDPR Articles 13 and 14, which are set out in detail at 4.4.3.

### General Processing; Second Principle – Purpose Limitation (GDPR Article 5)

#### Overview of Second General Processing Principle

GDPR Article 5(1)(b) states:

*Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.*

**Commentary** - The use of the term ‘incompatible’ suggests that the principle would be breached if the use of personal data was contradictory to the purposes it was obtained. However, if the use was merely different to that for which it was obtained (as opposed to contradictory) then the provision would be likely to be satisfied providing any new compatible purpose was notified to the data subject in accordance with the fairness requirements of the first principle.

When deciding whether any disclosure of personal data is compatible with the purpose(s) for which the personal data was obtained consideration must be given to the purpose(s) for which the personal data is intended to be processed once disclosed. Such decisions cannot be made retrospectively by controllers once the data has been obtained.

Incompatible use is likely to occur in the following scenario:

*Address details of police employees, originally obtained and held by the police force for staff administration purposes are disclosed to an outside organisation for subsequent direct marketing use; or the police force uses the details to send advertising material to employees.*

The ICO has published guidance on the Second GDPR Principle which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/).

There are a few exemptions to the Second General Principle which are set out below.

**Exemption – Crime & Taxation.** [DPA Schedule 2 Part 1 Paragraph 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/2/enacted) disapplies GDPR Articles 5(1)(a) & (b)[[8]](#footnote-8) as amended by the DPA to the extent that the application of those provisions would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of a tax or an imposition of a similar nature. [See 4.3.2.1](#_Exemptions_-_Crime)

**Exemption – Disclosure Required by Law.** [DPA Schedule 2 Part 1 Paragraph 5](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/5/enacted) disapplies GDPR Articles 5(1)(a) & (b)[[9]](#footnote-9) as amended by the DPA to the extent that the application of those provisions would prevent the controller from:

1. complying with an obligation to make personal data available to the public, or
2. complying with an obligation to disclose personal data required by an enactment, rule of law or order of a court or tribunal, or
3. making a disclosure where necessary or in connection with legal proceedings (including prospective ones), or making a disclosure necessary for obtaining legal advice, or making a disclosure that is otherwise necessary for establishing, exercising or defending legal rights.

[See 4.3.2.2.](#_Exemption_-_Disclosure)

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 5(1)(b) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of Article 5(1)(b) would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

### General Processing; Third Principle – Data Minimisation (GDPA Article 5)

#### Overview of Third General Processing Principle

GDPR Article 5(1)(c) states:

*Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*

**Commentary** - To comply with this principle, the police will seek to identify the minimum amount of personal data that is required in order properly to fulfil their purpose(s). That personal data must also be adequate for the purpose(s). Clearly there is a crucial requirement to first define the purpose(s) of the processing in order to meet these obligations.

The police will regularly monitor compliance with this principle as changes in circumstances or failure to keep the information up-to-date may mean that personal data that was originally compliant becomes non-compliant. Notwithstanding the Act there will be significant practical business benefits for the police if the personal data it processes is adequate, relevant and not excessive.

For additional commentary on ‘data quality’ see 4.2.9 below.

The ICO has published guidance on the Third GDPR Principle which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/).

There is one exemption to this general principle which may be relevant to police force’s media activities which is set out immediately below.

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 5(1)(c) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of Article 5(1)(c) would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

#### Adequacy

**Commentary** - All personal data processed by the police must be sufficient for the purpose(s) for which it is used or likely to be used. The personal data must be clear in meaning and sufficient for others to understand at the present time and in the future.

Those creating personal data must ensure that it is adequate, unambiguous and professionally worded. Opinions must be distinguishable from matters of fact.

The police force must put in place appropriate measures to ensure that personal data held on police systems relating to one individual cannot be confused with that of another individual with the same name.

This may be achieved by the inclusion of additional identifiers, such as date of birth and/or descriptive information.

Adequacy will also be achieved through the use of common data standards which may mean, for example, that the police record home addresses, descriptive information and other personal data in a format which assists interoperability of, and transfer between, different police information systems.

#### Relevance & Excessiveness

**Commentary** - To establish relevance, a necessity test will identify the minimum amount of personal data that is required to achieve the specific purpose(s).

Some processing operations, such as staff administration, may require the use of a great deal of a particular data subject’s personal data. In other circumstances only a minimal amount is necessary.

It is excessive to hold a class of data on all individuals where that particular item of data is only relevant in certain individual cases.

The police will adopt practices to ensure that personal data that fails to meet the requisite criteria for relevancy is either brought up to those criteria, or rejected. When determining relevance consideration must be given to the necessity and proportionality of processing the personal data.

Personal data must not be excessive in relation to the purpose for which it is held. It is difficult to argue that irrelevant information is not also excessive information.

If personal data is kept for longer than necessary (see fifth principle at 4.2.6 below) then it is likely to be both irrelevant and excessive.

### General Processing; Fourth Principle – Accuracy (GDPR Article 5)

#### Overview of Fourth General Processing Principle

GDPR Article 5(1)(d) states:

*Personal data shall be accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.*

**Commentary** - As with the third principle, compliance with this principle has obvious business benefits for the police.

The principle has three elements. The first, requiring accuracy of personal data, is unconditional, while the second element only requires the personal data to be kept up-to-date ‘where necessary’. The third requires the erasure or rectification of inaccurate personal data without delay having considered the purpose of the processing.

These elements are covered in more detail within the remainder of 4.2.5.

For additional guidance on ‘data quality’ see 4.2.9 below.

The ICO has published guidance on the Fourth GDPR Principle which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/).

There is one exemption to this general principle which may be relevant to police force’s media activities which is set out immediately below.

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 5(1)(d) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of Article 5(1)(d) would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

#### Accuracy

**Commentary** - [DPA Part 7 Section 205 General interpretation](http://www.legislation.gov.uk/ukpga/2018/12/section/205) contains the following useful definition:

*“inaccurate”, in relation to personal data, means incorrect or misleading as to any matter of fact.*

Great care must be exercised in the collection of personal data. All staff, when recording personal data, must ensure that it is accurately recorded and where desirable its source is readily available.

Where there is any doubt regarding accuracy, information must be clarified with the source.

Police forces must adopt procedures to prevent factual inaccuracies being entered onto police

information systems. This may be achieved by:

* Ensuring as far as possible that the source of the personal data is reliable;
* Taking steps to verify the personal data if possible with another source or if reasonable, with the data subject, at the time of collection or at another convenient opportunity;
* Using automatic validation procedures to ensure procedures for data entry and the information system itself does not introduce inaccuracies;
* Using constrained fields in computer databases.

Personal data is ‘inaccurate’ if it is incorrect or misleading as to any matter of fact. Consequently, personal data that is presented as an opinion and does not claim to be fact cannot be challenged on the grounds of inaccuracy.

#### Kept Up-to-date

**Commentary** - The second part of the fourth principle, which refers to keeping personal data up-to-date, is qualified in that updating is only required ‘where necessary’.

The purpose for which the data are held or used will be relevant in deciding whether such updating is required. If the personal data is intended to be used merely as an ‘historical’ record or snap shot in time then updating would be inappropriate.

However, sometimes it is important for the purpose that the personal data reflects the data subject’s current circumstances. Within the police service it is likely that such updating would be required in the following scenario:

* In order to keep up-to-date home address and next of kin details within a police force’s collection of personnel records;

In the example given above steps must be taken to ensure that the personal data is kept up-to- date, or when the personal data is used, account will be taken of the fact that circumstances may have changed.

When determining whether or not an item of personal data requires updating staff may consider the following:

* Is there a record of when the personal data was recorded or last updated?
* Are all those involved with the personal data aware that the personal does not necessarily reflect the current position?
* Are effective steps taken to update the personal data – for example, by checking back at intervals with the original source or with the data subject?
* Is the fact that the personal data is out of date likely to prejudice the purpose of the processing or cause damage or distress to the data subject?

#### Erasure and Rectification without delay

**Commentary** - Where inaccuracies come to light, the police must take steps to lessen the damage or distress caused to the data subject or any other person by:

* Ensuring the inaccurate personal data is rectified or erased as soon as possible;
* Passing the corrected personal data to any third-party to whom the inaccurate personal data may had already been disclosed;
* Ensuring any other consequences which may have arisen before the personal data was
* corrected have been acted upon to minimise the damage or distress;
* Acting on reports of inaccuracies received from other organisations or individuals.

### General Processing: Fifth Principle – Storage Limitation (GDPA Article 5)

#### Overview Fifth General Processing Principle

GDPR Article 5(1)(e) states:

*Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.*

**Commentary** - The fifth principle requires the police to consider the purpose for which personal data is being held and once that purpose has been concluded the police will either cease processing the personal data (usually through its secure disposal, deletion or destruction), or will de-personalise it in such a way that it is no longer personal data or able to be ‘reformed’ into personal data.

The police are likely, for practical purposes, to follow the former rather than the latter and adopt a policy of regular review of personal data to establish whether it is still required and dispose as necessary.

Within police forces a systematic approach will be followed including the definition of review

periods for particular categories of documents or information containing personal data. At the end of such periods they will be reviewed and disposed of if no longer required.

Police forces may need to consider certain statutory requirements which may specify required

retention periods, or the potential value of some personal data and other information which may suggest further retention for historic purposes.

On a practical level within police forces information asset owners must ensure that review and ‘disposal where necessary’ procedures are adopted for systems within their control which apply to both computer and manually-held personal data. However, information system owners must exercise care, particularly with regards to personal data held on computer equipment, to ensure that disposal does mean permanent and complete deletion and that there is no risk of the personal data being ‘reformed’ or retrieved.

The standard retention periods for personal data subject to general processing must be documented by police forces, and as far as is possible consistent standard retention periods should be adopted by all police forces. Any such documentation should set out the circumstances in which deviation from the standard retention period, resulting in either shorter or longer retention, is permissible.

Whatever standard periods are adopted, police forces must maintain a flexible approach towards retention issues which allow individual cases to be assessed properly and proportionate decisions reached regarding retention. This can be achieved through the adoption of exceptional case review procedures and through chief officers, in their capacity as ‘controllers’, retaining the right and responsibility to make individual judgements where appropriate.

The ICO has published guidance on the Fifth GDPR Principle which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/).

The police force must implement processes to resolve data quality disputes or complaints regarding the retention or otherwise of personal data.

There is one exemption to this general principle which may be relevant to police force’s media activities which is set out immediately below.

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 5(1)(e) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of Article 5(1)(e) would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

### General Processing: Sixth Principle – Integrity & Confidentiality (GDPR Article 5)

#### Overview Sixth General Processing Principle

[GDPR Article 5(1)(f)](https://gdpr-info.eu/art-5-gdpr/) states:

*Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

[GDPR Article 32](https://gdpr-info.eu/art-32-gdpr/) states:

*1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

*(a) the pseudonymisation and encryption of personal data;*

*(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*

*(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*

*(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

*2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*

*3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.*

*4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.*

GDPR Recital 75 (Risks to the Rights and Freedoms of Natural Persons) states:

*The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.*

GDPR Recital 76 (Risk Assessment) states:

*The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. 2Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.*

GDPR Recital 77 (Risk Assessment Guidelines) states:

*Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. 2The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.*

GDPR Recital 78 (Appropriate Technical and Organisational Measures) states:

*The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. 2In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. 3Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. 4When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. 5The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.*

GDPR Recital 79 (Allocation of the Responsibilities) states:

*The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.*

GDPR Recital 83 (Security of Processing) states:

*In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. 2Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. 3In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.*

**Commentary** – [GDPR Article 5(1)(f)](https://gdpr-info.eu/art-5-gdpr/) and [GDPR Article 32](https://gdpr-info.eu/art-32-gdpr/) require the police to process personal data in a secure manner. The ICO’s guidance stipulates that, in practice, this means that police forces must have appropriate security to prevent the personal data they hold being accidentally or deliberately compromised. In particular, the controller will need to:

* design and organise their security to fit the nature of the personal data they hold and the harm that may result from a security breach;
* be clear about who in their organisation is responsible for ensuring information security;
* make sure they have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
* be ready to respond to any breach of security swiftly and effectively.

The NPCC via the Information Assurance Portfolio, which reports to IMORCC, has developed extensive guidance and policy around information security (also known as information assurance) and police forces should comply with that material.

The ICO has published guidance on the Sixth GDPR Principle which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/).

The Data Protection Officer must maintain effective working relationships with colleagues responsible for information security/assurance.

#### Data Breach Management & Reporting

[GDPR Article 33](https://gdpr-info.eu/art-33-gdpr/) (Notification of a personal data breach to the supervisory authority [ICO]) states:

*1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*

*2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.*

*3. The notification referred to in paragraph 1 shall at least:*

*(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;*

*(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;*

*(c) describe the likely consequences of the personal data breach;*

*(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.*

*4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.*

*5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.*

GDPR Article 34 (Communication of data breach to the data subject) states:

*1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.*

*2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).*

*3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:*

*(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;*

*(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;*

*(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.*

*4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.*

GDPR Recital 86 (Notification of Data Subjects in Case of Data Breaches) states:

*The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. 2The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. 3Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. 4For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.*

GDPR Recital 87 (Promptness of Reporting / Notification) states:

*It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. 2The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. 3Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.*

GDPR Recital 88 (Format and Procedures of the Notification) states:

*In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. 2Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.*

**Commentary** – A personal data breach could lead to a loss of control over data, limitation of rights, reputational damage and other social or economic disadvantages. Therefore, in the event of a data breach whereby there is a risk to the rights and freedoms of the individual, [GDPR Article 33](https://gdpr-info.eu/art-33-gdpr/) requires police forces to inform the ICO without undue delay, and where feasible, within 72 hours of becoming aware of it and give details as to how they are mitigating that risk.

When there is a high risk to the rights and freedoms of an individual as a result of a data breach the data subject(s) should also be notified of the data breach in good time so they may take the necessary precautions to protect themselves. The communication should be made as soon as possible relative to the risk, for example if there is an immediate risk of damage a quick response to data subjects would be advisable (this can be a mass communication if applicable).

[Appendix C](#_Appendix_C:_Personal) to this manual contains specific guidance on the management of police personal data breaches.

The ICO has published guidance on GDPR Personal Data Breaches which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/). It includes a useful self-assessment tool to determine whether the ICO should be informed of the breach. The ICO has also published resources for Personal Data Breach Reporting which can be found [here](https://ico.org.uk/for-organisations/gdpr-resources/#pdb).

The Data Protection Officer must ensure their police force has appropriate measures in place to identify, manage and mitigate personal data breaches relating to General Processing.

### General Processing; Accountability Requirement

GDPR Article 5(2) states:

*“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 [The GDPR Principles]”*

**Commentary** – The accountability requirement means that not only do forces have to comply with the GDPR Principles, they must also be able to demonstrate compliance with them.

The ICO has published guidance on Accountability which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accountability-principle/), and on Accountability & Governance which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/).

The Data Protection Officer must ensure appropriate measures are in place to assess their forces’ compliance with the GDPR/DPA Part 2 Accountability requirement.

### Police Approach to Data Quality on Major IT Systems

#### Overview Data Quality on Major IT Systems

**Commentary** - The recommended police approach to ensuring good quality personal data within major police information systems consists of the following four elements, which are explored in greater detail below:

* Effective Governance.
* Preventative Activity.
* Identification/Reporting Activity.
* Rectification Activity.

The police force must adopt appropriate measures to ensure that personal data and other information used in General Processing is of the necessary quality and meets GDPR/DPA Part 2 requirements.

#### Effective Governance

**Commentary** - Individual responsibilities:

* Users - All staff will ensure personal data entered onto major police information systems by them is of good quality, and is in accordance with associated policy, procedure and guidance. They will adopt a ‘right first time approach’ to data entry.
* Supervisors - All staff with a quality assurance role will ensure that any poor quality data entered by staff whose work they quality assure is identified and rectified, and any necessary preventative activity occurs to reduce the chances of re-occurrence of the poor quality data input. They will liaise with their police force’s data quality leads as is necessary.
* Business process owners – All individuals responsible for creating, maintaining and developing business processes involving the use of personal data will ensure those business processes include preventative, identification/reporting and rectification activities to reduce the instances of poor quality data. They will liaise with their police force’s data quality leads as is necessary.

Oversight responsibilities:

* Information Asset Owners must maintain oversight of data quality of information processed within their systems. They must consider any data quality performance reports and make any necessary interventions including escalation to the police force’s Senior Information Risk Owner where appropriate.
* Police forces will ensure that within their organisation there is clarity as to who should undertake preventative, identification/reporting and rectification activities relating to their major IT systems.

Data Quality Leads:

* Each police force will identify an individual(s) to act as their data quality lead, to promote the importance of good data quality, liaise with information asset owners and business process owners, supervisors and users within and beyond their organisation (collaboratively), as is necessary.

#### Preventative Activity

* **Commentary** - Police forces will use the Data Protection Impact Assessment process to ensure that technical measures are adopted as far as is practical/proportionate during the development of major IT systems to reduce the instances of poor quality data. Such measures may be informed by identification/reporting and rectification activities set out later in this chapter. The technical measures may include:
  + use of constrained value (cv) lists;
  + use of field validation allowing only acceptable input into certain fields;
  + making the completion of certain fields mandatory preventing navigation away until they have been completed;
  + seeking amendments to major IT systems to correct in a timely manner any identified technical issue that contributes to poor quality data;
  + adopting measures to prevent the automated migration of poor quality legacy data into major IT systems.
* Police forces will ensure that all users are appropriately trained in the use of major IT systems and understand the need for good data quality, particularly its impact on searching, business decision-making, linking, de-duplication and automated disposal of records. Training and understanding products must also encompass wider information management aspects such as the Data Protection Act requirements for good quality data.
* Police forces will ensure that:
  + business processes involving use of major IT systems are documented and available to users;
  + those business processes are designed to reduce the likelihood of instances of poor quality data;
  + those business processes are regularly reviewed and amended in the light of experience as necessary to reduce the likelihood of instances of poor quality data;
  + they have in a place a force policy and/or procedure concerning data quality and a forum for the discussion of the issue of data quality;
  + they identify and suggest technical or business changes to improve the quality of data input;
  + they develop and issue any necessary internal/local communications around data quality;
  + they have appropriate resource undertaking preventative activity.
* Force data quality leads will ensure that necessary data quality-related guidance and communications are issued where necessary within their organisation or across multiple organisations.

#### Identification/Reporting Activity

* **Commentary** - Users will report instances of poor data quality they identify to their supervisors or business process owners so that rectification and prevention activities may be undertaken.
* Supervisors, data quality staff and others with a quality assurance role will ensure that any poor quality data entered by users whose input they quality assure is identified and reported so that rectification can occur and any necessary preventative activity occurs to reduce the chances of re-occurrence of the poor quality data input.
* Significant data quality issues that are identified by users or supervisors may be reported to data quality leads.
* Police forces will develop and run reports to assess the quality of data within major IT systems. Due to resource constraints such reporting will focus on the data fields with greatest associated business and operational risk, and potential duplicate records.
* Police forces will create and maintain issues logs summarising the underlying causes of poor quality data and maintain records of their data quality activities.
* Police forces’ data quality leads will also report on data quality performance to their information asset owners, local management board or equivalent as they see fit/or as instructed.

#### Rectification Activity

* **Commentary** - The identification/reporting activity described above will act as one of the prompts for the undertaking of rectification activity.
* Police forces are expected to resource rectification activity appropriately for that activity, and for it to be clear who should undertake what rectification work.
* All those undertaking rectification work should report any significant underlying issue that has contributed to the poor quality data (e.g. technical, business process, or training) to their force’s data quality lead and business process owner in order that potential preventative activities can be considered.

## General Data Processing Exemptions/Restrictions to Data Subject Rights (DPA Part 2 Section 15)

### Overview

**Commentary** - GDPR Article 23 permitted the UK Government to include within the Act exemptions and restrictions which disapply elements of the GDPR concerning compliance with the General Data Protection Principles and subject rights in certain circumstances.

**It is important to note that the exemptions do not provide an automatic blanket ability to disapply all the provisions relevant to a particular exemption – instead the exemptions can only be applied as far as is necessary.**

Those exemptions and restrictions are introduced in [DPA Part 2 Section 15](http://www.legislation.gov.uk/ukpga/2018/12/section/15) which provides signposts to DPA Schedules 2, 3 and 4 where they are set out in extensive and convoluted detail. Within Schedule 2 there are 24 and those covered in the following guidance are in bold: **2 Crime & taxation: general**, 3 Crime and taxation: risk assessment systems, 4 Immigration, **5 Information required to be disclosed by law etc or in connection with legal proceedings**, **7 Functions designed to protect the public etc**, 8 Audit functions, 9 Functions of the Bank of England, 10 Regulatory functions relating to legal services, the health service and children’s services, 11 Regulatory functions of certain other persons, 13 Parliamentary Privilege, 14 Judicial appointments, judicial independence and judicial proceedings, 15 Crown honours, dignities and appointments, **16 Protection of the rights of others: general**, **17 Assumption of reasonableness for health workers, social workers and education workers**, **19 Legal Professional Privilege**, **20 Self incrimination**, 21 Corporate Finance, **22 Management forecasts**, **23 Negotiations**, **24 Confidential references**, 25 Exam scripts and exam marks, **26 Journalistic, academic, artistic and literary purposes**, **27 Research & statistics**, and **28 Archiving in the public interest**.

Those exemptions and restrictions relating to manual unstructured data held by police forces (as FOI Public Authorities) for General Processing within the Applied GDPR are set out in DPA Part 2 Section 24.

Those exemptions and restrictions relating to manual unstructured data held by police forces (as FOI Public Authorities) used specifically for longstanding historical purposes General Processing within the Applied GDPR are set out in DPA Part 2 Section 25.

The provisions most relevant to police General Processing are detailed in the remainder of this sub-section.

The ICO has published guidance on GDPR Individual Rights which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/).

### DPA Schedule 2 Part 1 Exemptions etc. from the GDPR

DPA Schedule 2 Part 1 Paragraph 1 states:

*In this Part of this Schedule, “the listed GDPR provisions” means—*

*(a) the following provisions of the GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the GDPR)—*

*(i) Article 13(1) to (3) (personal data collected from data subject: information to be provided);*

*(ii) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);*

*(iii) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);*

*(iv) Article 16 (right to rectification);*

*(v) Article 17(1) and (2) (right to erasure);*

*(vi) Article 18(1) (restriction of processing);*

*(vii) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);*

*(viii) Article 20(1) and (2) (right to data portability);*

*(ix) Article 21(1) (objections to processing);*

*(x) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in sub-paragraphs (i) to (ix); and*

*(b) the following provisions of the GDPR (the application of which may be adapted by virtue of Article 6(3) of the GDPR)—*

*(i) Article 5(1)(a) (lawful, fair and transparent processing), other than the lawfulness requirements set out in Article 6;*

*(ii) Article 5(1)(b) (purpose limitation).*

**Commentary** - Part 1 Paragraph 1 of the schedule lists the “Listed GDPR Provisions” which can be restricted or adapted by the exemptions set out in the remaining five paragraphs of DPA Schedule 2 Part 1. Rather confusingly different sets of “Listed GDPR Provisions” exist for DPA Schedule 2 Parts 1, 2, 4, 5 & 6 relevant only to those parts respectively.

The Listed GDPR Provisions encompass large parts of the GDPR provision including fairness (including privacy notices), data subject rights and general data protection principles.

DPA Schedule 2 Part 1 Paragraphs 2 and 3, which are explored in detail at 4.3.2.1 below, have the same effect as DPA 1998 Section 29. DPA Schedule 2 Part 1 Paragraph 4 concerns restrictions on the application of the Listed GDPR Provisions in relation to immigration control and these are not directly relevant to policing and is not covered by this manual. DPA Schedule 2 Part 1 Paragraph 5 (Information required to be disclosed by law etc. or in connection with legal proceedings) have the same effect as DPA 1998 Sections 34 & 35.This explored in detail at 4.3.2.2.

DPA Schedule 2 Part 2 Paragraph 7 (Functions designed to protect the public etc.) are explored in detail at 4.3.3.1. This disapplies elements of the data subject rights under GDPR Articles 13 to 21. DPA Schedule 2 Part 2 Paragraphs 8 to 13 are not relevant to policing.

DPA Schedule 2 Part 3 disapplies elements of the data subject rights under GDPR Article 15 concerning the disclosure of information relating to persons other than the data subject.

DPA Schedule 2 Part 4 disapplies elements of the data subject rights under GDPR Articles 13 to 15.

DPA Schedule 2 Part 5 disapplies elements of the GDPR for reasons relating to freedom of expression.

DPA Schedule 2 Part 6 disapplies elements of the data subject rights under GDPR Articles 15, 16, 18. 19 and 20 where the processing is for scientific or historical research, or archiving purposes.

The ICO has published guidance on the GDPR Exemptions which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/).

#### Exemptions - Crime & Taxation General (DPA Schedule 2 Part 1 Paragraph 2)

DPA Schedule 2 Part 1 Paragraph 2 states:

*(1) The listed GDPR provisions* [defined at DPA Schedule 2 Part 1 Paragraph 1] *do not apply to personal data processed for any of the following purposes—*

*(a) the prevention or detection of crime,*

*(b) the apprehension or prosecution of offenders, or*

*(c) the assessment or collection of a tax or duty or an imposition of a similar nature,*

*to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).*

*(2) Sub-paragraph (3) applies where—*

*(a) personal data is processed by a person (“Controller 1”) for any of the purposes mentioned in sub-paragraph (1)(a) to (c), and*

*(b) another person (“Controller 2”) obtains the data from Controller 1 for the purpose of discharging statutory functions and processes it for the purpose of discharging statutory functions.*

*(3) Controller 2 is exempt from the obligations in the following provisions of the GDPR—*

*(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided),*

*(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided),*

*(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers), and*

*(d) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in paragraphs (a) to (c),*

*to the same extent that Controller 1 is exempt from those obligations by virtue of sub-paragraph (1).*

**Commentary** - DPA Schedule 2 Part 1 Paragraph 2 (Crime & taxation: general) restricts the application of the Listed GDPR Provisions to personal data processed for crime and taxation purposes, to the extent that the processing would be likely to prejudice those purposes. Sub-paragraphs (2) and (3) make provision relating to the further processing of personal data collected for the crime and taxation purposes.

The exemption allows data processed under General Processing to be provided to the police for law enforcement purposes without the Act being breached.

DPA Schedule 2 Part 1 Paragraph 3 (Crime & taxation: risk assessment systems) applies where personal data is processed for the crime and taxation purposes by a data controller who is a public body and the restrictions are necessary for the smooth running of a risk assessment system. It is not directly relevant to policing so is not covered by this manual.

The ICO has published guidance on the GDPR Crime and Taxation General exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex1).

#### Exemption - Disclosure Required by Law (DPA Schedule 2 Part 1 Paragraph 5)

DPA Schedule 2 Part 1 Paragraph 5 states:

*(1) The listed GDPR provisions*  [defined at DPA Schedule 2 Part 1 Paragraph 1] *do not apply to personal data consisting of information that the controller is obliged by an enactment to make available to the public, to the extent that the application of those provisions would prevent the controller from complying with that obligation.*

*(2) The listed GDPR provisions do not apply to personal data where disclosure of the data is required by an enactment, a rule of law or an order of a court or tribunal, to the extent that the application of those provisions would prevent the controller from making the disclosure.*

*(3) The listed GDPR provisions do not apply to personal data where disclosure of the data—*

*(a) is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings),*

*(b) is necessary for the purpose of obtaining legal advice, or*

*(c) is otherwise necessary for the purposes of establishing, exercising or*

*defending legal rights, to the extent that the application of those provisions would prevent the*

*controller from making the disclosure.*.

**Commentary** - DPA Schedule 2 Part 1 Paragraph 5(1) restricts the application of the listed GDPR provisions to the processing of data protection where the data controller is obliged, under an enactment, to disclose personal data to the public, to the extent the application of those provisions would prevent compliance with that obligation.

Paragraph 5(2) and (3) restrict the listed GDPR provisions where the disclosure of personal data is required by law or necessary for the purposes of or in connection with legal proceedings or necessary for obtaining legal advice or establishing exercising or defending legal rights.

The ICO has published guidance on the GDPR Disclosure Required by Law exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex3).

### DPA Schedule 2 Part 2 Exemptions etc. from the GDPR

DPA Schedule 2 Part 2 Paragraph 6 states:

*In this Part of this Schedule, “the listed GDPR provisions” means the following provisions of the GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the GDPR)—*

*(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided);*

*(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);*

*(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);*

*(d) Article 16 (right to rectification);*

*(e) Article 17(1) and (2) (right to erasure);*

*(f) Article 18(1) (restriction of processing);*

*(g) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);*

*(h) Article 20(1) and (2) (right to data portability);*

*(i) Article 21(1) (objections to processing);*

*(j) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in sub-paragraphs (a) to (i).*

**Commentary** - DPA Schedule 2 Part 2 Paragraph 6 lists the “Listed GDPR Provisions” which can be restricted or adapted by the exemptions set out in the remaining seven paragraphs of DPA Schedule 2 Part 2. Rather confusingly different sets of “Listed GDPR Provisions” exist for DPA Schedule 2 Parts 1, 2, 4, 5 & 6 relevant only to those parts respectively.

The ICO has published guidance on the GDPR Exemptions which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/).

#### Exemption – Functions designed to protect the public etc. (DPA Schedule 2 Part 2 Paragraph 7)

DPA Schedule 2 Part 2 paragraph 7 states:

*The listed GDPR provisions* [defined at DPA Schedule 2 Part 2 Paragraph 6] *do not apply to personal data processed for the purposes of discharging a function that—*

*(a) is designed as described in column 1 of the Table, and*

*(b) meets the condition relating to the function specified in column 2 of the Table,*

*to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.*

The table referred to follows the above and the functions and conditions within it relevant to policing are as follows:

*2. The function is designed to protect members of the public against—*

*(a) dishonesty, malpractice or other seriously improper conduct, or*

*(b) unfitness or incompetence.*

[Where]

*The function is—*

*(a) conferred on a person by an enactment,*

*(b) a function of the Crown, a Minister of the Crown or a government department, or*

*(c) of a public nature, and is exercised in the public interest.*

**Commentary** - The scenario (c) above is relevant to non-criminal investigations by the police into the conduct of staff or officers.

*4. The function is designed—*

*(a) to secure the health, safety and welfare of persons at work, or*

*(b) to protect persons other than those at work against risk to health or safety arising out of or in connection with the action of persons at work.*

[Where]

*The function is—*

*(a) conferred on a person by an enactment,*

*(b) a function of the Crown, a Minister of the Crown or a government department, or*

*(c) of a public nature, and is exercised in the public interest.*

**Commentary** - The scenario above is relevant to health and safety, and welfare activities conducted by a police force in relation to its own officers and staff and members of the public.

The ICO has published guidance on the GDPR Functions designed to protect the public etc. exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex8).

#### Other Exemptions (DPA Schedule 2 Part 2 Paragraphs 8 to 15)

**Commentary** - The exemptions set out within the remaining part of DPA Schedule 2 Part 2 (Paragraphs 8 to 15) are not relevant to policing.

### DPA Schedule 2 Part 3 Exemptions etc. from the GDPR

#### Exemption - Protection of the rights of others: general (DPA Schedule 2 Part 3 Paragraph 16)

DPA Schedule 2 Part 3 Paragraph 16 states:

*(1) Article 15(1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers), and Article 5 of the GDPR so far as its provisions correspond to the rights and obligations provided for in Article 15(1) to (3), do not oblige a controller to disclose information to the data subject to the extent that doing so would involve disclosing information relating to another individual who can be identified from the information.*

*(2) Sub-paragraph (1) does not remove the controller’s obligation where—*

*(a) the other individual has consented to the disclosure of the information to the data subject, or*

*(b) it is reasonable to disclose the information to the data subject without the consent of the other individual.*

*(3) In determining whether it is reasonable to disclose the information without consent, the controller must have regard to all the relevant circumstances, including—*

*(a) the type of information that would be disclosed,*

*(b) any duty of confidentiality owed to the other individual,*

*(c) any steps taken by the controller with a view to seeking the consent of the other individual,*

*(d) whether the other individual is capable of giving consent, and*

*(e) any express refusal of consent by the other individual.*

*(4) For the purposes of this paragraph—*

*(a) “information relating to another individual” includes information identifying the other individual as the source of information;*

*(b) an individual can be identified from information to be provided to a data subject by a controller if the individual can be identified from—*

*(i) that information, or*

*(ii) that information and any other information that the controller reasonably believes the data subject is likely to possess or obtain.*

**Commentary** - These provisions are similar to those within the DPA 1998 and mean that a police force is not obliged to disclose information under GDPR Article 15 if to do so would mean disclosing information relating to another individual who can be identified from the information, except where there the other individual has consented; or it is reasonable in all circumstances to comply with the request without that individual's consent.

The NPCC’s policy is that in the absence in law of a requirement to seek consent police forces should simply consider the reasonableness test set out at DPA Schedule 2 Part 3 Paragraph 14(2)(b). If the other individual is a health professional to the data subject the provisions of DPA Schedule 2 Part 3 Paragraph 15 should be considered when determining reasonableness (see 4.3.4.2).

The ICO has published guidance on the GDPR Protection of the rights of others exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex36).

#### Exemption - Assumption of reasonableness for health workers, social workers and education workers (DPA Schedule 2 Part 3 Paragraph 17)

DPA Schedule 2 Part 3 Paragraph 17 states:

*(1) For the purposes of paragraph 16(2)(b), [of DPA Schedule 2 Part 3] it is to be considered reasonable for a controller to disclose information to a data subject without the consent of the other individual where—*

*(a) the health data test is met,*

*(b) the social work data test is met, or*

*(c) the education data test is met.*

*(2) The health data test is met if—*

*(a) the information in question is contained in a health record, and*

*(b) the other individual is a health professional who has compiled or contributed to the health record or who, in his or her capacity as a health professional, has been involved in the diagnosis, care or treatment of the data subject*.

**Commentary** - This exemption must be read in conjunction with DPA Schedule 2 Part 3 Paragraph 16 and is relevant to the disclosure under the right of access to personal data within health records relating to officers and staff which have been created by health professionals working for police forces.

The ICO has published guidance on the GDPR Assumption of reasonableness for health workers, social workers and education workers exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex20).

The remaining DPA Schedule 2 Part 3 Paragraph 15(3) to (5) are not relevant to policing and are not covered by this manual.

### DPA Schedule 2 Part 4 Exemptions etc. from the GDPR

DPA Schedule 2 Part 4 Paragraph 18 states:

*In this Part of this Schedule, “the listed GDPR provisions” means the following provisions of the GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the GDPR)—*

*(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided);*

*(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);*

*(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);*

*(d) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in sub-paragraphs (a) to (c).*

**Commentary** - Part 4 Paragraph 18 of the schedule lists the “Listed GDPR Provisions” which can be restricted or adapted by the exemptions set out in the remaining 7 paragraphs of DPA Schedule 2 Part 4. Rather confusingly different sets of “Listed GDPR Provisions” exist for DPA Schedule 2 Parts 1, 2, 4, 5 & 6 relevant only to those parts respectively.

The ICO has published guidance on the GDPR Exemptions which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/).

#### Exemption – Legal Professional Privilege (DPA Schedule 2 Part 4 Paragraph 19)

DPA Schedule 2 Part 3 Paragraph 19 states:

*The listed GDPR provisions do not apply to personal data that consists of information in respect of which a claim to legal professional privilege or, in Scotland, confidentiality of communications, could be maintained in legal proceedings.*

**Commentary** - This paragraph, which will be most relevant to police forces’ legal services activities, restricts the application of the listed GDPR provisions to personal data that consists of material over which legal privilege (or in Scotland, confidentiality in communications) can be claimed or maintained in legal proceedings.

This provision could be used to withhold personal data contained in legal advice to the chief officer from the police force solicitor sought via the right of access.

The ICO has published guidance on the GDPR Legal Professional Privilege exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex4).

#### Exemption – Self Incrimination (DPA Schedule 2 Part 4 Paragraph 20)

DPA Schedule 2 Part 4 Paragraph 20 states:

*(1) A person need not comply with the listed GDPR provisions* [those at DPA Schedule 2 Part 4 Paragraph 18] *to the extent that compliance would, by revealing evidence of the commission of an offence, expose the person to proceedings for that offence.*

*(2) The reference to an offence in sub-paragraph (1) does not include an offence under—*

*(a) this Act,*

*(b) section 5 of the Perjury Act 1911 (false statements made otherwise than on oath),*

*(c) section 44(2) of the Criminal Law (Consolidation) (Scotland) Act 1995 (false statements made otherwise than on oath), or*

*(d) Article 10 of the Perjury (Northern Ireland) Order 1979 (S.I. 1979/1714 (N.I. 19)) (false statutory declarations and other false unsworn statements).*

*(3) Information disclosed by any person in compliance with Article 15 of the GDPR is not admissible against the person in proceedings for an offence under this Act.*

**Commentary** - This paragraph restricts the obligation to comply with the listed GDPR provisions to the extent that compliance would result in self-incrimination. It also provides that information disclosed by a person in compliance with Article 15 is not admissible against the person in proceedings for an offence under Parts 5 or 6 of the Act. This replicates the exemption in paragraph 11 of Schedule 7 to the 1998 Act.

It is unlikely to be of relevance to Police Data Protection Professionals but is included in this manual to provide clarity that it does not apply to DPA-related offences.

The ICO has published guidance on the GDPR Self Incrimination exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex5).

#### Exemption – Corporate Finance (DPA Schedule 2 Part 4 Paragraph 21)

**Commentary** - This exemption is unlikely to be of relevance to policing and consequently is not covered by this manual.

The ICO has published guidance on the GDPR Corporate Finance exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex31).

#### Exemption – Management Forecasts (DPA Schedule 2 Part 4 Paragraph 22)

DPA Schedule 2 Part 4 Paragraph 22 states:

*The listed GDPR provisions* [those at DPA Schedule 2 Part 4 Paragraph 18] *do not apply to personal data processed for the purposes of management forecasting or management planning in relation to a business or other activity, to the extent that the application of those provisions would be likely to prejudice the conduct of the business or activity concerned.*

**Commentary** - This paragraph, relevant to police force internal business reviews, restricts the application of the listed GDPR provisions to personal data processed for management forecasting or management planning purposes, to the extent the application of those provisions would prejudice the conduct of the business or activity concerned. It prevents the right of access being used as a route to obtain premature or inappropriate access to police forces’ management forecasts or plans.

The ICO has published guidance on the GDPR Management Forecasts exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex32).

#### Exemption – Negotiations (DPA Schedule 2 Part 4 Paragraph 23)

DPA Schedule 2 Part 4 Paragraph 23 states:

*The listed GDPR provisions* [those at DPA Schedule 2 Part 4 Paragraph 18] *do not apply to personal data that consists of records of the intentions of the controller in relation to any negotiations with the data subject to the extent that the application of those provisions would be likely to prejudice those negotiations.*

**Commentary** - This paragraph restricts the application of the listed GDPR provisions to personal data that consists of the data controller’s record of his or her intentions in relation to any negotiations with the data subject, to the extent that the application of those provisions would be likely to prejudice the negotiation.

Within policing this provision may be used to withhold confidential personal data sought under the right of access that had been prepared in relation to a forthcoming redundancy offer to the requestor, withhold information relating to forthcoming employment tribunals or withhold information relating to potential settlement/redundancy figures.

The ICO has published guidance on the GDPR Negotiations exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex33).

#### Exemption – Confidential References (DPA Schedule 2 Part 4 Paragraph 24)

DPA Schedule 2 Part 4 Paragraph 24 states:

*The listed GDPR provisions* [those at DPA Schedule 2 Part 4 Paragraph 18] *do not apply to personal data consisting of a reference given (or to be given) in confidence for the purposes of—*

1. *the education, training or employment (or prospective education, training or employment) of the data subject,*

*(b) the placement (or prospective placement) of the data subject as a volunteer,*

*(c) the appointment (or prospective appointment) of the data subject to any office, or*

*(d) the provision (or prospective provision) by the data subject of any service.*

**Commentary** - This paragraph restricts the application of the listed GDPR provisions to personal data consisting of a reference given (or to be given) in confidence, for example for education or employment purposes. It would encompass a confidential reference provided or received by a police force.

The ICO has published guidance on the GDPR Confidential References exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex34).

#### Exemption – Exam Scripts and Exam Marks (DPA Schedule 2 Part 4 Paragraph 25)

**Commentary** - DPA Schedule 2 Part 4 Paragraph 25 relates to information recorded by candidates in exams, but is unlikely to be of relevance to policing.

The ICO has published guidance on the GDPR Exam Scripts and Exam Marks exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex35).

### DPA Schedule 2 Part 5 Exemptions etc. from the GDPR

#### Exemption – Journalistic, Artistic & Literary Purposes/Special Purposes (DPA Schedule 2 Part 5 Paragraph 26)

DPA Schedule 2 Part 4 Paragraph 26 states:

*(1) In this paragraph, “the special purposes” means one or more of the following—*

*(a) the purposes of journalism;*

*(b) academic purposes;*

*(c) artistic purposes;*

*(d) literary purposes.*

*(2) Sub-paragraph (3) applies to the processing of personal data carried out for the special purposes if—*

*(a) the processing is being carried out with a view to the publication by a person of journalistic, academic, artistic or literary material, and*

*(b) the controller reasonably believes that the publication of the material would be in the public interest.*

*(3) The listed GDPR provisions* [defined in 9 below] *do not apply to the extent that the controller reasonably believes that the application of those provisions would be incompatible with the special purposes.*

*(4) In determining whether publication would be in the public interest the controller must take into account the special importance of the public interest in the freedom of expression and information.*

*(5) In determining whether it is reasonable to believe that publication would be in the public interest, the controller must have regard to any of the codes of practice or guidelines listed in sub-paragraph (6) that is relevant to the publication in question.*

*(6) The codes of practice and guidelines are—*

*(a) BBC Editorial Guidelines;*

*(b) Ofcom Broadcasting Code;*

*(c) Editors’ Code of Practice.*

*(7) The Secretary of State may by regulations amend the list in sub-paragraph (6).*

*(8) Regulations under sub-paragraph (7) are subject to the affirmative resolution procedure.*

*(9) For the purposes of this paragraph, the listed GDPR provisions are the following provisions of the GDPR (which may be exempted or derogated from by virtue of Article 85(2) of the GDPR)—*

*(a) in Chapter II of the GDPR (principles)—*

*(i) Article 5(1)(a) to (e) (principles relating to processing);*

*(ii) Article 6 (lawfulness);*

*(iii) Article 7 (conditions for consent);*

*(iv) Article 8(1) and (2) (child’s consent);*

*(v) Article 9 (processing of special categories of data);*

*(vi) Article 10 (data relating to criminal convictions etc);*

*(vii) Article 11(2) (processing not requiring identification);*

*(b) in Chapter III of the GDPR (rights of the data subject)—*

*(i) Article 13(1) to (3) (personal data collected from data subject: information to be provided);*

*(ii) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);*

*(iii) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);*

*(iv) Article 16 (right to rectification);*

*(v) Article 17(1) and (2) (right to erasure);*

*(vi) Article 18(1)(a), (b) and (d) (restriction of processing);*

*(vii) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);*

*(viii) Article 20(1) and (2) (right to data portability);*

*(ix) Article 21(1) (objections to processing);*

*(c) in Chapter IV of the GDPR (controller and processor)—*

*(i) Article 34(1) and (4) (communication of personal data breach to the data subject);*

*(ii) Article 36 (requirement for controller to consult Commissioner prior to high risk processing);*

*(d) in Chapter V of the GDPR (transfers of data to third countries etc), Article 44 (general principles for transfers);*

*(e) in Chapter VII of the GDPR (co-operation and consistency)—*

*(i) Articles 60 to 62 (co-operation);*

*(ii) Articles 63 to 67 (consistency).*

**Commentary** - DPA Schedule 2 Part 5 Paragraph 26, which is most relevant to police forces’ media activities, provides that the GDPR provisions listed in paragraph 26(9) will not apply when personal data is being processed with a view to publication for one or more of the special purposes (as defined in paragraph 26(1)), and the controller reasonably believes that the publication would be in the public interest and that the application of any of the listed GDPR provisions[[10]](#footnote-10) would be incompatible with the special purposes.

Paragraphs 26(4) to (6) set out the matters the controller must take into consideration when considering whether publication would be in the public interest, including whether guidance on such matters is covered in any relevant codes of practice listed in paragraph 26(6).

Paragraph 26 also provides an exemption from GDPR Articles 60 to 67 which are not relevant to policing and are therefore not covered by this manual.

The ICO has published guidance on the GDPR Journalistic, Artistic & Literary Purposes/Special Purposes exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex16).

### DPA Schedule 2 Part 6 Exemptions etc. from the GDPR

#### Exemption – Research & Statistics (DPA Schedule 2 Part 6 Paragraph 27)

DPA Schedule 2 Part 6 Paragraph 27 states:

*(1) The listed GDPR provisions do not apply to personal data processed for—*

*(a) scientific or historical research purposes, or*

*(b) statistical purposes, to the extent that the application of those provisions would prevent or seriously impair the achievement of the purposes in question.*

*This is subject to sub-paragraph (3).*

*(2) For the purposes of this paragraph, the listed GDPR provisions are the following provisions of the GDPR (the rights in which may be derogated from by virtue of Article 89(2) of the GDPR)—*

*(a) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);*

*(b) Article 16 (right to rectification);*

*(c) Article 18(1) (restriction of processing);*

*(d) Article 21(1) (objections to processing).*

*(3) The exemption in sub-paragraph (1) is available only where—*

*(a) the personal data is processed in accordance with Article 89(1) of the GDPR (as supplemented by section 19), and*

*(b) as regards the disapplication of Article 15(1) to (3), the results of the research or any resulting statistics are not made available in a form which identifies a data subject.*

[DPA Part 2 Section 19 Processing for archiving, research and statistical purposes: safeguards](http://www.legislation.gov.uk/ukpga/2018/12/section/19) states:

*(1) This section makes provision about—*

*(a) processing of personal data that is necessary for archiving purposes in the public interest,*

*(b) processing of personal data that is necessary for scientific or historical research purposes, and*

*(c) processing of personal data that is necessary for statistical purposes.*

*(2) Such processing does not satisfy the requirement in Article 89(1) of the GDPR for the processing to be subject to appropriate safeguards for the rights and freedoms of the data subject if it is likely to cause substantial damage or substantial distress to a data subject.*

*(3) Such processing does not satisfy that requirement if the processing is carried out for the purposes of measures or decisions with respect to a particular data subject, unless the purposes for which the processing is necessary include the purposes of approved medical research.*

*(4) In this section—*

*“approved medical research” means medical research carried out by a person who has approval to carry out that research from—*

1. *a research ethics committee recognised or established by the Health Research Authority under Chapter 2 of Part 3 of the Care Act 2014, or*
2. *a body appointed by any of the following for the purpose of assessing the ethics of research involving individuals—*

*(i) the Secretary of State, the Scottish Ministers, the Welsh Ministers, or a Northern Ireland department;*

*(ii) a relevant NHS body;*

*(iii) United Kingdom Research and Innovation or a body that is a Research Council for the purposes of the Science and Technology Act 1965;*

*(iv) an institution that is a research institution for the purposes of Chapter 4A of Part 7 of the Income Tax (Earnings and Pensions) Act 2003 (see section 457 of that Act);*

*“relevant NHS body” means—*

*(a) an NHS trust or NHS foundation trust in England,*

*(b) an NHS trust or Local Health Board in Wales,*

*(c) a Health Board or Special Health Board constituted under section 2 of the National Health Service (Scotland) Act 1978,*

*(d) the Common Services Agency for the Scottish Health Service, or*

*(e) any of the health and social care bodies in Northern Ireland falling within paragraphs (a) to (e) of section 1(5) of the Health and Social Care (Reform) Act (Northern Ireland) 2009 (c. 1 (N.I.)).*

*(5) The Secretary of State may by regulations change the meaning of “approved medical research” for the purposes of this section, including by amending subsection (4).*

*(6) Regulations under subsection (5) are subject to the affirmative resolution procedure.*

**Commentary** - DPA Schedule 2 Part 6 Paragraph 27 restricts the application of the listed GDPR provisions relating to data subjects’ rights (defined at Paragraph 27(2)[[11]](#footnote-11)) where personal data is processed for scientific or historical research and statistical purposes where this would prevent or seriously impair achievement of those purposes and the relevant safeguards are met.

The safeguards are that the data is processed in accordance with Article 89(1), as supplemented by [DPA Part 2 Section 19](http://www.legislation.gov.uk/ukpga/2018/12/section/19), and the results of research or any resulting statistics are not made available in a form which identifies the data subject.

Paragraph 27 will be of greatest relevance to police force research concerning the effectiveness of activities.

The ICO has published guidance on the GDPR Research & Statistics exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex17).

#### Exemption – Archiving in the public interest (DPA Schedule 2 Part 6 Paragraph 28)

DPA Schedule 2 Part 6 Paragraph 28 states:

*(1) The listed GDPR provisions do not apply to personal data processed for archiving purposes in the public interest to the extent that the application of those provisions would prevent or seriously impair the achievement of those purposes.*

*This is subject to sub-paragraph (3).*

*(2) For the purposes of this paragraph, the listed GDPR provisions are the following provisions of the GDPR (the rights in which may be derogated from by virtue of Article 89(3) of the GDPR)—*

*(a) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);*

*(b) Article 16 (right to rectification);*

*(c) Article 18(1) (restriction of processing);*

*(d) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);*

*(e) Article 20(1) (right to data portability);*

*(f) Article 21(1) (objections to processing).*

*(3) The exemption in sub-paragraph (1) is available only where the personal data is processed in accordance with Article 89(1) of the GDPR (as supplemented by section 19).*

GDPR Article 89(1) states:

*Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in* *order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.*

[DPA Part 2 Section 19 Processing for archiving, research and statistical purposes: safeguards](http://www.legislation.gov.uk/ukpga/2018/12/section/19) states:

*19 Processing for archiving, research and statistical purposes: safeguards*

*(1) This section makes provision about—*

*(a) processing of personal data that is necessary for archiving purposes in the public interest,*

*(b) processing of personal data that is necessary for scientific or historical research purposes, and*

*(c) processing of personal data that is necessary for statistical purposes.*

*(2) Such processing does not satisfy the requirement in Article 89(1) of the GDPR for the processing to be subject to appropriate safeguards for the rights and freedoms of the data subject if it is likely to cause substantial damage or substantial distress to a data subject.*

*(3) Such processing does not satisfy that requirement if the processing is carried out for the purposes of measures or decisions with respect to a particular data subject, unless the purposes for which the processing is necessary include the purposes of approved medical research.*

*(4) In this section—*

*“approved medical research” means medical research carried out by a person who has approval to carry out that research from—*

1. *a research ethics committee recognised or established by the Health Research Authority under Chapter 2 of Part 3 of the Care Act 2014, or*
2. *a body appointed by any of the following for the purpose of assessing the ethics of research involving individuals—*

*(i) the Secretary of State, the Scottish Ministers, the Welsh Ministers, or a Northern Ireland department;*

*(ii) a relevant NHS body;*

*(iii) United Kingdom Research and Innovation or a body that is a Research Council for the purposes of the Science and Technology Act 1965;*

*(iv) an institution that is a research institution for the purposes of Chapter 4A of Part 7 of the Income Tax (Earnings and Pensions) Act 2003 (see section 457 of that Act);*

*“relevant NHS body” means—*

*(a) an NHS trust or NHS foundation trust in England,*

*(b) an NHS trust or Local Health Board in Wales,*

*(c) a Health Board or Special Health Board constituted under section 2 of the National Health Service (Scotland) Act 1978,*

*(d) the Common Services Agency for the Scottish Health Service, or*

*(e) any of the health and social care bodies in Northern Ireland falling within paragraphs (a) to (e) of section 1(5) of the Health and Social Care (Reform) Act (Northern Ireland) 2009 (c. 1 (N.I.)).*

*(5) The Secretary of State may by regulations change the meaning of “approved medical research” for the purposes of this section, including by amending subsection (4).*

*(6) Regulations under subsection (5) are subject to the affirmative resolution procedure.*

**Commentary** - Paragraph 28, relevant to police forces’ museum activities, restricts the application of the listed GDPR provisions (defined at Paragraph 28(2)[[12]](#footnote-12)) relating to data subjects’ rights where personal data is processed for archiving purposes in the public interest and the applications of those provisions would prevent or seriously impair achievement of those purposes and the relevant safeguards are met. The safeguards are that the data is processed in accordance with Article 89(1), as supplemented by DPA Section 19.

The ICO has published guidance on the GDPR Archiving in the public interest exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex18).

### DPA Schedule 3 Exemptions etc. from the GDPR: health, social work, education and child abuse

**Commentary** – The DPA Schedule 3 provisions are unlikely to be of relevance to policing.

The ICO has published guidance on these GDPR exemptions which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/).

### DPA Schedule 4 Exemptions etc. from the GDPR: disclosure prohibited or restricted by an enactment

**Commentary** – The DPA Schedule 4 provisions are unlikely to be of relevance to policing.

The ICO has published guidance on the GDPR disclosure prohibited or restricted by an enactment exemption which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex6).

## General Processing Rights

### Overview of General Processing Rights

**Commentary** - The rights that individuals had over their data in the 1998 Act were carried over to the GDPR and Act, but in some cases these were strengthened and have been added to.

As with the 1998 Act the GDPR and Act recognise that there are some limited circumstances where it is appropriate to create exemptions or restrictions to the usual rights that individuals have over their personal data. There is also provision to allow the Secretary of State to create new exemptions if required. The remainder of 4.4 sets out all General Processing rights and any associated exemptions or restrictions to those rights. At the end of 4.4 a table can be found summarizing those exemptions and restrictions

The GDPR/DPA Part 2 rights are:

* Information to be provided where personal data is collected from the data subject (GDPR Article 13)
* Information to be provided where personal data has not been obtained from the data subject (GDPR Article 14)
* Right of access by the data subject (GDPR Article 15)
* Right to rectification (GDPR Article 16)
* Right to erasure (‘right to be forgotten’) (GDPR Article 17)
* Right to restriction of processing (GDPR Article 18)
* Notification obligation regarding rectification or erasure of personal data or restriction of processing (GDPR Article 19)
* Right to data portability (GDPR Article 20)
* Right to object (GDPR Article 21)
* Automated individual decision-making, including profiling (GDPR Article 22)

The rights under GDPR/DPA Part 2 and DPA Part 3 differ, so it is of crucial importance that when faced with any rights application police forces identify which of the two regimes the processing falls under. GDPR Articles 20 and 21 having no equivalent in DPA Part 3 (see 5.1.3).

DPA Part 7 Section 179 sets out that any enactment or rule of law prohibiting or restricting the disclosure of information or authorizing the withholding of information (other than any within the Act) cannot remove or restrict subject rights set out in the GDPR/DPA Part 2 or those under DPA Part 3. Consequently, the only restrictions of data subjects’ GDPR rights which can be used are those set out in the Act.

The ICO has published guidance on the GDPR rights which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/).

The police force must:

• ensure that all officers and staff are able to recognise any instance where a data subject requests to exercise one of their GDPR/DPA Part 2 rights, and know how to progress such requests

* create and maintain a policy or procedure setting out how GDPR/DPA Part 2 rights are managed by them and make this publicly available.

### Transparent information, communication and modalities for the exercise of the rights of the data subject (GDPR Article 12)

[GDPR Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject)](https://gdpr-info.eu/art-12-gdpr/) states:

*1 .The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.*

*2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.*

*3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.*

*4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.*

*5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:*

*(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or*

*(b) refuse to act on the request.*

*The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.*

*6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.*

*7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.*

*8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.*

There are four GDPR Recitals associated with GDPR Article 12. The first of these is [GDPR Recital 58 (“The Principle of Transparency”)](https://gdpr-info.eu/recitals/no-58/) which states:

*The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.*

The second is [GDPR Recital 59 (“Procedures for the exercise of Data Subjects’ Rights”).](https://gdpr-info.eu/recitals/no-59/) It states:

*Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.*

The third is [GDPR Recital 60 (“Information Obligations”)](https://gdpr-info.eu/recitals/no-60/) which states:

*The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.*

The fourth is [GDPR Recital 73 (“Restrictions of Rights & Principles”).](https://gdpr-info.eu/recitals/no-73/) It states:

*Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.*

**Commentary** – GDPR Article 12 and the associated recitals set out various requirements that must be met when the rights under GDPR Articles 13 to 22 are applied (and GDPR Article 34 Communication of a personal data breach to a data subject is applicable). Those requirements concern cost, clarity, format, timescale of response, confirmation of identity, delay reporting, complaint right to the ICO and judicial remedy, evidencing manifestly unfoundedness or excessiveness of requests, and use of icons.

The police force must ensure all relevant requirements arising from GDPR Article 12 and its associated articles are considered when designing processes to generally manage subject rights and specifically when considering each individual application of a right by a data subject.

### Right to be Informed (Transparency & Privacy Notice) (GDPR Articles 13 & 14)

**Commentary** - Compliance with GDPR Articles 13 and 14, which must be read in conjunction with GDPR Article 12, will usually satisfy the fairness and transparency elements of the First General Processing Principle.

The GDPR Articles 13 and 14 respectively set out the information to be supplied to a data subject where personal data is collected from them and not from them.

In either case GDPR Article 12(1) requires the information provided to the data subject to be:

*in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.*

GDPR Article 12(5) requires the information to be provided free of charge.

GDPR Article 12(7) states that the information:

*may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.*

The table below sets out what information must be provided under GDPR Articles 13 and 14. Note GDPR Article 13(4) and GDPR Article 14(5) disapply some of these requirements in particular circumstances (see immediately below table).

|  |  |  |
| --- | --- | --- |
| **What information must be supplied?** | **GDPR Article 13: Data obtained directly from data subject** | **GDPR Article 14: Data not obtained directly from data subject** |
| Identity and contact details of the controller (and where applicable, the controller’s representative – unlikely to be applicable to police forces) | 1(a) | 1(a) |
| Identity and contact details of the police force’s data protection officer | 1(b) | 1(b) |
| Purpose(s) of the processing and the legal basis for the processing | 1(c) | 1(c) |
| The legitimate interests of the controller or third party, where processing under Article 6(1) (not applicable to police forces) | 1(d) | 2(b) |
| Categories of personal data | - | 1(d) |
| Any recipient or categories of recipients of the personal data (if any) | 1(e) | 1(e) |
| Details of transfers to third country and safeguards, where applicable | 1(f) | 1(f) |
| Retention period or criteria used to determine the retention period | 2(a) | 2(a) |
| The existence of each of data subject’s rights – access, rectification or erasure or restriction of processing, objection and data portability | 2(b) | 2(c) |
| The right to withdraw consent at any time if processing is based on Article 6(1) or Article 9(2)(a), where relevant | 2(c) | 2(d) |
| The right to lodge a complaint with a supervisory authority (ICO) | 2(d) | 2(e) |
| The source the personal data originates from and whether it came from publicly accessible sources | - | 2(f) |
| Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data | 2(e) | - |
| The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences | 2(f) | 2(g) |
| Information to be provided | At time of being obtained | 3(a) - Within a reasonable period after being obtained, up to a maximum of one month  3(b) – If the personal data is used to communicate with the data subject, at the latest when the communication first takes place  3(c) – If disclosure to another recipient is envisaged, at the latest before the personal data is disclosed |

GDPR Article 13(4) disapplies GDPR Article 13(1) to (3) where and insofar as the data subject already has the information.

GDPR Article 14(5) disapplies GDPR Article 14(1) to (4) where and insofar as the data subject already has the information, or obtaining or disclosing is expressly laid down in law and which protects the data subject’s legitimate interests, or the personal data must remain confidential subject to an obligation of professional secrecy regulated by law, or the provision:

*of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.*

GDPR Article 13(3) requires the police force to provide information under GDPR Article 13(2) to the data subject from whom the data was obtained in cases where there is to be further processing of the personal data for a purpose different to the initial purpose. This must be done prior to the new processing commencing. A similar requirement arises under GDPR Article 14(4) to provide information under Article 14(2) where there is a change in purpose of processing. See 4.2.2.3 regarding lawful processing – change of purpose.

GDPR Article 26(1) requires Joint Controllers (see 4.5.3) to determine their respective responsibilities under GDPR Articles 13 and 14 by means of arrangement between them and suggests that it could include the designation of a contact point for data subjects.

Police forces should adopt a tiered approach to Privacy Notices. At the top, a high-level Privacy Notice template is being developed. They may choose to use a template for that purpose which can be found at [4.4.3.1](#_Toc505013791) and [Appendix G](#_Appendix_G:_High-Level), or develop their own versions as they see fit.

Beneath the high-level Privacy Notices police forces should develop a series of more specific lower-level Privacy Notices for their key General Processing operations. They may choose to use a template for that purpose which can be found at [4.4.3.2](#_Lower-Level_Specific_Privacy) and [Appendix H](#_Appendix_H:_Lower-Level), or develop their own versions as they see fit.

Work on developing these lower-level Privacy Notices should be prioritized according to the volume, purpose and nature of the processing.

Police forces may wish to produce specific privacy notices relating to the personal data they process for their officers, staff and others who may work on their behalf.

As with all publications police forces must ensure they have measures in place to ensure their Privacy Notices are easily accessible by diverse groups in compliance with the [Equality Act 2010](http://www.legislation.gov.uk/ukpga/2010/15/contents).

Care should be taken to ensure when personal data obtained for Law Enforcement Processing is subsequently used for General Processing fairness requirements are not overlooked when the new processing is being considered.

The ICO has published guidance on the GDPR Right to be Informed which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/) and more detailed guidance [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/). The ICO has also published a Privacy Notice Template which can be found [here](https://ico.org.uk/media/for-organisations/documents/2259798/pn-template-microbusiness-201908.docx). The ICO’s own Privacy Notice can be found [here](https://ico.org.uk/global/privacy-notice/). The ICO’s own internal Staff Privacy Notice can be found [here](https://ico.org.uk/media/about-the-ico/documents/2615803/staff-privacy-notice.pdf).

The police force must ensure Privacy Notices are provided that meet the requirements of the GDPR/DPA Part 2.

The Data Protection Officer must monitor the police force’s compliance with the GDPR Right to be Informed and make any necessary interventions.

There are a number of exemptions to parts of GDPR Articles 13 and 14, and those relevant to the police are highlighted below.

**Exemption – Crime & Taxation.** [DPA Schedule 2 Part 1 Paragraph 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/2/enacted) disapplies GDPR Article 13(1) to (3) and Article 14(1) to (4) to the extent that the application of those provisions would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of a tax or an imposition of a similar nature. [See 4.3.2.1](#_Exemptions_-_Crime).

**Exemption – Disclosure Required by Law.** [DPA Schedule 2 Part 1 Paragraph 5](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/5/enacted) disapplies GDPR Article 13(1) to (3) and Article 14(1) to (4) to the extent that the application of those provisions would prevent the controller from:

1. complying with an obligation to make personal data available to the public, or
2. complying with an obligation to disclose personal data required by an enactment, rule of law or order of a court or tribunal, or
3. (iii) making a disclosure where necessary or in connection with legal proceedings (including prospective ones), or making a disclosure necessary for obtaining legal advice, or making a disclosure that is otherwise necessary for establishing, exercising or defending legal rights.

[See 4.3.2.2](#_Exemption_-_Disclosure).

**Exemption – Functions designed to protect the public etc.** [DPA Schedule 2 Part 2 Paragraph 7](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/7/enacted) disapplies GDPR Article 13(1) to (3) and Article 14(1) to (4) to the extent that the application of those provisions would prejudice the proper discharge of functions:

* designed to protect the public against dishonesty, malpractice, serious improper conduct, unfitness or incompetence by anyone whose activity brings them into contact with the public
* relating to health and safety and welfare at work.

[See 4.3.3.1](#_Exemption_–_Functions).

**Exemption – Legal Professional Privilege**. [DPA Schedule 2 Part 4 Paragraph 19](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/19/enacted) disapplies GDPR Article 13(1) to (3) and Article 14(1) to (4) in respect of personal data that is subject to Legal Professional Privilege or for Scotland Confidentiality of Communications. [See 4.3.5.1](#_Exemption_–_Legal)

**Exemption – Self Incrimination** – [DPA Schedule 2 Part 4 Paragraph 20](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/20/enacted) disapplies GDPR Article 13(1) to (3) and Article 14(1) to (4) to the extent that the application of those provisions would, by revealing evidence of the commission of a non-DPA-related offence, expose the person to proceedings for that offence. [See 4.3.5.2](#_Exemption_–_Self).

**Exemption – Management Forecasts** – [DPA Schedule 2 Part 4 Paragraph 22](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/22/enacted) disapplies GDPR Article 13(1) to (3) and Article 14(1) to (4) in relation to personal data processed for business management forecasting or planning activities to the extent that the application of those provisions would be likely to prejudice the conduct of those activities. [See 4.3.5.4](#_Exemption_–_Management)

**Exemption – Negotiations** – [DPA Schedule 2 Part 4 Paragraph 23](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/23/enacted) disapplies GDPR Article 13(1) to (3) and Article 14(1) to (4) in relation to personal data that consists of records of the intentions of the controller in relation to negotiations with the data subject to the extent that the application of those provisions would be likely to prejudice the conduct of those negotiations. [See 4.3.5.5](#_Exemption_–_Negotiations).

**Exemption – Confidential References** – [DPA Schedule 2 Part 4 Paragraph 24](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/24/enacted) disapplies GDPR Article 13(1) to (3) and Article 14(1) to (4) in relation to personal data that consists of confidential references about the data subject. [See 4.3.5.6.](#_Exemption_–_Confidential)

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 13(1) to (3) and Article 14(1) to (4) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of GDPR Article 13(1) to (3) and Article 14(1) to (4) would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

#### High-Level Privacy Notice

This can be found at [11.7 Appendix G](#_Appendix_G:_High-Level). Use of it is not mandated by the NPCC.

#### Lower-Level Specific Privacy Notice Template

This can be found at [11.8 Appendix H](#_Appendix_H:_Lower-Level). Use of it is not mandated by the NPCC.

### Right of Access by the Data Subject (GDPR Article 15, DPA Part 2 Section 12)

GDPR Article 15 states:

*(1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:*

*(a) the purposes of the processing;*

*(b) the categories of personal data concerned;*

*(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;*

*(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;*

*(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;*

*(f) the right to lodge a complaint with a supervisory authority;*

*(g) where the personal data are not collected from the data subject, any available information as to their source;*

*(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*

*2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.*

*3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.*

*4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others*.

There are two GDPR Recitals associated with GDPR Article 15. The first, GDPR Recital 63 (“Right of Access”), states:

*A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates*.

The second, GDPR Recital 64 (“Identity Verification”) states:

*The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests*.

[DPA Part 2 Section 12 Limits on fees that may be charged by controllers](http://www.legislation.gov.uk/ukpga/2018/12/section/12) states:

*(1) The Secretary of State may by regulations specify limits on the fees that a controller may charge in reliance on—*

*(a) Article 12(5) of the GDPR (reasonable fees when responding to manifestly unfounded or excessive requests), or*

*(b) Article 15(3) of the GDPR (reasonable fees for provision of further copies).*

*(2) The Secretary of State may by regulations—*

*(a) require controllers of a description specified in the regulations to produce and publish guidance about the fees that they charge in reliance on those provisions, and*

*(b) specify what the guidance must include.*

*(3) Regulations under this section are subject to the negative resolution procedure.*

**Commentary** – GDPR Article 15 and its two associated recitals, which must be read in conjunction with GDPR Article 12, give data subjects the right, subject to exemptions, to be given confirmation whether or not their personal data is subject of General Processing (GDPR/DPA Part 2) by a police force. Where processing is occurring, and again subject to exemptions, they have a right of access to that information (presumably viewing it), be given a copy of it, and be provided with up to nine items of supplementary information associated with the processing (specified in GDPR Article 15(1) & (2)) within a statutory timescale of between one and three months. The right may be exercised verbally, a significant change from the 1998 Act.

GDPR Article 15(3) requires that where an application has been made electronically the police force must respond electronically in a commonly used form unless the data subject requires otherwise. It is assumed this would encompass use of email, and applications such as Microsoft Word or Excel, common to all police forces. That paragraph also enables police forces to charge a fee for additional copies based on administrative costs. Police forces are encouraged to determine a fee scale that incorporates staff time spent to provide the copy, any costs for materials on which the copy is provided, plus any postage and packing costs.

GDPR Article 15(4) means that consideration must be given to the privacy and other rights and freedoms of individuals other than the data subject when considering disclosure and any disclosure must be limited as far as is necessary to preserve the rights and freedoms of any other individuals. In practical terms this will mean that some responses to right of access requests will need to be redacted to obscure the identity of such individuals and preserve their privacy. Judgements in this area have to be made on a case-by-case basis looking at the specific circumstances and the role and relationship between the data subject and other individuals.

[DPA Part 2 Section 12](http://www.legislation.gov.uk/ukpga/2018/12/section/12) enables the Secretary of State to specify by Regulations limits on the fees that police forces may charge for manifestly unfounded or excessive requests for information by the data subject, or for provision of further copies of information already provided. No Regulations have been published to date. The NPCC’s position is that even if a fee is offered or paid police forces should not undertake unfounded or excessive requests as a consistent approach should be adopted for all data subjects irrespective of their ability or otherwise to pay a fee.

GDPR Recital 63 confirms the intention of the right of access is to enable data subjects “to be aware of, and verify, the lawfulness of the processing.” Potentially any use of the right for purposes other than these could be regarded as an abuse of process or tend to support a view that the request was being manifestly unfounded or excessive.

GDPR Recital 63 also requires the exercise of the right of access to be made easily, and for this reason police forces must ensure their right of access processes are designed and operated with this in mind. The recital also encourages providing data subjects with suitably secure access to their data – within policing it may be possible to develop such a facility for officers and staff to access their personal data within their personnel records.

[DPA Part 6 Section 173](http://www.legislation.gov.uk/ukpga/2018/12/section/173) makes it an offence is to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the data subject would have been entitled to receive under this right.

See 6.3.4 for details of the right of access to the Police National Computer and other Law Enforcement Processing.

When handling requests for access police forces should pay regard to the I[nformation Commissioner’s Subject Access Code of Practice](https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf) and any subsequent replacement, and also consider the contents below following each bold subheadings.

**Verbal requests** - Police forces must adopt appropriate measures to ensure that verbal requests for access are recognised as such when they occur and for them to be progressed without delay. This requires all officers and staff to be adequately trained so that they can recognise a request, obtain any necessary confirmation of identity, be able to record it correctly and know what to do with it. If possible, the data subject should be asked to validate any written record of the request at the time it is made by the police officer or member of staff.

**Confirmation of identity** – A request cannot be regarded as valid until the identity of the requestor/data subject is confirmed. Police forces should develop reasonable measures in this regard, and may choose a proportionate approach and require greater evidence to confirm identity if the request encompasses special categories of personal data. There will be circumstances where the identity of the data subject is already confirmed (e.g. a police employee or detained person) and consequently there is no further requirement to confirm identity. In other cases there will be a need to obtain that confirmation, ideally at the time the request is made. The NPCC does not set out any standard for confirming identity of requestors/data subjects, but typically those individuals should provide documentary evidence of their full name and current address. If they are seeking access to images then provision of a photograph of themselves is likely to be necessary and this may also assist identification.

**Application form** – Although an application form is not required under the GDPR or Act for those exercising their subject rights, it is a useful administrative device for providing a definitive record of any request made that can confirm the scope of the request, assist the processing of the request, and provide useful evidence in cases should a dispute arises between the data subject and police force. An application form has been developed by the NPCC which can be found at 3.4.4.1. It is designed for those exercising their GDPR Article 15/DPA Part 2 and DPA Part 3 right of access.

Police forces are encouraged to make the form available on their websites in prominent positions along with suitable completion guidance, adjacent their privacy notices. Ideally the form should enable requestors/data subjects to complete and submit online or allow them to print it off to be completed and posted to the police force.

Forms that include an optional request for the requestor/data subject to confirm the reason for their request will help identify enforced subject access and potential manifestly unfounded or excessive requests. When designing application forms necessary consideration must be given to disability and diversity requirements

**Sufficient information to locate personal data** – It is in the interests of the data subject/requestor and the police force for there to be sufficient information within the request in order to enable the personal data to be located. Consequently should a request be vague, excessive, unfounded or ambiguous police forces should contact the data subject/requestor to seek necessary clarity or narrowing of the request promptly once the request has been received. The failure of a data subject/requestor to engage in this process may be regarded as evidence to support rejection of a request as manifestly unfounded or excessive.

**Manifestly unfounded or excessive** – neither of these terms are defined in the GDPR or in the Act. The explanatory notes issued with the Data Protection Bill stated: “An example of an excessive request for information is one that repeats the substance of previous requests.” The NPCC’s view is that the term is likely to encompass:

* a request that sought information available or previously supplied via an alternative route e.g. material associate with a grievance already supplied under Human Resources processes (excessive)
* a request that sought information previously supplied under the right of access (excessive)
* a request that came from a requestor already in dispute with the police force where there is evidence of a malicious, disruptive or time-wasting intent on their part (manifestly unfounded)
* a request that is for reasons other than enabling the data subject to be aware of and verify the lawfulness of the processing (manifestly unfounded)
* a request from a parent purporting to be on behalf of a child when the circumstances suggest this is not the case (manifestly unfounded)
* a request displaying characteristic indicators of a vexatious request under the Freedom of Information Act 2000 set out in the [Commissioner’s guidance on dealing with vexatious requests](https://ico.org.uk/media/for-organisations/documents/1198/dealing-with-vexatious-requests.pdf)
* a request that would take in excess of [30?] man-hours[[13]](#footnote-13) to respond to in the initial month or multiples of that thereafter (excessive)

Any police force claiming a request to be manifestly unfounded or excessive has to explain its rationale for that view to the data subject/requestor and, more often than not, to the ICO in due course.

**Timescales** – All requests must be progressed promptly after receipt by a police force and the personal data supplied within one month (subject to below). It is important that this is undertaken so that any issues relating to the request, such as its potential for being manifestly unfounded or excessive, can be readily addressed and any necessary engagement with the data subject carried out. The NPCC’s position (accepted by the ICO) is that ‘the clock does not start ticking’ until the identity of the requestor has been confirmed as the data subject, it is clear which elements of the right of access the requestor is exercising, and sufficient information has been provided to search for the information sought.

A police force is able to use GDPR Article 12(4) to extend the deadline for a further two months, where necessary, having taken into account the complexity and number of requests (from the particular data subject); but notification of this extension must occur within the initial month, the earlier the better. When determining whether an extension is required police forces should consider factors such as:

* which elements of the right the requestor/data subject wishes to utilize
* the time already expended on the request
* the volume of information that must be searched to identify information pertinent to the request
* the structure of the information to be searched and the personal data within it
* the sensitivity, purpose and nature of the processing
* the practicalities of extracting or copying the personal data from its source
* the practicalities of identifying potential redactions and then applying redactions
* the level of resource available to conduct the work
* the overall projected timescale for completing the response to the request, including searching, consideration of redactions, applying redactions, checking and issuing the response
* whether the data subject/requestor is prepared to reduce the scope of their request

[consider whether we want to suggest a standard form of words for an extension]

It is important to note that any notification of extension is likely to make a ‘neither confirm nor deny’ response impractical to use should the police force ultimately determine that due to exemptions/restrictions no confirmation of processing can be given nor any personal data disclosed to the data subject/requestor.

**Record Keeping** – Police forces must maintain records that provide a record of:

* contact with the data subject/requestor
* searches made to retrieve personal data
* results of those searches
* redactions applied
* any decision-making or rationale setting out why exemptions or restrictions have been applied
* the response(s) to the requestor

Such records must be able to withstand Commissioner and legal scrutiny and should be retained in accordance with the NPCC’s National Retention Schedule.

**Collection/delivery** – If data subject requires a force to deliver their right of access response via a courier, Royal Mail Special Delivery Guaranteed or Royal Mail Signed For, as opposed to Royal Mail First or Second Class the police force is able to charge a delivery fee for that enhanced service which takes into account the price differential from Royal Mail First Class and the cost of any associated administrative work. However, where a police force determines, having considered the nature of the personal data contained in the response, that use of Royal Mail First or Second Class is not an appropriate and that Royal Mail Special Delivery Guaranteed, Royal Mail Signed For, or a courier is the most appropriate means of response then that additional cost should not be passed on to the data subject.

Responses may also be provided via email or through personal collection from designated police premises where requested by the data subject.

**Request via Solicitors** – Police forces may receive requests on behalf of data subjects from solicitors. These should be accepted once the solicitors have provided confirmation that they have confirmed the identity of the data subject/requestor and are acting on behalf of them in respect of the right of access request.

**Requests from children** – GDPR Article 15 is a right afforded to all data subjects including children (those aged 15 years or less for the purposes of this manual [check Scotland, Northern Ireland view])

The ICO has provided guidance on acceptance of right of access by or on behalf of a child in its 1998 Act [Subject Access Code of Practice Version 1.2](https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf). The NPCC’s position is that a right of access request received directly from a child should be accepted provided that the police force is content that the child is capable of understanding this right and that the request has been freely made by them. Responses to such requests must go back directly to the child. Where an adult, usually a parent, exercises the right of access of a child a police force should not accept that request if it is not convinced the adult genuinely seeking to exercise the child’s right for the child – in the past there have been instances where estranged parents attempt to misuse the right of access right of their child, with the request actually being made for the benefit of one of the parents, not the child. Responses to such requests may go back to the child or the adult acting on their behalf.

**Joint Controllers** – Police forces acting as joint controllers must ensure that any documentation between them setting out their respective responsibilities under the Act encompasses how a right of access request to personal data that is jointly processed will be managed. It will usually be best practice for the police force that created or originated the personal data, if different from the receiving force, to provide a view on whether any exemptions/restrictions should be applied when providing the response.

**Access outside of GDPR Article 15** – Police forces may have in place processes to grant access to personal information that do not require recourse to formal applications under GDPR Article 15. Typically these will allow officers and staff to access their personnel records, and such processes should not necessarily be curtailed by the GDPR and Act.

The ICO has published guidance on the GDPR Right of Access which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/). The ICO’s guidance on what constitutes a month which can be found [here](https://ico.org.uk/your-data-matters/time-limits-for-responding-to-data-protection-rights-requests/).

The police force must implement suitable measures to ensure the GDPR Right of Access can be facilitated .

The Data Protection Officer must monitor the police force’s compliance with the GDPR Right of Access and make any necessary interventions.

There are number of exemptions from this right, the most relevant of which to the police are set out below.

**Exemption – Crime & Taxation.** [DPA Schedule 2 Part 1 Paragraph 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/2/enacted) disapplies GDPR Article 15(1) to (3) to the extent that the application of those provisions would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of a tax or an imposition of a similar nature. [See 4.3.2.1](#_Exemptions_-_Crime)

**Exemption – Disclosure Required by Law.** [DPA Schedule 2 Part 1 Paragraph 5](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/5/enacted) disapplies GDPR Article 15(1) to (3) to the extent that the application of those provisions would prevent the controller from:

1. complying with an obligation to make personal data available to the public, or
2. complying with an obligation to disclose personal data required by an enactment, rule of law or order of a court or tribunal, or
3. making a disclosure where necessary or in connection with legal proceedings (including prospective ones), or making a disclosure necessary for obtaining legal advice, or making a disclosure that is otherwise necessary for establishing, exercising or defending legal rights.

[See 4.3.2.2.](#_Exemption_-_Disclosure)

**Exemption – Functions designed to protect the public etc.** [DPA Schedule 2 Part 2 Paragraph 7](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/7/enacted) disapplies GDPR Article 15(1) to (3) to the extent that the application of those provisions would prejudice the proper discharge of functions:

* designed to protect the public against dishonesty, malpractice, serious improper conduct, unfitness or incompetence by anyone whose activity brings them into contact with the public
* relating to health and safety and welfare at work.

[See 4.3.3.1](#_Exemption_–_Functions)

**Exemption – Protection of the rights of others.** [DPA Schedule 2 Part 3 Paragraph 16](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/16/enacted) means that a police force is not obliged to disclose information under GDPR Article 15 if to do so would mean disclosing information relating to another individual who can be identified from the information, except where the other individual has consented; or it is reasonable in all circumstances to comply with the request without that individual's consent. DPA Schedule 2 Part 3 Paragraph 15(1) & (2) sets out an assumption of reasonableness in some circumstances if the other individual is a health worker. [See 4.3.4.1](#_Exemption_-_Protection) and [4.3.4.2.](#_Exemption_-_Assumption)

**Exemption – Legal Professional Privilege**. [DPA Schedule 2 Part 4 Paragraph 19](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/19/enacted) disapplies GDPR Article 15(1) to (3) in respect of personal data that is subject to Legal Professional Privilege or for Scotland Confidentiality of Communications. [See 4.3.5.1](#_Exemption_–_Legal)

**Exemption – Self Incrimination** – [DPA Schedule 2 Part 4 Paragraph 20](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/20/enacted) disapplies GDPR Article 15(1) to (3) to the extent that the application of those provisions would, by revealing evidence of the of the commission of a non-DPA-related offence, expose the person to proceedings for that offence. [See 4.3.5.2](#_Exemption_–_Self)

**Exemption – Management Forecasts** – [DPA Schedule 2 Part 4 Paragraph 22](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/22/enacted) disapplies Article 15(1) to (3) in relation to personal data processed for business management forecasting or planning activities to the extent that the application of those provisions would be likely to prejudice the conduct of those activities. [See 4.3.5.4](#_Exemption_–_Management)

**Exemption – Negotiations** – [DPA Schedule 2 Part 4 Paragraph 23](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/23/enacted) disapplies GDPR Article 15(1) to (3) in relation to personal data that consists of records of the intentions of the controller in relation to negotiations with the data subject to the extent that the application of those provisions would be likely to prejudice the conduct of those negotiations. [See 4.3.5.5](#_Exemption_–_Negotiations).

**Exemption – Confidential References** – [DPA Schedule 2 Part 4 Paragraph 24](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/24/enacted) disapplies GDPR Article 15(1) to (3) in relation to personal data that consists of confidential references about the data subject. [See 4.3.5.6.](#_Exemption_–_Confidential)

**Exemption – Journalistic, Artistic, Literary Purposes/Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 15(1) to (3) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of GDPR Article 15(1) to (3) would be incompatible with any of the Special Purposes. [See 4.3.6.1](#_Exemption_–_Journalistic,).

**Exemption – Research & Statistics**. [DPA Schedule 2 Part 6 Paragraph 27](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/27/enacted) disapplies GDPR Article 15(1) to (3) in respect of personal data that processed for scientific & historical research or statistical purposes. [See 4.3.7.1.](#_Exemption_–_Research)

**Exemption – Archiving in the Public Interest**. [DPA Schedule 2 Part 6 Paragraph 28](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/28/enacted) disapplies GDPR Article 15(1) to (3) in respect of personal data that processed for archiving purposes in the public interest. See [4.3.7.2](#_Exemption_–_Archiving).

#### Right of Access Application Form

If the NPCC determines a standard Right of Access Application Form should be developed for all forces to use it will be included as an Appendix to this Manual of Guidance and referenced from this point in the manual.

#### Enforced Right of Access (DPA Part 7 Section 184)

**Commentary** - [DPA Part 7 Section 184](http://www.legislation.gov.uk/ukpga/2018/12/section/184) makes it an offence for an employer to require employees or contractors, or for a person to require another person who provides goods, facilities or services, to provide certain records obtained via subject access requests as a condition of their employment or contract. See [9.4.4](#_Offence;_Prohibition_of) for further details.

### Right to Rectification (GDPR Article 16)

GDPR Article 16 states:

*The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.*

The GDPR Recital associated with this right is GDPR Recital 65 (“Right of Rectification & Erasure”) which states:

*A data subject should have the right to have personal data concerning him or her rectified and a ‘right to be forgotten’ where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.*

**Commentary** – GDPR Article 16, which must be read in conjunction with [GDPR Article 12](#_Transparent_information,_communicat) and [GDPR Article 18](#_Right_to_Restriction), provides that data subjects are entitled to have personal data rectified if it is inaccurate or incomplete. It must be done within one month, or three months in complex cases. Where no action is taken they have the right to be informed of how to seek a judicial remedy. [DPA Part 7 Section 205 General interpretation](http://www.legislation.gov.uk/ukpga/2018/12/section/205) confirms that the definition of month in respect of this right is that set out in [Article 3 of Regulation (ECC, Euratom) No. 1182/71 of the Council of 3rd June 1971](file:///C:\Users\42006032\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\AppData\Local\Temp\DOC_1.en.xhtml).

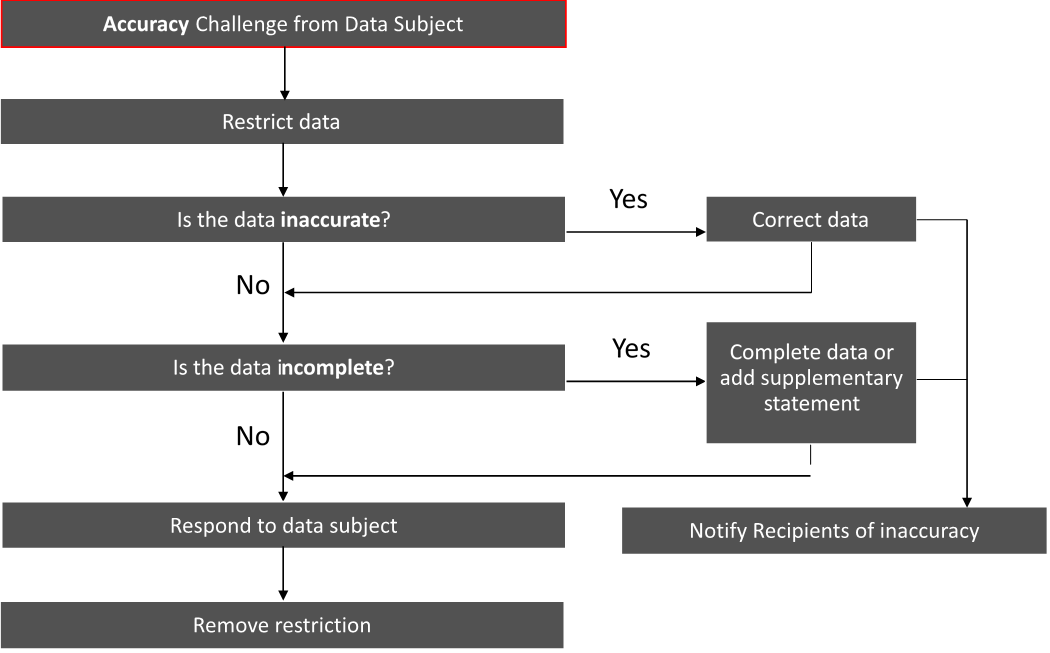
The ICO has published guidance on the GDPR Right to Rectification which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/). The ICO’s guidance on what constitutes a month which can be found [here](https://ico.org.uk/your-data-matters/time-limits-for-responding-to-data-protection-rights-requests/).

The police force must implement suitable measures to ensure the GDPR Right to Rectification can be facilitated. These will include:

• ensuring that all officers and staff are able to recognise any instance where a data subject requests to exercise this right, and know how to progress such requests

* creating and maintaining a policy or procedure setting out how this right is managed by them and make this publicly available.

The table below provides a workflow setting out how such requests should be managed.



Once the right has been exercised and is being considered, but it is not practical to restrict access to the information subject of the rectification requests, police forces should where practical append or signpost a report to alert officers and staff of the request which should also indicate the grounds of challenge.

The Data Protection Officer must monitor the police force’s compliance with the GDPR Right to Rectification and make any necessary interventions.

There are number of exemptions from this right which are set out below.

**Exemption – Crime & Taxation.** [DPA Schedule 2 Part 1 Paragraph 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/2/enacted) disapplies GDPR Article 16 to the extent that the application of that provision would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of a tax or an imposition of a similar nature. [See 4.3.2.1](#_Exemptions_-_Crime)

**Exemption – Disclosure Required by Law.** [DPA Schedule 2 Part 1 Paragraph 5](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/5/enacted) disapplies GDPR Article 16 to the extent that the application of that provision would prevent the controller from:

1. complying with an obligation to make personal data available to the public, or
2. complying with an obligation to disclose personal data required by an enactment, rule of law or order of a court or tribunal, or
3. (iii) making a disclosure where necessary or in connection with legal proceedings (including prospective ones), or making a disclosure necessary for obtaining legal advice, or making a disclosure that is otherwise necessary for establishing, exercising or defending legal rights.

[See 4.3.2.2.](#_Exemption_-_Disclosure)

**Exemption – Functions designed to protect the public etc.** [DPA Schedule 2 Part 2 Paragraph 7](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/7/enacted) disapplies GDPR Article 16 to the extent that the application of that provision would prejudice the proper discharge of functions:

* designed to protect the public against dishonesty, malpractice, serious improper conduct, unfitness or incompetence by anyone whose activity brings them into contact with the public
* relating to health and safety and welfare at work.

[See 4.3.3.1](#_Exemption_–_Functions)

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 16 where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of GDPR Article 16 would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

**Exemption – Research & Statistics**. [DPA Schedule 2 Part 6 Paragraph 27](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/27/enacted) disapplies GDPR Article 16 in respect of personal data that processed for scientific & historical research or statistical purposes. [See 4.3.7.1.](#_Exemption_–_Research)

**Exemption – Archiving in the Public Interest**. [DPA Schedule 2 Part 6 Paragraph 28](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/28/enacted) disapplies GDPR Article 16 in respect of personal data that processed for archiving purposes in the public interest. See [4.3.7.2.](file:///C:\Users\42006032\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\HK41YRSQ\4.3.7.2)

### Right to Erasure (“Right to be Forgotten”) (GDPR Article 17)

GDPR Article 17 states:

*1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:*

*(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;*

*(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;*

*(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);*

*(d) the personal data have been unlawfully processed;*

*(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;*

*(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).*

*2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.*

*3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:*

*(a) for exercising the right of freedom of expression and information;*

*(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*

*(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);*

*(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or*

*(e) for the establishment, exercise or defence of legal claims.*

There are two GDPR Recitals associated with this right. The first is GDPR Recital 65 (“Right of Rectification & Erasure”) which states:

*A data subject should have the right to have personal data concerning him or her rectified and a ‘right to be forgotten’ where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.*

The second GDPR Recital associated with this right is GDPR Recital 66 (“Right to be Forgotten”) which states:

*To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.*

**Commentary** – GDPR Article 17, which must be read in conjunction with [GDPR Article 12](#_Transparent_information,_communicat) and [GDPR Article 18](#_Right_to_Restriction), provides that data subjects have a right to have their personal data erased in specific circumstances:

* where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
* when the individual withdraws consent
* when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
* when the personal data was unlawfully processed
* when the personal data has to be erased in order to comply with a legal obligation
* when the personal data is processed in relation to the offer of information society services to a child

The tables below summarise this right.



The ICO has published guidance on the GDPR Right to Erasure (“Right to be Forgotten”) which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/). The ICO’s guidance on what constitutes a month which can be found [here](https://ico.org.uk/your-data-matters/time-limits-for-responding-to-data-protection-rights-requests/).

The police force must implement suitable measures to ensure the GDPR Right to Erasure can be facilitated.

The Data Protection Officer must monitor the police force’s compliance with the GDPR Right to Erasure and make any necessary interventions.

There are number of exemptions from this right which are set out below.

**Exemption – Crime & Taxation.** [DPA Schedule 2 Part 1 Paragraph 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/2/enacted) disapplies GDPR Article 17(1) & (2) to the extent that the application of those provisions would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of a tax or an imposition of a similar nature. [See 4.3.2.1](#_Exemptions_-_Crime)

**Exemption – Disclosure Required by Law.** [DPA Schedule 2 Part 1 Paragraph 5](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/5/enacted) disapplies GDPR Article 17(1) & (2) to the extent that the application of those provisions would prevent the controller from:

1. complying with an obligation to make personal data available to the public, or
2. complying with an obligation to disclose personal data required by an enactment, rule of law or order of a court or tribunal, or
3. making a disclosure where necessary or in connection with legal proceedings (including prospective ones), or making a disclosure necessary for obtaining legal advice, or making a disclosure that is otherwise necessary for establishing, exercising or defending legal rights.

[See 4.3.2.2.](#_Exemption_-_Disclosure)

**Exemption – Functions designed to protect the public etc.** [DPA Schedule 2 Part 2 Paragraph 7](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/7/enacted) disapplies GDPR Article 17(1) & (2) to the extent that the application of those provisions would prejudice the proper discharge of functions:

* designed to protect the public against dishonesty, malpractice, serious improper conduct, unfitness or incompetence by anyone whose activity brings them into contact with the public
* relating to health and safety and welfare at work.

[See 4.3.3.1](#_Exemption_–_Functions)

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 17(1) & (2) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of GDPR Article 16 would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

### Right to Restriction of Processing (GDPR Article 18)

GDPR Article 18 states:

*1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:*

*(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;*

*(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;*

*(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;*

*(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.*

*2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.*

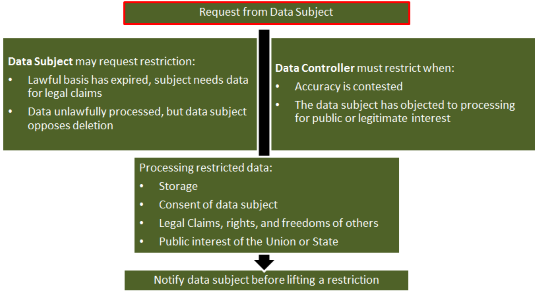
*3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.*

The associated GDPR Recital 67 (“Restriction of Processing”) states:

*Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.*

**Commentary** – GDPR Article 18, which must be read in conjunction with [GDPR Article 12](#_Transparent_information,_communicat), provides that where it is claimed that data is inaccurate (GDPR Article 16) or the right to erasure has been exercised (GDPR Article 17) individuals can require the controller to restrict processing until verification checks have been completed. Individuals may also require controllers to restrict processing where there is no legal basis and it is only needed for legal claims.

The table below summarises how such requests should be managed.



The ICO has published guidance on the GDPR Right to Restriction of Processing which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/). The ICO’s guidance on what constitutes a month which can be found [here](https://ico.org.uk/your-data-matters/time-limits-for-responding-to-data-protection-rights-requests/).

The police force must implement suitable measures to ensure the GDPR Right to Restriction of Processing can be facilitated .

The Data Protection Officer must monitor the police force’s compliance with the GDPR Right to Restriction of Processing and make any necessary interventions.

There are a number of exemptions from GDPR Article 18 which are set out below.

**Exemption – Crime & Taxation.** [DPA Schedule 2 Part 1 Paragraph 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/2/enacted) disapplies GDPR Article 18(1) to the extent that the application of that provision would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of a tax or an imposition of a similar nature. [See 4.3.2.1](#_Exemptions_-_Crime)

**Exemption – Disclosure Required by Law.** [DPA Schedule 2 Part 1 Paragraph 5](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/5/enacted) disapplies GDPR Article 18(1) to the extent that the application of that provision would prevent the controller from:

1. complying with an obligation to make personal data available to the public, or
2. complying with an obligation to disclose personal data required by an enactment, rule of law or order of a court or tribunal, or
3. (iii) making a disclosure where necessary or in connection with legal proceedings (including prospective ones), or making a disclosure necessary for obtaining legal advice, or making a disclosure that is otherwise necessary for establishing, exercising or defending legal rights.

[See 4.3.2.2.](#_Exemption_-_Disclosure)

**Exemption – Functions designed to protect the public etc.** [DPA Schedule 2 Part 2 Paragraph 7](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/7/enacted) disapplies GDPR Article 18(1) to the extent that the application of that provision would prejudice the proper discharge of functions:

* designed to protect the public against dishonesty, malpractice, serious improper conduct, unfitness or incompetence by anyone whose activity brings them into contact with the public
* relating to health and safety and welfare at work.

[See 4.3.3.1](#_Exemption_–_Functions)

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 18(1)(a), (b) & (d) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of GDPR Article 18(1)(a), (b) & (d) would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

**Exemption – Research & Statistics**. [DPA Schedule 2 Part 6 Paragraph 27](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/27/enacted) disapplies GDPR Article 18(1) in respect of personal data that processed for scientific & historical research or statistical purposes. [See 4.3.7.1](file:///C:\Users\42006032\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\HK41YRSQ\See%204.3.7.1).

**Exemption – Archiving in the Public Interest**. [DPA Schedule 2 Part 6 Paragraph 28](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/28/enacted) disapplies GDPR Article 18(1) in respect of personal data that processed for archiving purposes in the public interest. See [4.3.7.2](#_Exemption_–_Archiving).

### Notification obligation regarding rectification or erasure of personal data or restriction of processing (GDPR Article 19)

GDPR Article 19 states:

*The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.*

The associated GDPR Recital 66 (“Right to be Forgotten”) states:

*To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.*

**Commentary** – Compliance with GDPR Article 19, which must be read in conjunction with GDPR Article 12, places an obligation on police forces to inform parties to whom personal data subject of rectification, erasure or restriction has been disclosed in order that they can take necessary steps to do the same. As well as the exemptions from the right set out below the right does permit a police force not to carry out the notification if it is either impossible or involves disproportionate effort. The GDPR does not provide a definition of disproportionate effort, but the ICO’s guidance to the 1998 Act includes the following in respect of the right of access which may be of some use with regard to GDPR Article 19:

*the Court of Appeal has clarified that data controllers can take into account difficulties which occur throughout the process of complying with a request, including difficulties in finding the requested information*.

The police force must implement suitable measures to ensure the GDPR Notification obligation regarding rectification or erasure of personal data or restriction of processing is facilitated.

The Data Protection Officer must monitor the police force’s compliance with the GDPR Notification obligation regarding rectification or erasure of personal data or restriction of processing and make any necessary interventions.

There are two exemptions relevant to GDPR Article 19 which are set out below.

**Exemption – Crime & Taxation.** [DPA Schedule 2 Part 1 Paragraph 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/2/enacted) disapplies GDPR Article 19 to the extent that the application of that provision would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of a tax or an imposition of a similar nature. [See 4.3.2.1.](#_Exemptions_-_Crime)

**Exemption – Archiving in the Public Interest**. [DPA Schedule 2 Part 6 Paragraph 28](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/28/enacted) disapplies GDPR Article 19 in respect of personal data that processed for archiving purposes in the public interest. See [4.3.7.2](#_Exemption_–_Archiving).

### Right to Data Portability (GDPR Article 20)

GDPR Article 20 states:

*1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:*

*(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and*

*(b) the processing is carried out by automated means.*

*2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.*

*3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.*

*4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others*

The associated GDPR Recital 68 (“Right to Data Portability”) states:

*To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.*

**Commentary** - Compliance with GDPR Article 20, which must be read in conjunction with GDPR Article 12, allows data subjects to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The personal data must be provided in a structured, commonly used and machine readable form. The information must be provided free of charge.

The ICO has published guidance on the GDPR Right to Data Portability which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/). The ICO’s guidance on what constitutes a month which can be found [here](https://ico.org.uk/your-data-matters/time-limits-for-responding-to-data-protection-rights-requests/).

The police force must implement suitable measures to ensure the GDPR Right to Data Portability can be facilitated.

The Data Protection Officer must monitor the police force’s compliance with the GDPR Right to Data Portability and make any necessary interventions.

[DPA Part 6 Section 173](http://www.legislation.gov.uk/ukpga/2018/12/section/173) makes it an offence is to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the data subject would have been entitled to receive under this right.

Exemptions from the right are set out below.

**Exemption – Crime & Taxation.** [DPA Schedule 2 Part 1 Paragraph 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/2/enacted) disapplies GDPR Article 20(1) & (2) to the extent that the application of those provisions would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of a tax or an imposition of a similar nature. [See 4.3.2.1](#_Exemptions_-_Crime)

**Exemption – Disclosure Required by Law.** [DPA Schedule 2 Part 1 Paragraph 5](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/5/enacted) disapplies GDPR Article 20(1) & (2) to the extent that the application of those provisions would prevent the controller from:

1. complying with an obligation to make personal data available to the public, or
2. complying with an obligation to disclose personal data required by an enactment, rule of law or order of a court or tribunal, or
3. (iii) making a disclosure where necessary or in connection with legal proceedings (including prospective ones), or making a disclosure necessary for obtaining legal advice, or making a disclosure that is otherwise necessary for establishing, exercising or defending legal rights.

[See 4.3.2.2.](#_Exemption_-_Disclosure)

**Exemption – Functions designed to protect the public etc.** [DPA Schedule 2 Part 2 Paragraph 7](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/7/enacted) disapplies GDPR Article 20(1) & (2) to the extent that the application of those provisions would prejudice the proper discharge of functions:

* designed to protect the public against dishonesty, malpractice, serious improper conduct, unfitness or incompetence by anyone whose activity brings them into contact with the public
* relating to health and safety and welfare at work.

[See 4.3.3.1](#_Exemption_–_Functions)

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 20(1) & (2) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of GDPR Article 20(1) & (2) would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

**Exemption – Archiving in the Public Interest**. [DPA Schedule 2 Part 6 Paragraph 28](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/28/enacted) disapplies GDPR Article 20(1) in respect of personal data that processed for archiving purposes in the public interest. See [4.3.7.2](#_Exemption_–_Archiving).

### Right to Object (GDPR Article 21)

GDPR Article 21 states:

*1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.*

*2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.*

*3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.*

*4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.*

*5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.*

*6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.*

There are two associated GDPR Recitals, of which only one[[14]](#footnote-14), GDPR Recital 69 (“Right to Object”) is likely to be relevant to policing. It states:

*Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.*

**Commentary** – Compliance with GDPR Article 21, which must be read in conjunction with GDPR Article 12, provides that in addition to direct marketing, data subjects have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling), and processing for purposes of scientific/historical research and statistics.

The table below summarises this right.



The ICO has published guidance on the GDPR Right to Object which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/). The ICO’s guidance on what constitutes a month which can be found [here](https://ico.org.uk/your-data-matters/time-limits-for-responding-to-data-protection-rights-requests/).

The police force must implement suitable measures to ensure the GDPR Right to Object can be facilitated.

The Data Protection Officer must monitor the police force’s compliance with the GDPR Right to Object and make any necessary interventions.

Exemptions from the right are set out below.

**Exemption – Crime & Taxation.** [DPA Schedule 2 Part 1 Paragraph 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/2/enacted) disapplies GDPR Article 21(1) to the extent that the application of that provision would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of a tax or an imposition of a similar nature. [See 4.3.2.1](#_Exemptions_-_Crime)

**Exemption – Disclosure Required by Law.** [DPA Schedule 2 Part 1 Paragraph 5](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/5/enacted) disapplies GDPR Article 21(1) to the extent that the application of that provision would prevent the controller from:

1. complying with an obligation to make personal data available to the public, or
2. complying with an obligation to disclose personal data required by an enactment, rule of law or order of a court or tribunal, or
3. (iii) making a disclosure where necessary or in connection with legal proceedings (including prospective ones), or making a disclosure necessary for obtaining legal advice, or making a disclosure that is otherwise necessary for establishing, exercising or defending legal rights.

[See 4.3.2.2.](#_Exemption_-_Disclosure)

**Exemption – Functions designed to protect the public etc.** [DPA Schedule 2 Part 2 Paragraph 7](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/7/enacted) disapplies GDPR Article 21(1) to the extent that the application of that provision would prejudice the proper discharge of functions:

* designed to protect the public against dishonesty, malpractice, serious improper conduct, unfitness or incompetence by anyone whose activity brings them into contact with the public
* relating to health and safety and welfare at work.

[See 4.3.3.1](#_Exemption_–_Functions)

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 21(1) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of GDPR Article 21(1) would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

**Exemption – Research & Statistics**. [DPA Schedule 2 Part 6 Paragraph 27](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/27/enacted) disapplies GDPR Article 21(1) in respect of personal data that processed for scientific & historical research or statistical purposes. [See 4.3.7.1.](file:///C:\Users\42006032\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\HK41YRSQ\See%204.3.7.1)

**Exemption – Archiving in the Public Interest**. [DPA Schedule 2 Part 6 Paragraph 28](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/28/enacted) disapplies GDPR Article 21(1) in respect of personal data that processed for archiving purposes in the public interest. See [4.3.7.2](#_Exemption_–_Archiving).

### Automated individual decision-making, including profiling (GDPR Article 22)

GDPR Article 22 states:

*1.The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*

*2. Paragraph 1 shall not apply if the decision:*

*(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;*

*(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or*

*(c) is based on the data subject's explicit consent.*

*3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision*.

*4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.*

There are three GDPR Recitals associated with GDPR Article 22. The first is GDPR Recital 71 (“Profiling”) which states:

*The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes ‘profiling’ that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.* *In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.*

The second is GDPR Recital 72 (“Guidance of the European Data Protection Board regarding profiling”) is not directly relevant to policing.

The third is GDPR Recital 91 (“Necessity of a DPIA”) which states:

*This* [the requirement to conduct a DPIA] *should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.*

[DPA Part 2 Section 14 Automated decision-making authorised by law: safeguards](http://www.legislation.gov.uk/ukpga/2018/12/section/14) states:

*(1) This section makes provision for the purposes of Article 22(2)(b) of the GDPR (exception from Article 22(1) of the GDPR for significant decisions based solely on automated processing that are authorised by law and subject to safeguards for the data subject’s rights, freedoms and legitimate interests).*

*(2) A decision is a “significant decision” for the purposes of this section if, in relation to a data subject, it—*

*(a) produces legal effects concerning the data subject, or*

*(b) similarly significantly affects the data subject.*

*(3) A decision is a “qualifying significant decision” for the purposes of this section if—*

*(a) it is a significant decision in relation to a data subject,*

*(b) it is required or authorised by law, and*

*(c) it does not fall within Article 22(2)(a) or (c) of the GDPR (decisions necessary to a contract or made with the data subject’s consent).*

*(4) Where a controller takes a qualifying significant decision in relation to a data subject based solely on automated processing—*

*(a) the controller must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing, and*

*(b) the data subject may, before the end of the period of 21 days beginning with receipt of the notification, request the controller to—*

*(i) reconsider the decision, or*

*(ii) take a new decision that is not based solely on automated processing.*

*(5) If a request is made to a controller under subsection (4), the controller must, before the end of the period of 21 days beginning with receipt of the request—*

*(a) consider the request, including any information provided by the data subject that is relevant to it,*

*(b) comply with the request, and*

*(c) by notice in writing inform the data subject of—*

*(i) the steps taken to comply with the request, and*

*(ii) the outcome of complying with the request.*

*(6) The Secretary of State may by regulations make such further provision as the Secretary of State considers appropriate to provide suitable measures to safeguard a data subject’s rights, freedoms and legitimate interests in connection with the taking of qualifying significant decisions based solely on automated processing.*

*(7) Regulations under subsection (6)—*

*(a) may amend this section, and*

*(b) are subject to the affirmative resolution procedure.* *(6) In connection with this section, a controller has the powers and obligations under Article 12 of the GDPR (transparency, procedure for extending time for acting on request, fees, manifestly unfounded or excessive requests etc) that*

*apply in connection with Article 22 of the GDPR.*

*(7) The Secretary of State may by regulations make such further provision as the Secretary of State considers appropriate to provide suitable measures to safeguard a data subject’s rights, freedoms and legitimate interests in connection with the taking of qualifying significant decisions based solely on automated processing.*

*(8) Regulations under subsection (7)—*

*(a) may amend this section, and*

*(b) are subject to the affirmative resolution procedure.*

**Commentary** – Compliance with GDPR Article 22, which must be read in conjunction with GDPR Article 12, gives data subjects the right to object to decisions made about them solely on the basis of automated processing, where those decisions have legal or other significant effects. This includes processing where there is no human intervention, for example, when data is collected about an individual’s personal finances, which is then processed to calculate creditworthiness. [DPA Part 2 Section 14](http://www.legislation.gov.uk/ukpga/2018/12/section/14) provides safeguards that apply in relation to certain types of automated decision-making including profiling.

Within policing the only area of activity which this is likely to relate to is where automated processes are used to sift recruitment applications. The NPCC’s view is that profiling by police forces to predict whether an individual with certain characteristics is more likely to offend than another person without those characteristics falls under Law Enforcement Processing (Part 3 of the Act).

The ICO has published guidance on the GDPR Rights regarding Automated individual decision-making, including profiling, which can be accessed [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/). The ICO’s guidance on what constitutes a month which can be found [here](https://ico.org.uk/your-data-matters/time-limits-for-responding-to-data-protection-rights-requests/).

The police force must implement suitable measures to ensure the GDPR Rights regarding Automated individual decision-making, including profiling, can be facilitated.

The Data Protection Officer must monitor the police force’s compliance with the GDPR Rights regarding Automated individual decision-making, including profiling, and make any necessary interventions.

There are no DPA Schedule 2 exemptions from GDPR Article 22.

### Data subject’s rights and other prohibitions and restrictions (Part 7 Section 186)

[DPA Part 7 Section 186 Part 7 Data subject’s rights and other prohibitions and restrictions](http://www.legislation.gov.uk/ukpga/2018/12/section/186) states:

(1) An enactment or rule of law prohibiting or restricting the disclosure of information, or authorising the withholding of information, does not remove or restrict the obligations and rights provided for in the provisions listed in subsection (2), except as provided by or under the provisions listed in subsection (3).

(2) The provisions providing obligations and rights are—

(a) Chapter III of the GDPR (rights of the data subject),

(b) Chapter 3 of Part 3 of this Act (law enforcement processing: rights of the data subject), and

(c) Chapter 3 of Part 4 of this Act (intelligence services processing: rights of the data subject).

(3) The provisions providing exceptions are—

(a) in Chapter 2 of Part 2 of this Act, sections 15 and 16 and Schedules 2, 3 and 4,

(b) in Chapter 3 of Part 2 of this Act, sections 23, 24, 25 and 26,

(c) in Part 3 of this Act, sections 44(4), 45(4) and 48(3), and

(d) in Part 4 of this Act, Chapter 6 .

**Commentary** – [DPA Part 7 Section 186](http://www.legislation.gov.uk/ukpga/2018/12/section/186) confirms that any legislation or rule of law that prohibits or restricts the disclosure of information or authorizing the withholding of information cannot restrict subject rights except in prescribed circumstances.

### Summary table of exemptions and restrictions from General Processing Rights

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Article 13(1) to (3)** | **Article 14(1) to (4)** | **Article 15(1) to (3)**  **Access etc** | **Article 16**  **Rectification** | **Article 17(1) & (2)**  **Erasure** | **Article 18(1)**  **Restriction** | **Article 19 Notification Obligation** | **Article 20(1) & (2) Portability** | **Article 21(1) Objection** |
| **Sch 2**  **Part 1 (Restrictions based on Article 6(3) & 23(1)** | (2) Crime & taxation general  (5) Disclosure required by law | (2) Crime & Taxation (5) Disclosure required by law | (2) Crime & Taxation (5) Disclosure required by law | (2) Crime & Taxation (5) Disclosure required by law | (2) Crime & Taxation (5) Disclosure required by law | (2) Crime & Taxation (5) Disclosure required by law | (2) Crime & Taxation (5) Disclosure required by law | (2) Crime & Taxation (5) Disclosure required by law | (2) Crime & Taxation (5) Disclosure required by law |
| **Sch 2 Part 2 (Restrictions based on Article 13-21 & 34)** | (7) Functions designed to protect the public | (7) Functions designed to protect the public | (7) Functions designed to protect the public | (7) Functions designed to protect the public | (7) Functions designed to protect the public | (7) Functions designed to protect the public | (7) Functions designed to protect the public | (7) Functions designed to protect the public | (7) Functions designed to protect the public |
| **Sch 2 Part 3 (Protection of Rights of Others)** | N/A | N/A | (16) Protection of the rights of others general  (17) Health Workers | N/A | N/A | N/A | N/A | N/A | N/A |
| **Sch 2 Part 4 (Restrictions based on Article 23(1))** | (19) Legal Professional Privilege  (20) Self Incrimination  (22) Management Forecasts  (23) Negotiations  (24) Confidential References | (19) Legal Professional Privilege  (20) Self Incrimination  (22) Management Forecasts  (23) Negotiations  (24) Confidential References | (19) Legal Professional Privilege  (20) Self Incrimination  (22) Management Forecasts  (23) Negotiations  (24) Confidential References | N/A | N/A | N/A | N/A | N/A | N/A |
| **Sch 2 Part 5 (Exemptions based on Article 85(2)** | (26) Special Purposes | (26) Special Purposes | (26) Special Purposes | (26) Special Purposes | (26) Special Purposes | (26) Special Purposes | (26) Special Purposes | (26) Special Purposes | (26) Special Purposes |
| **Sch 2 Part 6**  **(Derogation for research, statistics & archiving)** | N/A | N/A | (27) Research & Statistics  (28) Archiving | (27) Research & Statistics  (28) Archiving | N/A | (27) Research & Statistics  (28) Archiving | (28) Archiving | (28) Archiving\* | (27) Research & Statistics  (28) Archiving |

## General Processing Controller & Processor Obligations

### Overview & Scope (GDPR Article 24)

GDPR Article 24 (Responsibility of the Controller) states:

*(1) Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*

*(2) Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.*

*(3) Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.*

There are four GDPR Recitals associated with GDPR Article 24. The first, GDPR Recital 74 (“Responsibility & Liability of the Controller”), states:

*The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller’s behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.*

The second, GDPR Recital 75 (“Risks to the rights of natural persons”), states:

*The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.*

The third, GDPR Recital 76 (“Risk Assessment”), states:

*The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.*

The fourth, GDPR Recital 77 (“Risks to the rights of natural persons”), states:

*Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.*

**Commentary** - GDPR Article 24(1) requires police forces to carefully consider all their processing activities and not only ensure appropriate technical and organisational measures are in place and regularly reviewed to comply with the GDPR, but also to both ensure and be able to demonstrate that compliance with the GDPR. Those measures may include, but are not limited to:

Technical

* Adoption and ongoing review of access control to IT systems
* Monitoring and audit of access and use of IT systems
* Building and room access control
* Online application form for subject rights applications
* Monitoring and reporting of data quality in higher risk information systems

Organisational

* Designation of an executive-level officer with oversight of Data Protection matters
* Designation of a Data Protection Officer with appropriate resource to support that role
* Designation of Information Asset Owners for all systems processing personal data
* Adoption of a Data Protection policy with regular review
* Implementation of Data Protection training including stand-alone and integrated into other training
* Maintenance of records of processing activities
* Implementation and regular review of operating procedures for higher risk information systems
* Adoption of privacy notices
* Adoption of measures to ensure data minimisation
* Adoption of measures to ensure data quality
* Adoption of measures to ensure transparency and accountability
* Adoption of measures to ensure no excessive retention of personal data
* Adoption of measures to ensure integrity and confidentiality of personal data
* Demonstrable adherence to relevant Codes of Practice
* Award of appropriate certification
* Adoption of Data Protection by design and default, and Data Protection Impact Assessments
* Data Protection audits and compliance testing

GDPR Article 24(2) requires the measures to include the proportionate implementation of appropriate data protection polices for the General Processing operations judged to pose the highest risks or greatest impacts on data subjects. The NPCC’s position is that this requirement must be met through police forces formally implementing:

* a publicly available Data Protection policy, setting out in general terms how the General Processing requirements will be met, and
* specific policies or operating procedures for those General Processing operations identified as being of greatest risk to data subjects

For practical purposes the former should also encompass Law Enforcement Processing, and it could include a commitment to comply with this Manual.

The ICO has published guidance on Accountability and Governance which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/).

### Data Protection by Design & Default (GDPR Article 25)

GDPR Article 25 (Data protection by design & default) states:

*1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*

*3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.*

The associated GDPR Recital 78 (“Appropriate technical and organisational measures”) states:

*The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.*

**Commentary** - The requirements of GDPR Article 25 are best met through the undertaking of a Data Protection Impact Assessment which is a means of identifying the necessary privacy solutions at the design stage of any project. See [4.5.2.1](#_Data_Protection_Impact).

[11.9 Appendix I](#_Appendix_I:_Information) Information Management IT System Requirements contains a document that sets out these requirements and a check list.

The ICO has published guidance on Data Protection by Design & Default which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/).

#### Data Protection Impact Assessments and Prior Consultation with the ICO (GDPR Article 35)

GDPR Article 35 (Data protection impact assessment) states:

*1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*

*2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.*

*3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:*

*(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*

*(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*

*(c) a systematic monitoring of a publicly accessible area on a large scale.*

*4. The supervisory authority* [ICO] *shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.*

*5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.*

*6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.*

*7. The assessment shall contain at least:*

*(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*

*(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*

*(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*

*(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*

*8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.*

*9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.*

*10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.*

*11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.*

There are seven GDPR Recitals associated GDPR Article 35. The first, Recital 75 (“Risks to the rights and freedoms of natural persons”), states:

*The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.*

A second associated GDPR Recital 84 (“Risk evaluation and impact assessment”) states:

*In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.*

A third associated GDPR Recital 89 (“Elimination of the general reporting requirement”) states:

*Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.*

A fourth associated GDPR Recital 90 (“Data protection impact assessment”) states:

*In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.*

A fifth associated GDPR Recital 91 (“Necessity of a data protection impact assessment”) states:

*This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.*

A sixth associated GDPR Recital 92 (“Broader data protection impact assessment”) states:

*There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.*

A seventh associated GDPR Recital 93 (“Data protection impact assessment at authorities”) states:

*In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.*

GDPR Article 36 (Prior Consultation) states:

*1. The controller shall consult the supervisory authority* [ICO] *prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.*

*2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.*

*3.When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:*

*(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;*

*(b) the purposes and means of the intended processing;*

*(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;*

*(d) where applicable, the contact details of the data protection officer;*

*(e) the data protection impact assessment provided for in Article 35; and (f) any other information requested by the supervisory authority.*

*4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.*

*5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.*

There are three GDPR Recitals associated with GDPR Article 36. One is GDPR Recital 94 (“Consultation of the supervisory authority”) which states:

*Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons*.

A second associated GDPR Recital 95 (“Support by the processor”) states:

*The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.*

A third associated GDPR Recital 96 (“Consultation of the supervisory authority in the course of a legislative process”) is not directly relevant to police forces.

**Commentary** - Data Protection Impact Assessments (previously known as privacy impact assessments or PIAs) are a valuable tool which police forces can use to identify the most effective way to comply with their data protection obligations and meet data subjects’ expectations of privacy. The ICO has promoted the use of the predecessor voluntary PIAs as an integral part of taking a privacy by design approach for several years. An effective DPIA allows police forces to identify and mitigate problems at an early stage.

[11.11 Appendix K](file:///\\42users.netr.ecis.police.uk\data$\42006032\Documents\6032\2019\National%20Work\MoG\MoG%20Appendix%20K%20DPIA%20ICO%20Derived%20Template.pdf) contains a DPIA template derived from the ICO’s template. It combines sections 5 & 6 of the ICO template into a single large table which has been populated with potential information risks and potential risk treatments. Use is not mandatory.

The ICO has issued an overview for DPIA’s for general processing which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/) and more detailed guidance can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/).

The police force must adopt effective polices and processes to ensure that consideration is given, at an early stage in all projects or initiatives involving personal data, as to whether a DPIA is required, and where one is necessary it is undertaken in accordance with the GDPR.

The Data Protection Officer must monitor compliance with the GDPR obligation to conduct DPIA’s in some circumstances and make any necessary interventions.

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 36 (requirement for controller to consult the ICO prior to high risk processing) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of GDPR Article 36 would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

### Joint Controllers (GDPR Article 26)

GDPR Article 26 states:

*1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.*

*2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.*

*3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.*

The associated GDPR Recital 79 (“Allocation of the responsibilities) states:

*The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.*

**Commentary -** Although the GDPR does not explicitly require the responsibilities of joint controllers to be documented in writing clearly there is practical benefit in doing so especially with regard to data subjects’ rights and transparency. Consequently police forces are encouraged, when conducting General Processing jointly, create a written agreement - a “Joint Controllership Agreement” - either as a standalone document or within other documentation) setting out their responsibilities, and within that include as a minimum a description of:

* the General Processing that is subject to joint controllership, including the purpose of the General Processing, the personal data involved, a description of the joint General Processing operations including data flows, and the jurisdiction and limits to the processing (i.e. at what point the processing commences jointly and ceases jointly).
* how failures to comply with the Joint Controllership Agreement or any other agreed ‘business rules’, or failures of the joint General Processing to comply with any of the General Data Protection GDPR or Act will be managed, including any liabilities or legal consequences arising.
* how subject rights, complaints and disputes will be managed.
* how Freedom of Information Act 2000 requests for information will be managed.
* how civil court orders requiring the disclosure of the jointly processed data will be managed.
* how information security incidents (“data breaches”) relating to the joint General Processing will be managed.
* how compliance with the Joint Controllership Agreement will be assessed and managed.
* how liaison with the ICO will be managed.

With many police forces operating collaborative departments which undertake General Processing (e.g. Human Resources, Finance and Payroll, and IT Services) it is imperative that Joint Data Controllership Agreements are developed.

Neither the GDPR nor the Act make mention of ‘controllers in common,’ a concept of the 1998 Act – the situation where separate controllers each have access to a single pool of personal data but each individually determines the purpose and means of the processing rather than making those determinations together. That scenario will persist under the Act, and consequently where a Joint Data Controllership Agreement is not required it is nevertheless desirable that an Information Sharing Agreement is in place between the controllers.

[Appendix F](#_Appendix_F:_Joint_1) provides Joint Controllers Definitions & Arrangements

The ICO has published guidance titled ‘What does it mean if you are joint controllers’ which can been found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/).

The police force should create and maintain Joint Controllership Agreements for all instances of joint controllership under the GDPR/DPA Part 2.

The Data Protection Officer must monitor compliance with the GDPR Article 26 (Joint Controllership Arrangements) obligation and make any necessary interventions .

#### Police collaborative units

**Commentary** - In recent years there has been a marked increase in the number of projects and initiatives to establish collaborative units serving two or more police forces and partner agencies. Such units often have the benefits of improving service delivery, increasing information sharing across police force boundaries, and delivering financial savings at a time of austerity.

However, projects and initiatives to create collaborative units must take into account Data Protection and other information management requirements if they are to be successfully delivered in a manner that is legally compliant.

A police force’s Chief Officer, as controller, is legally responsible for ensuring that their police force complies with the requirements of the Act.

Historically the scope of this responsibility has been fairly easy to define, as the processing of personal data by any police force has tended, with a few notable exceptions8, to involve police officers and staff using their own force information systems to handle, use or disclose personal data exclusively for the police force’s purposes.

The trend for the creation of collaborative units to deliver certain activity on behalf of more than one police force has meant that there is an increased risk those boundaries in the area of collaborative units can become ill-defined.

As a consequence it may be unclear as to who is the controller for personal data processed within a collaborative unit, leading to uncertainty as to the data protection and wider information management regime that should be followed.

This problem will be exacerbated where police forces involved in the collaboration have divergent or even contradictory policies and procedures around matters such as appropriate access or use of information systems, information security/assurance (including incident reporting), information sharing and information management governance arrangements.

The solution is for an approach of Data Protection by design and default, including Data Protection Impact Assessment to be adopted whenever there is an intention to establish collaborative units between police forces or their partners. That process will identify the privacy risks and the mitigations that should be put in place to counter those risks (see 4.5.2).

Although this Manual states there is no need for information sharing agreements between police forces, where a collaborative unit is created it will be necessary to clearly define and document controllership and set out how data protection and other information management matters will be managed within the unit – that documentation should form part of the overall collaboration agreement between the police forces.

Appendix O provides a project management-based approach to deliver Data Protection compliance.

### Obligations on Processors (GDPR Article 28 and GDPR Article 29)

GDPR Article 28 (Processor) states:

*1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*

*2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.*

*3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:*

*(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;*

*(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;*

*(c) takes all measures required pursuant to Article 32;*

*(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;*

*(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;*

*(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;*

*(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;*

*(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.*

*With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.*

*4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.*

*5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.*

*6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.*

*7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).*

*8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.*

*9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.*

*10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.*

The associated GDPR Recital 81 (“The use of processors”) states:

*To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject- matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.*

GDPR Article 29 (Processing under the authority of the controller or processor) states:

*The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.*

There is no associated GDPR recital.

**Commentary -** All police forces are likely to use processors (external organisations or individuals other than their own employees) to carry out work which involves the use of personal data on their behalf. Likely examples of data processors working for the police include:

* hardware/software suppliers & maintenance companies
* payroll suppliers
* confidential waste disposal contractors
* other persons working with the police, including volunteers where necessary

The obligations arising from Articles 28 and 29 will usually be met through the provision of a contract, commonly known as a ‘Data Processing Contract’. Data processing contracts will specify exactly what the processor is and is not permitted to do. The NPCC is considering the development of a General Data Processing Contract Template for police forces to use which will appear as an appendix to this Manual of Guidance.

Police Data Protection Professionals will be required to provide necessary advice and guidance to assist the police force in choosing processors that are able to satisfy the technical and organisational standards required by the police service to maintain an appropriate level of protection for the information concerned and of the associated data subjects’ rights.

Specialist technical advice may be forthcoming form force information assurance and records management staff, while Police Data Protection Professionals will also advise on the terms and conditions to be included in any contract where the processing of police information is undertaken.

It will be a matter for police forces to decide who will produce the necessary processing contracts. However, it is usually the case that the contracts and purchasing department will have responsibility for the production of any agreements where procurement is involved with any financial implication. In these cases, the Data Protection Officer will be consulted and be expected to provide advice and guidance on the terms and conditions to be included to ensure compliance with the Act’s requirements.

It will also be necessary for Police Data Protection Professionals to liaise with contracts and supplies departments to identify occasions where procurement contracts involve access to police information assets or premises in order to ensure appropriate terms and conditions are included in the contract.

There are a number of circumstances where police forces use the services of a processor but there are no financial considerations included. In such cases, the responsibility to complete a data processing contract to fulfil the Chief Officer’s responsibilities under the Act may fall to Police Data Protection Professionals.

[11.12 Appendix K](#_Appendix_K:_National) contains a Data Processing Contract Template for General Processing and supporting documents that police forces may wish to use.

The ICO has published guidance titled ‘What does it mean if you are a processor’ which can been found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-a-processor/), and further guidance titled ‘Contracts and liabilities between controllers and processors’ which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/). It includes more detailed guidance, one of which is titled ‘What needs to be included in the contract?’ which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/what-needs-to-be-included-in-the-contract/), and ‘Contracts’ which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/).

The police force must ensure that when (i) it act as a Processor for other Controllers or (ii) appoints Processors, Data Processing Contracts are in place that satisfy GDPR Article 28 and 29 obligations.

The Data Protection Officer must monitor compliance with GDPR Article 28 and 29 (Data Processing Contract) obligations and make any necessary interventions.

### Records of Processing Activities (RoPA) (GDPR Article 30)

**Commentary** - GDPR Article 30(1) and (2) contain provisions requiring police forces to maintain records of their processing activities, and for similar records to be maintained by any processor processing personal data on the force’s behalf. The requirements apply to any representative of the police force or their processor. However, under GDPR Article 30 (5) the provisions do not apply to enterprises or organisations employing fewer than 250 people, unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in GDPR Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

The table below sets out what those records of processing activities must contain:

|  |  |  |
| --- | --- | --- |
| **What information must be recorded?** | **GDPR Article 30(1) – by Police Force** | **GDPR Article 30(2) – by Data Processor** |
| the name and contact details of the controller/processor and, where applicable, the joint controller, the controller's/processor’s representative and the data protection officer | (a) | (a) |
| the purposes of the processing | (b) | - |
| the categories of processing carried out on behalf of each controller | - | (b) |
| a description of the categories of data subjects and of the categories of personal data | (c) | - |
| the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations | (d) | - |
| where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards | (e) | (c) |
| where possible, the envisaged time limits for erasure of the different categories of data | (f) | - |
| where possible, a general description of the technical and organisational security measures referred to in Article 32(1). | (g) | (d) |

The records must be in writing, including in electronic form (GDPR Article 30(3)), and must be made available to the ICO upon request (GDPR Article 30(4)).

The ICO has published guidance titled ‘Documentation’ which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/). It covers GDPR Article 30 obligations.

The police force must ensure that it maintains Records of Processing Activities as required by GDPR Article 30.

The Data Protection Officer must monitor their force’s compliance with GDPR Article 30 (Record of Processing Activities) and make any necessary interventions.

### General Data Processing & Procurement

The NPCC is currently considering the inclusion of specific content for this Manual of Guidance concerning obligations arising from GDPR/DPA Part 2. If it is determined such content is of value it will be added in due course.

### HR Processing

The NPCC is currently considering the inclusion of specific content for this Manual of Guidance concerning obligations arising from GDPR/DPA Part 2. If it is determined such content is of value it will be added in due course.

## Transfers to Third Countries or International Organisations (GDPR Articles 44 to 49)

GDPR Article 44 General Principles for Transfers states:

*Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this* Chapter *shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*

There are two GDPR Recitals associated with GDPR Article 44. The first, GDPR Recital 101 (“General Principles for International Data Transfers”), states:

*Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation.   
The increase in such flows has raised new challenges and concerns with regard to the protection of personal data.   
However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation.   
In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation.   
A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.*

The second, GDPR Recital 101 (“International Agreements for an Appropriate Level of Data Protection”), states:

*This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects.   
Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.*

GDPR Article 45 Transfers on the basis of an adequacy decision states:

*1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. 2Such a transfer shall not require any specific authorisation.*

*2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:*

*(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;*

*(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and*

*(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.*

*3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).*

*4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.*

*5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2). On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).*

*6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.*

*7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.*

*8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.*

*9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.*

There are five GDPR Recitals associated with GDPR Article 45. The first, GDPR Recital 103 (“Appropriate Level of Data Protection Based on an Adequacy Decision”), states:

*The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection.   
In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation.   
The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.*

The second, GDPR Recital 104 (“Criteria for an Adequacy Decision”), states:

*In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law.   
The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country.   
The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors.   
In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States’ data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.*

The third, GDPR Recital 105 (“Consideration of International Agreements for an Adequacy Decision”), states:

*Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country’s or international organisation’s participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations.   
In particular, the third country’s accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account.   
The Commission should consult the Board when assessing the level of protection in third countries or international organisations.*

The fourth, GDPR Recital 106 (“Monitoring and Periodic Review of the Level of Data Protection”), states:

*The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC.   
In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning.   
That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation.   
For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources.   
The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council (12) as established under this Regulation, to the European Parliament and to the Council.*

The fifth, GDPR Recital 107 (“Amendment, Revocation and Suspension of Adequacy Decisions”), states:

*The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection.   
Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled.   
In that case, provision should be made for consultations between the Commission and such third countries or international organisations.   
The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.*

GDPR Article 46 Transfers subject to appropriate safeguards states:

*1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.*

*2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:*

*(a) a legally binding and enforceable instrument between public authorities or bodies;*

*(b) binding corporate rules in accordance with Article 47;*

*(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);*

*(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);*

*(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights; or*

*(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights.*

*3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:*

*(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or*

*(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.*

*4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.*

*5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.*

There are two GDPR Recitals associated with GDPR Article 46. The first, GDPR Recital 108 (“Appropriate Safeguards”), states:

*In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject.   
Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority.   
Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country.   
They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default.   
Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects.   
Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.*

The second, GDPR Recital 109 (“Standard Data Protection Clauses”), states:

*The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.*

GDPR Article 47 Binding corporate rules states:

*1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:*

*(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;*

*(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and*

*(c) fulfil the requirements laid down in paragraph 2.*

*2. The binding corporate rules referred to in paragraph 1 shall specify at least:*

*(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;*

*(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;*

*(c) their legally binding nature, both internally and externally;*

*(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;*

*(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;*

*(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;*

*(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;*

*(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;*

*(i) the complaint procedures;*

*(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;*

*(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;*

*(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);*

*(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and*

*(n) the appropriate data protection training to personnel having permanent or regular access to personal data.*

*3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. 2Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).*

GDPR Recital 110 (“Binding Corporate Rules”) is the only recital associated with GDPR Article 47. It states:

*A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.*

GDPR Article 48 Transfers or disclosures not authorised by Union law states:

*Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter*.

GDPR Recital 111 (“Rules in Third Countries Contrary to the Regulation”) is the only recital associated with GDPR Article 48. It states:

*Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States.   
This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State.   
The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation.   
Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met.   
This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.*

GDPR Article 49 Derogations for specific situations states:

*1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:*

*(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;*

*(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject’s request;*

*(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;*

*(d) the transfer is necessary for important reasons of public interest;*

*(e) the transfer is necessary for the establishment, exercise or defence of legal claims;*

*(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;*

*(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.*

*Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.*

*2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register.   
Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.*

*3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.*

*4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.*

*5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.*

*6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.*

There are five GDPR Recitals associated with GDPR Article 49. The first, GDPR Recital 111 (“Appropriate Safeguards”), states:

The second, GDPR Recital 112 (“Exceptions for Certain Cases of International Transfers”), states:

*Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies.   
Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest.   
In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.*

The third, GDPR Recital 113 (“Transfers Qualified as Not Repetitive and that Only Concern a Limited Number of Data Subjects”), states:

*Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer.   
The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data.   
Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable.   
For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.   
The controller should inform the supervisory authority and the data subject about the transfer.*

The fourth, GDPR Recital 114 (“Safeguarding of Enforceability of Rights and Obligations in the Absence of an Adequacy Decision”), states:

*In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.*

The fifth, GDPR Recital 115 (“Rules in Third Countries Contrary to the Regulation”), states:

*Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States.   
This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State.   
The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation.   
Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met.   
This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.*

[DPA Part 2 Section 18 Transfers of personal data to third countries etc.](http://www.legislation.gov.uk/ukpga/2018/12/section/18/enacted) states:

*(1) The Secretary of State may by regulations specify, for the purposes of Article 49(1)(d) of the GDPR—*

*(a) circumstances in which a transfer of personal data to a third country or international organisation is to be taken to be necessary for important reasons of public interest, and*

*(b) circumstances in which a transfer of personal data to a third country or international organisation which is not required by an enactment is not to be taken to be necessary for important reasons of public interest.*

*(2) The Secretary of State may by regulations restrict the transfer of a category of personal data to a third country or international organisation where—*

*(a) the transfer is not authorised by an adequacy decision under Article 45(3) of the GDPR, and*

*(b) the Secretary of State considers the restriction to be necessary for important reasons of public interest.*

*(3) Regulations under this section—*

*(a) are subject to the made affirmative resolution procedure where the Secretary of State has made an urgency statement in respect of them;*

*(b) are otherwise subject to the affirmative resolution procedure.*

*(4) For the purposes of this section, an urgency statement is a reasoned statement that the Secretary of State considers it desirable for the regulations to come into force without delay.*

**Commentary –** GDPR Articles 44 to 49 inclusive set out the framework thatregulates international transfers of personal data.

DPA Part 2 Section 18(1) allows the Secretary of State to specify through regulations circumstances in which international transfers of personal data are or are not taken to be necessary for important reasons of public interest.DPA Part 2 Section 18(2) allows the Secretary of State to specify through regulations limitations on data transfers to a third country or international organisation, in the absence of an adequacy decision and when such limitations are for important reasons of public interest. DPA Part 2 Section 18(3) and (4) set out further provisions concerning regulations created under DPA Part 2 Section 18(1) or (2).

The ICO has issued guidance on international transfers to [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/) which does not need to contextualized for policing. Guidance on data protection and Brexit can be found [here](https://ico.org.uk/for-organisations/data-protection-and-brexit/).

The police force must adopt measures to ensure international or third country transfers of personal data under GDPR/DPA Part 2 are conducted in compliance with GDPR Articles 44 to 49. These should include maintaining a register of such transfers which will set out how the transfers are compliant.

The Data Protection Officer must test their force’s compliance with GDPR Articles 44 to 49 (Transfers to Third Countries etc.).

**Exemption – Special Purposes.** [DPA Schedule 2 Part 5 Paragraph 26](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/26/enacted) disapplies GDPR Article 44 (general principles for transfers) where personal data is being processed for a view for publication for journalistic, artistic or literary purposes (collectively termed ‘Special Purposes’), the publication would be in the public interest, and the application of GDPR Article 44 would be incompatible with any of the Special Purposes. See [4.3.6.1](#_Exemption_–_Journalistic,).

## Processing for archiving, research and statistical purposes (GDPR Article 89)

GDPR Article 89 (Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes) states:

*1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.*

*2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.*

*3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.*

*4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.*

[DPA Part 2 Section 19 (Processing for archiving, research and statistical purposes: safeguards)](http://www.legislation.gov.uk/ukpga/2018/12/section/19/enacted) supplements GDPR Article 89(1) and the parts of relevance to policing state:

*(1) This section makes provision about—*

*(a) processing of personal data that is necessary for archiving purposes in the public interest,*

*(b) processing of personal data that is necessary for scientific or historical research purposes, and*

*(c) processing of personal data that is necessary for statistical purposes.*

*(2) Such processing does not satisfy the requirement in Article 89(1) of the GDPR for the processing to be subject to appropriate safeguards for the rights and freedoms of the data subject if it is likely to cause substantial damage or substantial distress to a data subject.*

**Commentary** – Police forces may process personal data for historical research or archiving in the public interest purposes (e.g. records relating to former officers and staff, or crimes of historic importance). The provisions within GDPR Article 89 and DPA Part 2 Section 19 provide necessary safeguards, prohibiting such processing if it causes substantial damage or distress to the data subject.

## Re-use of Data Collected for General Processing for Law Enforcement Processing

**Commentary** – In general terms non-police UK-based controllers are able to provide personal data collected by them for General Processing Purposes to police forces for Law Enforcement Processing without breaching GDPR/DPA Part 2 by virtue of the Crime and Taxation General exemption ([DPA Schedule 2 Part 1 Paragraph 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/2/enacted)).

The following sets out the considerations such controllers are likely to make in advance of making such a disclosure:

1. Identify the personal data to be disclosed
2. Confirm whether the disclosure would involve any Special Category Data as defined at [GDPR Article 9(1)](https://gdpr-info.eu/art-9-gdpr/) and/or ‘Criminal Offence Data’ as defined at [GDPR Article 10](https://gdpr-info.eu/art-10-gdpr/) and further defined at [DPA Part 2 Section 11](http://www.legislation.gov.uk/ukpga/2018/12/section/11).
3. Satisfy themselves that one of the [GDPR Article 6(1)](https://gdpr-info.eu/art-6-gdpr/) Processing Condition exists for the disclosure – the most likely to apply would be GDPR Article 6(1)(d) vital interests, (e) public task, or (f) legitimate interests (f is not available to public authorities)
4. If the disclosure involves Special Category Data satisfy themselves that a [GDPR Article 9(2)](https://gdpr-info.eu/art-9-gdpr/) Special Processing Condition exists in addition to the [GDPR Article 6(1)](https://gdpr-info.eu/art-6-gdpr/) Processing Condition required above – the most likely to apply would be GDPR Article 9(2)(c) vital interests or (g) substantial public interest
5. In addition, if the disclosure involves Special Category Data and the Special Processing Condition at GDPR Article 9(2)(g) applies satisfy themselves that a condition in [DPA Schedule 1 Part 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1) applies too and an appropriate policy document exists in accordance with [DPA Schedule 1 Part 4](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/part/4).
6. If the disclosure involves ‘Criminal Offence Data’ satisfy themselves that the disclosure would comply with [GDPR Article 10](https://gdpr-info.eu/art-10-gdpr/), a [DPA Schedule 1 Part 1, 2 or 3](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1) is condition is met, an appropriate policy document exists in accordance with [DPA Schedule 1 Part 4](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/part/4)
7. Consider the extent to which the Crime and Taxation General exemption ([DPA Schedule 2 Part 1 Paragraph 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/2/enacted)) provides relief from (i) the preceding requirements, and (ii) the fair processing elements of the 1st GDPR Principle. Note - the exemption provides relief as far as is required from the First General Principle (GDPR Article 5(1)(a) lawful, fair and transparent processing) except the lawfulness requirements in GDPR Article 6.
8. Satisfy themselves that the disclosure would be compliant with the other five General Data Protection Principles, having also considered the relief provided by the Crime and Taxation General exemption ([DPA Schedule 2 Part 1 Paragraph 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/paragraph/2/enacted)) which allows the Second General Principle (GDPR Article 5(1)(b) (purpose limitation).

Similar considerations could be given by police forces when determining whether to process personal data previously processed by them for General Processing Purposes for Law Enforcement Processing without breaching GDPR/DPA Part 2.

The ICO has published a blog titled ‘Data Protection law does not prevent information sharing to save lives and stop crime’ which can be found [here](https://ico.org.uk/about-the-ico/news-and-events/blog-data-protection-law-does-not-prevent-information-sharing-to-save-lives-and-stop-crime/).

## Information Sharing Under the GDPR Guidance & Template (Appendix M)

**Commentary** – Appendix M provides guidance and a template for information sharing under the GDPR which forces may wish to adapt for their own purposes.

# Comparison between General Processing and Law Enforcement obligations

## Overview

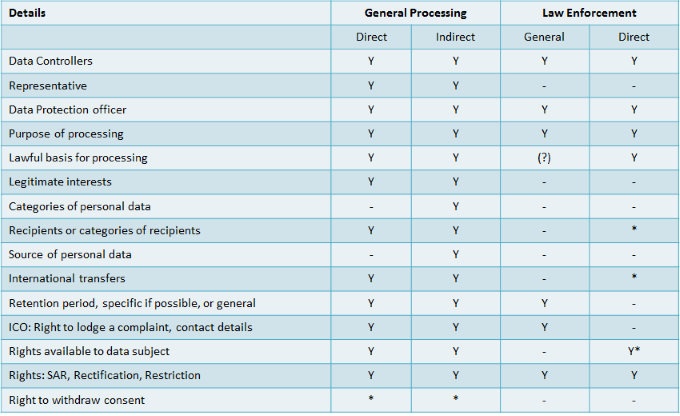
**Commentary** – Although the General Processing and Law Enforcement regimes under the Data Protection legislation are similar there are a number of interesting differences which are set out in summary form in the remainder of this chapter.

## Data Protection Principles Comparison

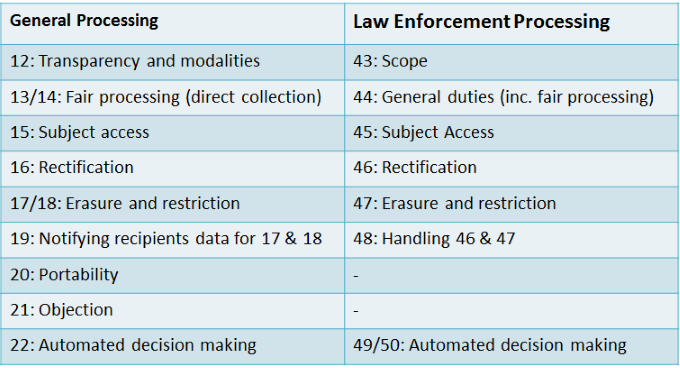
**Commentary** – The DPA and GDPR each introduced six data protection principles for law enforcement processing and general processing respectively.

Both sets of principles are broadly consistent with one another. The most significant difference between the two regimes is that the first law enforcement processing principle does not require transparency, unlike its general processing comparison.

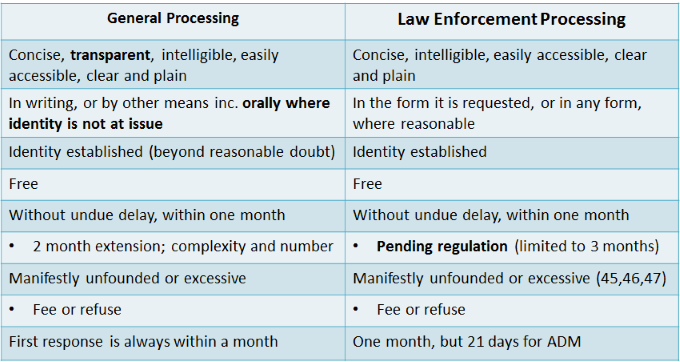
## Fair Processing Comparison



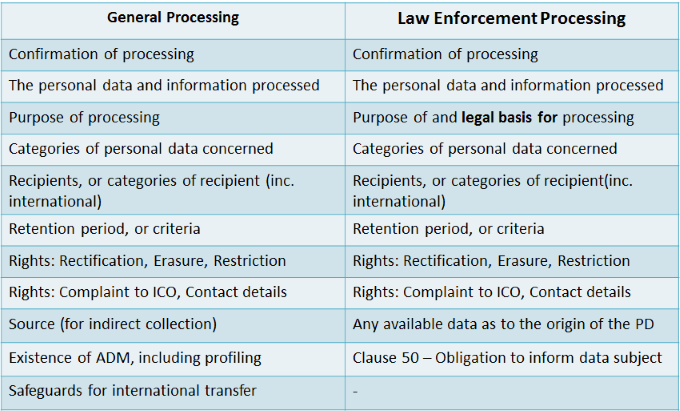
## Data Subject Rights Comparison



## Data Subject Rights Requirements Comparison



## Information to be supplied under the Right of Access Comparison



## Data Controller and Data Processor Obligations Comparison

The NPCC is currently considering whether there is a requirement to add this content to future versions of this document.

## Exemptions/Restrictions Comparison

The NPCC is currently considering whether there is a requirement to add this content to future versions of this document.

# Law Enforcement Processing (Part 3 of DPA)

## Scope: Competent Authorities & Law Enforcement Purposes (DPA Part 3 Section 29, Section 30, Section 31)

[DPA Part 3 Section 29 Processing to which this part applies](http://www.legislation.gov.uk/ukpga/2018/12/section/29) states:

*(1) This Part applies to—*

*(a) the processing by a competent authority of personal data wholly or partly by automated means, and*

*(b) the processing by a competent authority otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system.*

*(2) Any reference in this Part to the processing of personal data is to processing to which this Part applies.*

*(3) For the meaning of “competent authority”, see section 30.*

[DPA Part 3 Section 30 Meaning of competent authority](http://www.legislation.gov.uk/ukpga/2018/12/section/30) includes:

*(1) In this Part, “competent authority” means—*

*(a) a person specified in* [*Schedule 7*](http://www.legislation.gov.uk/ukpga/2018/12/schedule/7)*, and*

*(b) any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes.*

*(2) But an intelligence service is not a competent authority within the meaning of this Part.*

DPA Part 3 Section 30 Paragraphs (3) to (6) are not relevant to policing.

*(7) In this section—*

*“intelligence service” means—*

*(a) the Security Service;*

*(b) the Secret Intelligence Service;*

*(c) the Government Communications Headquarters;*

*“statutory function” means a function under or by virtue of an enactment.*

[DPA Part 3 Section 31 The law enforcement purposes](http://www.legislation.gov.uk/ukpga/2018/12/section/31) states:

*For the purposes of this Part, “the law enforcement purposes” are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*.

**Commentary** - The GDPR does not apply to the processing of personal data by “competent authorities” (broadly the police and other criminal justice agencies) “for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security”.

Instead, alongside of the GDPR, the European Parliament and Council adopted the Law Enforcement Directive (EU) 2016/6802 “on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data”.

Unlike the GDPR, this Law Enforcement Directive (“LED”) was not directly applicable EU law; accordingly Part 3 of the Act (together with provisions in Parts 5 to 7 which apply across the GDPR, LED and intelligence services regimes) transpose the provisions of the LED into UK law.

Technically the LED only applies in relation to the cross-border processing of personal data for law enforcement purposes but the DPA Part 3 also applies it to the domestic processing of personal data for such purposes to ensure that there is a single domestic and cross-border regime for the processing of personal data for law enforcement purposes.

DPA Part 3 was designed to be technology neutral. Accordingly, the provisions within it cover the processing of personal data by computer systems or paper based structured filing systems (see 3.10). Files which are not structured according to specific criteria do not fall within the scope of DPA Part 3.

Not all processing of personal data by a competent authority will be for law enforcement purposes. This is because where a controller determines that the processing will take place for another purpose, this will be general processing and governed by the GDPR/DPA Part 2.

See 3.24 more commentary on ‘competent authorities’.

The ICO has issued guidance on law enforcement processing which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/).

### Examples of Police Law Enforcement Processing

Police Law Enforcement Processing includes the collection or creation, retention, use, disclosure and deletion of personal data about suspects, witness, victims and other identifiable living individuals in following scenarios:

* Crime prevention activities such as disclosing a warning to the public the name and description of a known dangerous offender or disclosing the name and description of a wanted person into the public domain in order to locate them.
* Managing incidents.
* Managing offenders.
* Recording allegations of crime.
* Investigating allegations of crime.
* Gathering intelligence on individuals.
* Gathering evidence for prosecutions.
* Disclosing information on suspects or offenders to partner agencies involved in crime and disorder activity.

## Law Enforcement Principles

### Overview and general duty of Controller (DPA Part 3 Section 34)

[DPA Part 3 Section 34 Overview and general duty of controller](http://www.legislation.gov.uk/ukpga/2018/12/section/34) states:

*(1) This Chapter sets out the six data protection principles as follows—*

*(a) section 35(1) sets out the first data protection principle (requirement that processing be lawful and fair);*

*(b) section 36(1) sets out the second data protection principle (requirement that purposes of processing be specified, explicit and legitimate);*

*(c) section 37 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);*

*(d) section 38(1) sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);*

*(e) section 39(1) sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);*

*(f) section 40 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner).*

*(2) In addition—*

*(a) each of sections 35, 36, 38 and 39 makes provision to supplement the principle to which it relates, and*

*(b) sections 41 and 42 make provision about the safeguards that apply in relation to certain types of processing.*

*(3) The controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with this Chapter.*

**Commentary** – [DPA Part 3 Section 34](http://www.legislation.gov.uk/ukpga/2018/12/section/34) introduces the six data protection principles governing the processing of personal data for law enforcement purposes. Chief Officers are under an obligation to comply with those by virtue of DPA Part 3 Section 34(3), and must be able to demonstrate compliance with the principles.

The principles are similar to the first, second, third, fourth, fifth and seventh principles in the 1998 Act. The equivalents of sixth and eighth principles of the 1998 Act are covered by DPA Part 3 Sections 43 to 54 (rights) and DPA Part 3 Sections 72 to 78.

The ICO has issued guidance introducing the law enforcement principles which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib1).

### First Law Enforcement Principle – Lawful & Fair Processing (DPA Part 3 Section 35)

[DPA Part 3 Section 35 The first data protection principle](http://www.legislation.gov.uk/ukpga/2018/12/section/35) states:

*(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.*

*(2) The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either—*

*(a) the data subject has given consent to the processing for that purpose, or*

*(b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority.*

*(3) In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).*

*(4) The first case is where—*

*(a) the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and*

*(b) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).*

*(5) The second case is where—*

*(a) the processing is strictly necessary for the law enforcement purpose,*

*(b) the processing meets at least one of the conditions in* [*Schedule 8*](http://www.legislation.gov.uk/ukpga/2018/12/schedule/8)*, and*

*(c) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).*

DPA Part 3 Section 35 Paragraphs 6 & 7 are not relevant to policing. DPA Part 3 Section 35 concludes:

*(8) In this section, “sensitive processing” means—*

*(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;*

*(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;*

*(c) the processing of data concerning health;*

*(d) the processing of data concerning an individual’s sex life or sexual orientation.*

**Commentary** – [DPA Part 3 Section 35](http://www.legislation.gov.uk/ukpga/2018/12/section/35) sets out the First Law Enforcement Principle which requires that law enforcement processing must be “lawful and fair”. In contrast to the First General Data Protection Principle, there is no requirement for personal data to be processed in a transparent manner. The [Explanatory Notes](http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf) for the Act set out why: *“180…This omission recognises the inherent sensitivities of processing for the law enforcement purposes by competent authorities, particularly where transparency would undermine or compromise covert techniques and capabilities, and/or sensitive or covert operations including, for example, where investigatory powers under the Regulation of Investigatory Powers Act 2000 or Investigatory Powers Act 2016 are engaged…”*

“Lawful” means processing authorised by statute, common law or royal prerogative. Paragraph 181 of the [Explanatory Notes](http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf) for the Act give the examples of Part 5 of the Police and Criminal Evidence Act 1984 (in England and Wales, this authorises the taking and retention of DNA and fingerprints) and the Domestic Violence Disclosure Scheme (this relies on the police’s common law powers to disclose information, where necessary, to prevent crime).

The requirement to process data fairly does not prevent the police from carrying out, for example, covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences as long as they comply with the law – for example, covert surveillance carried out under part 2 of the Regulation of Investigatory Powers Act 2000.

DPA Part 3 Section 35 uses the term “sensitive processing” (as defined in subsection (8)) and subsections (4) and (5) specify the two circumstances when sensitive processing may take place for law enforcement purposes – these are explored in 6.2.2.1 below.

The ICO has issued guidance on the first law enforcement principle which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2).

#### Schedule 8 Conditions for Sensitive Processing Under Part 3 (Schedule 8)

[DPA Schedule 8 Conditions for sensitive processing under part 3](http://www.legislation.gov.uk/ukpga/2018/12/schedule/8) states:

***Statutory etc purposes***

*1 This condition is met if the processing—*

*(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and*

*(b) is necessary for reasons of substantial public interest.*

***Administration of justice***

*2 This condition is met if the processing is necessary for the administration of justice.*

***Protecting individual’s vital interests***

*3 This condition is met if the processing is necessary to protect the vital interests of the data subject or of another individual.*

***Safeguarding of children and individuals at risk***

*4 (1) This condition is met if –*

*(a) the processing is necessary for the purposes of—*

*(i) protecting an individual from neglect or physical, mental or emotional harm, or*

*(ii) protecting the physical, mental or emotional well-being of an individual,*

*(b) the individual is—*

*(i) aged under 18, or*

*(ii) aged 18 or over and at risk,*

*(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and*

*(d) the processing is necessary for reasons of substantial public interest.*

*(2) The reasons mentioned in sub-paragraph (1)(c) are—*

*(a) in the circumstances, consent to the processing cannot be given by the data subject;*

*(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;*

*(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in subparagraph (1)(a).*

*(3) For the purposes of this paragraph, an individual aged 18 or over is “at risk” if the controller has reasonable cause to suspect that the individual—*

*(a) has needs for care and support,*

*(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and*

*(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.*

*(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.*

***Personal data already in the public domain***

*5 This condition is met if the processing relates to personal data which is manifestly made public by the data subject.*

***Legal claims***

*6 This condition is met if the processing—*

*(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),*

*(b) is necessary for the purpose of obtaining legal advice, or*

*(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.*

***Judicial acts***

*7 This condition is met if the processing is necessary when a court or other judicial authority is acting in its judicial capacity.*

***Preventing fraud***

*8 (1) This condition is met if the processing—*

*(a) is necessary for the purposes of preventing fraud or a particular kind of fraud, and*

*(b) consists of—*

*(i) the disclosure of personal data by a competent authority as a member of an anti-fraud organisation,*

*(ii) the disclosure of personal data by a competent authority in accordance with arrangements made by an anti-fraud organisation, or*

*(iii) the processing of personal data disclosed as described in subparagraph*

*(2) In this paragraph, “anti-fraud organisation” has the same meaning as in section 68 of the Serious Crime Act 2007.*

***Archiving etc***

*9 This condition is met if the processing is necessary—*

*(a) for archiving purposes in the public interest,*

*(b) for scientific or historical research purposes, or*

*(c) for statistical purposes.*

**Commentary** – Sensitive processing can take place for law enforcement purposes when the data subject has given consent to the processing (DPA Part 3 Section 35(4)) or if the processing is “strictly necessary” for one or more of the purposes set out in DPA Schedule 8.

In both of the above cases, the police force must have an “appropriate policy” in place ([DPA Part 3 Section 42](http://www.legislation.gov.uk/ukpga/2018/12/section/42) sets out what these should include – [see 6.7](#_Toc510348039)). Paragraph 184 of the [Explanatory Notes](http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf) for the Act point out that the Article 29 Working Party has said that “strictly necessary” has to be understood: *“as a call to pay particular attention to the necessity principle in the context of processing special categories of data, as well as to foresee precise and particularly solid justifications for the processing of such data.”*

Although the DPA provides consent from a data subject as a grounds for sensitive processing of their personal data the likelihood is, bearing mind the possibility of consent being withdrawn, that in all but the most exceptional circumstances the alternative approach of meeting one of the DPA Schedule 8 conditions is likely to be adopted by police forces.

The necessary condition for crime prevention and investigation is likely to be found at condition 1 where the police’s common law power which underpins the policing purpose naturally achieves the public interest requirement at condition 1(b). Where an investigation proceeds to prosecution condition 2 (Administration of Justice) is likely to apply.

Condition 3 (Protecting individual’s vital interests) will often apply to missing persons inquiries or work with vulnerable people.

Condition 4 (Safeguarding of children and individuals at risk) will apply to child abuse, domestic abuse, and other public protection activities.

Condition 5 (Personal data already in the public domain) is perhaps the condition least likely to be used by the police.

Condition 6 (Legal claims) can apply to criminal legal proceedings, police liaison with the Crown Prosecution Service, Public Prosecution Service for Northern Ireland, and the Crown Office and Procurator Fiscal Service.

Condition 7 (Judicial acts) is unlikely to apply to policing, while condition 8 (preventing fraud) will be pertinent to fraud investigations.

Condition 9 (Archiving etc) will most often apply in relation to the retention of information of potential historic interest, and criminological and other research.

The ICO has issued guidance on sensitive processing which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib3) and [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib4).

### Second Law Enforcement Principle – Specific, explicit & legitimate purpose (DPA Part 3 Section 36)

[DPA Part 3 Section 36 The second data protection principle](http://www.legislation.gov.uk/ukpga/2018/12/section/36) states:

*(1) The second data protection principle is that—*

*(a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and*

*(b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.*

*(2) Paragraph (b) of the second data protection principle is subject to subsections (3) and (4).*

*(3) Personal data collected for a law enforcement purpose may be processed for any other law enforcement purpose (whether by the controller that collected the data or by another controller) provided that—*

*(a) the controller is authorised by law to process the data for the other purpose, and*

*(b) the processing is necessary and proportionate to that other purpose.*

*(4) Personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law.*

**Commentary** – This Law Enforcement Principle requires personal data to be processed for “specified, explicit and legitimate” law enforcement purposes - one or more of the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security.

This personal data can be processed for a different law enforcement purpose than the initial one as long as the purpose is lawful, proportionate and necessary. Paragraph 185 of the [Explanatory Notes](http://www.legislation.gov.uk/ukpga/2018/12/notes) for the Act give the following example: *“…the Crown Prosecution Service could process personal data in connection with the prosecution of a criminal offence, whereas the police working alongside the prosecutor would be processing the personal data in connection with the investigation of the offence…”*

The ICO has issued guidance on the second law enforcement principle which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib5).

### Third Law Enforcement Principle – Adequate, relevant & not excessive (DPA Part 3 Section 37)

#### Introduction

[DPA Part 3 Section 37 The third data protection principle](http://www.legislation.gov.uk/ukpga/2018/12/section/37) states:

*The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.*

**Commentary** – This Law Enforcement Principle requires the police to identify the minimum amount of personal data that is required in order properly to fulfil their purpose(s). That personal data must also be adequate for the purpose(s). Clearly there is a crucial requirement to first define the purpose(s) of the processing in order to meet these obligations.

The police will regularly monitor compliance with this principle as changes in circumstances or failure to keep the information up-to-date may mean that personal data that was originally compliant becomes non-compliant. Notwithstanding the Act there will be significant practical operational benefits for the police if the personal data it processes is adequate, relevant and not excessive.

Irrelevant data is also likely to be viewed as excessive.

For additional commentary on the police’s approach to ‘data quality’ see 4.2.9 above.

#### Adequacy

**Commentary** - All personal data processed by the police must be sufficient for the purpose(s) for which it is used or likely to be used. The personal data must be clear in meaning and sufficient for others to understand at the present time and in the future.

Those creating personal data must ensure that it is adequate, unambiguous and professionally worded. Opinions must be distinguishable from matters of fact.

The police force must ensure that appropriate measures are put in place to ensure that personal data held on police systems used for Law Enforcement Processing and relating to one individual cannot be confused with that of another individual with the same name.

Adequacy will also be achieved through the use of common data standards which may mean, for example, that the police record home addresses, descriptive information and other personal data in a format which assists interoperability of, and transfer between, different police information systems.

#### Relevance & Excessiveness

**Commentary** - To establish relevance, a necessity test will identify the minimum amount of personal data that is required to achieve the specific purpose(s).

Some processing operations, such as those necessary for a major crime investigation, may require the use of a great deal of a suspect’s data subject’s personal data. In other circumstances only a minimal amount may be necessary.

It is excessive to hold a class of data on all individuals where that particular item of data is only relevant in certain individual cases.

The police will adopt practices to ensure that personal data that fails to meet the requisite criteria for relevancy is either brought up to those criteria, or rejected. When determining relevance consideration must be given to the necessity and proportionality of processing the personal data.

Personal data must not be excessive in relation to the purpose for which it is held. It is difficult to argue that irrelevant information is not also excessive information.

If personal data is kept for longer than necessary (see fifth Law Enforcement Principle at 6.2.7 below) then it is likely to be both irrelevant and excessive.

The ICO has issued guidance on the third, fourth and fifth law enforcement principles which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib6).

As a result of concerns over excessive processing of data within police Gangs Matrixes the ICO has issued a checklist to assit forces which may be found [here](https://ico.org.uk/for-organisations/in-your-sector/police-justice/processing-gangs-information-a-checklist-for-police-forces/).

### Fourth Law Enforcement Principle – Accurate & kept-up-to-date where necessary (DPA Part 3 Section 38)

#### Introduction

[DPA Part 3 Section 38 The fourth data protection](http://www.legislation.gov.uk/ukpga/2018/12/section/38) principle states:

*(1) The fourth data protection principle is that—*

*(a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and*

*(b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.*

*(2) In processing personal data for any of the law enforcement purposes, personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments.*

*(3) In processing personal data for any of the law enforcement purposes, a clear distinction must, where relevant and as far as possible, be made between personal data relating to different categories of data subject, such as—*

*(a) persons suspected of having committed or being about to commit a criminal offence;*

*(b) persons convicted of a criminal offence;*

*(c) persons who are or may be victims of a criminal offence;*

*(d) witnesses or other persons with information about offences.*

*(4) All reasonable steps must be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes.*

*(5) For that purpose—*

*(a) the quality of personal data must be verified before it is transmitted or made available,*

*(b) in all transmissions of personal data, the necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of the data and the extent to which it is up to date must be included, and*

*(c) if, after personal data has been transmitted, it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.*

**Commentary** - As with the Third Law Enforcement Principle, compliance with the Fourth Law Enforcement Principle has obvious operational and public confidence benefits for the police.

The principle, which is far more comprehensive than its GDPR/DPA Part 2 equivalent has several key elements, requiring that:

* The personal data is accurate and there is a distinction as far as is possible between fact-based and opinion-based personal data.
* The personal data is kept up-to-date ‘where necessary’.
* Where relevant and as far as is possible the personal data provides a distinction between suspects, offenders, victims (included alleged victims), and witnesses or other people with information about offences.
* Reasonable steps are taken to ensure inaccurate data is erased or rectified without delay having considered the purpose of the processing.
* Reasonable steps are taken to ensure inaccurate, incomplete or out-of-date personal data is not transmitted or made available, and if the transmission turns out to be incorrect or unlawful the recipient must be notified without delay.

These elements are covered in more detail within the remainder of 6.2.5.

For additional guidance on ‘data quality’ see 4.2.9 above.

#### Accurate, Distinction between Fact and Opinion

**Commentary** – [DPA Part 3 Section 38(1)(a)](http://www.legislation.gov.uk/ukpga/2018/12/section/38) includes the requirement that personal data processed for law enforcement purposes is accurate. [DPA Part 7 Section 205 General interpretation](http://www.legislation.gov.uk/ukpga/2018/12/section/205) contains the following useful definition: *“inaccurate”, in relation to personal data, means incorrect or misleading as to any matter of fact.*

[DPA Part 3 Section 38(2)](http://www.legislation.gov.uk/ukpga/2018/12/section/38) requires that as far as is possible personal data based on facts must be distinguished from that based on personal assessments.

Personal data that is presented as an opinion and does not claim to be fact cannot be challenged on the grounds of inaccuracy.The [Explanatory Notes](http://www.legislation.gov.uk/ukpga/2018/12/notes) issued with the Act usefully state: *“In the law enforcement context, the principle of accuracy of data must take account of the circumstances in which data is being processed. It is accepted that, for example, statements by victims and witnesses containing personal data will be based on the subjective perceptions of the person making the statement. Such statements are not always verifiable and are subject to challenge during the legal process. In such cases, the requirement for accuracy would not apply to the content of the statement but to the fact that a specific statement has been made.”*

This Law Enforcement Principle requires that great care must be exercised in the collection of personal data. All personnel, when recording personal data, must ensure that it is accurately recorded and where desirable its source is readily available. Where there is any doubt regarding accuracy, information must be clarified with the source where possible and where such clarification would not prejudice law enforcement purposes.

The police force must adopt procedures to prevent factual inaccuracies being entered onto police information systems. This may be achieved by:

* Ensuring as far as possible that the source of the personal data is reliable;
* Taking steps to verify the personal data, if possible, with another source or if reasonable, with the data subject, at the time of collection or at another convenient opportunity;
* Using automatic validation procedures to ensure procedures for data entry and the information system itself does not introduce inaccuracies;
* Using constrained fields in computer databases.

#### Kept Up-to-date

**Commentary** –DPA Part 3 Section 38(1)(a) includes the requirement that personal data processed for law enforcement purposes must be kept up-to-date, but this is qualified in that updating is only required ‘where necessary’.

The purpose for which the personal data is held or used will be relevant in deciding whether such updating is necessary. If the personal data is intended to be used merely as an ‘historical’ record or snap shot in time then updating would be inappropriate. Updating could involve either replacing older personal data with equivalent newer personal data or through appending the newer personal data to the older personal data. The latter approach is likely to be used where the police become aware of an offender’s new home address, but there remains an operational requirement to maintain records of their previous addresses.

When determining whether or not an item of personal data requires updating personnel may consider the following:

* Is there a record of when the personal data was recorded or last updated?
* Are all those involved with the personal data aware that the personal does not necessarily reflect the current position?
* Are effective steps taken to update the personal data – for example, by checking back at intervals with the original source or with the data subject?
* Is the fact that the personal data is out of date likely to prejudice the purpose of the processing.

#### Distinction between Suspects, Offenders, Victims, Witnesses and Others

**Commentary** – [DPA Part 3 Section 38(1)(b)](http://www.legislation.gov.uk/ukpga/2018/12/section/38) includes the requirement, where relevant and as far as is possible, that personal data provides a distinction between suspects, offenders, victims (included alleged victims), and witnesses or other people with information about offences when processing for law enforcement purposes.

The words ‘where relevant and as far as possible’ mean that this requirement is qualified and may not be necessary in all cases.

The likelihood is that in all but exceptional cases police information systems will readily and clearly identify the status of data subjects within the classifications under this part of the Act. It is also likely that some individuals will be recorded in one or more of the categories depending on the context – for example a convicted person may also the victim of crime.

This requirement is one of many that must considered when police forces develop or update information systems.

#### Erased or Rectified

**Commentary** – [DPA Part 3 Section 38(1)(b)](http://www.legislation.gov.uk/ukpga/2018/12/section/38) places a requirement on police forces to either erase or rectify personal data processed for law enforcement purposes without delay once it has been determined that the information is inaccurate.

*‘*Without delay’ indicates there should be no delay between determining the information is inaccurate and beginning its rectification or erasure.

For additional guidance on ‘data quality’ see 4.2.9 above.

#### Disclosure of Inaccurate, Incomplete or Out-of-date Information

**Commentary** – [DPA Part 3 Section 38(4)](http://www.legislation.gov.uk/ukpga/2018/12/section/38) places a requirement that ‘all reasonable steps’ must be taken to ensure that inaccurate, incomplete or not up-to-date is not transmitted or made available for any of the law enforcement purposes. ‘All reasonable steps’ are not defined, but any determination of reasonableness will consider the nature of the personal data involved, its sensitivity and volume, the processing operations in question, technical or IT capabilities and the potential harm or impact on the data subject, to ensure that the steps taken are proportionate.

[DPA Part 3 Section 38(5)](http://www.legislation.gov.uk/ukpga/2018/12/section/38) expands on this obligation requiring all reasonable steps are taken to verify the quality of personal data before it is shared and to include ‘necessary information’ to allow the recipient to assess the degree of accuracy, completeness and reliability of the information and the extent to which it is up to date. ‘Necessary information’ could potentially be a statement explaining what verification had been conducted, known deficiencies in the data or similar data in the past, the source and the perceived reliability of the personal data, or a reliability grading from a known scale.

Irrespective of the Act police forces ought to ensure the steps required by DPA Part 3 Section 38(4) and (5) are taken for operational purposes.

If it is subsequently discovered that the personal data shared is incorrect or unlawful the recipient must be notified of that fact without delay. The Act is silent on whether such a notification should or should not be in writing, but police best practice is to make a written notification in addition to or instead of a verbal one.

For additional guidance on ‘data quality’ see 4.2.9 above.

The ICO has issued guidance on the third, fourth and fifth law enforcement principles which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib6).

### Fifth Law Enforcement Principle – Kept no longer than is necessary (DPA Part 3 Section 39)

[DPA Part 3 Section 39 The fifth data protection principle](http://www.legislation.gov.uk/ukpga/2018/12/section/39) states:

*(1) The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.*

*(2) Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.*

**Commentary** – [DPA Part 3 Section 39](http://www.legislation.gov.uk/ukpga/2018/12/section/39) requires the police to identify which of the law enforcement purposes applies and once that purpose has been concluded the police will either cease processing the personal data (usually through its secure disposal, deletion or destruction), or will de-personalise it in such a way that it is no longer personal data or able to be ‘reformed’ into personal data. The police are likely, for practical purposes, to follow the former rather than the latter and adopt a policy of regular review of personal data to establish whether it is still required and dispose as necessary. The principle also requires periodic review of the need to retain personal data.

Within police forces a systematic approach will be followed including the definition of review periods for particular categories of documents or information containing personal data. At the end of such periods they will be reviewed and disposed of if no longer required.

Police forces may need to consider certain statutory requirements which may specify required retention periods, or the potential value of some personal data and other information which may suggest further retention for historic purposes.

On a practical level within police forces information asset owners must ensure that review and ‘disposal where necessary’ procedures are adopted for systems within their control which apply to both computer and manually-held personal data. However, information asset owners must exercise care, particularly with regards to personal data held on computer equipment, to ensure that disposal does mean permanent and complete deletion and that there is no risk of the personal data being ‘reformed’ or retrieved.

Whatever standard periods are adopted, police forces must maintain a flexible approach towards retention issues which allow individual cases to be assessed properly and proportionate decisions reached regarding retention. This can be achieved through the adoption of exceptional case review procedures and through chief officers, in their capacity as ‘controllers’, retaining the right and responsibility to make individual judgements where appropriate.

Some personal data processed for law enforcement purposes falls under the scope of the [Code of Practice on the Management of Police Information](http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf) and the supporting guidance that has been published by the College of Policing as [Authorised Professional Practice Management of Police Information.](https://www.app.college.police.uk/app-content/information-management/management-of-police-information/) The latter includes a framework to manage the retention, review and disposal of police information and where police forces follow that guidance they will comply with the Fifth Law Enforcement Principle.

The standard retention periods for personal data which falls outside the scope of the Authorised Professional Practice Management of Police Information must be documented by police forces, and as far as is possible consistent standard retention periods should be adopted by all police forces. Any such documentation should set out the circumstances in which deviation from the standard retention period, resulting in either shorter or longer retention, is permissible.

The ICO has issued guidance on the third, fourth and fifth law enforcement principles which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib6).

The police force must implement appropriate measures to resolve data quality disputes or complaints regarding the retention or otherwise of personal data.

### Sixth Law Enforcement Principle – Processed securely (DPA Part 3 Section 40, Section 66)

[DPA Part 3 Section 40 The sixth data protection principle](http://www.legislation.gov.uk/ukpga/2018/12/section/40) states:

*The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).*

[DPA Part 3 Section 66 Security of processing](http://www.legislation.gov.uk/ukpga/2018/12/section/66) states:

*(1) Each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data.*

*(2) In the case of automated processing, each controller and each processor must, following an evaluation of the risks, implement measures designed to—*

*(a) prevent unauthorised processing or unauthorised interference with the systems used in connection with it,*

*(b) ensure that it is possible to establish the precise details of any processing that takes place,*

*(c) ensure that any systems used in connection with the processing function properly and may, in the case of interruption, be restored, and*

*(d) ensure that stored personal data cannot be corrupted if a system used in connection with the processing malfunctions.*

**Commentary** – [DPA Part 3 Section 40](http://www.legislation.gov.uk/ukpga/2018/12/section/40) and [DPA Part 3 Section 66](http://www.legislation.gov.uk/ukpga/2018/12/section/66) require the police to process personal data in a secure manner.

The key aspect is the requirement to ensure that personal data is protected according to the risk. Risks will need to be evaluated and appropriate measures implemented.

The ICO’s guidance stipulates that, in practice, this means that police forces must have appropriate security to prevent the personal data they hold being accidentally or deliberately compromised. In particular, the police force will need to:

* design and organise their security to fit the nature of the personal data they hold and the harm that may result from a security breach;
* be clear about who in their organisation is responsible for ensuring information security;
* make sure they have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
* be ready to respond to any breach of security swiftly and effectively.

The NPCC via the Information Assurance Portfolio, which reports to IMORCC, has developed extensive guidance and policy around information security (also known as information assurance) and police forces should comply with that material.

The ICO has issued guidance on the sixth law enforcement principles which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib7).

The Data Protection Officer and colleagues responsible for information security/assurance must maintain effective working relationships with one another to ensure matters of mutual interest are dealt with appropriately.

#### Data Breach Reporting (DPA Part 3 Section 67 & Section 68) (Appendix C)

[DPA Part 3 Section 67 Notification of a personal data breach to the Commissioner](http://www.legislation.gov.uk/ukpga/2018/12/section/67) states:

*(1) If a controller becomes aware of a personal data breach in relation to personal data for which the controller is responsible, the controller must notify the breach to the Commissioner—*

*(a) without undue delay, and*

*(b) where feasible, not later than 72 hours after becoming aware of it.*

*(2) Subsection (1) does not apply if the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals.*

*(3) Where the notification to the Commissioner is not made within 72 hours, the notification must be accompanied by reasons for the delay.*

*(4) Subject to subsection (5), the notification must include—*

*(a) a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;*

*(b) the name and contact details of the data protection officer or other contact point from whom more information can be obtained;*

*(c) a description of the likely consequences of the personal data breach;*

*(d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.*

*(5) Where and to the extent that it is not possible to provide all the information mentioned in subsection (4) at the same time, the information may be provided in phases without undue further delay.*

*(6) The controller must record the following information in relation to a personal data breach—*

*(a) the facts relating to the breach,*

*(b) its effects, and*

*(c) the remedial action taken.*

*(7) The information mentioned in subsection (6) must be recorded in such a way as to enable the Commissioner to verify compliance with this section.*

*(8) Where a personal data breach involves personal data that has been transmitted by or to a person who is a controller under the law of another member State, the information mentioned in subsection (6) must be communicated to that person without undue delay.*

*(9) If a processor becomes aware of a personal data breach (in relation to personal data processed by the processor), the processor must notify the controller without undue delay.*

[DPA Part 3 Section 68 Communication of a personal data breach to the data subject](http://www.legislation.gov.uk/ukpga/2018/12/section/68) states:

*(1) Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller must inform the data subject of the breach without undue delay.*

*(2) The information given to the data subject must include the following—*

*(a) a description of the nature of the breach;*

*(b) the name and contact details of the data protection officer or other contact point from whom more information can be obtained;*

*(c) a description of the likely consequences of the personal data breach;*

*(d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.*

*(3) The duty under subsection (1) does not apply where—*

*(a) the controller has implemented appropriate technological and organisational protection measures which were applied to the personal data affected by the breach,*

*(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in subsection (1) is no longer likely to materialise, or*

*(c) it would involve a disproportionate effort.*

*(4) An example of a case which may fall within subsection (3)(a) is where measures that render personal data unintelligible to any person not authorized to access the data have been applied, such as encryption.*

*(5) In a case falling within subsection (3)(c) (but not within subsection (3)(a) or (b)), the information mentioned in subsection (2) must be made available to the data subject in another equally effective way, for example, by means of a public communication.*

*(6) Where the controller has not informed the data subject of the breach the Commissioner, on being notified under section 67 and after considering the likelihood of the breach resulting in a high risk, may—*

*(a) require the controller to notify the data subject of the breach, or*

*(b) decide that the controller is not required to do so because any of paragraphs (a) to (c) of subsection (3) applies.*

*(7) The controller may restrict, wholly or partly, the provision of information to the data subject under subsection (1) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to—*

*(a) avoid obstructing an official or legal inquiry, investigation or procedure;*

*(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;*

*(c) protect public security;*

*(d) protect national security;*

*(e) protect the rights and freedoms of others.*

*(8) Subsection (6) does not apply where the controller’s decision not to inform the data subject of the breach was made in reliance on subsection (7).*

*(9) The duties in section 52(1) and (2) apply in relation to information that the controller is required to provide to the data subject under this section as they apply in relation to information that the controller is required to provide to the data subject under Chapter 3.*

**Commentary** – A personal data breach could lead to a loss of control over data, limitation of rights, reputational damage and other social or economic disadvantages. Therefore, in the event of a data breach whereby there is a risk to the rights and freedoms of the individual, [DPA Part 3 Section 67](http://www.legislation.gov.uk/ukpga/2018/12/section/67) requires police forces to inform the ICO without undue delay, and where feasible, within 72 hours of becoming aware of it and give details as to how they are mitigating that risk.

When there is a high risk to the rights and freedoms of an individual as a result of a data breach the data subject(s) should also be notified of the data breach in good time so they may take the necessary precautions to protect themselves. The communication should be made as soon as possible relative to the risk, for example if there is an immediate risk of damage a quick response to data subjects would be advisable (this can be a mass communication if applicable).

Given the nature of the data being processed, [DPA Part 3 Section 68](http://www.legislation.gov.uk/ukpga/2018/12/section/68) enables police forces to restrict the data subject’s right by withholding notice of a data breach in certain circumstances where notifying a data subject would reveal the existence of the data to the detriment of an ongoing criminal investigation etc.

[Appendix C](#_Appendix_C:_Personal) to this manual contains specific guidance on the management of police personal data breaches.

The ICO has issued guidance on the law enforcement processing personal data breaches which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/personal-data-breaches/). It includes a useful self-assessment tool to determine whether the ICO should be informed of the breach.

The Data Protection Officer must ensure their police force has appropriate measures in place to identify, manage and mitigate personal data breaches in relation to Law Enforcement Processing.

## Law Enforcement Processing Rights

### Overview

Commentary - The rights that individuals had over their data in the 1998 Act were carried over to the DPA Part 3 with some modifications. These rights are not as extensive as those available under the GDPR/DPA Part 2.

As with the 1998 Act DPA Part 3 recognises that there are some limited circumstances where it is appropriate to create exemptions or restrictions to the usual rights that individuals have over their personal data. These can be found summarised at [6.3.8](#_Summary_table_of).

The DPA Part 3 rights are:

* [Information for Data Subjects (DPA Part 3 Section 44)](#_Information_for_Data)
* [Right of Access (DPA Part 3 Section 45)](#_Right_of_Access)
* [Rights to Rectification, Erasure & Restriction (DPA Part 3 Sections 46 to 48)](#_Rights_to_Rectification,_1)
* [Rights to Automated Decision Making (DPA Part 3 Sections 49 & 50)](#_Rights_re_Automated)
* [Exercise of rights through Commissioner (DPA Part 3 Section 51)](#_Exercise_of_rights)

The rights need to be read in connection with Law Enforcement Processing Rights: Overview & Scope (DPA Part 3 Section 43), and DPA Part 3 Section 44 s 51 to 54.

The ICO has issued guidance on the law enforcement information rights which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/).

### Law Enforcement Processing Rights: Overview & Scope (DPA Part 3 Section 43)

[DPA Part 3 Section 43 Overview and scope](http://www.legislation.gov.uk/ukpga/2018/12/section/43) states:

*(1) This Chapter [3] [DPA Part 3 Sections 43-54] —*

*(a) imposes general duties on the controller to make information available (see section 44);*

*(b) confers a right of access by the data subject (see section 45);*

*(c) confers rights on the data subject with respect to the rectification of personal data and the erasure of personal data or the restriction of its processing (see sections 46 to 48);*

*(d) regulates automated decision-making (see sections 49 and 50);*

*(e) makes supplementary provision (see sections 51 to 54).*

*(2) This Chapter applies only in relation to the processing of personal data for a law enforcement purpose.*

*(3) But sections 44 to 48 do not apply in relation to the processing of relevant personal data in the course of a criminal investigation or criminal proceedings, including proceedings for the purpose of executing a criminal penalty.*

*(4) In subsection (3), “relevant personal data” means personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority.*

*(5) In this Chapter, “the controller”, in relation to a data subject, means the controller in relation to personal data relating to the data subject.*

**Commentary** – [DPA Part 3 Section 43](http://www.legislation.gov.uk/ukpga/2018/12/section/43) gives an introduction to data subjects’ law enforcement processing rights and the obligations on police forces to facilitate the exercise of those rights which concern access, rectification, erasure or restriction of processing. It does not extend to rights regarding automated decision-making.

**Exemption/Restriction** – [DPA Part 3 Section 43(3) & (4)](http://www.legislation.gov.uk/ukpga/2018/12/section/43) mean that those rights do not apply in relation to the processing of “relevant personal data” in the course of a criminal investigation or criminal proceedings where the judge or other judicial authority is controller of the personal data and it is contained in a judicial decision or in other documents which are created during a criminal investigation or proceedings and made by or on behalf of the judge or judicial authority. Subsection (4) defines “relevant personal data” – that definition does not encompass police investigations and cases prior to their submission to court when they are being processed by the police. [need a legal view on this point]

As an alternative, access to “relevant personal data” is managed in accordance with the appropriate legislation covering the disclosure of information in criminal proceedings, such as (in England and Wales) the Criminal Procedure and Investigations Act 1996. Where a police force is commissioned by a court or other judicial authority to create a document DPA Part 3 Section 43(3) extends to that document and the personal data contained within it. The original personal data processed by the police force used to inform the document will remain subject to the provisions in [DPA Part 3 Section 44](http://www.legislation.gov.uk/ukpga/2018/12/section/44), [Section 45](http://www.legislation.gov.uk/ukpga/2018/12/section/45), [Section 46](http://www.legislation.gov.uk/ukpga/2018/12/section/46), [Section 47](http://www.legislation.gov.uk/ukpga/2018/12/section/47) and [Section 48](http://www.legislation.gov.uk/ukpga/2018/12/section/48).

The ICO has issued guidance on the law enforcement information rights which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/).

### Information for Data Subjects (DPA Part 3 Section 44) (Appendix G & Appendix N)

[DPA Part 3 Section 44 Information: controller’s general duties](http://www.legislation.gov.uk/ukpga/2018/12/section/44) commences:

*(1) The controller must make available to data subjects the following information (whether by making the information generally available to the public or in any other way)—*

*(a) the identity and the contact details of the controller;*

*(b) where applicable, the contact details of the data protection officer (see sections 69 to 71);*

*(c) the purposes for which the controller processes personal data;*

*(d) the existence of the rights of data subjects to request from the controller—*

*(i) access to personal data (see section 45),*

*(ii) rectification of personal data (see section 46), and*

*(iii) erasure of personal data or the restriction of its processing (see section 47);*

*(e) the existence of the right to lodge a complaint with the Commissioner and the contact details of the Commissioner.*

**Commentary** – [DPA Part 3 Section 44](http://www.legislation.gov.uk/ukpga/2018/12/section/44) imposes general duties on police forces in respect of the provision of information to data subjects. DPA Part 3 Section 44 (1) sets out a minimum list of information that must be available to the public – i.e. not just data subjects. Such generic information may be provided through a police force’s website and police forces are encouraged to comply with the ICO’s [Privacy Notices Code of Practice](https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/).

In addition, it should be provided to any data subject exercising their DPA Part 3 rights.

A template for a High-Level Privacy Notice can be found at Appendix G and Lower-Level Specific Privacy Notice for Law Enforcement Processing can be found at Appendix N.

**Exemption/Restriction** – None exist to DPA Part 3 Section 44(1).

The ICO has issued guidance on the law enforcement information rights which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/).

The police force should develop and maintain a standard document meeting the requirements of DPA Part 3 Section 44(1) (Information for Data Subjects).

[DPA Part 3 Section 44](http://www.legislation.gov.uk/ukpga/2018/12/section/44) continues:

*(2) The controller must also, in specific cases for the purpose of enabling the exercise of a data subject’s rights under this Part [3], give the data subject the following—*

*(a) information about the legal basis for the processing;*

*(b) information about the period for which the personal data will be stored or, where that is not possible, about the criteria used to determine that period;*

*(c) where applicable, information about the categories of recipients of the personal data (including recipients in third countries or international organisations);*

*(d) such further information as is necessary to enable the exercise of the data subject’s rights under this Part.*

*(3) An example of where further information may be necessary as mentioned in subsection (2)(d) is where the personal data being processed was collected without the knowledge of the data subject.*

*(4) The controller may restrict, wholly or partly, the provision of information to the data subject under subsection (2) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to—*

*(a) avoid obstructing an official or legal inquiry, investigation or procedure;*

*(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;*

*(c) protect public security;*

*(d) protect national security;*

*(e) protect the rights and freedoms of others.*

**Commentary** – [DPA Part 3 Section 44(2)](http://www.legislation.gov.uk/ukpga/2018/12/section/44) sets out additional information which a police force must provide in specific cases to a data subject to enable the data subject to exercise his or her rights under DPA Part 3, most often in a case where the personal data was collected without the knowledge of the data subject (Subsection (3)).

**Exemption/Restriction** - The requirement is qualified and DPA Part 3 Section 44(4) sets out grounds when a restriction may be applied by the police.

The grounds most relevant to the police are:

* 4(b) which permits the police to disregard DPA Part 3 Section 44(2) if not doing so would be likely to prejudice prevention, detection, investigation or prosecution of criminal offences – this would typically be the case in relation to intelligence material collected by the police to the ignorance of the data subject, or where disclosure would reveal sensitive policing techniques or operations
* 4(e) which permits the police to disregard DPA Part 3 Section 44(2) where necessary to protect the rights and freedoms of others – this will typically be used to protect the identities of other people whose personal data was intertwined with that of the requestor/data subject.

In either case the outcome will usually be the complete or partial restriction of the right in question.

It is not clear whether the Subsection (2) obligations (restricted as necessary) should be applied proactively in the advance of any rights applications or reactively by police forces when rights are sought.

[DPA Part 3 Section 44](http://www.legislation.gov.uk/ukpga/2018/12/section/44) continues:

*(5) Where the provision of information to a data subject under subsection (2) is restricted, wholly or partly, the controller must inform the data subject in writing without undue delay—*

*(a) that the provision of information has been restricted,*

*(b) of the reasons for the restriction,*

*(c) of the data subject’s right to make a request to the Commissioner under section 51,*

*(d) of the data subject’s right to lodge a complaint with the Commissioner, and*

*(e) of the data subject’s right to apply to a court under section 167.*

*(6) Subsection (5)(a) and (b) do not apply to the extent that complying with them would undermine the purpose of the restriction.*

**Commentary** – [DPA Part 3 Section 44(5)](http://www.legislation.gov.uk/ukpga/2018/12/section/44) places an obligation on the police to confirm whether a restriction to Subsection (2) has been applied and other information to the data subject.

**Exemption/Restriction** - Again this is conditional and by virtue of DPA Part 3 Section 44(6) which allows Subsection (5)(a) and (b) to be disregarded to the extent necessary to prevent the restriction being undermined. It is interesting to note that there is no relief available from DPA Part 3 Section 44(5)(c),(d) or (e).

[DPA Part 3 Section 44](http://www.legislation.gov.uk/ukpga/2018/12/section/44) concludes:

*(7) The controller must—*

*(a) record the reasons for a decision to restrict (whether wholly or partly) the provision of information to a data subject under subsection (2), and*

*(b) if requested to do so by the Commissioner, make the record available to the Commissioner.*

**Commentary** – DPA Part 3 Section 44(6) requires police forces to record the rationale for any use of restrictions of Subsection (2) and provide that information to the ICO upon request.

Police forces must therefore ensure that in all cases where such a restriction is employed a written rationale is maintained within its records.

The ICO has issued guidance on the law enforcement processing right to be informed which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/).

The Data Protection Officer must monitor their police forces’ compliance with the DPA Part 3 Section 44 (Information for Data Subjects) obligations and make any necessary interventions.

### Right of Access (DPA Part 3 Section 45)

[DPA Part 3 Section 45 Right of access by the data subject](http://www.legislation.gov.uk/ukpga/2018/12/section/45) commences:

*(1) A data subject is entitled to obtain from the controller—*

*(a) confirmation as to whether or not personal data concerning him or her is being processed, and*

*(b) where that is the case, access to the personal data and the information set out in subsection (2).*

**Commentary** – [DPA Part 3 Section 45](http://www.legislation.gov.uk/ukpga/2018/12/section/45) must be read in connection with [DPA Part 3 Section 43](http://www.legislation.gov.uk/ukpga/2018/12/section/43), [Section 44](http://www.legislation.gov.uk/ukpga/2018/12/section/44) and [Section 52](http://www.legislation.gov.uk/ukpga/2018/12/section/52).

DPA Part 3 Section 45(1) provides data subject with the right to be:

* informed whether a police force is processing their personal data,
* be provided access to that personal data, and
* be provided with additional information set out in the subsequent subsection

[DPA Part 6 Section 173](http://www.legislation.gov.uk/ukpga/2018/12/section/173) makes it an offence is to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the data subject would have been entitled to receive under this right.

**Exemption/restriction** - all of which may be restricted by the provisions set out at DPA Part 3 Section 45(4) (see below). In addition, [DPA Part 3 Section 52](http://www.legislation.gov.uk/ukpga/2018/12/section/52) sets out requirements concerning the form of the provision of information under the right of access.

[DPA Part 3 Section 45](http://www.legislation.gov.uk/ukpga/2018/12/section/45) continues:

*(2) That information is—*

*(a) the purposes of and legal basis for the processing;*

*(b) the categories of personal data concerned;*

*(c) the recipients or categories of recipients to whom the personal data has been disclosed (including recipients or categories of recipients in third countries or international organisations);*

*(d) the period for which it is envisaged that the personal data will be stored or, where that is not possible, the criteria used to determine that period;*

*(e) the existence of the data subject’s rights to request from the controller—*

*(i) rectification of personal data (see section 46), and*

*(ii) erasure of personal data or the restriction of its processing (see section 47);*

*(f) the existence of the data subject’s right to lodge a complaint with the Commissioner and the contact details of the Commissioner;*

*(g) communication of the personal data undergoing processing and of any available information as to its origin.*

**Commentary** – The information required (subject to restrictions) under this subsection include from (a) to (d) information likely to be specific to the particular processing operation(s) being employed by the police force with regard to the data subject’s personal data, and from (e) to (g) generic information applicable to all processing by the police force.

Historically the right of access has been seen primarily as a right to obtain a copy of personal data being processed, with lesser emphasis on the information set out under this subsection. However, police forces must comply with the subsection should the data subject’s application encompass them. In the spirit of transparency required by the Act police forces are encouraged to develop right of access application forms\* that allow applicants to specifically request some or all of the information required by this subsection, as well as allowing applications to the personal data itself.

\*there is no obligation for applicants to use right of access application forms, indeed applications can be made verbally, but the NPCC’s position is that such forms allow applicants to fully understand their rights as well as assisting in the administration of the application.

[DPA Part 3 Section 45](http://www.legislation.gov.uk/ukpga/2018/12/section/45) continues:

*(3) Where a data subject makes a request under subsection (1), the information to which the data subject is entitled must be provided in writing —*

*(a) without undue delay, and*

*(b) in any event, before the end of the applicable time period (as to which see section 54).*

**Commentary** – This subsection requires police forces to commence work on a right of access application as and complete that work as soon as possible, and within the time period required by DPA Part 3 Section 54, usually one month (see [6.3.6.4](#_Applicable_Time_Period)). [DPA Part 7 Section 205 General interpretation](http://www.legislation.gov.uk/ukpga/2018/12/section/205) confirms that the definition of month in respect of this right is that set out in [Article 3 of Regulation (ECC, Euratom) No. 1182/71 of the Council of 3rd June 1971](file:///C:\Users\42006032\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\AppData\Local\Temp\DOC_1.en.xhtml).

The police force must adopt appropriate measures to ensure that Right of Access applications are sent to their teams processing such applications without delay and this requires the police forces to make all staff and officers aware of the right, the requirement for no delay, and the team to which such applications must be sent.

The police force must that records must be kept of the date of receipt of any Right of Access request and the consequential statutory deadline, and appropriate measures must be adopted to monitor progress to ensure any delay is mitigated. If the statutory deadline is likely to be missed police forces must communicate that fact at the earliest opportunity to the applicant.

[DPA Part 3 Section 45](http://www.legislation.gov.uk/ukpga/2018/12/section/45) continues:

*(4) The controller may restrict, wholly or partly, the rights conferred by subsection (1) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to—*

*(a) avoid obstructing an official or legal inquiry, investigation or procedure;*

*(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;*

*(c) protect public security;*

*(d) protect national security;*

*(e) protect the rights and freedoms of others.*

**Exemption/Restriction** – This subsection allows police forces to restrict the rights under Subsection (1) in certain circumstances set out at (a) to (e). It is important to note that the restrictions can only be applied as far as is necessary and can only be applied as long as is necessary. Consequently a blanket application of the restriction to all of an applicant’s personal data or permanent application of the restriction are not permitted.

On the latter point it is often the case that personal data collected without the knowledge of the data subject who is a suspect in an investigation needs to be initially protected from disclosure to them to avoid prejudicing the investigation while the investigation is proceeding, but at a later date there would be no harm in disclosure if the personal data had been disclosed to the individual during interview.

Police forces must adopt processes that ensure the application of these restrictions is only to the extent required and is only for the necessary duration.

The following are provided as examples of when each of the restrictions are likely to be engaged:

*(a) avoid obstructing an official or legal inquiry, investigation or procedure*

This is likely to be relevant to personal data processed for inquests, family court proceedings, non-criminal internal discipline enquiries, and inquiries such as the Independent Inquiry into Child Sexual Abuse.

*(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties*

This is likely to be relevant to the following police activities: crime prevention, all criminal investigations (including those by police force Professional Standards Departments), criminal prosecutions, vetting of staff, officers and others working for or on behalf of the police force; and would encompass some or all personal data processed within intelligence, crime management, case and custody information systems.

*(c) protect public security*

The term ‘public security’ is not defined in the Act, however, any scenario where this is relevant is likely to be captured by the restriction at (b) immediately above.

*(d) protect national security*

This is likely to be relevant to personal data collected by the police for counter-terrorism purposes. As such the personal data is also likely to be subject of the restriction at (b) and police forces may wish, for operational purposes, to apply the restriction at (b) rather than (d).

*(e) protect the rights and freedoms of others*

This is relevant to personal data that would also relate to other individuals as well as the applicant.

[DPA Part 3 Section 45](http://www.legislation.gov.uk/ukpga/2018/12/section/45) continues:

*(5) Where the rights of a data subject under subsection (1) are restricted, wholly or partly, the controller must inform the data subject in writing without undue delay—*

*(a) that the rights of the data subject have been restricted,*

*(b) of the reasons for the restriction,*

*(c) of the data subject’s right to make a request to the Commissioner under section 51,*

*(d) of the data subject’s right to lodge a complaint with the Commissioner, and*

*(e) of the data subject’s right to apply to a court under section 165.*

*(6) Subsection (5)(a) and (b) do not apply to the extent that the provision of the information would undermine the purpose of the restriction.*

**Commentary** – [DPA Part 3 Section 45(5)](http://www.legislation.gov.uk/ukpga/2018/12/section/45) places an obligation on the police to confirm whether a restriction to Subsection (1) has been applied and other information to the data subject.

**Exemption/Restriction** - Again this is conditional and by virtue of Subsection (6) which allows Subsection (5)(a) and (b) to be disregarded to the extent necessary to prevent the restriction being undermined. It is interesting to note that there is no relief available from Subsections (5)(c),(d) or (e).

[DPA Part 3 Section 45](http://www.legislation.gov.uk/ukpga/2018/12/section/45) concludes:

*(7) The controller must—*

*(a) record the reasons for a decision to restrict (whether wholly or partly) the rights of a data subject under subsection (1), and*

*(b) if requested to do so by the Commissioner, make the record available to the Commissioner.*

**Commentary** – DPA Part 3 Section 45(6) requires police forces to record the rationale for any use of restrictions of Subsection (1) and provide that information to the ICO upon request.

The police force must ensure that in all cases where a restriction is employed in response to a Right of Access application a written rationale is maintained within its records.

#### Law Enforcement Right of Access Considerations

The right of access to personal data held on the Police National Computer is facilitated on behalf of police forces by the [ACRO Criminal Records Office](https://www.acro.police.uk/subject_access.aspx).

[DPA Part 7 Section 186](http://www.legislation.gov.uk/ukpga/2018/12/section/186) sets out that any enactment or rule of law prohibiting or restricting the disclosure of information or authorizing the withholding of information apart from the Act cannot remove or restrict subject rights set out in the GDPR/DPA Part 2 or those under DPA Part 3. Consequently the only restrictions of data subjects’ DPA Part 3 rights which can be used are those set out in the Act.

When handling right of access requests police forces should pay regard to the I[nformation Commissioner’s Subject Access Code of Practice](https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf) and any subsequent replacement, and also consider the contents below following each bold subheadings.

**Verbal requests** - Police forces must adopt appropriate measures to ensure that verbal requests for access are recognised as such when they occur and for them to be progressed without delay. This requires all officers and staff to be adequately trained so that they can recognise a request, obtain any necessary confirmation of identity, be able to record it correctly and know what to do with it. If possible, the data subject should be asked to validate any written record of the request at the time it is made by the police officer or member of staff.

**Confirmation of identity** – A request cannot be regarded as valid until the identity of the requestor/data subject is confirmed. Police forces should develop reasonable measures in this regard, and may choose a proportionate approach and require greater evidence to confirm identity if the request encompasses special categories of personal data. There will be circumstances where the identity of the data subject is already confirmed (e.g. a police employee or detained person) and consequently there is no further requirement to confirm identity. In other cases there will be a need to obtain that confirmation, ideally at the time the request is made. The NPCC does not set out any standard for confirming identity of requestors/data subjects, but typically those individuals should provide documentary evidence of their full name and current address. If they are seeking access to images then provision of a photograph of themselves is likely to be necessary and this may also assist identification.

**Application form** – Although an application form is not required under the GDPR or Act for those exercising their subject rights, it is a useful administrative device for providing a definitive record of any request made that can confirm the scope of the request, assist the processing of the request, and provide useful evidence in cases should a dispute arises between the data subject and police force. An application form has been developed by the NPCC which can be found at 6.3.4.2. It is designed for those exercising their GDPR Article 15/DPA Part 2 and DPA Part 3 right of access.

Police forces are encouraged to make the form available on their websites in prominent positions along with suitable completion guidance, adjacent their privacy notices. Ideally the form should enable requestors/data subjects to complete and submit online or allow them to print it off to be completed and posted to the police force.

Forms that include an optional request for the requestor/data subject to confirm the reason for their request will help identify enforced subject access and potential manifestly unfounded or excessive requests. When designing application forms necessary consideration must be given to disability and diversity requirements

**Sufficient information to locate personal data** – It is in the interests of the data subject/requestor and the police force for there to be sufficient information within the request in order to enable the personal data to be located. Consequently should a request be vague, excessive, unfounded or ambiguous police forces should contact the data subject/requestor to seek necessary clarity or narrowing of the request promptly once the request has been received. The failure of a data subject/requestor to engage in this process may be regarded as evidence to support rejection of a request as manifestly unfounded or excessive.

**Manifestly unfounded or excessive** – see 6.3.8.1 Manifestly Unfounded or Excessive Requests ([DPA Part 3 Section 53](http://www.legislation.gov.uk/ukpga/2018/12/section/53)).

**Timescales** – All requests must be progressed promptly after receipt by a police force and the personal data supplied within one month (subject to below). It is important that this is undertaken so that any issues relating to the request, such as its potential for being manifestly unfounded or excessive, can be readily addressed and any necessary engagement with the data subject carried out. The NPCC’s position is that ‘the clock does not start ticking’ until the identity of the requestor has been confirmed as the data subject, it is clear which elements of the right of access the requestor is exercising, and sufficient information has been provided to search for the information sought.

**Record Keeping** – Police forces must maintain records that provide a record of:

* contact with the data subject/requestor
* searches made to retrieve personal data
* results of those searches
* redactions applied
* any decision-making or rational setting out why exemptions or restrictions have been applied
* the response(s) to the requestor

Such records must be able to withstand ICO and legal scrutiny and should be retained in accordance with the NPCC’s National Retention Schedule.

**Collection/delivery** – If data subject requires a force to deliver their right of access response via a courier, Royal Mail Special Delivery Guaranteed or Royal Mail Signed For, as opposed to Royal Mail First or Second Class the police force is able to charge a delivery fee for that enhanced service which takes into account the price differential from Royal Mail First Class and the cost of any associated administrative work. However, where a police force determines, having considered the nature of the personal data contained in the response, that use of Royal Mail First or Second Class is not an appropriate and that Royal Mail Special Delivery Guaranteed, Royal Mail Signed For, or a courier is the most appropriate means of response then that additional cost should not be passed on to the data subject.

Responses may also be provided via email or through personal collection from designated police premises where requested by the data subject.

**Request via Solicitors** – Police forces may receive requests on behalf of data subjects from solicitors. These should be accepted once the solicitors have provided confirmation that they have confirmed the identity of the data subject/requestor and are acting on behalf of them in respect of the right of access request.

**Requests from children** – GDPR Article 15 is a right afforded to all data subjects including children (those aged 15 years or less for the purposes of this manual and the ICO has provided guidance on acceptance of right of access by or on behalf of a child in its 1998 Act [Subject Access Code of Practice Version 1.2](https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf). The NPCC’s position is that a right of access request received directly from a child should be accepted provided that the police force is content that the child is capable of understanding this right and that the request has been freely made by them. Responses to such requests must go back directly to the child. Where an adult, usually a parent, exercises the right of access of a child a police force should not accept that request if it is not convinced the adult genuinely seeking to exercise the child’s right for the child – in the past there have been instances where estranged parents attempt to misuse the right of access right of their child, with the request actually being made for the benefit of one of the parents, not the child. Responses to such requests may go back to the child or the adult acting on their behalf.

**Joint Controllers** – Police forces acting as joint controllers must ensure that any documentation between them setting out their respective responsibilities under the Act encompasses how a right of access request to personal data that is jointly processed will be managed. It will usually be best practice for the police force that created or originated the personal data, if different from the receiving force, to provide a view on whether any exemptions/restrictions should be applied when providing the response.

**Exemption/Restriction** – [DPA Part 3 Section 44(4)](#Section_44) allows a police force to withhold information under this right concerning the legal basis for processing, retention period, recipients, and rights in five scenarios including in a *necessary and propotionate manner to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties* and *in a necessary and proportionate manner to protect the rights and freedoms of others.*. See [DPA Part 3 Section 44(4)(a to e)](#Section_44) within 6.3.3 above.

The ICO has issued guidance on the law enforcement processing right of access which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/).

The Data Protection Officer must monitor their police force’s compliance with the DPA Part 3 Section 45 Right of Access and make any necessary interventions.

#### Enforced Subject Access

**Commentary** - [DPA Part 7 Section 184](http://www.legislation.gov.uk/ukpga/2018/12/section/184) makes it an offence for an employer to require employees or contractors, or for a person to require another person who provides goods, facilities or services, to provide certain records obtained via subject access requests as a condition of their employment or contract. See 9.4.4 for further details.

### Rights to Rectification, Erasure or Restriction (DPA Part 3 Section 46 & Section 47)

#### Introduction

**Commentary** - DPA Part 3 Sections 46 and 47 enable a data subject to ask for data to be corrected, or erased or the processing restricted, while DPA Part 3 Section 48 sets out provisions applicable to both preceding sections.

#### Right to Rectification (DPA Part 3 Section 46)

[DPA Part 3 Section 46 Right to rectification](http://www.legislation.gov.uk/ukpga/2018/12/section/46) states:

*(1) The controller must, if so requested by a data subject, rectify without undue delay inaccurate personal data relating to the data subject.*

*(2) Where personal data is inaccurate because it is incomplete, the controller must, if so requested by a data subject, complete it.*

*(3) The duty under subsection (2) may, in appropriate cases, be fulfilled by the provision of a supplementary statement.*

*(4) Where the controller would be required to rectify personal data under this section but the personal data must be maintained for the purposes of evidence, the controller must (instead of rectifying the personal data) restrict its processing.*

**Commentary** – [DPA Part 3 Section 46](http://www.legislation.gov.uk/ukpga/2018/12/section/46) allows a data subject to request that a police force rectifies, without undue delay, their personal data known to be inaccurate. No definition is given of ‘undue delay’, nor is a statutory time limit set. However, a definition is provided for ‘inaccurate’ - [DPA Part 7 Section 205 General interpretation](http://www.legislation.gov.uk/ukpga/2018/12/section/205) states that ‘inaccurate’, *in relation to personal data means incorrect or misleading as to any matter of fact.* Personal data that is presented as an opinion and does not claim to be fact cannot be challenged on the grounds of inaccuracy.

**Exemption/Restriction** - The right is conditional, with Subsection (4) permitting the police to retain inaccurate personal data that is used as evidence, provided that its processing is restricted. [DPA Part 3 Section 46](http://www.legislation.gov.uk/ukpga/2018/12/section/46) has to be read in conjunction with [DPA Part 3 Section 48](http://www.legislation.gov.uk/ukpga/2018/12/section/48).

Within policing an example of inaccurate personal data would be a conviction record on the Police National Computer where a disposal of ‘guilty’ had been recorded when it should have been ‘not guilty’.

Where the police have accurately recorded ‘erroneous’ personal data received from the data subject or someone else, perhaps in the form of an allegation the personal data is not regarded as inaccurate. However, should the data subject contest that accuracy it is good practice, where practical, to append the record with the data subject’s view. The following is an example of this in the policing context:

*A data subject disputes the accuracy of personal data supplied by a third-party to the police which is now held in an intelligence record. When the police recorded the personal data reasonable steps were taken to ensure its accuracy. In such circumstances, where the police are satisfied they have accurately recorded what may have originally been an allegation of something that did occur the police force will append the record explaining the accuracy dispute and the data subject’s views.*

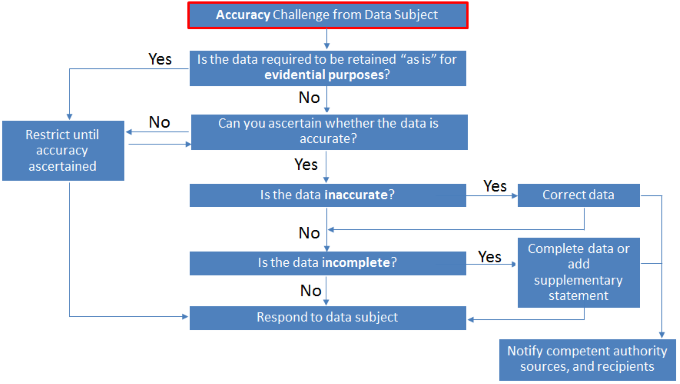
Subsection (2) identifies that some personal data may be inaccurate because it is incomplete and police forces must if requested by the data subject complete that data, in some cases by the provision of a supplementary statement to be read alongside the incomplete information.

DPA Part 3 Section 47(3) provides a provision for when a data subject contests the accuracy of personal data and it is not possible to ascertain whether it is accurate or not – if that is the case the police force must restrict its processing and, if in due course the restriction is removed, inform the data subject of that removal (as per DPA Part 3 Section 48(10).

[DPA Part 3 Section 46](http://www.legislation.gov.uk/ukpga/2018/12/section/46) has to be read in conjunction with [DPA Part 3 Section 48](http://www.legislation.gov.uk/ukpga/2018/12/section/48).

Measures necessary to ensure compliance with this right are likely to include ensuring all officers, staff and processors are made aware of the right, and where applications under it should be directed.

The process diagram below is designed to summarise how applications under DPA Part 3 Section 46 should be managed by police forces.



The ICO has issued guidance on the law enforcement processing right to rectification which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-rectification/).

The police force must adopt appropriate measures to ensure that applications for the DPA Part 3 Section 46 Right to Rectification are identified and processed without delay.

The Data Protection Officer must monitor their police force’s compliance with the DPA Part 3 Section 46 Right to Rectification and make any necessary interventions.

#### Right to Erasure or Restriction (DPA Part 3 Section 47)

[DPA Part 3 Section 47 Right to erasure or restriction of processing](http://www.legislation.gov.uk/ukpga/2018/12/section/47) states:

*(1) The controller must erase personal data without undue delay where—*

*(a) the processing of the personal data would infringe section 35, 36(1) to (3), 37, 38(1), 39(1), 40, 41 or 42, or*

*(b) the controller has a legal obligation to erase the data.*

*(2) Where the controller would be required to erase personal data under subsection (1) but the personal data must be maintained for the purposes of evidence, the controller must (instead of erasing the personal data) restrict its processing.*

*(3) Where a data subject contests the accuracy of personal data (whether in making a request under this section or section 46 or in any other way), but it is not possible to ascertain whether it is accurate or not, the controller must restrict its processing.*

*(4) A data subject may request the controller to erase personal data or to restrict its processing (but the duties of the controller under this section apply whether or not such a request is made).*

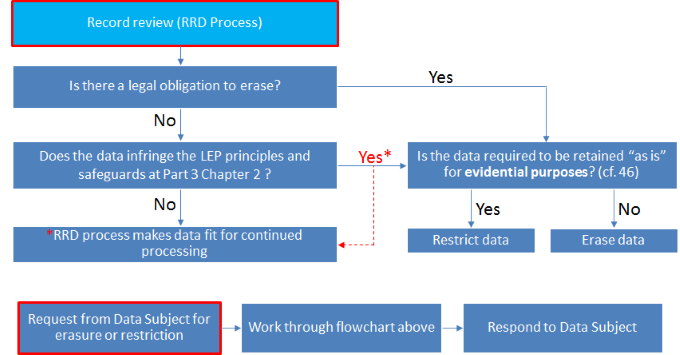
**Commentary** – Police forces must erase personal data without undue delay if there is a legal obligation to do so or the processing would infringe any of the following provisions of the Act, except where the personal data is required for evidence:

* First Law Enforcement Principle ([Section 35](#_First_Law_Enforcement))
* Second Law Enforcement Principle - partial ([Section 36(1) to (3](#_Second_Law_Enforcement)))
* Third Law Enforcement Principle ([Section 37](#_Third_Law_Enforcement))
* Fourth Law Enforcement Principle – partial ([Section 38(1)](#_Fourth_Law_Enforcement))
* Fifth Law Enforcement Principle – partial ([Section 39(1)](#_Fifth_Law_Enforcement))
* Sixth Data Protection Principle ([Section 40](#_Sixth_Law_Enforcement))
* Safeguards: Archiving ([Section 41](#_Safeguards:_Archiving_(Section))
* Safeguards: Sensitive Processing ([Section 42](#_Safeguards:_Sensitive_Processing))

**Exemption/Restriction** – DPA Part 3 Section 47(2) if the personal data is required for evidence and cannot be erased it must be restricted. It must also be restricted when a data subject challenges its accuracy but it is not possible to ascertain whether it is accurate or not (Subsection (3)). It is important to note that the right to erasure or restriction does not have to be triggered by an application from a data subject (Subsection (4)).

[DPA Part 3 Section 47](http://www.legislation.gov.uk/ukpga/2018/12/section/47) has to be read in conjunction with [DPA Part 3 Section 48](http://www.legislation.gov.uk/ukpga/2018/12/section/48).

The process diagram below is designed to summarise how applications under DPA Part 3 Section 47 should be managed by police forces.



The ICO has issued guidance on the law enforcement processing right to erasure or restriction which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-erasure-and-the-right-to-restriction/).

The police force must adopt appropriate measures to ensure that applications for the DPA Part 3 Section 7 Right to Erasure and Restriction of personal data are identified and processed without delay.

The Data Protection Officer must monitor their police force’s compliance with the DPA Part 3 Section 47 Right to Erasure or Restriction and make any necessary interventions.

#### Rights to Rectification, Erasure & Restriction, Supplementary (DPA Part 3 Section 48)

[DPA Part 3 Section 48 Rights under section 46 or 47: supplementary](http://www.legislation.gov.uk/ukpga/2018/12/section/48) applies to the preceding two sections of the Act and commences:

*(1) Where a data subject requests the rectification or erasure of personal data or the restriction of its processing, the controller must inform the data subject in writing—*

*(a) whether the request has been granted, and*

*(b) if it has been refused—*

*(i) of the reasons for the refusal,*

*(ii) of the data subject’s right to make a request to the Commissioner under section 51,*

*(iii) of the data subject’s right to lodge a complaint with the Commissioner, and*

*(iv) of the data subject’s right to apply to a court under section 167.*

*(2) The controller must comply with the duty under subsection (1)—*

*(a) without undue delay, and*

*(b) in any event, before the end of the applicable time period (see section 54).*

*(3) The controller may restrict, wholly or partly, the provision of information to the data subject under subsection (1)(b)(i) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to—*

*(a) avoid obstructing an official or legal inquiry, investigation or procedure;*

*(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;*

*(c) protect public security;*

*(d) protect national security;*

*(e) protect the rights and freedoms of others.*

**Commentary** – Whenever a data subject exercises their rights to rectification erasure or the police force must process the application without undue delay and respond to the applicant in writing (including email) within the applicable time period, usually one month. [DPA Part 7 Section 205 General interpretation](http://www.legislation.gov.uk/ukpga/2018/12/section/205) confirms that the definition of month in respect of these rights is that set out in [Article 3 of Regulation (ECC, Euratom) No. 1182/71 of the Council of 3rd June 1971](file:///C:\Users\42006032\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\AppData\Local\Temp\DOC_1.en.xhtml).

Where the application is refused, reasons for doing so must be provided together with information as to other rights the data subject may want to utilize except where Subsection (3) applies.

It is important to note that the restrictions can only be applied as far as is necessary and can only be applied as long as is necessary. Consequently a blanket application of the restriction to all of an applicant’s personal data or permanent application of the restriction are not permitted.

**Exemption/Restriction** - Subsection (3) sets out grounds when a restriction may be applied by the police.

[DPA Part 3 Section 48](http://www.legislation.gov.uk/ukpga/2018/12/section/48) continues:

*(4) Where the rights of a data subject under subsection (1) are restricted, wholly or partly, the controller must inform the data subject in writing without undue delay—*

*(a) that the rights of the data subject have been restricted,*

*(b) of the reasons for the restriction,*

*(c) of the data subject’s right to lodge a complaint with the Commissioner, and*

*(d) of the data subject’s right to apply to a court under section 167.*

*(5) Subsection (4)(a) and (b) do not apply to the extent that the provision of the information would undermine the purpose of the restriction.*

**Commentary** – Subsection (4) places an obligation on the police to confirm whether a restriction to Subsection (1) has been applied and other information to the data subject. Again this is conditional and by virtue of Subsection (5) which allows Subsection (4)(a) and (b) to be disregarded to the extent necessary to prevent the restriction being undermined. It is interesting to note that there is no relief available from Subsections (4)(c) and (d) so in all cases applicants must be informed of their right to lodge a complaint with the ICO or apply to court for a Compliance Order under DPA Part 6 Section 165.

[DPA Part 3 Section 48](http://www.legislation.gov.uk/ukpga/2018/12/section/48) continues:

*(6) The controller must—*

*(a) record the reasons for a decision to restrict (whether wholly or partly) the provision of information to a data subject under subsection (1)(b)(i), and*

*(b) if requested to do so by the Commissioner, make the record available to the Commissioner.*

**Commentary** – This subsection requires police forces to record the rationale for any use of restrictions of Subsection (1) and provide that information to the ICO upon request. Police forces must therefore ensure that in all cases where such a restriction is employed a written rationale is maintained within its records.

[DPA Part 3 Section 48](http://www.legislation.gov.uk/ukpga/2018/12/section/48) concludes:

*(7) Where the controller rectifies personal data, it must notify the competent authority (if any) from which the inaccurate personal data originated.*

*(8) In subsection (7), the reference to a competent authority includes (in addition to a competent authority within the meaning of this Part) any person that is a competent authority for the purposes of the Law Enforcement Directive in a member State other than the United Kingdom.*

*(9) Where the controller rectifies, erases or restricts the processing of personal data which has been disclosed by the controller—*

*(a) the controller must notify the recipients, and*

*(b) the recipients must similarly rectify, erase or restrict the processing of the personal data (so far as they retain responsibility for it).*

*(10) Where processing is restricted in accordance with section 47(3), the controller must inform the data subject before lifting the restriction.*

**Commentary** – Subsections (7) and (8) place a requirement for police forces who have rectified personal data to inform any Competent Authority from whom that data had originated of any decision to rectify. It is interesting to note that the requirement does not extend to bodies other than Competent Authorities nor does it apply to erasure or restriction. Appropriate measures must be adopted to ensure this takes place where necessary.

Subsection (9) places a potentially onerous obligation on the police force to contact all recipients of personal data which had previously been disclosed by the police force but had subsequently been rectified, erased or restricted, in order for those recipients to apply the same rectification, erasure or restriction to the personal data now in their possession. Police forces’ ability to meet this requirement will be proportionate to the records of disclosure they may maintain. Police forces are likely to be recipients of personal data from other Competent Authorities and in such cases they will need to apply any ‘inherited’ rectification, erasure or restriction – in the case of erasure or restriction this may potentially be in conflict with their own requirements to continue to retain or process without restrictions.

Each police force must adopt appropriate measures to ensure recipients to whom personal data is disclosed are advised of subsequent decisions by the police force to rectify, erase or restrict personal data. In addition, they must adopt suitable measures to ensure they rectify, erase or restrict personal data in accordance with any notification from other Competent Authorities from whom the data had been received.

Subsection (10) requires police forces to inform data subjects of the removal of any restriction that had been applied as a consequence of an unresolvable accuracy dispute.

The Data Protection Officer must monitor their police force’s compliance with the supplementary aspects of the Rights to Rectification, Erasure & Restriction and make any necessary interventions.

### Rights re Automated Decision-Making (DPA Part 3 Section 49 & Section 50)

[DPA Part 3 Section 49 Right not to be subject to automated decision-making](http://www.legislation.gov.uk/ukpga/2018/12/section/49) states:

*(1) A controller may not take a significant decision based solely on automated processing unless that decision is required or authorised by law.*

*(2) A decision is a “significant decision” for the purpose of this section if, in relation to a data subject, it—*

*(a) produces an adverse legal effect concerning the data subject, or*

*(b) significantly affects the data subject.*

[DPA Part 3 Section 50 Automated decision-making authorized by law: safeguards](http://www.legislation.gov.uk/ukpga/2018/12/section/50) includes:

*(1) A decision is a “qualifying significant decision” for the purposes of this section if—*

*(a) it is a significant decision in relation to a data subject, and*

*(b) it is required or authorised by law.*

*(2) Where a controller takes a qualifying significant decision in relation to a data subject based solely on automated processing—*

*(a) the controller must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing, and*

*(b) the data subject may, before the end of the period of 21 days beginning with receipt of the notification, request the controller to—*

*(i) reconsider the decision, or*

*(ii) take a new decision that is not based solely on automated processing.*

*(3) If a request is made to a controller under subsection (2), the controller must, before the end of the period of 21 days beginning with receipt of the request—*

*(a) consider the request, including any information provided by the data subject that is relevant to it,*

*(b) comply with the request, and*

*(c) by notice in writing inform the data subject of—*

*(i) the steps taken to comply with the request, and*

*(ii) the outcome of complying with the request.*

[DPA Part 3 Section 50](http://www.legislation.gov.uk/ukpga/2018/12/section/50) Paragraphs 4 and 5 are not directly relevant to policing.

[DPA Part 3 Section 50](http://www.legislation.gov.uk/ukpga/2018/12/section/50) concludes:

*(6) In this section “significant decision” has the meaning given by section 49(2).*

**Commentary** – [DPA Part 3 Section 49](http://www.legislation.gov.uk/ukpga/2018/12/section/49) prohibits police forces from making “significant decisions” based solely on automated processing unless the decision is required or authorised by law. A “significant decision” is one which results in adverse legal effects concerning the data subject or significantly affects the data subject.

Where the police force is required or authorised by law to make a significant decision, DPA Part 3 Section 50 sets out the safeguards that will apply to such a decision (which is defined as a “qualifying significant decision”). Such safeguards include a duty on the police to inform the data subject of an automated decision and his or her right to request that the controller reconsider the decision or take a new decision on the basis of human intervention.

These provisions are in relation to fully automated decision-making and not to automated processing which is defined at DPA Part 1 Section 3(4). Automated processing (including profiling) is when an operation is carried out on data without the need for human intervention. It is regularly used in law enforcement to filter down large data sets to manageable amounts for a human operator to then use.

By contrast, automated decision-making is a form of automated processing and requires the final decision to be made without human interference.

In practice, currently automated decision-making that leads to an adverse outcome is rarely used in the law enforcement context and is unlikely to have any operational implications.

The ICO has issued guidance on the law enforcement processing right not to be subject of automated decision-making which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/right-not-to-be-subject-to-automated-decision-making/).

The police force must adopt appropriate measures to ensure that applications for the DPA Part 3 Section 49 & 50 Rights re Automated Decision-Making of personal data are identified and processed without delay.

The Data Protection Officer must monitor their police force’s compliance with the DPA Part 3 Section 49 & 50 Rights re Automated Decision-Making and make any necessary interventions.

### Subject Rights: Supplementary (DPA Part 3 Section 51)

#### Exercise of rights through the Commissioner

[DPA Part 3 Section 51 Exercise of rights through the Commissioner](http://www.legislation.gov.uk/ukpga/2018/12/section/51) states:

*(1) This section applies where a controller—*

*(a) restricts under section 44(4) the information provided to the data subject under section 44(2) (duty of the data controller to give the data subject additional information),*

*(b) restricts under section 45(4) the data subject’s rights under section 45(1) (right of access), or*

*(c) refuses a request by the data subject for rectification under section 46 or for erasure or restriction of processing under section 47.*

*(2) The data subject may—*

*(a) where subsection (1)(a) or (b) applies, request the Commissioner to check that the restriction imposed by the controller was lawful;*

*(b) where subsection (1)(c) applies, request the Commissioner to check that the refusal of the data subject’s request was lawful.*

*(3) The Commissioner must take such steps as appear to the Commissioner to be appropriate to respond to a request under subsection (2) (which may include the exercise of any of the powers conferred by sections 142 and 146).*

*(4) After taking those steps, the Commissioner must inform the data subject—*

*(a) where subsection (1)(a) or (b) applies, whether the Commissioner is satisfied that the restriction imposed by the controller was lawful;*

*(b) where subsection (1)(c) applies, whether the Commissioner is satisfied that the controller’s refusal of the data subject’s request was lawful.*

*(5) The Commissioner must also inform the data subject of the data subject’s right to apply to a court under section 167.*

*(6) Where the Commissioner is not satisfied as mentioned in subsection (4)(a) or (b), the Commissioner may also inform the data subject of any further steps that the Commissioner is considering taking under Part 6.*

**Commentary** – [DPA Part 3 Section 51](http://www.legislation.gov.uk/ukpga/2018/12/section/51) allows data subjects to ask the ICO to review the lawful basis of some aspects of a police force’s response to subject rights applications where the police force has either (i) restricted the provision of certain information to the data subject concerning legal basis for processing, retention, recipients and rights, (ii) restricted the right of access, or (iii) refused to erase or restrict processing.

Where the ICO approaches a police force under DPA Section 51 the Data Protection Officer must provide all reasonable assistance to the ICO.

### Form of Provision of Information (DPA Part 3 Section 52)

[DPA Part 3 Section 52 Form of provision of information etc.](http://www.legislation.gov.uk/ukpga/2018/12/section/52) states:

*(1) The controller must take reasonable steps to ensure that any information that is required by this Chapter [DPA Part 3 Sections 43 to 54] to be provided to the data subject is provided in a concise, intelligible and easily accessible form, using clear and plain language.*

*(2) Subject to subsection (3), the information may be provided in any form, including electronic form.*

*(3) Where information is provided in response to a request by the data subject under section 45, 46, 47 or 50, the controller must provide the information in the same form as the request where it is practicable to do so.*

*(4) Where the controller has reasonable doubts about the identity of an individual making a request under section 45, 46 or 47, the controller may—*

*(a) request the provision of additional information to enable the controller to confirm the identity, and*

*(b) delay dealing with the request until the identity is confirmed.*

*(5) Subject to section 53, any information that is required by this Chapter to be provided to the data subject must be provided free of charge.*

*(6) The controller must facilitate the exercise of the rights of the data subject under sections 45 to 50.*

**Commentary** – [DPA Part 3 Section 52(1)](http://www.legislation.gov.uk/ukpga/2018/12/section/52) requires information provided in response to subject rights applications to be understandable to the data subject, which means in certain circumstances police forces may have to explain abbreviations and jargon.

In addition, the provisions at [DPA Part 3 Section 51(2) & (3)](http://www.legislation.gov.uk/ukpga/2018/12/section/51) means that responses to right of access rectification, erasure, restriction and automated decision-making rights requests must be in the same form as the request where practical to do so, including in electronic form.

[DPA Part 3 Section 51(4)](http://www.legislation.gov.uk/ukpga/2018/12/section/51) allows a police force to delay dealing with rights of access, rectification, erasure or restriction of processing requests until it is satisfied that the requestor is the data subject.

[DPA Part 3 Section 51(5](http://www.legislation.gov.uk/ukpga/2018/12/section/51)) removes the opportunity to charge any fee in respect of the rights under DPA Part 3 Sections 43 to 54.

The police force must adopt appropriate measures to ensure that its response to Rights applications satisfy DPA Part 3 Section 52 requirements (Form of Provision of Information).

The Data Protection Officer must monitor their police force’s compliance with the DPA Part 3 Section 52 requirements (Form of Provision of Information) and make any necessary interventions.

#### Manifestly Unfounded or Excessive Requests (DPA Part 3 Section 53)

[DPA Part 3 Section 53 Manifestly unfounded or excessive requests by the data subject](http://www.legislation.gov.uk/ukpga/2018/12/section/53) states:

*(1) Where a request from a data subject under section 45, 46 or 47 is manifestly unfounded or excessive, the controller may—*

*(a) charge a reasonable fee for dealing with the request, or*

*(b) refuse to act on the request.*

*(2) An example of a request that may be excessive is one that merely repeats the substance of previous requests.*

*(3) In any proceedings where there is an issue as to whether a request under section 45, 46 47 or 50 is manifestly unfounded or excessive, it is for the controller to show that it is.*

DPA Part 3 Section 53 Paragraphs 4 & 5 are not directly relevant to policing.

**Commentary** – This provision is relevant to the rights of access, rectification, erasure or restriction of processing requests. “Manifestly unfounded or excessive” requests are likely to include requests that are repetitious, or malicious, or where they represent an abuse of the rights to access, for example by providing false or misleading information.

Data subjects might attempt to use the right of access, rectification, erasure or restriction of processing as a means to harass police forces with no real purpose other than to cause disruption. This can be in the form of repeated requests over a relatively short period of time or extending over several years, or where the police force has provided the data subject with their personal data through an alternative disclosure mechanism.

Neither of the terms “Manifestly unfounded” or “excessive” are defined in the Act. The explanatory notes issued with the Data Protection Bill stated: “An example of an excessive request for information is one that repeats the substance of previous requests.” The NPCC’s view is that the term is likely to encompass:

* a request that sought information available or previously supplied via an alternative route e.g. pre-trial disclosure under DPIA or disclosure of a custody record under PACE (excessive)
* a request that sought information previously supplied under the right of access (excessive)
* a request that came from a requestor already in dispute with the police force where there is evidence of a malicious, disruptive or time-wasting intent on their part (manifestly unfounded)
* a request that is for reasons other than enabling the data subject to be aware of and verify the lawfulness of the processing (manifestly unfounded)
* a request from a parent purporting to be on behalf of a child when the circumstances suggest this is not the case (manifestly unfounded)
* a request displaying characteristic indicators of a vexatious request under the Freedom of Information Act 2000 set out in the [Commissioner’s guidance on dealing with vexatious requests](https://ico.org.uk/media/for-organisations/documents/1198/dealing-with-vexatious-requests.pdf)
* a request that would take in excess of 30 man-hours to respond to (excessive)[[15]](#footnote-15)

Any police force claiming a request to be manifestly unfounded or excessive has to explain its rationale for that view to the data subject/requestor and, more often than not, to the ICO in due course.

In these circumstances the police force can charge a reasonable fee (subject to any prescribed maximum) to act on the request or can refuse the request entirely – NPCC’s position is that the latter option be followed by police forces as it ensures a consistent and fair approach irrespective of the financial means of data subjects, and allows police forces to focus limited resource on requests that are neither unfounded nor excessive.

The ICO has issued guidance on ‘manifestly unfounded or excessive’ in relation to rights concerning law enforcement processing which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/).

#### Applicable Time Period (DPA Part 3 Section 54)

[DPA Part 3 Section 54 Meaning of “applicable time period](http://www.legislation.gov.uk/ukpga/2018/12/section/54)” states:

*(1) This section defines “the applicable time period” for the purposes of sections 45(3)(b) and 48(2)(b).*

*(2) “The applicable time period” means the period of one month, or such longer period as may be specified in regulations, beginning with the relevant day.*

*(3) “The relevant day” means the latest of the following days—*

*(a) the day on which the controller receives the request in question;*

*(b) the day on which the controller receives the information (if any) requested in connection with a request under section 52(4);*

*(c) the day on which the fee (if any) charged in connection with the request under section 53 is paid.*

DPA Part 3 Section 54 Paragraphs 4 to 6 are not directly relevant to policing.

**Commentary** – [DPA Part 7 Section 205 General interpretation](http://www.legislation.gov.uk/ukpga/2018/12/section/205) confirms that the definition of month in respect of DPA Part 3 Section 54 is that set out in [Article 3 of Regulation (ECC, Euratom) No. 1182/71 of the Council of 3rd June 1971](file:///C:\Users\42006032\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\AppData\Local\Temp\DOC_1.en.xhtml).

The Act **does not provide an opportunity for police forces to extend this period** by up to two months as is available with requests under the right of access under GDPR/DPA Part 2.

The ICO has [advised](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib6):

If you receive a request on 30 June the time limit will start on 1 July and the deadline will be 1 August. If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond. For practical purposes if a consistent number of days is required (e.g. for a computer system), you should adopt a 28-day period to ensure compliance is always within a calendar month.

### Data subject’s rights and other prohibitions and restrictions (DPA Part 7 Section 186)

[DPA Part 7 Section 186 Part 7 Data subject’s rights and other prohibitions and restrictions](http://www.legislation.gov.uk/ukpga/2018/12/section/186) states:

(1) An enactment or rule of law prohibiting or restricting the disclosure of information, or authorising the withholding of information, does not remove or restrict the obligations and rights provided for in the provisions listed in subsection (2), except as provided by or under the provisions listed in subsection (3).

(2) The provisions providing obligations and rights are—

(a) Chapter III of the GDPR (rights of the data subject),

(b) Chapter 3 of Part 3 of this Act (law enforcement processing: rights of the data subject), and

(c) Chapter 3 of Part 4 of this Act (intelligence services processing: rights of the data subject).

(3) The provisions providing exceptions are—

(a) in Chapter 2 of Part 2 of this Act, sections 15 and 16 and Schedules 2, 3 and 4,

(b) in Chapter 3 of Part 2 of this Act, sections 23, 24, 25 and 26,

(c) in Part 3 of this Act, sections 44(4), 45(4) and 48(3), and

(d) in Part 4 of this Act, Chapter 6 .

**Commentary** – DPA Part 7 Section 186 confirms that any legislation or rule of law that prohibits or restricts the disclosure of information or authorizing the withholding of information cannot restrict subject rights except in prescribed circumstances.

### Summary table of exemptions and restrictions from Law Enforcement Rights

|  |  |  |  |
| --- | --- | --- | --- |
| **Provisions to be Exempted/ Restricted\*** | **Summary** | **Available Exemption/ Restriction** | **Grounds for Exemption** |
| Sections 44 to 48 Rights | Rights concerning information made available, access, rectification, erasure, restriction | Section 43(3) & (4) | Applies to all *relevant personal data* which is defined as *personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority.*  [does not appear to be applicable to police] |
| Section 44 (1) Information for the public | Provision of general information to assist the public in exercising their DPA Part 3 Rights | None | None |
| Section 44(2)  Information for Data Subjects | Provision of information concerning legal basis for processing, retention period, recipients, and rights | Section 44(4)(a) to (e) | Applies where necessary and proportionate to:  (a) avoid obstructing an official or legal inquiry, investigation or procedure;  (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;  (c) protect public security;  (d) protect national security;  (e) protect the rights and freedoms of others. |
| Section 44(5)(a) &(b)  Information for Data Subjects | Provision of information confirming that Section 44(2) had been restricted and/or the reasons for that restriction | Section 44(6) | Where providing that information would undermine the restriction of Section 44(2) |
| Section 45(1)  Right of Access | Right of access & additional information | Section 45(4) | Applies where necessary and proportionate to:  (a) avoid obstructing an official or legal inquiry, investigation or procedure;  (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;  (c) protect public security;  (d) protect national security;  (e) protect the rights and freedoms of others. |
| Section 45(5)(a) & (b)  Right of Access | Information confirming that Section 45(1) had been restricted and/or the reasons for that restriction | Section 45(6) | Applies where providing that information would undermine the restriction of Section 45(2) |
| Section 45 | Right of access | Section 53(1)(b) | Applies where the request is manifestly unfounded or excessive – allows the request to be rejected |
| Section 46(1) to (3)  Right to Rectification | Right to have personal data rectified if inaccurate | Section 46(4) | Applies where the personal data is inaccurate but is required for evidence – in which case it must be restricted rather than rectified |
| Section 46(1) to (3)  Right to Rectification | Right to have personal data rectified if inaccurate | Section 47(3) | Applies where it is not possible to establish if the personal data is inaccurate – in which case it must be restricted rather than rectified |
| Section 46 Right to Rectification | Right to have personal data rectified if inaccurate | Section 53(1)(b) | Applies where the request is manifestly unfounded or excessive – allows the request to be rejected |
| Section 47(1)  Right to Erasure | Right to have non-compliant data erased | Section 47(2) | Applies where the personal data is required for evidence – in which case it must be restricted rather than erased |
| Section 47(1)  Right to Erasure | Right to have inaccurate data erased | Section 47(3) | Applies where it is not possible to establish if the personal data is inaccurate – in which case it must be restricted rather than erased |
| Section 47(1)  Right to Erasure | Right to have personal data erased | Section 53(1)(b) | Applies where the request is manifestly unfounded or excessive – allows the request to be rejected |
| Section 48(1)(b)(i)  Rights to Rectification, Erasure & Restriction | Right to be informed of rationale for any refusal re a request under Sections 46 to 48 | Section 48(3) | Applies where necessary and proportionate to:  (a) avoid obstructing an official or legal inquiry, investigation or procedure;  (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;  (c) protect public security;  (d) protect national security;  (e) protect the rights and freedoms of others. |
| Section 49 & 50 | Rights re Automated Decision-Making | None | None |

\* To the degree necessary only

## Law Enforcement Controller & Processor Obligations

### Overview & Scope (DPA Part 3 Section 55)

[DPA Part 3 Section 55 Overview and scope](http://www.legislation.gov.uk/ukpga/2018/12/section/55) states:

*(1) This Chapter—*

*(a) sets out the general obligations of controllers and processors (see sections 56 to 65);*

*(b) sets out specific obligations of controllers and processors with respect to security (see section 66);*

*(c) sets out specific obligations of controllers and processors with respect to personal data breaches (see sections 67 and 68);*

*(d) makes provision for the designation, position of protection officers (see sections 69 to 71).*

*(2) This Chapter applies only in relation to the processing of personal data for a law enforcement purpose.*

*(3) Where a controller is required by any provision of this Chapter to implement appropriate technical and organisational measures, the controller must (in deciding what measures are appropriate) take into account—*

*(a) the latest developments in technology,*

*(b) the cost of implementation,*

*(c) the nature, scope, context and purposes of processing, and*

*(d) the risks for the rights and freedoms of individuals arising from the processing.*

**Commentary** – [DPA Part 3 Section 55](http://www.legislation.gov.uk/ukpga/2018/12/section/55) provides an introduction for [Sections 56 to 71](http://www.legislation.gov.uk/ukpga/2018/12/part/3/chapter/4) of the Act, setting out obligations that apply to police forces as controllers and any processors carrying out processing of personal data for them.

Overall the measures implemented must be proportionate to the processing activities, should adhere to the data principles and the outcome of any data protection impact assessment. The intention is to ensure that data protection is mainstreamed in processing operations, particularly in the planning of new proposals or projects, although equally relevant for existing processing operations.

Instead of data protection considerations emerging once plans are in place or the processing has begun, this places an obligation on the controller to put in place appropriate technical and organisational measures to implement the data protection principles from the outset. This aims to ensure police forces only process personal data which is necessary for the specific purposes of the processing and the processing reflects and complies with the principles.

The ICO has issued guidance on law enforcement processing accountability and governance which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/accountability-and-governance/logging/).

### Obligation to Ensure Compliance (DPA Part 3 Section 56 & Section 57)

[DPA Part 3 Section 56 General obligations of the controller](http://www.legislation.gov.uk/ukpga/2018/12/section/56) states:

*(1) Each controller must implement appropriate technical and organizational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of this Part.*

*(2) Where proportionate in relation to the processing, the measures implemented to comply with the duty under subsection (1) must include appropriate data protection policies.*

*(3) The technical and organisational measures implemented under subsection (1) must be reviewed and updated where necessary.*

**Commentary** – [DPA Part 3 Section 56](http://www.legislation.gov.uk/ukpga/2018/12/section/56) imposes a general obligation on police forces to take appropriate technical and organisational measures to ensure that the requirements of [DPA Part 3](http://www.legislation.gov.uk/ukpga/2018/12/part/3) are complied with.

Subsection (1) means that not only do the measures have to be in place but there is a requirement to be able to demonstrate compliance. That requirement indicates that police forces should examine their law enforcement processing and proactively identify documentation that helps show compliance.

This will include a wide variety of documents such as Records of Processing Activities, Data Protection Impact Assessments, policies, procedures, information sharing agreements, data processing contracts, training materials and records, and records of rights applications and performance. The records should encompass technological measures, which are primarily likely to be concerned with the security of personal data.

Consideration may be given to making some of this information publicly available where to do so would not risk harm to law enforcement processing and the policing purposes. In addition, forces should be prepared to reactively respond effectively to any external challenge to demonstrate compliance.

Subsection (2) specifically sets out the mandatory requirement for data protection policies to exist amongst all the measures. The fact that the term is in the plural further emphasizes the importance attached to this by the Act.

The term ‘appropriate’ features in those two subsections and this indicates consideration must be given to the nature of the personal data being processed for law enforcement purposes and the nature of the processing. Clearly law enforcement processing involves some very sensitive, intrusive and potentially risky processing, so police forces should ensure their measures are commensurate with that status.

Subsection (3) requires the measures to be reviewed and updated where necessary, so forces should use a combination of planned reviews and reviews triggered by circumstance such as new case law, enforcement activity and communications from the ICO, NPCC advice, and local factors such as complaints, disputes, and audit.

The ICO’s current guidance for data protection by design and default for law enforcement processing can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/accountability-and-governance/data-protection-by-design-and-by-default/).

The Data Protection Officer must monitor their police forces’ ongoing compliance with the DPA Part 3 Section 56 obligations to ensure compliance and make any necessary interventions.

[DPA Part 3 Section 57 Data protection by design and default](http://www.legislation.gov.uk/ukpga/2018/12/section/57) states:

*(1) Each controller must implement appropriate technical and organizational measures which are designed—*

*(a) to implement the data protection principles in an effective manner, and*

*(b) to integrate into the processing itself the safeguards necessary for that purpose.*

*(2) The duty under subsection (1) applies both at the time of the determination of the means of processing the data and at the time of the processing itself.*

*(3) Each controller must implement appropriate technical and organizational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.*

*(4) The duty under subsection (3) applies to—*

*(a) the amount of personal data collected,*

*(b) the extent of its processing,*

*(c) the period of its storage, and*

*(d) its accessibility.*

*(5) In particular, the measures implemented to comply with the duty under subsection (3) must ensure that, by default, personal data is not made accessible to an indefinite number of people without an individual’s intervention.*

**Commentary** – [DPA Part 3 Section 57](http://www.legislation.gov.uk/ukpga/2018/12/section/57) supplements the previous section’s requirement to have appropriate technical and organisational measures in place by also requiring them to be considered before processing occurs at the stage the means of processing is being considered.

Subsection (1) again uses the term ‘appropriate’ indicating the measures should be determined having considered the nature of the personal data to be processed and the nature of the processing. The requirement is for the principles to be satisfied effectively and for safeguards to be built into processing operations. This links to the DPA Part 3 Section 64 obligation to carry out Data Protection Impact Assessments which are a means of identify necessary measures.

Subsection (2) makes it clear these considerations must be made in advance of processing starting, as well as on an ongoing basis once it has started.

Subsections (3) and (4) build upon the two preceding subsections by requiring the default position to be that measures must be adopted so that once each specific processing purpose has been be identified only the personal data necessary for the purpose is processed. In addition, the extent to the processing, the period it occurs for, and access to it the personal data must also be considered. Finally, subsection (5) sets out the key point that the personal data cannot be made accessible to an indefinite number of people without an individual having first considered it.

The ICO’s current guidance for data protection by design and default for law enforcement processing can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/accountability-and-governance/data-protection-by-design-and-by-default/).

The Data Protection Officer must monitor their police forces’ ongoing compliance with the DPA Part 3 Section 57 (Data Protection by Design & Default) obligations and make any necessary interventions.

### Joint Controller Clarity of Responsibilities (DPA Part 3 Section 58) (Appendix F)

[DPA Part 3 Section 58 Joint controllers](http://www.legislation.gov.uk/ukpga/2018/12/section/58) states:

*(1) Where two or more competent authorities jointly determine the purposes and means of processing personal data, they are joint controllers for the purposes of this Part.*

*(2) Joint controllers must, in a transparent manner, determine their respective responsibilities for compliance with this Part by means of an arrangement between them, except to the extent that those responsibilities are determined under or by virtue of an enactment.*

*(3) The arrangement must designate the controller which is to be the contact point for data subjects.*

**Commentary** – [DPA Part 3 Section 58](http://www.legislation.gov.uk/ukpga/2018/12/section/58) sets out the need for clarity of responsibilities where a police force operates as a joint controller with another competent authority.

Subsection (1) establishes that where two or more competent authorities jointly determine the purposes and means of law enforcement processing of personal data they will be joint controllers for that processing.

Subsection (2) requires the joint controllers to unambiguously identify their DPA Part 3 responsibilities through a transparent arrangement between them. The NPPC’s position is that this should be documented in or referred to in any collaborative agreement between a police force and another competent authority, such as the Police Act 1996 Section 22A agreements in use between police forces across England and Wales. Where the joint responsibilities are fully set out in legislation there is no need for such arrangements.

Subsection (3) requires the arrangement to set out which controller is to be the contact point for data subjects. This appears not to preclude more than one controller from acting in that capacity.

[Appendix F](#_Appendix_F:_Joint_1) provides Joint Controllers Definitions & Arrangements

The ICO does not appear to have issued guidance on DPA Part 3 Section 58.

The Data Protection Officer must ensure that where their police force undertake joint controllership in respect of law enforcement processing a document is produced and maintained to satisfy their DPA Part 3 Section 58 obligations.

#### Police collaborative units

**Commentary** - In recent years there has been a marked increase in the number of projects and initiatives to establish collaborative units serving two or more police forces and partner agencies. Such units often have the benefits of improving service delivery, increasing information sharing across police force boundaries, and delivering financial savings at a time of austerity.

However, projects and initiatives to create collaborative units must take into account Data Protection and other information management requirements if they are to be successfully delivered in a manner that is legally compliant.

A police force’s Chief Officer, as controller, is legally responsible for ensuring that their police force complies with the requirements of the Act.

Historically the scope of this responsibility has been fairly easy to define, as the processing of personal data by any police force has tended, with a few notable exceptions8, to involve police officers and staff using their own force information systems to handle, use or disclose personal data exclusively for the police force’s purposes.

The trend for the creation of collaborative units to deliver certain activity on behalf of more than one police force has meant that there is an increased risk those boundaries in the area of collaborative units can become ill-defined.

As a consequence it may be unclear as to who is the controller for personal data processed within a collaborative unit, leading to uncertainty as to the data protection and wider information management regime that should be followed.

This problem will be exacerbated where police forces involved in the collaboration have divergent or even contradictory policies and procedures around matters such as appropriate access or use of information systems, information security/assurance (including incident reporting), information sharing and information management governance arrangements.

The solution is for an approach of Data Protection by design and default, including Data Protection Impact Assessment to be adopted whenever there is an intention to establish collaborative units between police forces or their partners. That process will identify the privacy risks and the mitigations that should be put in place to counter those risks.

Although this Manual states there is no need for information sharing agreements between police forces, where a collaborative unit is created it will be necessary to clearly define and document controllership and set out how data protection and other information management matters will be managed within the unit – that documentation should form part of the overall collaboration agreement between the police forces.

### Obligations on Processors (DPA Part 3 Section 59 & Section 60)

[DPA Part 3 Section 59 Processors](http://www.legislation.gov.uk/ukpga/2018/12/section/59) states:

*(1) This section applies to the use by a controller of a processor to carry out processing of personal data on behalf of the controller.*

*(2) The controller may use only a processor who provides guarantees to implement appropriate technical and organisational measures that are sufficient to secure that the processing will—*

*(a) meet the requirements of this Part, and*

*(b) ensure the protection of the rights of the data subject.*

*(3) The processor used by the controller may not engage another processor (“a sub-processor”) without the prior written authorisation of the controller, which may be specific or general.*

*(4) Where the controller gives a general written authorisation to a processor, the processor must inform the controller if the processor proposes to add to the number of sub-processors engaged by it or to replace any of them (so that the controller has the opportunity to object to the proposal).*

*(5) The processing by the processor must be governed by a contract in writing between the controller and the processor setting out the following—*

*(a) the subject-matter and duration of the processing;*

*(b) the nature and purpose of the processing;*

*(c) the type of personal data and categories of data subjects involved;*

*(d) the obligations and rights of the controller and processor.*

*(6) The contract must, in particular, provide that the processor must—*

*(a) act only on instructions from the controller,*

*(b) ensure that the persons authorised to process personal data are subject to an appropriate duty of confidentiality,*

*(c) assist the controller by any appropriate means to ensure compliance with the rights of the data subject under this Part,*

*(d) at the end of the provision of services by the processor to the controller—*

*(i) either delete or return to the controller (at the choice of the controller) the personal data to which the services relate, and*

*(ii) delete copies of the personal data unless subject to a legal obligation to store the copies,*

*(e) make available to the controller all information necessary to demonstrate compliance with this section, and*

*(f) comply with the requirements of this section for engaging subprocessors.*

*(7) The terms included in the contract in accordance with subsection (6)(a) must provide that the processor may transfer personal data to a third country or international organisation only if instructed by the controller to make the particular transfer.*

*(8) If a processor determines, in breach of this Part, the purposes and means of processing, the processor is to be treated for the purposes of this Part as a controller in respect of that processing.*

[DPA Part 3 Section 60 Processing under the authority of the controller or processor](http://www.legislation.gov.uk/ukpga/2018/12/section/60) states:

*A processor, and any person acting under the authority of a controller or processor, who has access to personal data may not process the data except—*

*(a) on instructions from the controller, or*

*(b) to comply with a legal obligation.*

**Commentary** – [DPA Part 3 Section 59](http://www.legislation.gov.uk/ukpga/2018/12/section/59) subsection (1) sets out that this section concerns the use by a police force (as a controller) of a processor to carry out law enforcement processing of personal data on behalf of the police force.

Subsection (2) requires that a police force can only use a processor where the processor is able to guarantee to implement the technical and organisational measures necessary to ensure it is compliant with DPA Part 3 and protects the rights of data subjects. The police forces must ensure it is satisfied that the processor can and does implement these measures, something that may require inspection or audit to gain the necessary reassurance.

Subsection (3) prohibits that processor from engaging with another processor without written authorisation from the police force. The authorisation can be specific or general.

Subsection (4) requires that where a police force has given general written authorisation to the processor specific permission from the police force must be sought before engaging any sub-processors or contractors.

Subsections (5), (6) & (7) require a contract in writing to exist between a police force and the processor and set out what that contract must include.

The final subsection confirms that if a processor breaches DPA Part 3 by determining the purposes and means of the law enforcement processing they will be regarded as controller in respect of that processing.

These obligations will usually be met through the provision of a contract, commonly known as a ‘data processing contract’. This can be a standalone document or form part of a wider contract.

Data protection officers will be required to provide necessary advice and guidance to assist the police force in choosing data processors that are able to satisfy the standards required by the police service to maintain an appropriate level of protection for the information concerned. Specialist technical advice may be forthcoming from force information security officer.

Where the data processor will process personal data outside of the EEA then DPA Part 3 Sections 72 to 78 must be considered.

A template data processing contract, design to satisfy DPA Part 3 law enforcement processing requirements is currently being developed for the NPCC.

[DPA Part 3 Section 60](http://www.legislation.gov.uk/ukpga/2018/12/section/60) is self-explanatory.

The ICO does not appear to have produced guidance on use of processors for law enforcement processing.

The police force must adopt measures to ensure (i) it only engages Processors who will implement the technical and organisational measures necessary to ensure compliance with the Act, (ii) data processing contracts are created that meet DPA Part 3 Section 59 & Section 60 obligations, and (iii) it conducts proportionate checks to ensure their data processors comply with the relevant data processing contract.

The Data Protection Officer must monitor their police force’s ongoing compliance with the DPA Part 3 Section 59 & Section 60 (Obligations on Processors) requirements and make any necessary interventions.

### Records of Processing Activities (RoPA) (DPA Part 3 Section 61)

[DPA Part 3 Section 61 Records of processing activities](http://www.legislation.gov.uk/ukpga/2018/12/section/61) states:

*(1) Each controller must maintain a record of all categories of processing activities for which the controller is responsible.*

*(2) The controller’s record must contain the following information—*

*(a) the name and contact details of the controller;*

*(b) where applicable, the name and contact details of the joint controller;*

*(c) where applicable, the name and contact details of the data protection officer;*

*(d) the purposes of the processing;*

*(e) the categories of recipients to whom personal data has been or will be disclosed (including recipients in third countries or international organisations);*

*(f) a description of the categories of—*

*(i) data subject, and*

*(ii) personal data;*

*(g) where applicable, details of the use of profiling;*

*(h) where applicable, the categories of transfers of personal data to a third country or an international organisation;*

*(i) an indication of the legal basis for the processing operations, including transfers, for which the personal data is intended;*

*(j) where possible, the envisaged time limits for erasure of the different categories of personal data;*

*(k) where possible, a general description of the technical and organisational security measures referred to in section 66.*

*(3) Each processor must maintain a record of all categories of processing activities carried out on behalf of a controller.*

*(4) The processor’s record must contain the following information—*

*(a) the name and contact details of the processor and of any other processors engaged by the processor in accordance with section 59(3);*

*(b) the name and contact details of the controller on behalf of which the processor is acting;*

*(c) where applicable, the name and contact details of the data protection officer;*

*(d) the categories of processing carried out on behalf of the controller;*

*(e) where applicable, details of transfers of personal data to a third country or an international organisation where explicitly instructed to do so by the controller, including the identification of that third country or international organisation;*

*(f) where possible, a general description of the technical and organisational security measures referred to in section 66.*

*(5) The controller and the processor must make the records kept under this section available to the Commissioner on request.*

**Commentary** – [DPA Part 3 Section 61](http://www.legislation.gov.uk/ukpga/2018/12/section/61) specifies what records should be kept by police forces and any processors they use. The records must be made available to the ICO on request, and are a means of demonstrating compliance with the Act.

Subsection (1) sets out the overall requirement to maintain a RoPA and subsection (2) states the minimum elements that must be included in those records. Subsections (3) and (4) extend this requirement to processors though the elements to be included differ from those applicable to the police force. Subsection (5) requires the records to be available to the ICO upon request.

It is important to note that RoPA should not be restricted to personal data held in digital form.

The ICO’s current guidance on records of processing activity for law enforcement processing can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/accountability-and-governance/documentation/).

The police force must adopt measures to ensure that Records of Processing Activities that meet DPA Part 3 Section 61 obligations, and that any Processors are reminded of this requirement for their processing on behalf of the police.

Data Protection Officers must monitor their police force’s ongoing compliance with the DPA Part 3 Section 61 obligations (Records of Processing Activities) and make any necessary interventions.

### Logging Requirements (DPA Part 3 Section 62)

[DPA Part 3 Section 62 Logging](http://www.legislation.gov.uk/ukpga/2018/12/section/62) states:

*(1) A controller (or, where personal data is processed on behalf of the controller by a processor, the processor) must keep logs for at least the following processing operations in automated processing systems—*

*(a) collection;*

*(b) alteration;*

*(c) consultation;*

*(d) disclosure (including transfers);*

*(e) combination;*

*(f) erasure.*

*(2) The logs of consultation must make it possible to establish—*

*(a) the justification for, and date and time of, the consultation, and*

*(b) so far as possible, the identity of the person who consulted the data.*

*(3) The logs of disclosure must make it possible to establish—*

*(a) the justification for, and date and time of, the disclosure, and*

*(b) so far as possible—*

*(i) the identity of the person who disclosed the data, and*

*(ii) the identity of the recipients of the data.*

*(4) The logs kept under subsection (1) may be used only for one or more of the following purposes—*

*(a) to verify the lawfulness of processing;*

*(b) to assist with self-monitoring by the controller or (as the case may be) the processor, including the conduct of internal disciplinary proceedings;*

*(c) to ensure the integrity and security of personal data;*

*(d) the purposes of criminal proceedings.*

*(5) The controller or (as the case may be) the processor must make the logs available to the Commissioner on request.*

**Commentary** – [DPA Part 3 Section 62](http://www.legislation.gov.uk/ukpga/2018/12/section/62) specifies the minimum information concerning processing activities that police forces or their processors must record in logs in ‘automated processing systems’. The term ‘automated processing system’ is not defined in the legislation, but the ICO advises in its guidance that it is interpreted to mean any system that undertakes processing by automated means, and is likely to involve human interaction (for example input of or access to data) at some point.

Subsection (1) sets out the minimum processing operations that must be logged. These encompass the complete information lifecycle.

Subsection (2) specifies that where the personal data is ‘consulted’ i.e. accessed and viewed the logs must enable the justification for, date and time that personal data is consulted to be established. The logs must also as far as possible establish who consulted the personal data.

Subsection (3) contains equivalent requirements for when the personal data is ‘disclosed’, including as far as is possible the identity of the person making the disclosure and the recipient of the personal data.

Subsection (4) places restrictions on the possible use of the logs.

Subsection (5) requires that the logs must be made available to the ICO upon request.

Many automated systems have existing logging capabilities; however, there is a requirement within the section to log erasure of personal data, as well as collection, alteration, consultation, etc. Logs of erasure should not reference the data itself – there is no need to retain a record of what was erased as that too would also be a record. Rather, the log should be able to specify that an item of data was erased on a specific date by a specific person.

Article 63(2) of the LED provides for a transitional period in respect of the logging requirements for automated processing systems set up before 6th May 2016; in such cases the requirements of [DPA Part 3 Section 62](http://www.legislation.gov.uk/ukpga/2018/12/section/62), must apply by 6th May 2023. This is set out in [DPA Schedule 20(14)](http://www.legislation.gov.uk/ukpga/2018/12/schedule/20).

As a consequence of these requirements it is important that any Data Protection Impact Assessment and associated project to implement IT systems processing personal data encompass the logging requirement.

The ICO’s current guidance on logging for law enforcement processing can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/accountability-and-governance/logging/).

The police force must adopt measures to ensure that where processing is for law enforcement purposes logs are maintained that meet DPA Part 3 Section 62 obligations, and that any processors are reminded of this requirement for their processing on behalf of the police.

The Data Protection Officer must monitor their police force’s ongoing compliance with the DPA Part 3 Section 62 (Logging) obligations and make any necessary interventions.

### Data Protection Impact Assessments (DPIA’s) (DPA Part 3 Section 64 & Section 65)

[DPA Part 3 Section 64 Data protection impact assessment](http://www.legislation.gov.uk/ukpga/2018/12/section/64) states:

*(1) Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment.*

*(2) A data protection impact assessment is an assessment of the impact of the envisaged processing operations on the protection of personal data.*

*(3) A data protection impact assessment must include the following—*

*(a) a general description of the envisaged processing operations;*

*(b) an assessment of the risks to the rights and freedoms of data subjects;*

*(c) the measures envisaged to address those risks;*

*(d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned.*

*(4) In deciding whether a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must take into account the nature, scope, context and purposes of the processing.*

**Commentary** – [DPA Part 3 Section 64](http://www.legislation.gov.uk/ukpga/2018/12/section/64) requires, through subsection (1), that DPIA’s should be undertaken where prospective law enforcement processing is likely to result in high risks to the rights and freedoms of individuals. Importantly the DPIA process must be carried out prior to the processing starting.

The Article 29 Data Protection Working Party has advised that ‘rights and freedoms’ of data subjects referred to in the GDPR equivalent of this DPA provision primarily concern the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

Subsection (4) requires any assessment to determine whether high risks will exist to consider the nature, scope, context and purposes of the processing.

Although carrying out a DPIA is not mandatory for every processing operation, the requirement to identify those cases where one is required means that there is a need for police forces to initially assess the risks associated with all law enforcement processing operations and conduct DPIA’s for those that are high risk.

Consequently the NPCC recommends that police forces adopt a screening process so that all prospective law enforcement processing is formally assessed and DPIA’s conducted where that initial assessment indicates high risk. This process should be repeated where processing operations are to be altered. It is important to note that processing includes every activity up to and including disposal of the personal data.

Law enforcement processing resulting in high risk is likely to arise in the following scenarios where the intention is to:

* process criminal data on a large scale;
* process data that could result in physical harm in the event of a security breach;
* monitor a public place or places on a large scale;
* use new technologies or techniques;
* process biometric or genetic data;
* combine, compare or match data from different sources;
* conduct systematic, extensive, or large scale profiling;
* process data relating to vulnerable people such as children;
* process special categories of data on a large scale, such as health data;
* collect data without a privacy notice;
* conduct large scale processing; consider the number of individuals involved, the volume and/or range of data and duration of the activity.

Subsection (2) explains that the intention of a DPIA is to determine the impact of the intended processing on the protection of the personal data.

Subsection (3) sets out a self-explanatory a non-exhaustive list of the elements that must be included in a DPIA.

The ICO is currently developing detailed guidance for DPIA’s for law enforcement processing, but has issued an overview [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/accountability-and-governance/data-protection-impact-assessments/).

The police force must adopt effective polices and processes to ensure that consideration is given, at an early stage in all projects or initiatives involving personal data, as to whether a DPIA is required, and where one is necessary it is undertaken in compliance with DPA Part 3 Section 64.

The Data Protection Officer must monitor compliance with DPA Part 3 Section 64 (DPIA’s) and make any necessary interventions.

[DPA Part 3 Section 65 Prior consultation with the Commissioner](http://www.legislation.gov.uk/ukpga/2018/12/section/65) states:

*(1) This section applies where a controller intends to create a filing system and process personal data forming part of it.*

*(2) The controller must consult the Commissioner prior to the processing if a data protection impact assessment prepared under section 64 indicates that the processing of the data would result in a high risk to the rights and freedoms of individuals (in the absence of measures to mitigate the risk).*

*(3) Where the controller is required to consult the Commissioner under subsection (2), the controller must give the Commissioner—*

*(a) the data protection impact assessment prepared under section 64, and*

*(b) any other information requested by the Commissioner to enable the Commissioner to make an assessment of the compliance of the processing with the requirements of this Part.*

*(4) Where the Commissioner is of the opinion that the intended processing referred to in subsection (1) would infringe any provision of this Part, the Commissioner must provide written advice to the controller and, where the controller is using a processor, to the processor.*

*(5) The written advice must be provided before the end of the period of 6 weeks beginning with receipt of the request for consultation by the controller or the processor.*

*(6) The Commissioner may extend the period of 6 weeks by a further period of one month, taking into account the complexity of the intended processing.*

*(7) If the Commissioner extends the period of 6 weeks, the Commissioner must—*

*(a) inform the controller and, where applicable, the processor of any such extension before the end of the period of one month beginning with receipt of the request for consultation, and*

*(b) provide reasons for the delay.*

**Commentary** – DPA Part 3 Section 65 requires that where a DPIA conducted under DPA Part 3 Section 64 has indicated there is a high residual risk associated with the processing the police force must consult with the ICO prior to commencing that processing. The ICO may provide written advice, usually within six weeks but longer in certain circumstances, as to how to conduct the processing or implement mitigating measures.

The ICO is currently developing detailed guidance for DPIA’s for law enforcement processing, but has issued an overview [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/accountability-and-governance/data-protection-impact-assessments/).

The police force must adopt effective polices and processes to ensure that, where a DPIA results in a residual high-risk prior, consultation occurs with the ICO in compliance with DPA Part 3 Section 64.

The Data Protection Officer must monitor compliance with DPA Part 3 Section 65 (prior consultation with the ICO) and make any necessary interventions.

## Transfers to Third Countries (DPA Part 3 Section 72, Section 73, Section 74, Section 75, Section 76, Section 77, and Section 78)

[DPA Part 3 Section 72 Overview and interpretation](http://www.legislation.gov.uk/ukpga/2018/12/section/72) states:

*(1) This Chapter deals with the transfer of personal data to third countries or international organisations, as follows—*

*(a) sections 73 to 76 set out the general conditions that apply;*

*(b) section 77 sets out the special conditions that apply where the intended recipient of personal data is not a relevant authority in a third country or an international organisation;*

*(c) section 78 makes special provision about subsequent transfers of personal data.*

*(2) In this Chapter, “relevant authority”, in relation to a third country, means any person based in a third country that has (in that country) functions comparable to those of a competent authority.*

**Commentary** – [DPA Part 3 Section 72](http://www.legislation.gov.uk/ukpga/2018/12/section/72) introduces DPA Part 3 Sections 73 to 78 which concern the transfer of personal data for law enforcement purposes to third countries or international organisations.

The transfer of personal data to a third country (which is defined in [DPA Part 3 Section 33(7)](https://www.legislation.gov.uk/ukpga/2018/12/section/33) as a country, territory that is not a member of the European Union) or to an international organisation by police forces should only take place:

* if it is necessary for a law enforcement purpose, and when the controller in the third country or international organisation carries out functions comparable to those of a Competent Authority such as a police force within the meaning of [DPA Part 3 Section 30](https://www.legislation.gov.uk/ukpga/2018/12/section/30) or
* in circumstances to a person as set out in [DPA Part 3 Section 77](https://www.legislation.gov.uk/ukpga/2018/12/section/77).

Where personal data is transferred by police forces to controllers, processors or other recipients in third countries or international organisations, the level of protection of individuals provided for in the UK by DPA Part 3 should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers or processors in the same, or in another, third country or international organisation.

[DPA Part 3 Section 73 General principles for transfers of personal](http://www.legislation.gov.uk/ukpga/2018/12/section/73) data states:

*(1) A controller may not transfer personal data to a third country or to an international organisation unless—*

*(a) the three conditions set out in subsections (2) to (4) are met, and*

*(b) in a case where the personal data was originally transmitted or otherwise made available to the controller or another competent authority by a member State other than the United Kingdom, that member State, or any person based in that member State which is a competent authority for the purposes of the Law Enforcement Directive, has authorised the transfer in accordance with the law of the member State.*

*(2) Condition 1 is that the transfer is necessary for any of the law enforcement purposes.*

*(3) Condition 2 is that the transfer—*

*(a) is based on an adequacy decision (see section 74),*

*(b )if not based on an adequacy decision, is based on there being appropriate safeguards (see section 75), or*

*(c) if not based on an adequacy decision or on there being appropriate safeguards, is based on special circumstances (see section 76).*

*(4) Condition 3 is that—*

*(a) the intended recipient is a relevant authority in a third country or an international organisation that is a relevant international organisation, or*

*(b) in a case where the controller is a competent authority specified in any of paragraphs 5 to 17, 21, 24 to 28, 34 to 51, 54 and 56 of Schedule 7—*

*(i) the intended recipient is a person in a third country other than a relevant authority, and*

*(ii) the additional conditions in section 77 are met.*

*(5) Authorisation is not required as mentioned in subsection (1)(b) if—*

*(a) the transfer is necessary for the prevention of an immediate and serious threat either to the public security of a member State or a third country or to the essential interests of a member State, and*

*(b) the authorisation cannot be obtained in good time.*

*(6) Where a transfer is made without the authorisation mentioned in subsection (1)(b), the authority in the member State which would have been responsible for deciding whether to authorise the transfer must be informed without delay.*

*(7 )In this section, “relevant international organisation” means an international organisation that carries out functions for any of the law enforcement purposes.*

[DPA Part 3 Section 74 Transfers on the basis of an adequacy decision](http://www.legislation.gov.uk/ukpga/2018/12/section/74) states:

*A transfer of personal data to a third country or an international organisation is based on an adequacy decision where—*

*(a)the European Commission has decided, in accordance with Article 36 of the Law Enforcement Directive, that—*

*(i)the third country or a territory or one or more specified sectors within that third country, or*

*(ii)(as the case may be) the international organisation,*

*ensures an adequate level of protection of personal data, and*

*(b)that decision has not been repealed or suspended, or amended in a way that demonstrates that the Commission no longer considers there to be an adequate level of protection of personal data.*

[DPA Part 3 Section 75 Transfers on the basis of appropriate safeguards](http://www.legislation.gov.uk/ukpga/2018/12/section/75) states:

*(1) A transfer of personal data to a third country or an international organisation is based on there being appropriate safeguards where—*

*(a) a legal instrument containing appropriate safeguards for the protection of personal data binds the intended recipient of the data, or*

*(b) the controller, having assessed all the circumstances surrounding transfers of that type of personal data to the third country or international organisation, concludes that appropriate safeguards exist to protect the data.*

*(2) The controller must inform the Commissioner about the categories of data transfers that take place in reliance on subsection (1)(b).*

*(3) Where a transfer of data takes place in reliance on subsection (1)—*

*(a) the transfer must be documented,*

*(b) the documentation must be provided to the Commissioner on request, and*

*(c) the documentation must include, in particular—*

*(i) the date and time of the transfer,*

*(ii) the name of and any other pertinent information about the recipient,*

*(iii) the justification for the transfer, and*

*(iv) a description of the personal data transferred.*

**Commentary** – [DPA Part 3 Section 73](http://www.legislation.gov.uk/ukpga/2018/12/section/73) requires any transfers of data to satisfy the conditions set out in subsections (2), (3) and (4). Subsection (2) requires the transfer to be necessary for any of the law enforcement purposes. Subsection (3) contains Condition two and relates to the standards of data protection in the recipient third country or international organisation.

The European Commission determines whether third countries, a territory or one or more specified sectors within a third country, or an international organisation, offer an adequate level of data protection. In such cases, transfers of personal data to those countries can take place without the need to obtain any specific authorisation, except where another Member State from which the personal data was obtained has to give its authorisation to the transfer. Adequacy decisions are published by the European Union [here](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en). They may be rescinded.

Transfers not based on such an adequacy decision are allowed only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where the police force has assessed all the circumstances surrounding transfers of that type of personal data and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist. Police forces are able to take into account cooperation agreements concluded between Europol or Eurojust and third countries which allow for the exchange of personal data when carrying out the assessment of all the circumstances

surrounding the data transfer.

A police force may also take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, a police force should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. While those conditions could be considered to be appropriate safeguards allowing the transfer of data, a police force should be able to require additional safeguards.

[DPA Part 3 Section 76 Transfers on the basis of special circumstances](http://www.legislation.gov.uk/ukpga/2018/12/section/76) states:

*(1) A transfer of personal data to a third country or international organisation is based on special circumstances where the transfer is necessary—*

*(a) to protect the vital interests of the data subject or another person,*

*(b) to safeguard the legitimate interests of the data subject,*

*(c) for the prevention of an immediate and serious threat to the public security of a member State or a third country,*

*(d) in individual cases for any of the law enforcement purposes, or*

*(e) in individual cases for a legal purpose.*

*(2) But subsection (1)(d) and (e) do not apply if the controller determines that fundamental rights and freedoms of the data subject override the public interest in the transfer.*

*(3) Where a transfer of data takes place in reliance on subsection (1)—*

*(a) the transfer must be documented,*

*(b) the documentation must be provided to the Commissioner on request, and*

*(c) the documentation must include, in particular—*

*(i) the date and time of the transfer,*

*(ii) the name of and any other pertinent information about the recipient,*

*(iii) the justification for the transfer, and*

*(iv) a description of the personal data transferred.*

*(4) For the purposes of this section, a transfer is necessary for a legal purpose if—*

*(a) it is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) relating to any of the law enforcement purposes,*

*(b) it is necessary for the purpose of obtaining legal advice in relation to any of the law enforcement purposes, or*

*(c) it is otherwise necessary for the purposes of establishing, exercising or defending legal rights in relation to any of the law enforcement purposes.*

**Commentary** – Where no adequacy decision or appropriate safeguards exist, [DPA Part 3 Section 76](https://www.legislation.gov.uk/ukpga/2018/12/section/76) provides that a transfer or a category of transfers could take place in any one of the following specific situations:

* if necessary to protect the vital interests of the data subject or another person;
* to safeguard legitimate interests of the data subject;
* for the prevention of an immediate and serious threat to the public security of a Member State or a third country;
* in an individual case for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
* in an individual case a legal purpose, including the establishment, exercise or defence of legal claims.

Such transfers should be documented and should be made available to the ICO on request in order to monitor the lawfulness of the transfer.

[DPA Part 3 Section 77 Transfers of personal data to persons other than relevant authorities](http://www.legislation.gov.uk/ukpga/2018/12/section/77) states:

*(1) The additional conditions referred to in section 73(4)(b)(ii) are the following four conditions.*

*(2) Condition 1 is that the transfer is strictly necessary in a specific case for the performance of a task of the transferring controller as provided by law for any of the law enforcement purposes.*

*(3) Condition 2 is that the transferring controller has determined that there are no fundamental rights and freedoms of the data subject concerned that override the public interest necessitating the transfer.*

*(4) Condition 3 is that the transferring controller considers that the transfer of the personal data to a relevant authority in the third country would be ineffective or inappropriate (for example, where the transfer could not be made in sufficient time to enable its purpose to be fulfilled).*

*(5) Condition 4 is that the transferring controller informs the intended recipient of the specific purpose or purposes for which the personal data may, so far as necessary, be processed.*

*(6) Where personal data is transferred to a person in a third country other than a relevant authority, the transferring controller must inform a relevant authority in that third country without undue delay of the transfer, unless this would be ineffective or inappropriate.*

*(7) The transferring controller must—*

*(a) document any transfer to a recipient in a third country other than a relevant authority, and*

*(b )inform the Commissioner about the transfer.*

*(8) This section does not affect the operation of any international agreement in force between member States and third countries in the field of judicial co-operation in criminal matters and police co-operation.*

**Commentary** – In specific individual cases, the regular procedures requiring transfer of personal data to a

relevant authority in a third country may be ineffective or inappropriate, in particular because the transfer could not be carried out in a timely manner, or because that authority in the third country does not respect the rule of law or international human rights norms and standards, so that a police force could decide to transfer personal data directly to recipients established in those third countries. This may be the case where there is an urgent need to transfer personal data to save the life of a person who is in danger of becoming a victim of a criminal offence or in the interest of preventing an imminent perpetration of a crime, including terrorism.

Such a transfer between police forces and recipients established in third countries should take place only in specific individual cases, and subject to the specific provisions of DPA Part 3. These provisions should not be considered to be derogations from any existing agreements and the requirements should apply in addition to the others in DPA Part 3 and with particular regard to the lawfulness of processing.

[DPA Part 3 Section 78 Subsequent transfers](http://www.legislation.gov.uk/ukpga/2018/12/section/78) states:

*(1) Where personal data is transferred in accordance with section 73, the transferring controller must make it a condition of the transfer that the data is not to be further transferred to a third country or international organisation without the authorisation of the transferring controller or another competent authority.*

*(2) A competent authority may give an authorisation under subsection (1) only where the further transfer is necessary for a law enforcement purpose.*

*(3 )In deciding whether to give the authorisation, the competent authority must take into account (among any other relevant factors)—*

*(a) the seriousness of the circumstances leading to the request for authorisation,*

*(b) the purpose for which the personal data was originally transferred, and*

*(c) the standards for the protection of personal data that apply in the third country or international organisation to which the personal data would be transferred.*

*(4) In a case where the personal data was originally transmitted or otherwise made available to the transferring controller or another competent authority by a member State other than the United Kingdom, an authorisation may not be given under subsection (1) unless that member State, or any person based in that member State which is a competent authority for the purposes of the Law Enforcement Directive, has authorised the transfer in accordance with the law of the member State.*

*(5) Authorisation is not required as mentioned in subsection (4) if—*

*(a) the transfer is necessary for the prevention of an immediate and serious threat either to the public security of a member State or a third country or to the essential interests of a member State, and*

*(b) the authorisation cannot be obtained in good time.*

*(6) Where a transfer is made without the authorisation mentioned in subsection (4), the authority in the member State which would have been responsible for deciding whether to authorise the transfer must be informed without delay.*

**Commentary** – [DPA Part 3 Section 78](https://www.legislation.gov.uk/ukpga/2018/12/section/78) requires that where personal data is transferred from the UK to third countries or international organisation, any subsequent transfer should, in principle, take place only after the police force from which the data was obtained has given its authorisation to the transfer.

Onward transfers of personal data should be subject to prior authorisation by the police force that carried out the original transfer (the original transfer should provide the recipient with any specific handling conditions).

When deciding on a request for the authorisation of an onward transfer, the police force that carried out the original transfer should take due account of all relevant factors, including the seriousness of the criminal offence, the specific conditions subject to which, and the purpose for which, the data was originally transferred, the nature and conditions of the execution of the criminal penalty, and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

The police force that carried out the original transfer should also be able to subject the onward transfer to specific conditions. Such specific conditions can be described, for example, in handling codes.

The ICO has issued guidance on international transfers [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/). Guidance on data protection and Brexit can be found [here](https://ico.org.uk/for-organisations/data-protection-and-brexit/).

The police force must document their regular overseas transfers of personal data for law enforcement purposes.

The Data Protection Officer must monitor compliance with DPA Part 3 Sections 72 to 78 (transfers to third countries and make any necessary interventions.

## Safeguards: Archiving (DPA Part 3 Section 41)

[DPA Part 3 Section 41 Safeguards: archiving](http://www.legislation.gov.uk/ukpga/2018/12/section/41) states:

*(1) This section applies in relation to the processing of personal data for a law enforcement purpose where the processing is necessary—*

*(a) for archiving purposes in the public interest,*

*(b) for scientific or historical research purposes, or*

*(c) for statistical purposes.*

*(2) The processing is not permitted if—*

*(a) it is carried out for the purposes of, or in connection with, measures or decisions with respect to a particular data subject, or*

*(b) it is likely to cause substantial damage or substantial distress to a data subject*.

**Commentary** – [DPA Part 3 Section 41](http://www.legislation.gov.uk/ukpga/2018/12/section/41) provides safeguards in relation to the processing of personal data for a law enforcement purpose where the processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes.

Such processing is prohibited where it is carried out in relation to a measure or decisions in respect of a particular data subject or it is likely to cause substantial damage or substantial distress to a data subject.

This provision is likely to apply where police forces choose to retain for historical or archiving purposes records of major investigations that have been subject of significant public and/or media interest. In addition to compliance with this provision there will usually is also a requirement to meet a condition for sensitive processing from DPA Schedule 8.

The ICO does not appear to have produced guidance on archiving safeguards for law enforcement processing.

The police force must adopt measures to ensure that where processing is for a law enforcement purpose and concerns archiving in the public interest, scientific, historical or statistical purposes that the processing is not used to make decisions about a data subject or is likely to cause substantial damage or substantial distress to a data subject.

The Data Protection Officer must monitor their police force’s ongoing compliance with the DPA Part 3 Section 41 (Safeguards: Archiving) obligations and make any necessary interventions.

## Safeguards: Sensitive Processing (Appropriate Policy Document) (DPA Part 3 Section 42) (Appendix D)

[DPA Part 3 Section 42 Safeguards: sensitive processing](http://www.legislation.gov.uk/ukpga/2018/12/section/42) states:

*(1) This section applies for the purposes of section 35(4) and (5) (which require a controller to have an appropriate policy document in place when carrying out sensitive processing in reliance on the consent of the data subject or, as the case may be, in reliance on a condition specified in Schedule 8).*

*(2) The controller has an appropriate policy document in place in relation to the sensitive processing if the controller has produced a document which—*

*(a) explains the controller’s procedures for securing compliance with the data protection principles (see section 34(1)) in connection with sensitive processing in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, and*

*(b) explains the controller’s policies as regards the retention and erasure of personal data processed in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, giving an indication of how long such personal data is likely to be retained.*

*(3) Where personal data is processed on the basis that an appropriate policy document is in place, the controller must during the relevant period—*

*(a) retain the appropriate policy document,*

*(b) review and (if appropriate) update it from time to time, and*

*(c) make it available to the Commissioner, on request, without charge.*

*(4) The record maintained by the controller under section 61(1) and, where the sensitive processing is carried out by a processor on behalf of the controller, the record maintained by the processor under section 61(3) must include the following information—*

*(a) whether the sensitive processing is carried out in reliance on the consent of the data subject or, if not, which condition in Schedule 8 is relied on,*

*(b) how the processing satisfies section 35 (lawfulness of processing), and*

*(c) whether the personal data is retained and erased in accordance with the policies described in subsection (2)(b) and, if it is not, the reasons for not following those policies.*

*(5) In this section, “relevant period”, in relation to sensitive processing in reliance on the consent of the data subject or in reliance on a condition specified in Schedule 8, means a period which—*

*(a) begins when the controller starts to carry out the sensitive processing in reliance on the data subject’s consent or (as the case may be) in reliance on that condition, and*

*(b) ends at the end of the period of 6 months beginning with the day the controller ceases to carry out the processing.*

**Commentary** – [DPA Part 3 Section 42](http://www.legislation.gov.uk/ukpga/2018/12/section/42) makes further provision concerning the requirement arising from the first law enforcement principle [DPA Part 3 Section 35(4) and (5)](http://www.legislation.gov.uk/ukpga/2018/12/section/35) for controllers, in certain circumstances, to have an appropriate policy document in place when carrying out sensitive processing in reliance on the consent of the data subject or, as the case may be, in reliance on a condition specified in [Schedule 8](http://www.legislation.gov.uk/ukpga/2018/12/schedule/8).

Subsection (1) introduces the requirement. Subsection (2) sets out what an appropriate policy document must include. Subsection (3) requires the appropriate policy document to be retained for the relevant period (which is set out in subsection 5), reviewed and updated if appropriate, and provided to the ICO upon request. Subsection (4) sets out what a processor must include in their Records of Processing Activities (under [DPA Part 3 Section 61](http://www.legislation.gov.uk/ukpga/2018/12/section/61)) where sensitive processing is involved.

[DPA Part 7 Section 205 General interpretation](http://www.legislation.gov.uk/ukpga/2018/12/section/205) confirms that the definition of month in respect of DPA Part 3 Section 42 is that set out in [Article 3 of Regulation (ECC, Euratom) No. 1182/71 of the Council of 3rd June 1971](file:///C:\Users\42006032\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\AppData\Local\Temp\DOC_1.en.xhtml).

An Appropriate Policy Template can be found at [Appendix D](#_Appendix_D:_Appendix).

A similar requirement for an Appropriate Policy Document arises for General processing via DPA Schedule 1 Part 4

The ICO has published an appropriate policy documents for law enforcement processing which can be found [here](https://ico.org.uk/media/for-organisations/documents/2616230/part-3-appropriate-policy-document.docx).

The police force must adopt measures to ensure that where processing is for law enforcement purposes by themselves or Processors appropriate policy documents are produced, where required, which meet DPA Part 3 Section 42 obligations.

The Data Protection Officer must monitor their police force’s ongoing compliance with the DPA Part 3 Section 42 (Appropriate Policy Document) obligations and make any necessary interventions.

## Re-use of Data Collected for Law Enforcement Processing for General Processing

**Commentary** – There will be circumstances where personal data is initially processed by a police force for one of the law enforcement purposes, but subsequently there emerges a desire or requirement by the police force to process the personal data for general purposes. Examples include disclosure of personal data of suspects, witnesses, victims and others by the police to employers or regulatory bodies.

When determining if such ‘movement from Part 3 to Part 2’ is appropriate police forces should:

* Confirm that the initial/current processing was/is for law enforcement purposes.
* Confirm that the initial/current processing was/is compliant with DPA Part 3 and any other lawful obligations
* Determine the nature, scope and purposes of the intended processing.
* Confirm that the intended processing is for general purposes.
* Test the intended processing for compliance with the GDPR/DPA Part 2

The ICO does not appear to have publish any specific guidance on the re-use of data collected for law enforcement processing for general processing.

## Request to external organisation for the disclosure of personal data to the police (Appendix E)

**Commentary** – The form at [Appendix E](#_Appendix_E:_Request) may be used by the police when making a formal request to other organisations for personal data where disclosure is necessary for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders. It places no compulsion on the recipient to disclose the information, but should provide necessary reassurance that a disclosure for these purposes is appropriate and in compliance with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

The form has also been published on the College of Policing’s Knowledge Hub.

# Intelligence Service Processing (Part 4 of the Act)

## Overview:

**Commentary** – The processing of personal data in connection with national security activities and processing by the Intelligence Services – defined as the Security Service, the Secret Intelligence Service and the Government Communications Headquarters - is not within scope of the GDPR, as a result of which the provisions of the GDPR were not designed to be applicable to the unique nature of intelligence service processing. Part 4 of the Act therefore provides a data protection regime for the processing of personal data by the intelligence services.

When police forces make disclosures of personal data to the Intelligence Services that processing is regarded as being Law Enforcement Processing and subject to DPA Part 3.

When the Intelligence Services make disclosures of personal data to police forces that processing is regarded as being Intelligence Services’ Processing and subject to DPA Part 4.

The ICO has published guidance on the processing of personal data by Intelligence Services which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

# Assessing Data Protection Compliance

## Audit

**Commentary** – Detailed guidance on audit, health checks on forces’ compliance with the GDPR and DPA, and transaction monitoring is currently under development.

## Consensual Audit by the Commissioner (DPA Part 5 Section 129)

[DPA Part 5 Section 129](http://www.legislation.gov.uk/ukpga/2018/12/section/129) states:

*(1) The Commissioner’s functions under Article 58(1) of the GDPR and paragraph 1 of Schedule 13 include power, with the consent of a controller or processor, to carry out an assessment of whether the controller or processor is complying with good practice in the processing of personal data.*

*(2) The Commissioner must inform the controller or processor of the results of such an assessment.*

*(3) In this section, “good practice in the processing of personal data” has the same meaning as in section 128.*

The definition of “good practice in the processing of personal data” is defined at [DPA Part 5 Section 128(5)](http://www.legislation.gov.uk/ukpga/2018/12/section/128) as follows:

*“good practice in the processing of personal data” means such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, including compliance with the requirements of the data protection legislation;*

**Commentary** – [DPA Part 5 Section 129](http://www.legislation.gov.uk/ukpga/2018/12/section/129) permits the ICO with the consent, in the case of the police, of a Chief Officer of a police force or a processor used by the police force to carry out an assessment of whether the controller or processor is complying with good practice. It requires the ICO to inform the controller or processor of the results of that assessment.

The definition of “good practice in the processing of personal data” indicates the processing is likely to be regarded as good practice by the ICO if police forces can show adequate consideration has been given to the interests of data subjects and others (presumably including the police force) and compliance with the GDPR and Act.

The intention appears to be that the Chief Officer can seek reassurance that processing by themselves or a processor working on their behalf meets good practice requirements, rather than a processor seeking an assessment of the Chief Officer’s processing.

It is unlikely that a particular processing operation by or on behalf of a police force would be considered anything other than meeting good practice requirements if the processing was being undertaken in accordance with published ICO guidance.

Where a police force is subject of audit by the ICO the likelihood, in the case of a failure to achieve best practice, is that the ICO will make recommendations for improvement that the police force will need to undertake.

## Aide Memoire for a model approach to assessing data protection compliance

**Commentary** – The tables below are intended to provide a structure for determining whether a particular processing operation is in compliance with data protection legislation. Table 1 provides a series of preliminary considerations which help determine the nature of any processing operation. From that table either Table 2 or 3 can then be considered for law enforcement and general processing respectively.

Beyond what is set out in the tables below there is also the requirement to satisfy controller and processor obligations ([DPA Part 3 Chapter 4](http://www.legislation.gov.uk/ukpga/2018/12/part/3/chapter/4/)) for law enforcement processing, or [GDPR Articles 24 to 43](https://gdpr-info.eu/chapter-4/) (Chapter 4) for general processing.

**Table 1**

|  |  |
| --- | --- |
| **FOR ANY PROCESSING…** |  |
| Confirm that **Personal Data** is involved and identify that information; |  |
| Identify **Data Subject(s)**; |  |
| Identify who is **Controller** (alone or joint) and status of any other party or parties involved including **Processors, Recipients, and Third Parties**; |  |
| Confirm the **Processing** operations in question including the point at which a controller’s jurisdiction starts and ends; |  |
| Identify if any **Third Country or International** **transfers** occur; |  |
| Confirm if any **Special Category Data** is being processed as defined at [GDPR Article 9(1):](https://gdpr-info.eu/art-9-gdpr/)  Reveals racial or ethnic origin;  Reveals political opinions;  Reveals religious or philosophical beliefs;  Reveals trade union membership;  Is genetic data or biometric data used to uniquely identify a person;  Is data concerning health;  Is data concerning a person’s sex life or sexual orientation; |  |
| Confirm if any ‘**Criminal Offence Data’** is being processed, as per [GDPR Article 10](https://gdpr-info.eu/art-10-gdpr/) *(personal data relating to criminal convictions and offences or related security measures)* and partially further defined at [DPA Part 2 Section 11](http://www.legislation.gov.uk/ukpga/2018/12/section/11) (*personal data relating to criminal convictions and offences or related security measures including* *the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.)*; |  |
| Confirm if there is any **Sensitive Processin**g, as defined at [DPA Part 3 Section 35(8)](http://www.legislation.gov.uk/ukpga/2018/12/section/35), occurring *(that revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic or biometric data; health related; concerning sex life or sexual orientation);* |  |
| Determine the **Purpose** of the processing; |  |
| Identify if the processing is:   * **Law Enforcement Processing** (DPA Part 3) *(for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security);* or, * **General Processing**(GDPR/DPA Part 2) *(anything other than for one of the law enforcement purposes),*   and follow instructions in either Table 2 or Table 3 below. |  |

**Table 2**

|  |  |
| --- | --- |
| **IF LAW ENFORCEMENT PROCESSING** *(for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security)* **…** |  |
| **Consider Law Enforcement 1st Principle (Lawful & Fair)** ([DPA Part 3 Section 35](http://www.legislation.gov.uk/ukpga/2018/12/section/35)) and ensure: |  |
| No rule of law prohibiting the processing is transgressed (including that arising from the application of any rights of rectification, erasure or restriction under the DPA); |  |
| The processing is authorised by either statute, common law, royal prerogative or by or under any other rule of law; |  |
| Either of the following two processing conditions under [DPA Part 3 Section 35(2)](http://www.legislation.gov.uk/ukpga/2018/12/section/35) apply:  Consent has been obtained, in compliance with ICO Guidance, or  Processing is necessary for task carried out by a [competent authority](http://www.legislation.gov.uk/ukpga/2018/12/section/30); |  |
| Where **Sensitive Processing** occurs (see Table 1) either of the two following cases exist:  [DPA Part 3 Section 35(4)](http://www.legislation.gov.uk/ukpga/2018/12/section/35) - Consent has been obtained, in compliance with ICO Guidance and an appropriate policy document exists [as per DPA Part 3 Section 42](http://www.legislation.gov.uk/ukpga/2018/12/section/42).  or  [DPA Part 3 Section 35(5)](http://www.legislation.gov.uk/ukpga/2018/12/section/35) - Processing is strictly necessary, an appropriate policy document exists [as per DPA Part 3 Section 42](http://www.legislation.gov.uk/ukpga/2018/12/section/42), and one of the following [DPA Schedule 8](http://www.legislation.gov.uk/ukpga/2018/12/schedule/8) conditions is met:  1 Statutory etc. purposes  2 Administration of justice  3 Protecting individual’s vital interests  4 Safeguarding of children and of individuals at risk  5 Personal data already in the public domain  6 Legal claims  7 Judicial acts  8 Preventing fraud  9 Archiving etc; |  |
| The processing is in accordance with data subjects’ reasonable expectations (fair); measures to provide privacy information are in place; the general notice adequately describes the purpose; direct notices provide information about specific categories of processing including retention periods and transfers. |  |
|  |  |
| **Consider Law Enforcement 2nd Principle (Specific, Explicit & Legitimate Purpose)** ([DPA Part 3 Section 36)](http://www.legislation.gov.uk/ukpga/2018/12/section/36) and ensure: |  |
| The purpose for collecting the personal data is specified, explicit and legitimate; |  |
| Processing is compatible with the purpose it was collected for; |  |
| Personal data collected for the law enforcement purpose is not otherwise processed unless it is authorised by law to do so. |  |
|  |  |
| **Consider Law Enforcement 3rd Principle (Adequate, Relevant & Not Excessive)** ([DPA Part 3 Section 37](http://www.legislation.gov.uk/ukpga/2018/12/section/37)) and ensure personal data is: |  |
| Adequate for the purpose; |  |
| Relevant to the purpose; |  |
| Not Excessive for purpose. |  |
|  |  |
| **Consider Law Enforcement 4th Principle (Accurate & Kept-up-to-date where necessary)** ([DPA Part 3 Section 37](http://www.legislation.gov.uk/ukpga/2018/12/section/37)) and ensure personal data: |  |
| Is accurate with distinction between fact-based and opinion-based; |  |
| Is kept up-to-date where necessary; |  |
| Distinguishes between suspects, offenders, victims, witness & others where relevant; |  |
| Is erased or rectified if inaccurate without delay; |  |
| Is not transmitted or made available if inaccurate, incomplete or out-of-date. |  |
|  |  |
| **Consider Law Enforcement 5th Principle (Kept no longer than is necessary)** ([DPA Part 3 Section 39](http://www.legislation.gov.uk/ukpga/2018/12/section/39)) and ensure: |  |
| Personal data is not kept longer than is necessary; |  |
| It is possible to justify the retention in relation to the purpose of the processing; |  |
| A written retention, review and deletion policy exists for the personal data; |  |
| Personal data is subject to periodic review and is anonymized, erased or disposed of when no longer needed. |  |
|  |  |
| **Consider Law Enforcement 6th Principle (Processed Securely)** ([DPA Part 3 Section 40](http://www.legislation.gov.uk/ukpga/2018/12/section/40)) and ensure: |  |
| Appropriate measures are in place to prevent the personal data being accidentally or deliberately compromised; |  |
| Those measures are commensurate to the nature of the personal data and the nature of harm that could result from a compromise or data breach; |  |
| Those measures include physical, technical, and procedural types and have been developed in consideration of the reliability and training of staff involved in the processing; |  |
| Appropriate measures are in place to swiftly and effectively identify, respond to and manage information security incidents and data breaches (including notification to the Commissioner and data subject) ([DPA Part 3 Sections 67](http://www.legislation.gov.uk/ukpga/2018/12/section/67) and [68](http://www.legislation.gov.uk/ukpga/2018/12/section/68)) involving the personal data; |  |
| [DPA Part 3 Section 66](http://www.legislation.gov.uk/ukpga/2018/12/section) Security of processing requirements are met. |  |
|  |  |
| **Consider Law Enforcement Accountability Requirement** [(DPA Part 3 Section 34(3)](http://www.legislation.gov.uk/ukpga/2018/12/section/34/)) and ensure: |  |
| It is possible to demonstrate compliance with all the Law Enforcement Principles. |  |
|  |  |
| **Consider Other DPA Part 3 Controller & Processor Obligations** and ensure: |  |
| Compliance with Controller’s general duties ([DPA Part 3 Section 44](http://www.legislation.gov.uk/ukpga/2018/12/section/44)); |  |
| Appropriate technical & organisational measures, including policy as required by [DPA Part 3 Section 56](http://www.legislation.gov.uk/ukpga/2018/12/section/56) are implemented; |  |
| Data Protection by Design & Default requirements set out in [DPA Part 3 Section 57](http://www.legislation.gov.uk/ukpga/2018/12/section/57) are met; |  |
| Where joint controllership exists that each parties’ respective obligations under [DPA Part 3 Section 58](http://www.legislation.gov.uk/ukpga/2018/12/section/58)  to comply with the GDPR are documented; |  |
| Where a processor is employed [DPA Part 3 Section 59](http://www.legislation.gov.uk/ukpga/2018/12/section/59) and [60](http://www.legislation.gov.uk/ukpga/2018/12/section/60) obligations are met including the requirement for a data processing contract to be place; |  |
| Records of processing arrangements are maintained in accordance with [DPA Part 3 Section 61](http://www.legislation.gov.uk/ukpga/2018/12/section/61); |  |
| Logs are maintained in accordance with [DPA Part 3 Section 62](http://www.legislation.gov.uk/ukpga/2018/12/section/62); |  |
| Data Protection Impact Assessments (DPIA’s) are conducted in accordance [DPA Part 3 Section 64](http://www.legislation.gov.uk/ukpga/2018/12/section/64) and [65](http://www.legislation.gov.uk/ukpga/2018/12/section/65) where required. |  |
|  |  |
| **Where necessary, consider transfers of personal data to countries or territories beyond the European Union or to international organisations for law enforcement purposes (**[**third countries)**](http://www.legislation.gov.uk/ukpga/2018/12/section/33) ([DPA Part 3 Chapter 5](http://www.legislation.gov.uk/ukpga/2018/12/part/3/chapter/5)) and ensure: |  |
| Where the transfer is to competent authorities it is in compliance with [DPA Part 3 Section 73](http://www.legislation.gov.uk/ukpga/2018/12/section/73) General principles for transfers of personal data, including where a third country is ‘adequate’ ([DPA Part 3 Section 74](http://www.legislation.gov.uk/ukpga/2018/12/section/74)) or where there are appropriate safeguards ([DPA Part 3 Section 75](http://www.legislation.gov.uk/ukpga/2018/12/section/75)), or special circumstances apply ([DPA Part 3 Section 76](http://www.legislation.gov.uk/ukpga/2018/12/section/76)).  or  Where the transfer is other than to competent authorities it is compliance with [DPA Part 3 Section 77](http://www.legislation.gov.uk/ukpga/2018/12/section/77); |  |
| Conditions regarding subsequent transfers are set as required by DPA [Part 3 Section 78](http://www.legislation.gov.uk/ukpga/2018/12/section/78). |  |
|  |  |
| **If processing is for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes** ensure it compliant with [DPA Part 3 Section 41](http://www.legislation.gov.uk/ukpga/2018/12/section/41). |  |

**Table 3**

|  |  |
| --- | --- |
| **IF GENERAL PROCESSING***…* |  |
| **Consider GDPR 1st Principle (Lawful, Fair & Transparent)** ([GDPR Article 5](https://gdpr-info.eu/art-5-gdpr/)) and ensure: |  |
| No rule of law prohibiting the processing is transgressed (including that arising from the application of any rights of rectification, erasure or restriction under the DPA/GDPR); |  |
| One of the five available [GDPR Article 6(1)](https://gdpr-info.eu/art-6-gdpr/) **Processing Conditions** exists for all of the personal data including Special Category Data and Criminal Offence Data *(Note: The Police are unable to use (f) Legitimate Interests)*:  (a) Consent;  (b) Contract;  (c) Legal Obligation;  (d) Vital Interests;  (e) Public Task (see [DPA Part 2 Section 8](http://www.legislation.gov.uk/ukpga/2018/12/section/8/enacted) for examples); |  |
| If **Consent** is used it complies with definition at [GDPR Article 4(11)](https://gdpr-info.eu/art-4-gdpr/), requirements at [GDPR Article 7 (Conditions for Consent)](https://gdpr-info.eu/art-7-gdpr/), and [ICO Guidance](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/) (subject to exemption for **Special Purposes** at DPA Schedule 2 Part 5 Paragraph 24); |  |
| For any **Special Category Data** being processed, in addition to a [GDPR Article 6(1)](https://gdpr-info.eu/art-6-gdpr/) **Processing Condition** being met, one of the following [GDPR Article 9(2)](https://gdpr-info.eu/art-9-gdpr/) **Special Processing Conditions** applies:  (a) Explicit Consent;  (b) Employment, Social Security & Social Protection;  (c) Vital Interests;  (d) Political, Philosophical, Religious or Trade Union  (e) Made Public by Data Subject;  (f) Defence of Legal Claims;  (g) Substantial Public Interest;  (h) Health and Social Care;  (i) Public Health;  (j) Archiving, Research & Statistics  **And**  in the case of (b) Employment, Social Security and Protection, or (h) Health and Social Care, or (i) Public Health, or (j) Archiving, Research and Statistics, a condition in [DPA Schedule 1 Part 1](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1) applies;  or  in the case of (g) Substantial Public Interest, a condition in [DPA Schedule 1 Part 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1) applies;  And  An **Appropriate Policy Document** is created and maintained in accordance with [DPA Schedule 1 Part 4](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/part/4) if a condition in DPA Schedule 1 Part 1 or 2 is used; |  |
| If the purpose of the processing differs from the initial purpose when the data was collected, and the processing is not based on consent or law, compatibility of the new use is tested using [GDPR Article 6(4)](https://gdpr-info.eu/art-6-gdpr/); |  |
| For any **Criminal Offence Data** being processed, in addition to a [GDPR Article 6(1)](https://gdpr-info.eu/art-6-gdpr/) **Processing Condition** being met; compliance with [GDPR Article 10](https://gdpr-info.eu/art-10-gdpr/) is achieved; a [DPA Schedule 1 Part 1, 2 or 3](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1) is condition is met, an **Appropriate Policy Document** is created in accordance with [DPA Schedule 1 Part 4;](http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/part/4) and the processing is authorised by law as a clear and foreseeable application of a common law task, function or power, a statutory provision, or statutory guidance; |  |
| Fairness & Transparency requirements under [GDPR Articles 12](https://gdpr-info.eu/art-12-gdpr/) [13](https://gdpr-info.eu/art-13-gdpr/) [14](https://gdpr-info.eu/art-14-gdpr/) are met; |  |
| Consideration is given to the appropriate use [DPA Schedule 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/) exemptions where justified. |  |
|  |  |
| **Consider GDPR 2nd Principle (Purpose Limitation)** ([GDPR Article 5](https://gdpr-info.eu/art-5-gdpr/)) and ensure: |  |
| Processing is in a manner that is compatible or where is for archiving in public interest, scientific or historical research or statistical purposes is exempt from that requirement by virtue of [GDPR 89(1);](https://gdpr-info.eu/art-89-gdpr/) |  |
| Consideration is given to the appropriate use [DPA Schedule 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/) exemptions where justified including:  **Crime & Taxation.** DPA Schedule 2 Part 1 Paragraph 2  **Disclosure Required by Law.** DPA Schedule 2 Part 1 Paragraph 3  **Special Purposes.** DPA Schedule 2 Part 5 Paragraph 24. |  |
|  |  |
| **Consider GDPR 3rd Principle (Data Minimisation)** ([GDPR Article 5](https://gdpr-info.eu/art-5-gdpr/)) and ensure: |  |
| Personal data is adequate for the purpose(s) of processing; |  |
| Personal data is relevant for the purpose(s) of processing; |  |
| Personal data is limited to that required for the purpose(s) of processing; |  |
| Consideration is given to the appropriate use [DPA Schedule 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/) exemptions where justified including:  **Crime & Taxation.** DPA Schedule 2 Part 1 Paragraph 2  **Disclosure Required by Law.** DPA Schedule 2 Part 1 Paragraph 3  **Special Purposes.** DPA Schedule 2 Part 5 Paragraph 24. |  |
|  |  |
| **Consider GDPR 4th Principle (Accuracy)** ([GDPR Article 5](https://gdpr-info.eu/art-5-gdpr/)) and ensure: |  |
| Personal data is accurate for the purpose(s) of the processing; |  |
| Personal data is up-to-date where necessary for the purpose(s) of the processing; |  |
| Personal data is erased or rectified without delay where required; |  |
| Consideration is given to the appropriate use [DPA Schedule 2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/) exemptions where justified including:  **Special Purposes.** DPA Schedule 2 Part 5 Paragraph 24. |  |
|  |  |
| **Consider GDPR 5th Principle (Storage Limitation)** ([GDPR Article 5](https://gdpr-info.eu/art-5-gdpr/)) and ensure: |  |
| Personal data enabling the identification of data subjects is retained no longer than is necessary for the purpose(s) of the processing;  except where continued retention is solely for archiving in the public interest, scientific or historical research or statistical purposes in accordance with [GDPR Article 89](https://gdpr-info.eu/art-89-gdpr/) & measures required by the GDPR are in place to safeguard the rights and freedoms of the data subjects. |  |
|  |  |
| **Consider GDPR 6th Principle (Integrity & Confidentiality)** ([GDPR Article 5](https://gdpr-info.eu/art-5-gdpr/)) and ensure: |  |
| Appropriate measures are in place to prevent the personal data being accidentally or deliberately compromised; |  |
| Those measures are commensurate to the nature of the personal data and the nature of harm that could result from a compromise or data breach; |  |
| Those measures include physical, technical, and procedural types and have been developed in consideration of the reliability and training of staff involved in the processing; |  |
| Appropriate measures are in place to swiftly and effectively identify, respond to and manage information security incidents and data breaches (including notification to the Commissioner and data subject) ([GDPR Article 33](https://gdpr-info.eu/art-33-gdpr/) and [34](https://gdpr-info.eu/art-34-gdpr/)) involving the personal data; |  |
| [GDPR Article 32](https://gdpr-info.eu/art-32-gdpr/) Security of processing requirements are met. |  |
|  |  |
| **Consider GDPR Accountability Requirement** ([GDPR Article 5](https://gdpr-info.eu/art-5-gdpr/)) and ensure: |  |
| It is possible to demonstrate compliance with all the GDPR Principles. |  |
|  |  |
| **Consider Other GDPR Controller & Processor Obligations** and ensure: |  |
| Appropriate technical & organisational measures, including policy as required by [GDPR Article 24](https://gdpr-info.eu/art-24-gdpr/) are implemented; |  |
| Data Protection by Design & Default requirements set out in [GDPR Article 25](https://gdpr-info.eu/art-25-gdpr/) are met; |  |
| Where joint controllership exists that each parties’ respective obligations under [GDPR Article 26](https://gdpr-info.eu/art-26-gdpr/) to comply with the GDPR are documented; |  |
| Where a processor is employed [GDPR Articles 28](https://gdpr-info.eu/art-28-gdpr/) and [29](https://gdpr-info.eu/art-29-gdpr/) obligations are met including the requirement for a data processing contract to be place; |  |
| Records of processing arrangements are maintained in accordance with [GDPR Article 30](https://gdpr-info.eu/art-30-gdpr/); |  |
| Data Protection Impact Assessments (DPIA’s) are conducted in accordance with [GDPR Articles 35](https://gdpr-info.eu/art-35-gdpr/) and [36](https://gdpr-info.eu/art-36-gdpr/) where required. |  |
|  |  |
| **Where necessary, consider restricted transfers of personal data for general processing purposes to countries or territories beyond the European Union or to international organisations (**[**third countries)**](http://www.legislation.gov.uk/ukpga/2018/12/section/33)and ensure: |  |
| The restricted transfer is in compliance with [GDPR Article 44](https://gdpr-info.eu/art-44-gdpr/) General principles for transfers of personal data, including where a third country is ‘adequate’ ([GDPR Article 45](https://gdpr-info.eu/art-45-gdpr/)) or where there are appropriate safeguards ([GDPR Article 46](https://gdpr-info.eu/art-46-gdpr/), [47](https://gdpr-info.eu/art-47-gdpr/) or [48](https://gdpr-info.eu/art-48-gdpr/)), or an [GDPR Article 49](https://gdpr-info.eu/art-49-gdpr/) condition applies. |  |

# The Commissioner, Enforcement & Offences (Part 5, 6 & 7 of Act)

## Co-operation with the Commissioner & their Powers

### Co-operation with the Commissioner (GDPR Article 31, DPA Part 5 Section 63)

GDPR Article 31 (Co-operation with the supervisory authority) states:

*The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.*

[DPA Part 3 Section 63 Co-operation with the Commissioner](http://www.legislation.gov.uk/ukpga/2018/12/section/63) states:

*Each controller and each processor must co-operate, on request, with the Commissioner in the performance of the Commissioner’s tasks.*

**Commentary** – GDPR Article 31 and [DPA Part 3 Section 63](http://www.legislation.gov.uk/ukpga/2018/12/section/63) require that police forces and any processor they use must co-operate with the Commissioner upon request in respect of any processing conducted by them.

The Data Protection Officer should ensure their police force and their Processors respond readily and comprehensively to any inquiry or request from the ICO. The police force may wish to set out this requirement in any data processing contract they initiate.

### Disclosure of information to the Commissioner (DPA Part 5 Section 131)

[DPA Part 5 Section 131 Disclosure of information to the Commissioner](http://www.legislation.gov.uk/ukpga/2018/12/section/131) states:

*(1) No enactment or rule of law prohibiting or restricting the disclosure of information precludes a person from providing the Commissioner with information necessary for the discharge of the Commissioner’s functions.*

*(2) But this section does not authorise the making of a disclosure which is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.*

*(3) Until the repeal of Part 1 of the Regulation of Investigatory Powers Act 2000 by paragraphs 45 and 54 of Schedule 10 to the Investigatory Powers Act 2016 is fully in force, subsection (2) has effect as if it included a reference to that Part.*

**Commentary** – [DPA Part 5 Section 131](http://www.legislation.gov.uk/ukpga/2018/12/section/131) makes clear that any person is not precluded by any other domestic legislation or rule of law from disclosing to the ICO information needed by the ICO in relation to the ICO’s functions as defined the GDPR and Act.

In addition, it encompasses other functions which have been conferred on the ICO by domestic legislation. The ICO has regulatory functions under the [Privacy and Electronic Communications Regulations 2003](http://www.legislation.gov.uk/uksi/2003/2426/contents/made), the [Environmental Information Regulations 2004 (S.I. 2004/3391),](http://www.legislation.gov.uk/uksi/2004/3391/contents/made) the [INSPIRE Regulations 2009 (S.I. 2009/3157](http://www.legislation.gov.uk/uksi/2009/3157/contents)) or the [INSPIRE (Scotland) Regulations (S.I. 2009/440](http://www.legislation.gov.uk/ssi/2009/440/contents/made)), the [Re-use of Public Sector Information Regulations 2015 (S.I. 2015/1415)](http://www.legislation.gov.uk/uksi/2015/1415/contents), the [Freedom of Information Act 2000](http://www.legislation.gov.uk/ukpga/2000/36/contents), the [Freedom of Information Act (Scotland) 2002](http://www.legislation.gov.uk/asp/2002/13/contents), the [Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (S.I. 2016/696](http://www.legislation.gov.uk/uksi/2016/696/contents/made)), and [Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market](https://publications.europa.eu/en/publication-detail/-/publication/23b61856-2e82-11e4-8c3c-01aa75ed71a1/language-en).

The ICO has produced guidance on the [Privacy and Electronic Communications Regulations 2003 (PECR)](https://ico.org.uk/for-organisations/guide-to-pecr/)

### Offence regarding breach of confidentiality by the Commissioner (DPA Part 5 Section 132)

[DPA Part 5 Section 132 Confidentiality of information](http://www.legislation.gov.uk/ukpga/2018/12/section/132) states:

*(1) A person who is or has been the Commissioner, or a member of the Commissioner’s staff or an agent of the Commissioner, must not disclose information which—*

*(a) has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, the discharging of the Commissioner’s functions,*

*(b) relates to an identified or identifiable individual or business, and*

*(c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources, unless the disclosure is made with lawful authority.*

*(2) For the purposes of subsection (1), a disclosure is made with lawful authority only if and to the extent that—*

*(a) the disclosure was made with the consent of the individual or of the person for the time being carrying on the business,* *(b) the information was obtained or provided as described in subsection (1)(a) for the purpose of its being made available to the public (in whatever manner),*

*(c) the disclosure was made for the purposes of, and is necessary for, the discharge of one or more of the Commissioner’s functions,*

*(d) the disclosure was made for the purposes of, and is necessary for, the discharge of an EU obligation,*

*(e) the disclosure was made for the purposes of criminal or civil proceedings, however arising, or*

*(f) having regard to the rights, freedoms and legitimate interests of any person, the disclosure was necessary in the public interest.*

*(3) It is an offence for a person knowingly or recklessly to disclose information in contravention of subsection (1).*

**Commentary** – [DPA Part 5 Section 132(1)](http://www.legislation.gov.uk/ukpga/2018/12/section/132) prohibits anyone who is currently or has previously been the ICO, a member of the ICO’s staff or an agent of the ICO from disclosing information obtained in the course of, or for the purposes of, the discharging of the ICO’s functions unless made with lawful authority. Subsection (2) provides the conditions for which information can be legally disclosed, and subsection (3) establishes that it is an offence to knowingly or recklessly disclose information without lawful authority.

This provision will be relevant to police forces that are in receipt of crime complaints regarding current or former ICO staff or agents disclosing confidential information without lawful authority. It is important to note that the offence is not limited to the disclosure of personal data but encompasses all information.

### Information Notices (DPA Part 6 Section 142, Section 143, Section 144)

[DPA Part 6 Section 142 Information notices](http://www.legislation.gov.uk/ukpga/2018/12/section/142) states:

*1) The Commissioner may, by written notice (an “information notice”)—*

*(a) require a controller or processor to provide the Commissioner with information that the Commissioner reasonably requires for the purposes of carrying out the Commissioner’s functions under the data protection legislation, or*

*(b) require any person to provide the Commissioner with information that the Commissioner reasonably requires for the purposes of –*

*(i) investigation a suspected failure of a type described in section 149(2) or a suspected offence under this Act, or*

*(ii) determining whether the processing of personal data is carried out by an individual in the course of a purely personal or household activity.*

*(2) An information notice must state –*

*(a)whether it is given under subsection (1)(a), (b)(i) or (b)(ii), and*

*(b) why the Commissioner requires the information.*

*(3) An information notice—*

*(a) may specify or describe particular information or a category of information;*

*(b) may specify the form in which the information must be provided;*

*(c) may specify the time at which, or the period within which, the information must be provided;*

*(d) may specify the place where the information must be provided;*

*(but see the restrictions in subsections (5) to (7)).*

*(4) An information notice must provide information about*

*(a) the consequences of failure to comply with it, and*

*(b) the rights under sections 162 and 164 (appeals etc).*

*(5) An information notice may not require a person to provide information before the end of the period within which an appeal can be brought against the notice.*

*(6) If an appeal is brought against an information notice, the information need not be provided pending the determination or withdrawal of the appeal.*

*(7) If an information notice—*

*(a) states that, in the Commissioner’s opinion, the information is required urgently, and*

*(b) gives the Commissioner’s reasons for reaching that opinion, subsections (5) and (6) do not apply but the notice must not require the information to be provided before the end of the period of 7 days beginning when the notice is given.*

*(8) The Commissioner may cancel an information notice by written notice to the person to whom it was given.*

*(9) In subsection (1), in relation to a person who is a controller or processor for the purposes of the GDPR, the reference to a controller or processor includes a representative of a controller or processor designated under Article 27 of the GDPR (representatives of controllers or processors not established in the European Union).*

*(10) Section 3(14)(c) does not apply to the reference to the processing of personal data in subsection (1)(b).*

**Commentary** – [DPA Part 5 Section 142](http://www.legislation.gov.uk/ukpga/2018/12/section/142) makes provision for Information Notices which can be used by the ICO to require a police force or a processor working on the police force’s behalf to provide information within a specified time limit. The section must be read in conjunction with [DPA Part 5 Section 143](file:///C:\Users\42006032\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\HK41YRSQ\.legislation.gov.uk\ukpga\2018\12\section\143) which sets out various restrictions on the ICO issuing Information Notices. An Information Notice may be appealed under [DPA Part 6 Section 162](http://www.legislation.gov.uk/ukpga/2018/12/section/162).

The Information Notice must:

* Explain why the ICO requires the information and whether it is given under subsection (1)(a), (b)(i) or (b)(ii).
* provide details about rights under [DPA Part 6 Section 162](http://www.legislation.gov.uk/ukpga/2018/12/section/162) and [Section 164](http://www.legislation.gov.uk/ukpga/2018/12/section/164) (appeals) and the consequences of a failure to comply with it.
* not require compliance with the measures in the notice before the end of the period in which an appeal could be brought (except where there is an urgent need for the information to be provided, in which case at least 24 hours must be given for information provision).

The Information Notice may include requirements about the information to be provided and how and when that information should be provided. If an appeal is brought against the Information Notice, the police force or their processor need not comply with it until the appeal has been withdrawn or decided (except where there is an urgent need for the information to be provided, in which case at least 24 hours must be given for information provision). The ICO is able to cancel an Information Notice.

Under the 1998 Act the ICO rarely issued Information Notices to police forces, instead seeking information necessary for assessments on an informal basis. Bearing in mind police forces’ duty to assist the ICO ([DPA Part 3 Section 63](http://www.legislation.gov.uk/ukpga/2018/12/section/63)) it is anticipated this approach will be maintained.

The Data Protection Officer must ensure their police force adopts appropriate measures to ensure that any Information Notice is readily and appropriately responded to.

[DPA Part 6 Section 143 Information notices: restrictions](http://www.legislation.gov.uk/ukpga/2018/12/section/143) states:

*(1) The Commissioner may not give an information notice with respect to the processing of personal data for the special purposes unless—*

*(a) a determination under section 174 with respect to the data or the processing has taken effect, or*

*(b) the Commissioner—*

*(i) has reasonable grounds for suspecting that such a determination could be made, and*

*(ii) the information is required for the purposes of making such a determination.*

*(2) An information notice does not require a person to give the Commissioner information to the extent that requiring the person to do so would involve an infringement of the privileges of either House of Parliament.*

*(3) An information notice does not require a person to give the Commissioner information in respect of a communication which is made—*

*(a) between a professional legal adviser and the adviser’s client, and*

*(b) in connection with the giving of legal advice to the client with respect to obligations, liabilities or rights under the data protection legislation.*

*(4) An information notice does not require a person to give the Commissioner information in respect of a communication which is made—*

*(a) between a professional legal adviser and the adviser’s client or between such an adviser or client and another person,*

*(b) in connection with or in contemplation of proceedings under or arising out of the data protection legislation, and*

*(c) for the purposes of such proceedings.*

*(5) In subsections (3) and (4), references to the client of a professional legal adviser include references to a person acting on behalf of the client.*

*(6) An information notice does not require a person to provide the Commissioner with information if doing so would, by revealing evidence of the commission of an offence expose the person to proceedings for that offence.*

*(7) The reference to an offence in subsection (6) does not include an offence under—*

*(a) this Act;*

*(b) section 5 of the Perjury Act 1911 (false statements made otherwise than on oath);*

*(c) section 44(2) of the Criminal Law (Consolidation) (Scotland) Act 1995 (false statements made otherwise than on oath);*

*(d) Article 10 of the Perjury (Northern Ireland) Order 1979 (S.I. 1979/1714 (N.I. 19)) (false statutory declarations and other false unsworn statements).*

*(8) An oral or written statement provided by a person in response to an information notice may not be used in evidence against that person on a prosecution for an offence under this Act (other than an offence under section 144) unless in the proceedings—*

*(a) in giving evidence the person provides information inconsistent with the statement, and*

*(b) evidence relating to the statement is adduced, or a question relating to it is asked, by that person or on that person’s behalf.*

*(9) In subsection (6), in relation to an information notice given to a representative of a controller or processor designated under Article 27 of the GDPR, the reference to the person providing the information being exposed to proceedings for an offence includes a reference to the controller or processor being exposed to such proceedings.*

**Commentary** – [DPA Part 6 Section 143](http://www.legislation.gov.uk/ukpga/2018/12/section/143) places certain restrictions on the ICO issuing Information Notices. The restrictions most relevant to policing are as follows:

Subsection 1 means that an Information Notice cannot be made regarding personal data processed for journalistic, academic, artistic or literary purposes, unless the ICO has made or is likely to make a written determination under [DPA Part 6 Section 174](http://www.legislation.gov.uk/ukpga/2018/12/section/174) explaining why it would be justified.

Subsections 3 to 5 provide that an Information Notice cannot compel a person to provide the ICO with details of communications with legal advisers about their compliance with data protection legislation or in connection with any proceedings brought under that legislation.

Subsection 6 provides that an Information Notice cannot compel a person to provide information that would expose them to proceedings for the commission of an offence, except in relation to the offences in this Act and the other offences listed in subsection 7.

The Data Protection Officer’s consideration of any Information Notice received should include an assessment as to whether any of the DPA Part 6 Section 147 restrictions apply.

[DPA Part 6 Section 144 False statements made in response to an information notice](http://www.legislation.gov.uk/ukpga/2018/12/section/144) states:

*It is an offence for a person, in response to an information notice—*

*(a) to make a statement which the person knows to be false in a material respect, or*

*(b) recklessly to make a statement which is false in a material respect.*

**Commentary** – [DPA Part 6 Section 144](http://www.legislation.gov.uk/ukpga/2018/12/section/144) makes it an offence for a person to intentionally or recklessly make a false statement in response to an Information Notice.

### Information Orders (DPA Part 6 Section 145)

[DPA Part 6 Section 145 Information orders](http://www.legislation.gov.uk/ukpga/2018/12/section/145) states:

*(1)This section applies if, on an application by the Commissioner, a court is satisfied that a person has failed to comply with a requirement of an information notice.*

*(2)The court may make an order requiring the person to provide to the Commissioner some or all of the following—*

*(a) information referred to in the information notice;*

*(b) other information which the court is satisfied the Commissioner requires, having regard to the statement included in the notice in accordance with section 142(2)(b).*

*(3) The order—*

*(a) may specify the form in which the information must be provided,*

*(b) must specify the time at which, or the period within which, the information must be provided, and*

*(c) may specify the place where the information must be provided.*

**Commentary** – [DPA Part 6 Section 145](http://www.legislation.gov.uk/ukpga/2018/12/section/145) provides an escalation beyond an Information Notice by giving the ICO the powers to ask a court to order a person to comply with an Information Notice. Where a person has failed to comply with an Information Notice the Information ICO may seek a court order requiring the person to provide the information referred to in the notice or other information which the court is satisfied the ICO requires as to why information is required. Failure to comply with an information order may put the person at risk of proceedings for contempt of court.

Under the 1998 Act the ICO rarely issued Information Orders to police forces, instead seeking information necessary for assessments on an informal basis. Bearing in mind police forces’ duty to assist the ICO ([DPA Part 3 Section 63](http://www.legislation.gov.uk/ukpga/2018/12/section/63)) it is anticipated this approach will be maintained.

The Data Protection Officer must ensure their police force adopts appropriate measures to ensure that any Information Order is readily and appropriately responded to.

### Assessment Notices (DPA Part 6 Section 146 & Section 147)

[DPA Part 6 Section 146 Assessment notices](http://www.legislation.gov.uk/ukpga/2018/12/section/146) states:

*(1) The Commissioner may by written notice (an “assessment notice”) require a controller or processor to permit the Commissioner to carry out an assessment of whether the controller or processor has complied or is complying with the data protection legislation.*

*(2) An assessment notice may require the controller or processor to do any of the following—*

*(a) permit the Commissioner to enter specified premises;*

*(b) direct the Commissioner to documents on the premises that are of a specified description;*

*(c) assist the Commissioner to view information of a specified description that is capable of being viewed using equipment on the premises;*

*(d) comply with a request from the Commissioner for—*

*(i) a copy of the documents to which the Commissioner is directed;*

*(ii) a copy (in such form as may be requested) of the information which the Commissioner is assisted to view;*

*(e) direct the Commissioner to equipment or other material on the premises which is of a specified description;*

*(f) permit the Commissioner to inspect or examine the documents, information, equipment or material to which the Commissioner is directed or which the Commissioner is assisted to view;*

*(g) provide the Commissioner with an explanation of such documents, information, equipment or material;*

*(h) permit the Commissioner to observe the processing of personal data that takes place on the premises;*

*(i) make available for interview by the Commissioner a specified number of people of a specified description who process personal data on behalf of the controller, not exceeding the number who are willing to be interviewed.*

*(3) In subsection (2), references to the Commissioner include references to the Commissioner’s officers and staff.*

*(4) An assessment notice must, in relation to each requirement imposed by the notice, specify the time or times at which, or period or periods within which, the requirement must be complied with (but see the restrictions in subsections (6) to (9)).*

*(5) An assessment notice must provide information about—*

*(a) the consequences of failure to comply with it, and*

*(b) the rights under sections 162 and 164 (appeals etc).*

*(6) An assessment notice may not require a person to do anything before the end of the period within which an appeal can be brought against the notice.*

*(7) If an appeal is brought against an assessment notice, the controller or processor need not comply with a requirement in the notice pending the determination or withdrawal of the appeal.*

*(8) If an assessment notice—*

*(a) states that, in the Commissioner’s opinion, it is necessary for the controller or processor to comply with a requirement in the notice urgently,*

*(b) gives the Commissioner’s reasons for reaching that opinion, and*

*(c) does not meet the conditions in subsection (9)(a) to (d),*

*subsections (6) and (7) do not apply but the notice must not require the controller or processor to comply with the requirement before the end of the period of 7 days beginning when the notice is given. (9) The Commissioner may cancel an assessment notice by written notice to the controller or processor to whom it was given.*

*(9) If an assessment notice—*

*(a) states that, in the Commissioner’s opinion, there are reasonable grounds for suspecting that a controller or processor has failed or is failing as described in section 149(2) or that an offence under this Act has been or is being committed,*

*(b) indicates the nature of the suspected failure or offence,*

*(c) does not specify domestic premises,*

*(d) states that, in the Commissioner’s opinion, it is necessary for the controller or processor to comply with a requirement in the notice in less than 7 days, and*

*(e) gives the Commissioner’s reasons for reaching that opinion,*

*subsections (6) and (7) do not apply.*

*(10) The Commissioner may cancel an assessment notice by written notice to the controller or processor to whom it was given.*

*(11) Where the Commissioner gives an assessment notice to a processor, the Commissioner must, so far as reasonably practicable, give a copy of the notice to each controller for whom the processor processes personal data.*

*(12) In this section—*

*“domestic premises” means premises, or a part of premises, used as a dwelling;*

*“specified” means specified in an assessment notice.*

**Commentary** – [DPA Part 6 Section 146](file:///C:\Users\42006032\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\HK41YRSQ\.legislation.gov.uk\ukpga\2018\12\section\146) gives the ICO the power to issue Assessment Notices to carry out an assessment of whether a police force or processor working on its behalf has complied or is complying with the data protection legislation. This is an escalation from the ICO’s powers regarding Information Notices or Information Orders.

This section should be read in conjunction with [DPA Part 6 Section 147](file:///C:\Users\42006032\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\HK41YRSQ\.legislation.gov.uk\ukpga\2018\12\section\147) which provides restrictions to the power. An Assessment Notice may be appealed under [DPA Part 6 Section 162](http://www.legislation.gov.uk/ukpga/2018/12/section/162).

An Assessment Notice may require a police or its processor to carry out various actions including permitting the ICO to enter premises or observe processing that takes place on the premises, or, assisting the ICO to view certain documents or other information (subsection 2).

Any Assessment Notice must set out the times or periods during which the actions must be undertaken (subsection 4), the consequences of a failure to comply with it, and the appeal rights against it (subsection 5). However, as with an Information Notice an Assessment Notice is prohibited from requiring a police force or its processor to do anything before the end of the period in which an appeal could be brought against the notice (subsection 6). In addition, if an appeal is brought against the notice, a police force or its processor need not comply with the notice until the appeal has been withdrawn or decided (subsection 7). Subsection 8 provides that subsections 6 and 7 do not apply where the ICO considers there is an urgent need for a police force or its processor to comply. In such circumstances the Assessment Notice must allow them a minimum of seven days to comply. In certain circumstances, the ICO may require a person to comply with an Assessment Notice in less than 7 days, including with immediate effect (subsection 9), while the ICO may cancel a notice in writing (subsection 10). Where the ICO serves an Assessment Notice on a police force’s processor the ICO must as far as is reasonably practicable copy that notice to the police force.

Under the 1998 Act the ICO rarely issued Assessment Notices to police forces. Bearing in mind police forces’ duty to assist the ICO ([DPA Part 3 Section 63](http://www.legislation.gov.uk/ukpga/2018/12/section/63)) it is anticipated this approach will be maintained.

The Data Protection Officer must ensure their police force adopts appropriate measures to ensure that any Assessment Notice is readily and appropriately responded to.

[DPA Part 6 Section 147 Assessment notices: restrictions](http://www.legislation.gov.uk/ukpga/2018/12/section/147) states:

*(1) An assessment notice does not require a person to do something to the extent that requiring the person to do it would involve an infringement of the privileges of either House of Parliament.*

*(2) An assessment notice does not have effect so far as compliance would result in the disclosure of a communication which is made—*

*(a) between a professional legal adviser and the adviser’s client, and*

*(b) in connection with the giving of legal advice to the client with respect to obligations, liabilities or rights under the data protection legislation.*

*(3) An assessment notice does not have effect so far as compliance would result in the disclosure of a communication which is made—*

*(a) between a professional legal adviser and the adviser’s client or between such an adviser or client and another person,*

*(b) in connection with or in contemplation of proceedings under or arising out of the data protection legislation, and*

*(c) for the purposes of such proceedings.*

*(4) In subsections (2) and (3)—*

*(a) references to the client of a professional legal adviser include references to a person acting on behalf of such a client, and*

*(b) references to a communication include—*

*(i) a copy or other record of the communication, and*

*(ii) anything enclosed with or referred to in the communication if made as described in subsection (2)(b) or in subsection (3)(b) and (c).*

*(5) The Commissioner may not give a controller or processor an assessment notice with respect to the processing of personal data for the special purposes.*

*(6) The Commissioner may not give an assessment notice to—*

*(a) a body specified in section 23(3) of the Freedom of Information Act 2000 (bodies dealing with security matters), or*

*(b) the Office for Standards in Education, Children’s Services and Skills in so far as it is a controller or processor in respect of information processed for the purposes of functions exercisable by Her Majesty’s Chief Inspector of Education, Children’s Services and Skills by virtue of section 5(1)(a) of the Care Standards Act 2000.*

**Commentary** – [DPA Part 6 Section 147](file:///C:\Users\42006032\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\HK41YRSQ\.legislation.gov.uk\ukpga\2018\12\section\147) set out various restrictions concerning Assessment Notices ([DPA Part 6 Section 146](http://www.legislation.gov.uk/ukpga/2018/12/section/146)). Those most relevant to policing are as follows:

Where compliance with the Assessment Notice would result in the disclosure of communications between a professional legal adviser and their client in respect of the client’s obligations under the data protection legislation or in respect of proceedings brought against the client there is no requirement to comply (subsections 2 & 3).

The ICO is precluded from issuing an Assessment Notice with respect to the processing of personal data for journalistic, academic, artistic or literary purposes (subsection 5).

The Data Protection Officer’s consideration of any Assessment Notice received must include an assessment as to whether any of the DPA Part 6 Section 147 restrictions apply.

### Destroying or falsifying information and documents etc. (DPA Part 6 Section 148)

[DPA Part 6 Section 148 Destroying or falsifying information and documents etc](http://www.legislation.gov.uk/ukpga/2018/12/section/148) states:

*(1) This section applies where a person—*

*(a) has been given an information notice requiring the person to provide the Commissioner with information, or*

*(b) has been given an assessment notice requiring the person to direct the Commissioner to a document, equipment or other material or to assist the Commissioner to view information.*

*(2) It is an offence for the person—*

*(a) to destroy or otherwise dispose of, conceal, block or (where relevant) falsify all or part of the information, document, equipment or material, or*

*(b) to cause or permit the destruction, disposal, concealment, blocking or (where relevant) falsification of all or part of the information, document, equipment or material,*

*with the intention of preventing the Commissioner from viewing, or being provided with or directed to, all or part of the information, document, equipment or material.*

*(3) It is a defence for a person charged with an offence under subsection (2) to prove that the destruction, disposal, concealment, blocking or falsification would have occurred in the absence of the person being given the notice.*

**Commentary** – [DPA Part 6 Section 148](http://www.legislation.gov.uk/ukpga/2018/12/section/148) provides that, where the ICO has issued an Information

Notice or an Assessment Notice it is an offence to destroy or otherwise dispose of, conceal, block or (where relevant) falsify it, with the intention of preventing the ICO from viewing or being provided with or directed to it.

It is a defence for a person charged with this offence to prove that the destruction, disposal, concealment, blocking or falsification would have taken place in the absence of the notice being given to the person.

The police force should ensure that all officers and staff are made aware of the offence under DPA Part 6 Section 148 Destroying or falsifying information and documents etc.

### Enforcement Notices (DPA Part 6 Section 149, Section 150, Section 151, Section 152, Section 153)

[DPA Part 6 Section 149 Enforcement notices](http://www.legislation.gov.uk/ukpga/2018/12/section/149) states:

*(1) Where the Commissioner is satisfied that a person has failed, or is failing, as described in subsection (2), (3), (4) or (5), the Commissioner may give the person a written notice (an “enforcement notice”) which requires the person—*

*(a) to take steps specified in the notice, or*

*(b) to refrain from taking steps specified in the notice,*

*or both (and see also sections 150 and 151).*

*(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following—*

*(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);*

*(b) a provision of Articles 12 to 22 of the GDPR or Part 3 or 4 of this Act conferring rights on a data subject;*

*(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors);*

*(d) a requirement to communicate a personal data breach to the Commissioner or a data subject under section 67, 68 or 108 of this Act;*

*(e) the principles for transfers of personal data to third countries, non-Convention countries and international organisations in Articles 44 to 49 of the GDPR or in sections 73 to 78 or 109 of this Act.*

*(3) The second type of failure is where a monitoring body has failed, or is failing, to comply with an obligation under Article 41 of the GDPR (monitoring of approved codes of conduct).*

*(4) The third type of failure is where a person who is a certification provider—*

*(a) does not meet the requirements for accreditation,*

*(b) has failed, or is failing, to comply with an obligation under Article 42 or 43 of the GDPR (certification of controllers and processors), or*

*(c) has failed, or is failing, to comply with any other provision of the GDPR (whether in the person’s capacity as a certification provider or otherwise).*

*(5) The fourth type of failure is where a controller has failed, or is failing, to comply with regulations under section 137.*

*(6) An enforcement notice given in reliance on subsection (2), (3) or (5) may only impose requirements which the Commissioner considers appropriate for the purpose of remedying the failure.*

*(7) An enforcement notice given in reliance on subsection (4) may only impose requirements which the Commissioner considers appropriate having regard to the failure (whether or not for the purpose of remedying the failure).*

*(8) The Secretary of State may by regulations confer power on the Commissioner to give an enforcement notice in respect of other failures to comply with the data protection legislation.*

*(9) Regulations under this section—*

*(a) may make provision about the giving of an enforcement notice in respect of the failure, including by amending this section and sections 150 to 152,*

*(b) may make provision about the giving of an information notice, an assessment notice or a penalty notice, or about powers of entry and inspection, in connection with the failure, including by amending sections 142, 143, 146, 147 and 155 to 157 and Schedules 15 and 16, and*

*(c) are subject to the affirmative resolution procedure.*

**Commentary** – [DPA Part 6 Section 149](http://www.legislation.gov.uk/ukpga/2018/12/section/149) gives the ICO the power to issue an Enforcement Notice which requires a police force or a processor working on its behalf to either take steps or refrain from taking steps specified in the notice for one or more of the failings or failures set out in subsections (2), (3), (4) and (5). The requirements that the ICO may impose when issuing an Enforcement Notice under those subsections are limited by subsections (6) and 7). The final two subsections allow the introduction of regulations to allow Enforcement Notices to be issued for failures not currently captured [DPA Part 6 Section 149](http://www.legislation.gov.uk/ukpga/2018/12/section/149).

This section should be read in conjunction with [DPA Part 6 Section 150](http://www.legislation.gov.uk/ukpga/2018/12/section/150), [DPA Part 6 Section 151](http://www.legislation.gov.uk/ukpga/2018/12/section/151), and [DPA Part 6 Section 152](http://www.legislation.gov.uk/ukpga/2018/12/section/152). An Enforcement Notice may be appealed under [DPA Part 6 Section 162](http://www.legislation.gov.uk/ukpga/2018/12/section/162).

The Data Protection Officer must ensure their force adopts appropriate measures to ensure that any Enforcement Notice is readily and appropriately responded to.

The ICO’s website shows provides details of the Enforcement Notices it has issued under data protection which can be found [here](https://ico.org.uk/action-weve-taken/enforcement/).

The Data Protection Officer must review all Enforcement Notices issued by the ICO against police forces and ensure any organisational learning arising is brought to their police force’s attention.

The Data Protection Officer’s consideration of any Enforcement Notice received must include an assessment as to whether the relevant [DPA Part 6 Section 150](http://www.legislation.gov.uk/ukpga/2018/12/section/150) requirements have been met by the notice, and whether the notice is in compliance with the restrictions in [DPA Part 6 Section 152](http://www.legislation.gov.uk/ukpga/2018/12/section/152).

[DPA Part 6 Section 150 Enforcement notices: supplementary](http://www.legislation.gov.uk/ukpga/2018/12/section/150) states:

*(1) An enforcement notice must—*

*(a) state what the person has failed or is failing to do, and*

*(b) give the Commissioner’s reasons for reaching that opinion.*

*(2) In deciding whether to give an enforcement notice in reliance on section 149(2), the Commissioner must consider whether the failure has caused or is likely to cause any person damage or distress.*

*(3) In relation to an enforcement notice given in reliance on section 149(2), the Commissioner’s power under section 149(1)(b) to require a person to refrain from taking specified steps includes power—*

*(a) to impose a ban relating to all processing of personal data, or*

*(b) to impose a ban relating only to a specified description of processing of personal data, including by specifying one or more of the following—*

*(i) a description of personal data;*

*(ii) the purpose or manner of the processing;*

*(iii) the time when the processing takes place.*

*(4) An enforcement notice may specify the time or times at which, or period or periods within which, a requirement imposed by the notice must be complied with (but see the restrictions in subsections (6) to (8)).*

*(5) An enforcement notice must provide information about—*

*(a) the consequences of failure to comply with it, and*

*(b) the rights under sections 162 and 164 (appeals etc).*

*(6) An enforcement notice must not specify a time for compliance with a requirement in the notice which falls before the end of the period within which an appeal can be brought against the notice.*

*(7) If an appeal is brought against an enforcement notice, a requirement in the notice need not be complied with pending the determination or withdrawal of the appeal.*

*(8) If an enforcement notice—*

*(a) states that, in the Commissioner’s opinion, it is necessary for a requirement to be complied with urgently, and*

*(b) gives the Commissioner’s reasons for reaching that opinion,*

*subsections (6) and (7) do not apply but the notice must not require the requirement to be complied with before the end of the period of 24 hours beginning when the notice is given.*

*(9) In this section, “specified” means specified in an enforcement notice.*

**Commentary** – [DPA Part 6 Section 150](http://www.legislation.gov.uk/ukpga/2018/12/section/150) sets out supplementary provisions regarding Enforcement Notices given under [DPA Part 6 Section 149](http://www.legislation.gov.uk/ukpga/2018/12/section/149).

Data Protection Officer’s consideration of any Enforcement Notice received should include an assessment as to whether the relevant DPA Part 6 Section 150 provisions have been met.

[DPA Part 6 Section 151 Enforcement notices: rectification and erasure of personal data](http://www.legislation.gov.uk/ukpga/2018/12/section/151) etc states:

*(1) Subsections (2) and (3) apply where an enforcement notice is given in respect of a failure by a controller or processor—*

*(a) to comply with a data protection principle relating to accuracy, or*

*(b) to comply with a data subject’s request to exercise rights under Article 16, 17 or 18 of the GDPR (right to rectification, erasure or restriction on processing) or section 46, 47 or 100 of this Act.*

*(2) If the enforcement notice requires the controller or processor to rectify or erase inaccurate personal data, it may also require the controller or processor to rectify or erase any other data which—*

*(a) is held by the controller or processor, and*

*(b) contains an expression of opinion which appears to the Commissioner to be based on the inaccurate personal data.*

*(3) Where a controller or processor has accurately recorded personal data provided by the data subject or a third party but the data is inaccurate, the enforcement notice may require the controller or processor—*

*(a) to take steps specified in the notice to ensure the accuracy of the data,*

*(b) if relevant, to secure that the data indicates the data subject’s view that the data is inaccurate, and*

*(c) to supplement the data with a statement of the true facts relating to the matters dealt with by the data that is approved by the Commissioner,*

*(as well as imposing requirements under subsection (2)).*

*(4) When deciding what steps it is reasonable to specify under subsection (3)(a), the Commissioner must have regard to the purpose for which the data was obtained and further processed.*

*(5) Subsections (6) and (7) apply where—*

*(a) an enforcement notice requires a controller or processor to rectify or erase personal data, or*

*(b) the Commissioner is satisfied that the processing of personal data which has been rectified or erased by the controller or processor involved a failure described in subsection (1).*

*(6) An enforcement notice may, if reasonably practicable, require the controller or processor to notify third parties to whom the data has been disclosed of the rectification or erasure.*

*(7) In determining whether it is reasonably practicable to require such notification, the Commissioner must have regard, in particular, to the number of people who would have to be notified.*

*(8) In this section, “data protection principle relating to accuracy” means the principle in—*

*(a) Article 5(1)(d) of the GDPR,*

*(b) section 38(1) of this Act, or*

*(c) section 89 of this Act*.

**Commentary** – [DPA Part 6 Section 151](http://www.legislation.gov.uk/ukpga/2018/12/section/151) applies where an Enforcement Notice issued under [DPA Part 6 Section 149](http://www.legislation.gov.uk/ukpga/2018/12/section/149) relates to a failure by a police force or its processor to comply with the data protection principle relating to accuracy (as defined in subsection (8)) or a failure to comply with a data subject’s rights to rectification, erasure or restriction of processing under Articles 16 to 18 of the GDPR or DPA Part 3 Section 46 or Section 47.

[DPA Part 6 Section 152 Enforcement notices: restrictions](http://www.legislation.gov.uk/ukpga/2018/12/section/152) states:

*(1) The Commissioner may not give a controller or processor an enforcement notice in reliance on section 149(2) with respect to the processing of personal data for the special purposes unless—*

*(a) a determination under section 174 with respect to the data or the processing has taken effect, and*

*(b) a court has granted leave for the notice to be given.*

*(2) A court must not grant leave for the purposes of subsection (1)(b) unless it is satisfied that—*

*(a) the Commissioner has reason to suspect a failure described in section 149(2) which is of substantial public importance, and*

*(b) the controller or processor has been given notice of the application for leave in accordance with rules of court or the case is urgent.*

*(3) An enforcement notice does not require a person to do something to the extent that requiring the person to do it would involve an infringement of the privileges of either House of Parliament.*

*(4) In the case of a joint controller in respect of the processing of personal data to which Part 3 or 4 applies whose responsibilities for compliance with that Part are determined in an arrangement under section 58 or 104, the Commissioner may only give the controller an enforcement notice in reliance on section 149(2) if the controller is responsible for compliance with the provision, requirement or principle in question.*

**Commentary** – [DPA Part 6 Section 152](http://www.legislation.gov.uk/ukpga/2018/12/section/152) sets out restrictions which apply to the ICO when issuing an Enforcement Notices on a police force or a processor working on its behalf.

[DPA Part 6 Section 153 Enforcement notices: cancellation and variation](http://www.legislation.gov.uk/ukpga/2018/12/section/153) states:

*(1) The Commissioner may cancel or vary an enforcement notice by giving written notice to the person to whom it was given.*

*(2) A person to whom an enforcement notice is given may apply in writing to the Commissioner for the cancellation or variation of the notice.*

*(3) An application under subsection (2) may be made only—*

*(a) after the end of the period within which an appeal can be brought against the notice, and*

*(b) on the ground that, by reason of a change of circumstances, one or more of the provisions of that notice need not be complied with in order to remedy the failure identified in the notice.*

**Commentary** – [DPA Part 6 Section 153](http://www.legislation.gov.uk/ukpga/2018/12/section/153) allows the ICO to cancel or amend an Enforcement Notice.

### Powers of Entry & Inspection (DPA Part 6 Section 154 & Schedule 15)

[DPA Part 6 Section 154](http://www.legislation.gov.uk/ukpga/2018/12/section/154) Powers of entry and inspection states:

*Schedule 15 makes provision about powers of entry and inspection.*

**Commentary** – [DPA Schedule 15](http://www.legislation.gov.uk/ukpga/2018/12/schedule/15) sets out various processes by which the ICO may obtain powers of entry and inspection through the granting of a warrant by a judge. It also includes offences that may be committed by a person who obstructs the warrant.

### Penalty Notices (DPA Part 6 Section 155, Section 156, Section 157, Section 158, Section 159, Schedule 16)

[DPA Part 6 Section 155 Penalty notices](http://www.legislation.gov.uk/ukpga/2018/12/section/155) states:

*(1) If the Commissioner is satisfied that a person—*

*(a) has failed or is failing as described in section 149(2), (3), (4) or (5), or*

*(b) has failed to comply with an information notice, an assessment notice or an enforcement notice,*

*the Commissioner may, by written notice (a “penalty notice”), require the person to pay to the Commissioner an amount in sterling specified in the notice.*

*(2) Subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the following, so far as relevant—*

*(a) to the extent that the notice concerns a matter to which the GDPR applies, the matters listed in Article 83(1) and (2) of the GDPR;*

*(b) to the extent that the notice concerns another matter, the matters listed in subsection (3).*

*(3) Those matters are—*

*(a) the nature, gravity and duration of the failure;*

*(b) the intentional or negligent character of the failure;*

*(c) any action taken by the controller or processor to mitigate the damage or distress suffered by data subjects;*

*(d) the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by the controller or processor in accordance with section 57, 66, 103 or 107;*

*(e) any relevant previous failures by the controller or processor;*

*(f) the degree of co-operation with the Commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure;*

*(g) the categories of personal data affected by the failure;*

*(h) the manner in which the infringement became known to the Commissioner, including whether, and if so to what extent, the controller or processor notified the Commissioner of the failure;*

*(i) the extent to which the controller or processor has complied with previous enforcement notices or penalty notices;*

*(j) adherence to approved codes of conduct or certification mechanisms;*

*(k) any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly);*

*(l) whether the penalty would be effective, proportionate and dissuasive.*

*(4) Subsections (2) and (3) do not apply in the case of a decision or determination relating to a failure described in section 149(5).*

*(5) Schedule 16 makes further provision about penalty notices, including provision requiring the Commissioner to give a notice of intent to impose a penalty and provision about payment, variation, cancellation and enforcement.*

*(6) The Secretary of State may by regulations—*

*(a) confer power on the Commissioner to give a penalty notice in respect of other failures to comply with the data protection legislation, and*

*(b) provide for the maximum penalty that may be imposed in relation to such failures to be either the standard maximum amount or the higher maximum amount.*

*(7) Regulations under this section—*

*(a) may make provision about the giving of penalty notices in respect of the failure,*

*(b) may amend this section and sections 156 to 158, and*

*(c) are subject to the affirmative resolution procedure.*

*(8) In this section, “higher maximum amount” and “standard maximum amount” have the same meaning as in section 157.*

[DPA Schedule 16 Penalties](http://www.legislation.gov.uk/ukpga/2018/12/schedule/16) is introduced by DPA Part 6 Section 155(5) and states:

***Meaning of “penalty”***

*1 In this Schedule, “penalty” means a penalty imposed by a penalty notice.*

*Notice of intent to impose penalty*

*2 (1)Before giving a person a penalty notice, the Commissioner must, by written notice (a “notice of intent”) inform the person that the Commissioner intends to give a penalty notice.*

*(2) The Commissioner may not give a penalty notice to a person in reliance on a notice of intent after the end of the period of 6 months beginning when the notice of intent is given, subject to sub-paragraph (3).*

*(3) The period for giving a penalty notice to a person may be extended by agreement between the Commissioner and the person.*

***Contents of notice of intent***

*3 (1) A notice of intent must contain the following information—*

*(a) the name and address of the person to whom the Commissioner proposes to give a penalty notice;*

*(b) the reasons why the Commissioner proposes to give a penalty notice (see sub-paragraph (2));*

*(c) an indication of the amount of the penalty the Commissioner proposes to impose, including any aggravating or mitigating factors that the Commissioner proposes to take into account.*

*(2) The information required under sub-paragraph (1)(b) includes—*

*(a) a description of the circumstances of the failure, and*

*(b) where the notice is given in respect of a failure described in section 149(2), the nature of the personal data involved in the failure.*

*(3) A notice of intent must also—*

*(a) state that the person may make written representations about the Commissioner’s intention to give a penalty notice, and*

*(b) specify the period within which such representations may be made.*

*(4) The period specified for making written representations must be a period of not less than 21 days beginning when the notice of intent is given.*

*(5) If the Commissioner considers that it is appropriate for the person to have an opportunity to make oral representations about the Commissioner’s intention to give a penalty notice, the notice of intent must also—*

*(a) state that the person may make such representations, and*

*(b) specify the arrangements for making such representations and the time at which, or the period within which, they may be made.*

***Giving a penalty notice***

*4 (1) The Commissioner may not give a penalty notice before a time, or before the end of a period, specified in the notice of intent for making oral or written representations.*

*(2) When deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must consider any oral or written representations made by the person in accordance with the notice of intent.*

*Contents of penalty notice*

*5 (1) A penalty notice must contain the following information—*

*(a) the name and address of the person to whom it is addressed;*

*(b) details of the notice of intent given to the person;*

*(c) whether the Commissioner received oral or written representations in accordance with the notice of intent;*

*(d) the reasons why the Commissioner proposes to impose the penalty (see sub-paragraph (2));*

*(e) the reasons for the amount of the penalty, including any aggravating or mitigating factors that the Commissioner has taken into account;*

*(f) details of how the penalty is to be paid;*

*(g) details of the rights of appeal under section 162;*

*(h) details of the Commissioner’s enforcement powers under this Schedule.*

*(2) The information required under sub-paragraph (1)(d) includes—*

*(a) a description of the circumstances of the failure, and*

*(b) where the notice is given in respect of a failure described in section 149(2), the nature of the personal data involved in the failure.*

***Period for payment of penalty***

*6 (1) A penalty must be paid to the Commissioner within the period specified in the penalty notice.*

*(2) The period specified must be a period of not less than 28 days beginning when the penalty notice is given.*

***Variation of penalty***

*7 (1) The Commissioner may vary a penalty notice by giving written notice (a “penalty variation notice”) to the person to whom it was given.*

*(2) A penalty variation notice must specify—*

*(a) the penalty notice concerned, and*

*(b) how it is varied.*

*(3) A penalty variation notice may not—*

*(a) reduce the period for payment of the penalty;*

*(b) increase the amount of the penalty;*

*(c) otherwise vary the penalty notice to the detriment of the person to whom it was given.*

*(4 )If—*

*(a) a penalty variation notice reduces the amount of the penalty, and*

*(b)when that notice is given, an amount has already been paid that exceeds the amount of the reduced penalty,*

*the Commissioner must repay the excess.*

***Cancellation of penalty***

*8 (1) The Commissioner may cancel a penalty notice by giving written notice to the person to whom it was given.*

*(2) If a penalty notice is cancelled, the Commissioner—*

*(a) may not take any further action under section 155 or this Schedule in relation to the failure to which that notice relates, and*

*(b )must repay any amount that has been paid in accordance with that notice.*

***Enforcement of payment***

*9 (1) The Commissioner must not take action to recover a penalty unless—*

*(a) the period specified in accordance with paragraph 6 has ended,*

*(b) any appeals against the penalty notice have been decided or otherwise ended,*

*(c) if the penalty notice has been varied, any appeals against the penalty variation notice have been decided or otherwise ended, and*

*(d) the period for the person to whom the penalty notice was given to appeal against the penalty, and any variation of it, has ended.*

*(2) In England and Wales, a penalty is recoverable—*

*(a) if the county court so orders, as if it were payable under an order of that court;*

*(b )if the High Court so orders, as if it were payable under an order of that court.*

*(3) In Scotland, a penalty may be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.*

*(4) In Northern Ireland, a penalty is recoverable—*

*(a) if a county court so orders, as if it were payable under an order of that court;*

*(b )if the High Court so orders, as if it were payable under an order of that court.*

**Commentary** – [DPA Part 6 Section 155](http://www.legislation.gov.uk/ukpga/2018/12/section/155) gives the ICO a power to give a Penalty Notice requiring a police force or its processor to pay the ICO an amount determined by the ICO. [DPA Schedule 16](http://www.legislation.gov.uk/ukpga/2018/12/schedule/16) makes further provisions in relation to a Penalty Notice. [DPA Part 6 Section 155](http://www.legislation.gov.uk/ukpga/2018/12/section/155) should be read in conjunction with [DPA Part 6 Section 156](http://www.legislation.gov.uk/ukpga/2018/12/section/156). A Penalty Notice may be appealed under [DPA Part 6 Section 162](http://www.legislation.gov.uk/ukpga/2018/12/section/162).

[DPA Schedule 16](http://www.legislation.gov.uk/ukpga/2018/12/schedule/16) provides:

* The ICO must give a Notice of Intent to the police force or its processor against whom they intend to issue a Penalty Notice. The latter has to be issued within six months of the Notice of Intent unless the recipient has agreed an extension of this interval (paragraph 2).
* The Notice of Intent must include an indication of the amount of the penalty, the nature of the offence, the period in which the recipient can make written representations about intended Penalty Notice, and whether they can make oral representations (paragraph 3).
* The ICO must first consider any oral or written representations before determining whether to give a penalty notice. The ICO must wait until after the time allocated for making oral or written statements by the person has passed before issuing a penalty notice (paragraph 4).
* The penalty notice must provide certain information and this may include reasons why the ICO proposes to impose the penalty, reasons for the amount specified and details on rights of appeal (paragraph 5).
* Any penalty must be paid within a specified period but that period cannot be less than 28 days (paragraph 6).
* The ICO may vary a penalty notice by given written notice and must meet certain requirements in the variation notice (paragraph 7).
* The ICO must follow certain procedures when cancelling a Penalty Notice (paragraph 8).
* Certain conditions must be satisfied before the ICO can enforce a penalty (paragraph 9).

The ICO’s website provides details of the Penalty Notices under data protection legislation and they can be found [here](https://ico.org.uk/action-weve-taken/enforcement/).

The ICO has produced guidance on penalties for failures to comply with DPA Part 3 obligations which can be found [here](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/penalties/).

The Data Protection Officer must review all monetary Penalty Notices issued by the ICO against police forces and ensure any organisational learning arising is brought to their police force’s attention.

The Data Protection Officer’s consideration of any Penalty Notice received should include an assessment as to whether any of the [DPA Part 6 Section 156](http://www.legislation.gov.uk/ukpga/2018/12/section/156) restrictions apply and to what extent relevant [DPA Schedule 16](http://www.legislation.gov.uk/ukpga/2018/12/schedule/16) requirements have been met.

[DPA Part 6 Section 156 Penalty notices: restrictions](http://www.legislation.gov.uk/ukpga/2018/12/section/156) states:

*(1) The Commissioner may not give a controller or processor a penalty notice in reliance on section 149(2) with respect to the processing of personal data for the special purposes unless—*

*(a) a determination under section 174 with respect to the data or the processing has taken effect, and*

*(b) a court has granted leave for the notice to be given.*

*(2) A court must not grant leave for the purposes of subsection (1)(b) unless it is satisfied that—*

*(a) the Commissioner has reason to suspect a failure described in section 149(2) which is of substantial public importance, and*

*(b) the controller or processor has been given notice of the application for leave in accordance with rules of court or the case is urgent.*

*(3) The Commissioner may not give a controller or processor a penalty notice with respect to the processing of personal data where the purposes and manner of the processing are determined by or on behalf of either House of Parliament.*

*(4) The Commissioner may not give a penalty notice to—*

*(a) the Crown Estate Commissioners, or*

*(b) a person who is a controller by virtue of section 209(4) (controller for the Royal Household etc).*

*(5) In the case of a joint controller in respect of the processing of personal data to which Part 3 or 4 applies whose responsibilities for compliance with that Part are determined in an arrangement under section 58 or 104, the Commissioner may only give the controller a penalty notice in reliance on section 149(2) if the controller is responsible for compliance with the provision, requirement or principle in question.*

**Commentary** – [DPA Part 6 Section 156](http://www.legislation.gov.uk/ukpga/2018/12/section/156) and Schedule 16 set out the restrictions placed on the ICO in relation to the ICO’s power to issue a Penalty Notice under [DPA Part 6 Section 155](http://www.legislation.gov.uk/ukpga/2018/12/section/155) in relation to different types of processing.

[DPA Part 6 Section 157 Penalty notices](http://www.legislation.gov.uk/ukpga/2018/12/section/157) states:

*(1) In relation to an infringement of a provision of the GDPR, the maximum amount of the penalty that may be imposed by a penalty notice is—*

*(a) the amount specified in Article 83 of the GDPR, or*

*(b) if an amount is not specified there, the standard maximum amount.*

*(2) In relation to an infringement of a provision of Part 3 of this Act, the maximum amount of the penalty that may be imposed by a penalty notice is—*

*(a) in relation to a failure to comply with section 35, 36, 37, 38(1), 39(1), 40, 44, 45, 46, 47, 48, 49, 52, 53, 73, 74, 75, 76, 77 or 78, the higher maximum amount, and*

*(b) otherwise, the standard maximum amount.*

*(3) In relation to an infringement of a provision of Part 4 of this Act, the maximum amount of the penalty that may be imposed by a penalty notice is—*

*(a) in relation to a failure to comply with section 86, 87, 88, 89, 90, 91, 93, 94, 100 or 109, the higher maximum amount, and*

*(b) otherwise, the standard maximum amount.*

*(4) In relation to a failure to comply with an information notice, an assessment notice or an enforcement notice, the maximum amount of the penalty that may be imposed by a penalty notice is the higher maximum amount.*

*(5) The “higher maximum amount” is—*

*(a) in the case of an undertaking, 20 million Euros or 4% of the undertaking’s total annual worldwide turnover in the preceding financial year, whichever is higher, or*

*(b) in any other case, 20 million Euros.*

*(6) The “standard maximum amount” is—*

*(a) in the case of an undertaking, 10 million Euros or 2% of the undertaking’s total annual worldwide turnover in the preceding financial year, whichever is higher, or*

*(b) in any other case, 10 million Euros.*

*(7) The maximum amount of a penalty in sterling must be determined by applying the spot rate of exchange set by the Bank of England on the day on which the penalty notice is given.*

**Commentary** – [DPA Part 6 Section 157](http://www.legislation.gov.uk/ukpga/2018/12/section/157) sets out the maximum fines that can be imposed for infringements of a provision of the GDPR, an infringement of a provision of DPA Parts 3 or a failure to comply with an Information Notice, Assessment Notice, or an Enforcement Notice.

There are two levels of penalty – a Higher Maximum Amount and a Standard Maximum Amount:

* The Higher Maximum Amount is 20 million Euros or 4% of a police force’s annual budget (or annual worldwide turnover in the case of a penalty against a processor working on behalf of the police force), whichever is the greater amount.
* The Standard Maximum Amount is 10 million Euros or 2% of a police force’s annual budget (or annual worldwide turnover in the case of a penalty against a processor working on behalf of the police force), whichever is the greater amount.

The Higher Maximum Amount applies for breaches of the DPA Part 3 Sections listed under subsection (2)(a). It also applies to breaches of GDPR Article 5, 6, 7, 9, 12 to 22, 44 to 49, 58 and 85 to 91.

The Standard Maximum Amount applies for breaches of the DPA Part 3 Sections other than those listed under subsection (2)(a). It also applies to breaches of GDPR Article 8, 11, 25 to 39, 42 & 43.

[DPA Part 6 Section 158 Penalty notices](http://www.legislation.gov.uk/ukpga/2018/12/section/158) states:

*(1) The Commissioner must produce and publish a document specifying the amount of the penalty for a failure to comply with regulations made under section 137.*

*(2) The Commissioner may specify different amounts for different types of failure.*

*(3) The maximum amount that may be specified is 150% of the highest charge payable by a controller in respect of a financial year in accordance with the regulations, disregarding any discount available under the regulations.*

*(4) The Commissioner—*

*(a) may alter or replace the document, and*

*(b) must publish any altered or replacement document.*

*(5) Before publishing a document under this section (including any altered or replacement document), the Commissioner must consult—*

*(a) the Secretary of State, and*

*(b) such other persons as the Commissioner considers appropriate.*

*(6) The Commissioner must arrange for a document published under this section (including any altered or replacement document) to be laid before Parliament.*

**Commentary** – [DPA Part 6 Section 158](http://www.legislation.gov.uk/ukpga/2018/12/section/158) places an obligation on the ICO to publish a document specifying the penalty amounts for a failure to comply with the Data Protection Fee introduced by the [Data Protection (Charges and Information) Regulations 2018](http://www.legislation.gov.uk/ukdsi/2018/9780111165782/pdfs/ukdsi_9780111165782_en.pdf).

[DPA Schedule 20(26)(1) & (2](http://www.legislation.gov.uk/ukpga/2018/12/schedule/20)) provides that the [Data Protection (Charges and Information) Regulations 2018](http://www.legislation.gov.uk/ukdsi/2018/9780111165782/pdfs/ukdsi_9780111165782_en.pdf), which were initially made under Section 108 of the Digital Economy Act 2017 and then duplicated in [DPA Part 5 Section 137](http://www.legislation.gov.uk/ukpga/2018/12/section/137), have the effect as if they were regulations made under [DPA Part 5 Section 137](http://www.legislation.gov.uk/ukpga/2018/12/section/137).

Under [DPA Part 6 Section 158(3)](http://www.legislation.gov.uk/ukpga/2018/12/section/158) the maximum penalty for non-payment of the fee is 150% of the highest charge payable in accordance with the fees regulations, disregarding any discount available under the fees regulations. For police forces this currently equates to £4,350.

[DPA Part 6 Section 159 Penalty notices](http://www.legislation.gov.uk/ukpga/2018/12/section/159) states:

*(1) For the purposes of Article 83 of the GDPR and section 157, the Secretary of State may by regulations—*

*(a) provide that a person of a description specified in the regulations is or is not an undertaking, and*

*(b) make provision about how an undertaking's turnover is to be determined.*

*(2) For the purposes of Article 83 of the GDPR, section 157 and section 158, the Secretary of State may by regulations provide that a period is or is not a financial year.*

*(3) Regulations under this section are subject to the affirmative resolution procedure*

**Commentary** – [DPA Part 6 Section 159](http://www.legislation.gov.uk/ukpga/2018/12/section/159) gives the Secretary of State with the power to introduce regulations for the purposes of GDPR Article 83 of the and DPA Part 6 Section 157 which make provision that a person is or is not an undertaking or about how an undertaking’s turnover is to be determined.

As of 23rd July 2020 no regulations had been issued under this provision.

### Appeals (DPA Part 6 Section 162, Section 163, Section 164)

[DPA Part 6 Section 162 Rights of appeal](http://www.legislation.gov.uk/ukpga/2018/12/section/162) states:

*(1) A person who is given any of the following notices may appeal to the Tribunal—*

*(a) an information notice;*

*(b) an assessment notice;*

*(c) an enforcement notice;*

*(d) a penalty notice;*

*(e) a penalty variation notice.*

*(2) A person who is given an enforcement notice may appeal to the Tribunal against the refusal of an application under section 153 for the cancellation or variation of the notice.*

*(3) A person who is given a penalty notice or a penalty variation notice may appeal to the Tribunal against the amount of the penalty specified in the notice, whether or not the person appeals against the notice.*

*(4) Where a determination is made under section 174 in respect of the processing of personal data, the controller or processor may appeal to the Tribunal against the determination.*

**Commentary** – DPA Part 6 Section 162 gives a police force or processor working on its behalf a right to appeal against an Information Notice, Assessment Notice, Enforcement Notice, Penalty Notice, or Penalty Variation Notice.

The provision also provides a right to appeal to The Tribunal against:

* a refusal to cancel or vary an Enforcement Notice
* the amount specified in a Penalty Notice or a Penalty Variation Notice.
* a determination made by the ICO under DPA Section 174 (whether the processing is for the Special Purposes).

The Data Protection Officer must ensure appropriate measures are place within their police forces to identify circumstances when appeals against notices are necessary.

[DPA Part 6 Section 163 Determination of appeals](http://www.legislation.gov.uk/ukpga/2018/12/section/163) states:

*(1) Subsections (2) to (4) apply where a person appeals to the Tribunal under section 162(1) or (3).*

*(2) The Tribunal may review any determination of fact on which the notice or decision against which the appeal is brought was based.*

*(3) If the Tribunal considers—*

*(a) that the notice or decision against which the appeal is brought is not in accordance with the law, or*

*(b) to the extent that the notice or decision involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently,*

*the Tribunal must allow the appeal or substitute another notice or decision which the Commissioner could have given or made.*

*(4) Otherwise, the Tribunal must dismiss the appeal.*

*(5) On an appeal under section 162(2), if the Tribunal considers that the enforcement notice ought to be cancelled or varied by reason of a change in circumstances, the Tribunal must cancel or vary the notice.*

*(6) On an appeal under section 162(4), the Tribunal may cancel the Commissioner's determination.*

**Commentary** – [DPA Part 6 Section 163](http://www.legislation.gov.uk/ukpga/2018/12/section/163) makes provision in relation to the determination of appeals under [DPA Part 6 Section 162](http://www.legislation.gov.uk/ukpga/2018/12/section/162) by the Upper Tribunal or the First-tier Tribunal.

[DPA Part 6 Section 164 Applications in respect of urgent notices](http://www.legislation.gov.uk/ukpga/2018/12/section/164) states:

*(1) This section applies where an information notice, an assessment notice or an enforcement notice given to a person contains an urgency statement.*

*(2) The person may apply to the court for either or both of the following—*

*(a) the disapplication of the urgency statement in relation to some or all of the requirements of the notice;*

*(b) a change to the time at which, or the period within which, a requirement of the notice must be complied with.*

*(3) On an application under subsection (2), the court may do any of the following—*

*(a) direct that the notice is to have effect as if it did not contain the urgency statement;*

*(b) direct that the inclusion of the urgency statement is not to have effect in relation to a requirement of the notice;*

*(c) vary the notice by changing the time at which, or the period within which, a requirement of the notice must be complied with;*

*(d) vary the notice by making other changes required to give effect to a direction under paragraph (a) or (b) or in consequence of a variation under paragraph (c).*

*(4) The decision of the court on an application under this section is final.*

*(5) In this section, “urgency statement” means—*

*(a) in relation to an information notice, a statement under section 142(7)(a),*

*(b) in relation to an assessment notice, a statement under section 146(8)(a) or (9)(d), and*

*(c) in relation to an enforcement notice, a statement under section 150(8)(a).*

**Commentary** – [DPA Part 6 Section 164](http://www.legislation.gov.uk/ukpga/2018/12/section/164) enables a police force or data processor working on its behalf which receives an Information Notice, Assessment Notice or Enforcement Notice requiring it to comply with it urgently to apply to the court to have the urgency statement set aside or for variation of the timetable for compliance. Where the ICO has also asked the court to impose an information order under DPA Part 6 Section 145 the court will determine the most appropriate approach to be taken.

## Commissioner’s Codes of Practice

### Overview

[DPA Part 5 Section 121 Data Sharing Code](http://www.legislation.gov.uk/ukpga/2018/12/section/121) states:

*(1) The Commissioner must prepare a code of practice which contains—*

*(a) practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation, and*

*(b) such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data.*

*(2) Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.*

*(3) Before preparing a code or amendments under this section, the Commissioner must consult the Secretary of State and such of the following as the Commissioner considers appropriate—*

*(a) trade associations;*

*(b) data subjects;*

*(c) persons who appear to the Commissioner to represent the interests of data subjects.*

*(4) A code under this section may include transitional provision or savings.*

*(5) In this section—*

*“good practice in the sharing of personal data” means such practice in the sharing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, including compliance with the requirements of the data protection legislation;*

*“the sharing of personal data” means the disclosure of personal data by transmission, dissemination or otherwise making it available;*

*“trade association” includes a body representing controllers or processors.*

[DPA Part 5 Section 122 Direct Marketing Code](http://www.legislation.gov.uk/ukpga/2018/12/section/122) states:

*(1) The Commissioner must prepare a code of practice which contains—*

*(a) practical guidance in relation to the carrying out of direct marketing in accordance with the requirements of the data protection legislation and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426), and*

*(b) such other guidance as the Commissioner considers appropriate to promote good practice in direct marketing.*

*(2) Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.*

*(3) Before preparing a code or amendments under this section, the Commissioner must consult the Secretary of State and such of the following as the Commissioner considers appropriate—*

*(a) trade associations;*

*(b) data subjects;*

*(c) persons who appear to the Commissioner to represent the interests of data subjects.*

*(4) A code under this section may include transitional provision or savings.*

*(5) In this section—*

*“direct marketing” means the communication (by whatever means) of advertising or marketing material which is directed to particular individuals;*

*“good practice in direct marketing” means such practice in direct marketing as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, including compliance with the requirements mentioned in subsection (1)(a);*

*“trade association” includes a body representing controllers or processors.*

[DPA Part 5 Section 123 Age-Appropriate Design Code](http://www.legislation.gov.uk/ukpga/2018/12/section/123) states:

*(1) The Commissioner must prepare a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age-appropriate design of relevant information society services which are likely to be accessed by children.*

*(2) Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.*

*(3) Before preparing a code or amendments under this section, the Commissioner must consult the Secretary of State and such other persons as the Commissioner considers appropriate, including—*

*(a) children,*

*(b) parents,*

*(c) persons who appear to the Commissioner to represent the interests of children,*

*(d) child development experts, and*

*(e) trade associations.*

*(4) In preparing a code or amendments under this section, the Commissioner must have regard—*

*(a) to the fact that children have different needs at different ages, and*

*(b) to the United Kingdom’s obligations under the United Nations Convention on the Rights of the Child.*

*(5) A code under this section may include transitional provision or savings.*

*(6) Any transitional provision included in the first code under this section must cease to have effect before the end of the period of 12 months beginning when the code comes into force.*

*(7) In this section—*

*“age-appropriate design” means the design of services so that they are appropriate for use by, and meet the development needs of, children;*

*“information society services” has the same meaning as in the GDPR, but does not include preventive or counselling services;*

*“relevant information society services” means information society services which involve the processing of personal data to which the GDPR applies;*

*“standards of age-appropriate design of relevant information society services” means such standards of age-appropriate design of such services as appear to the Commissioner to be desirable having regard to the best interests of children;*

*“trade association” includes a body representing controllers or processors;*

*“the United Nations Convention on the Rights of the Child” means the Convention on the Rights of the Child adopted by the General Assembly of the United Nations on 20 November 1989 (including any Protocols to that Convention which are in force in relation to the United Kingdom), subject to any reservations, objections or interpretative declarations by the United Kingdom for the time being in force.*

[DPA Part 5 Section 124 Data Protection & Journalism Code](http://www.legislation.gov.uk/ukpga/2018/12/section/123) states:

*(1) The Commissioner must prepare a code of practice which contains—*

*(a) practical guidance in relation to the processing of personal data for the purposes of journalism in accordance with the requirements of the data protection legislation, and*

*(b) such other guidance as the Commissioner considers appropriate to promote good practice in the processing of personal data for the purposes of journalism.*

*(2) Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.*

*(3) Before preparing a code or amendments under this section, the Commissioner must consult such of the following as the Commissioner considers appropriate—*

*(a) trade associations;*

*(b) data subjects;*

*(c) persons who appear to the Commissioner to represent the interests of data subjects.*

*(4) A code under this section may include transitional provision or savings.*

*(5) In this section—*

*“good practice in the processing of personal data for the purposes of journalism” means such practice in the processing of personal data for those purposes as appears to the Commissioner to be desirable having regard to—*

*(a) the interests of data subjects and others, including compliance with the requirements of the data protection legislation, and*

*(b) the special importance of the public interest in the freedom of expression and information;*

*“trade association” includes a body representing controllers or processors.*

[DPA Part 5 Section 127](http://www.legislation.gov.uk/ukpga/2018/12/section/127) Effects of codes issued under section 125(4) states:

*(1) A failure by a person to act in accordance with a provision of a code issued under section 125(4) does not of itself make that person liable to legal proceedings in a court or tribunal.*

*(2) A code issued under section 125(4), including an amendment or replacement code, is admissible in evidence in legal proceedings.*

*(3) In any proceedings before a court or tribunal, the court or tribunal must take into account a provision of a code issued under section 125(4) in determining a question arising in the proceedings if—*

*(a) the question relates to a time when the provision was in force, and*

*(b) the provision appears to the court or tribunal to be relevant to the question.*

*(4) Where the Commissioner is carrying out a function described in subsection (5), the Commissioner must take into account a provision of a code issued under section 125(4) in determining a question arising in connection with the carrying out of the function if—*

*(a) the question relates to a time when the provision was in force, and*

*(b) the provision appears to the Commissioner to be relevant to the*

*question.*

*(5) Those functions are functions under—*

*(a) the data protection legislation, or*

*(b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426).*

**Commentary** – [DPA Part 5 Section 121](http://www.legislation.gov.uk/ukpga/2018/12/section/121), [Section 122](http://www.legislation.gov.uk/ukpga/2018/12/section/122), [Section 123](http://www.legislation.gov.uk/ukpga/2018/12/section/123), [Section 124](http://www.legislation.gov.uk/ukpga/2018/12/section/124) place a statutory requirement on the ICO to publish codes of practice on Data-Sharing, Direct Marketing, Age-Appropriate Design and Journalism respectively. [DPA Part 5 Section 125](http://www.legislation.gov.uk/ukpga/2018/12/section/125) requires that the codes of practice must be laid before parliament for approval for publication by the ICO. [DPA Part 5 Section 126](http://www.legislation.gov.uk/ukpga/2018/12/section/126) places an obligation on the ICO to review and prepare amendments to the codes of practice. [DPA Part 5 Section 127](http://www.legislation.gov.uk/ukpga/2018/12/section/127) sets out the legal effect of codes published under DPA Part 5 Section 125. [DPA Part 5 Section 128](http://www.legislation.gov.uk/ukpga/2018/12/section/128) provides the Secretary of State with power to use regulations to require the ICO to prepare additional codes of practice.

As of 23rd July 2020 none of the four codes of practice required by the Act have been published.

However, the ICO’s website includes, as of 27th February 2019, the following code of practice predating the Act which may be of assistance while the new codes are developed: [Data Sharing Code of Practice (1998 Act)](https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf).

The Data Sharing code will be of particular relevance to police forces’ law enforcement and general processing activities. The Direct Marketing code will be of less relevant, but may be applicable in scenarios such as where a police forces offer services to former employees. The Journalism code may be relevant to police forces’ press offices activities. The Age-Appropriate Design code is likely to be of limited relevance to police forces as they are unlikely to be involved in ‘information society services’ as defined in Directive (EU) 2015/1535.

Upon publication the Data Protection Officer must ensure that their police force complies as a far as possible with any relevant Code of Practice issued under DPA Part 5 Sections 121 to 128. Any significant deviation from any Code of Practice should be identified and any rationale for that deviation be recorded.

## Handling allegations of criminal offences under the Act

### Offence not connected to the force

**Commentary** – Where a police force receives a complaint that a member of the public or another organisation may have committed or be committing a criminal offence under the Act, the allegation will be recorded by the police force in accordance with the National Crime Recording Standard and associated procedures.

Where an allegation is made the officer in the case will notify the case to the Head of Enforcement for the Information Commissioner:

Address:

The Head of Enforcement

Information Commissioner’s Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Telephone: 01625 545725

Where the offence relates solely to data protection matters, the ICO will deal with the investigation and prosecution.

In the event of offences under the Act being discovered by the Police in the course of their investigations into other matters (e.g. a fraud investigation) it is important that all evidence relating to data protection matters is secured. In such circumstances the ICO will provide advice as necessary and assist in the preparation of the case file, with regard to any data protection offences.

Where the circumstances of an offence committed under DPA Part 6 Section 170 may also constitute an offence under the Official Secrets Act 1989, the Police will investigate the matter and submit a file to the Director of Public Prosecution via the Crown Prosecution Service.

The ICO and/or the OIC will notify the data protection officer of the outcome of the investigation.

### Offence or misconduct identified by or reported to the police relating to police-held personal data

**Commentary** – This commentary concerns the misuse of police-held personal data by those working for or on behalf of a police force.

In these circumstances, details of the allegation must be forwarded to the police force’s Professional Standards Department (PSD).

The PSD will assess the circumstances of the case and identify a proportionate response to the allegation. The assessment will include consideration of all relevant factors including:

* The motive of the offender – was it a case of curiosity, was it for personal gain, was it for another person’s gain?;
* The nature of the personal data – what quantity was involved, what it related to, its sensitivity, and so on;
* The harm and/or distress, potential or otherwise, caused to the person to whom the personal data related and others;
* The level of intrusion or breach of privacy suffered;
* Previous misconduct or criminal breaches by the offender;
* Whether the offender was one of many;
* The wider public interest.

Where necessary (for example, confirmation that an offence has occurred), the PSD will seek the views of the force Data Protection Officer. The ICO may also be in a position to provide advice. In all cases the Data Protection Officer should be regularly appraised by the PSD of the progress of any investigation and prosecution into offences under the Act.

Having carried out the assessment, the PSD will be in a position to determine the seriousness of the offence. Although it is not possible to draw up definitive criteria to assess that seriousness, the scale of an offence will be apparent.

Those offences deemed to be low-level in nature - for example, a member of staff browsing a record containing a minimal amount of personal data out of curiosity, where there was little prospect of harm or distress – may be dealt with under misconduct only and will not necessarily require a criminal investigation. Each case will need to be assessed against the above criteria.

Those of a more serious nature – for example, a member of staff selling the names and addresses of witnesses in a forthcoming criminal trial to associates of the person charged – are likely to be considered high-level in nature and would be likely to merit a criminal investigation and prosecution.

A decision by the Crown Prosecution Service not to proceed with a prosecution under the Act should not preclude notification of the case to the ICO.

The ICO is particularly keen on pursuing those who procure the disclosure or sale of Police-held personal data.

PSD will notify the Data Protection Officer of the outcome of the case in order that any necessary remedial action can be identified and undertaken by the force.

Where a criminal investigation has concluded and guilt has been proven the PSD will inform the Head of Enforcement at the ICO, by providing the following details: name of individual, offence and court disposal.

### Offence identified or reported to the Information Commissioner relating to police-held personal data

**Commentary** – On occasion the ICO is likely to receive allegations that a police force or individuals working on its behalf have committed offences under the Act.

In such circumstances, the ICO will take primacy for the investigation and will notify the force’s Head of PSD of the complaint. This will allow the police force to consider running a misconduct investigation parallel to or in conjunction with the ICO’s criminal investigation.

Where the offender is a senior police officer of ACC or above the ICO will notify the Police & Crime Commissioner rather than the Head of PSD (or other appropriate authority as per statute).

### Victim care

**Commentary** – Police forces will take appropriate action within their powers and capabilities to mitigate any damage or distress caused to an individual by virtue of any offence under the Act.

## Offences

### Offence: Unlawful obtaining etc of personal data (DPA Part 6 Section 170)

[DPA Part 6 Section 170 Unlawful obtaining etc of personal data](http://www.legislation.gov.uk/ukpga/2018/12/section/170) states:

*(1) It is an offence for a person knowingly or recklessly—*

*(a) to obtain or disclose personal data without the consent of the controller,*

*(b) to procure the disclosure of personal data to another person without the consent of the controller, or*

*(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.*

*(2) It is a defence for a person charged with an offence under subsection (1) to prove that the obtaining, disclosing, procuring or retaining—*

*(a) was necessary for the purposes of preventing or detecting crime,*

*(b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or*

*(c) in the particular circumstances, was justified as being in the public interest.*

*(3) It is also a defence for a person charged with an offence under subsection (1) to prove that—*

*(a) the person acted in the reasonable belief that the person had a legal right to do the obtaining, disclosing, procuring or retaining,*

*(b) the person acted in the reasonable belief that the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it, or*

*(c) the person acted—*

*(i) for the special purposes,*

*(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and*

*(iii) in the reasonable belief that in the particular circumstances the obtaining, disclosing, procuring or retaining was justified as being in the public interest.*

*(4) It is an offence for a person to sell personal data if the person obtained the data in circumstances in which an offence under subsection (1) was committed.*

*(5) It is an offence for a person to offer to sell personal data if the person—*

*(a) has obtained the data in circumstances in which an offence under subsection (1) was committed, or*

*(b) subsequently obtains the data in such circumstances.*

*(6) For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale is an offer to sell the data.*

*(7) In this section—*

*(a) references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the GDPR or section 59(8) or 105(3) of this Act (processor to be treated as controller in certain circumstances);*

*(b) where there is more than one controller, such references are references to the consent of one or more of them.*

**Commentary** – DPA Part 6 Section 170 criminalises the deliberate or reckless obtaining, disclosing, procuring disclosure to another and retention of personal data without the consent of the data controller.

Subsection (1) sets out the elements of the offence. These reflect the elements of the previous offence in Section 55 of the 1998 Act, except for the addition of unlawful retention of data. This has been added to deal with situations where a person obtains data lawfully but then intentionally or recklessly retains it without the consent of the controller.

Subsections (2) and (3) provide defences for the subsection (1) offence, while subsections (4) to (6) make it an offence to sell or offer to sell personal data that was obtained, disclosed or retained unlawfully.

Within policing the offence is most commonly committed where officers and staff use their access to information systems for purposes other than those set out by force policy, procedure, or instructions and in a way that is contrary to their official role with the force.

The Data Protection Officer should ensure appropriate measures are in place to alert all officers, staff and others processing personal data on behalf of their Chief Constable of the existence and nature of the DPA Part 6 Section 170 offence of Unlawful Obtaining etc. of personal data.

### Offence: Re-identification of de-identified personal data (DPA Part 6 Section 171)

[DPA Part 6 Section 171 Re-identification of de-identified personal data](http://www.legislation.gov.uk/ukpga/2018/12/section/172) states:

*(1) It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.*

*(2) For the purposes of this section and section 172—*

*(a) personal data is “de-identified” if it has been processed in such a manner that it can no longer be attributed, without more, to a specific data subject;*

*(b) a person “re-identifies” information if the person takes steps which result in the information no longer being de-identified within the meaning of paragraph (a).*

*(3) It is a defence for a person charged with an offence under subsection (1) to prove that the re-identification—*

*(a) was necessary for the purposes of preventing or detecting crime,*

*(b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or*

*(c) in the particular circumstances, was justified as being in the public interest.*

*(4) It is also a defence for a person charged with an offence under subsection (1) to prove that—*

*(a) the person acted in the reasonable belief that the person—*

*(i) is the data subject to whom the information relates,*

*(ii) had the consent of that data subject, or*

*(iii) would have had such consent if the data subject had known about the re-identification and the circumstances of it,*

*(b) the person acted in the reasonable belief that the person—*

*(i) is the controller responsible for de-identifying the personal data,*

*(ii) had the consent of that controller, or*

*(iii) would have had such consent if that controller had known about the re-identification and the circumstances of it,*

*(c) the person acted—*

*(i) for the special purposes,*

*(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and*

*(iii) in the reasonable belief that in the particular circumstances the re-identification was justified as being in the public interest, or*

*(d) the effectiveness testing conditions were met (see section 172).*

*(5) It is an offence for a person knowingly or recklessly to process personal data that is information that has been re-identified where the person does so—*

*(a) without the consent of the controller responsible for de-identifying the personal data, and*

*(b) in circumstances in which the re-identification was an offence under subsection (1).*

*(6) It is a defence for a person charged with an offence under subsection (5) to prove that the processing—*

*(a) was necessary for the purposes of preventing or detecting crime,*

*(b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or*

*(c) in the particular circumstances, was justified as being in the public interest.*

*(7) It is also a defence for a person charged with an offence under subsection (5) to prove that—*

*(a) the person acted in the reasonable belief that the processing was lawful,*

*(b) the person acted in the reasonable belief that the person—*

*(i) had the consent of the controller responsible for de-identifying the personal data, or*

*(ii) would have had such consent if that controller had known about the processing and the circumstances of it, or*

*(c) the person acted—*

*(i) for the special purposes,*

*(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and*

*(iii) in the reasonable belief that in the particular circumstances the processing was justified as being in the public interest.*

*(8) In this section*

*(a) references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the GDPR or section 59(8) or 105(3) of this Act (processor to be treated as controller in certain circumstances);*

*(b) where there is more than one controller, such references are references to the consent of one or more of them.*

[DPA Part 6 Section 172 Re-identification: effectiveness testing conditions](http://www.legislation.gov.uk/ukpga/2018/12/section/172) states:

*(1) For the purposes of section 171, in relation to a person who re-identifies information that is de-identified personal data, “the effectiveness testing conditions” means the conditions in subsections (2) and (3).*

*(2) The first condition is that the person acted—*

*(a) with a view to testing the effectiveness of the de-identification of personal data,*

*(b) without intending to cause, or threaten to cause, damage or distress to a person, and*

*(c) in the reasonable belief that, in the particular circumstances, re-identifying the information was justified as being in the public interest.*

*(3) The second condition is that the person notified the Commissioner or the controller responsible for de-identifying the personal data about the re-identification—*

*(a) without undue delay, and*

*(b) where feasible, not later than 72 hours after becoming aware of it.*

*(4) Where there is more than one controller responsible for de-identifying personal data, the requirement in subsection (3) is satisfied if one or more of them is notified.*

**Commentary** – [DPA Part 6 Section 171](http://www.legislation.gov.uk/ukpga/2018/12/section/171) creates offences of knowingly or recklessly re-identifying information that has been de-identified without the consent of the controller who de-identified the data, and to process such information knowingly or recklessly without the consent of the controller.

Subsection (1) sets out the elements of the offence; subsection (2) defines the meaning of ‘de-identification’ and ‘re-identification’ for the purposes of the offence and reflects the definition of pseudonymisation at [GDPR Article 4(5)](https://gdpr-info.eu/art-4-gdpr/); subsections (3) and (4) provide defences to the subsection (1) offence; subsection (5) creates a related offence of knowingly or recklessly processing personal data that has been unlawfully re-identified; and subsections (6) and (7) provide defences to the subsection (5) offence.

[DPA Part 6 Section 172](http://www.legislation.gov.uk/ukpga/2018/12/section/172) creates a specific defence against the [DPA Part 6 Section 171](http://www.legislation.gov.uk/ukpga/2018/12/section/171) offences for those who re-identify information for the purposes of testing others’ de-identification mechanisms. It requires conditions set out in subsection (2) and (3) to be met for the defence to be valid.

The Data Protection Officer must ensure appropriate measures are in place to alert all officers, staff and others processing personal data on behalf of their Chief Constable of the existence and nature of the DPA Part 6 Section 171 offence of Re-identification of de-identified personal data.

### Offence: Alteration etc of personal data to prevent disclosure to data subject (DPA Part 6 Section 173)

[DPA Part 6 Section 173 Alteration etc of personal data to prevent disclosure to data subject](http://www.legislation.gov.uk/ukpga/2018/12/section/173)

states:

*(1) Subsection (3) applies where—*

*(a) a request has been made in exercise of a data subject access right, and*

*(b) the person making the request would have been entitled to receive information in response to that request.*

*(2) In this section, “data subject access right” means a right under—*

*(a) Article 15 of the GDPR (right of access by the data subject);*

*(b) Article 20 of the GDPR (right to data portability);*

*(c) section 45 of this Act (law enforcement processing: right of access by the data subject);*

*(d) section 94 of this Act (intelligence services processing: right of access by the data subject).*

*(3) It is an offence for a person listed in subsection (4) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.*

*(4) Those persons are—*

*(a) the controller, and*

*(b) a person who is employed by the controller, an officer of the controller or subject to the direction of the controller.*

*(5) It is a defence for a person charged with an offence under subsection (3) to prove that—*

*(a) the alteration, defacing, blocking, erasure, destruction or concealment of the information would have occurred in the absence of a request made in exercise of a data subject access right, or*

*(b) the person acted in the reasonable belief that the person making the request was not entitled to receive the information in response to the request.*

**Commentary** – [DPA Part 6 Section 173](http://www.legislation.gov.uk/ukpga/2018/12/section/173) criminalises the alteration of personal data to prevent disclosure following the exercise of any of the followings [GDPR Article 15](https://gdpr-info.eu/art-15-gdpr/) right of access, [GDPR Article 20](https://gdpr-info.eu/art-20-gdpr/) right to data portability, and [DPA Part 3 Section 45](http://www.legislation.gov.uk/ukpga/2018/12/section/45) right of access. It also has the same effect in relation to right of access applications to the intelligence services, which by definition are nor relevant to policing.

The offence is to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.

Unlike the similar offence in [Section 77 of the Freedom of Information Act](http://www.legislation.gov.uk/ukpga/2000/36/section/77), which applies only to public authorities, subsection (4) makes it clear that this offence can be committed by any data controller. Subsection (5) provides defences to the offence.

The Data Protection Officer must ensure appropriate measures are in place to:

• Alert police officers and staff processing right of access applications of the existence and nature of the DPA Part 6 Section 173 offence of alteration etc. of personal data to prevent disclosure to a data subject;

* Warn any colleague from who information is sought in response to a right of access application of the existence and nature of the offence of Alteration etc. of personal data to prevent disclosure to a data subject.

### Offence; Prohibition of requirement to produce relevant records (Enforced Right of Access) (DPA Part 7 Section 184)

DPA Part 7 Section 184 Prohibition of requirement to produce relevant records states:

*(1) It is an offence for a person (“P1”) to require another person to provide P1 with, or give P1 access to, a relevant record in connection with—*

*(a) the recruitment of an employee by P1,*

*(b) the continued employment of a person by P1, or*

*(c) a contract for the provision of services to P1.*

*(2) It is an offence for a person (“P2”) to require another person to provide P2 with, or give P2 access to, a relevant record if—*

*(a) P2 is involved in the provision of goods, facilities or services to the public or a section of the public, and*

*(b) the requirement is a condition of providing or offering to provide goods, facilities or services to the other person or to a third party.*

*(3) It is a defence for a person charged with an offence under subsection (1) or (2) to prove that imposing the requirement—*

*(a) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or*

*(b) in the particular circumstances, was justified as being in the public interest.*

*(4) The imposition of the requirement referred to in subsection (1) or (2) is not to be regarded as justified as being in the public interest on the ground that it would assist in the prevention or detection of crime, given Part 5 of the Police Act 1997 (certificates of criminal records etc).*

*(5) In subsections (1) and (2), the references to a person who requires another person to provide or give access to a relevant record include a person who asks another person to do so—*

*(a) knowing that, in the circumstances, it would be reasonable for the other person to feel obliged to comply with the request, or*

*(b) being reckless as to whether, in the circumstances, it would be reasonable for the other person to feel obliged to comply with the request,*

*and the references to a “requirement” in subsections (3) and (4) are to be interpreted accordingly.*

*(6) In this section—*

*“employment” means any employment, including—*

*(a) work under a contract for services or as an office-holder,*

*(b) work under an apprenticeship,*

*(c) work experience as part of a training course or in the course of training for employment, and*

*(d) voluntary work,*

*and “employee” is to be interpreted accordingly;*

*“relevant record” has the meaning given in Schedule 18 and references to a relevant record include—*

*(a) a part of such a record, and*

*(b) a copy of, or of part of, such a record.*

**Commentary** – [DPA Part 7 Section 184](http://www.legislation.gov.uk/ukpga/2018/12/section/184) makes it an offence for an employer to require employees or contractors, or for a person to require another person who provides goods, facilities or services, to provide certain records obtained via subject access requests as a condition of their employment or contract. It is also an offence for a provider of goods, facilities or services to the public to request such records from another as a condition for providing a service.

Subsections (1) and (2) set out the elements of the offence; subsection (3) provides certain defences; subsection (4) removes the use of the public interest defence on the grounds of prevention or detection of crime where the Disclosure & Barring Service provides a route for ‘background checks’; subsections (5) and (6) provide clarification and definitions of some terms used in the section.

The Data Protection Officer should ensure appropriate measures are in place to:

* Alert data subjects to this existence and nature of the DPA Part 7 Section 184 offence of enforced right of access in any communication setting out their rights of access;
* Alert police officers and staff processing right of access applications of the existence and nature of the offence of enforced right of access;
* Notify the ICO of such offences where suspected at the earliest opportunity in order that the ICO can advise on any actions to be taken by the police force.

### Offence: Breach of confidentiality by Commissioner (DPA Part 5 Section 132)

See 9.1.3 above

### Offence: False statements made in response to an Information Notice (DPA Part 6 Section 144)

See 9.1.4 above

### Destroying or falsifying information and documents etc. (DPA Part 6 Section 148)

See 9.1.7 above

### Penalties for Offences (DPA Part 7 Section 196)

[DPA Part 7 Section 196 Penalties for offences](http://www.legislation.gov.uk/ukpga/2018/12/section/196) states:

*(1) A person who commits an offence under section 119 or 173 or paragraph 15 of Schedule 15 is liable—*

*(a) on summary conviction in England and Wales, to a fine;*

*(b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding level 5 on the standard scale.*

*(2) A person who commits an offence under section 132, 144, 148, 170, 171 or 184 is liable—*

*(a) on summary conviction in England and Wales, to a fine;*

*(b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding the statutory maximum;*

*(c) on conviction on indictment, to a fine.*

*(3) Subsections (4) and (5) apply where a person is convicted of an offence under section 170 or 184.*

*(4) The court by or before which the person is convicted may order a document or other material to be forfeited, destroyed or erased if—*

*(a) it has been used in connection with the processing of personal data, and*

*(b) it appears to the court to be connected with the commission of the offence,*

*subject to subsection (5).*

*(5) If a person, other than the offender, who claims to be the owner of the material, or to be otherwise interested in the material, applies to be heard by the court, the court must not make an order under subsection (4) without giving the person an opportunity to show why the order should not be made.*

**Commentary** – [DPA Part 7 Section 196](http://www.legislation.gov.uk/ukpga/2018/12/section/196) sets out the penalties for the offences under this Act.

Subsection (1) sets out the penalties for the summary only offences at:

* [DPA Part 6 Section 173](http://www.legislation.gov.uk/ukpga/2018/12/section/173) alteration of personal data to prevent disclosure, and
* [DPA Schedule 15 Paragraph 15](http://www.legislation.gov.uk/ukpga/2018/12/schedule/15) obstructing the execution of a warrant.

The maximum penalty on summary conviction is an unlimited fine in England and Wales or a Level 5 fine in Scotland and Northern Ireland.

Subsection (2) sets out the maximum penalties for offences that can be tried summarily or on indictment. These include offences at:

* [DPA Part 6 Section 144](http://www.legislation.gov.uk/ukpga/2018/12/section/144) false statements made in response to information notices), DPA Part 6 Section 148 destroying or falsifying information and documents etc,
* [DPA Part 6 Section 170](http://www.legislation.gov.uk/ukpga/2018/12/section/170) unlawful obtaining etc of personal data,
* [DPA Part 6 Section 171](http://www.legislation.gov.uk/ukpga/2018/12/section/171) re-identification of de-identified personal data, and
* [DPA Part 7 Section 184](http://www.legislation.gov.uk/ukpga/2018/12/section/184) prohibition of requirement to produce relevant records.

In England and Wales, the maximum penalty when tried summarily or on indictment is an unlimited fine. In Scotland and Northern Ireland, the maximum penalty on summary conviction is a fine not exceeding the statutory maximum or an unlimited fine when tried on indictment.

Subsection (4) gives a power for the court to order the forfeiture and destruction of material obtained under offences under [DPA Part 6 Section 170](http://www.legislation.gov.uk/ukpga/2018/12/section/170) and [DPA Part 7 Section 184](http://www.legislation.gov.uk/ukpga/2018/12/section/184); while subsection (5) provides any individual other than the offender with an interest in the data the right to demonstrate to the court why it should not forfeit or destroy such material.

### Prosecution (DPA Part 7 Section 197)

[DPA Part 7 Section 197 Prosecution offences](http://www.legislation.gov.uk/ukpga/2018/12/section/197) states:

*(1) In England and Wales, proceedings for an offence under this Act may be instituted only—*

*(a) by the Commissioner, or*

*(b) by or with the consent of the Director of Public Prosecutions.*

*(2) In Northern Ireland, proceedings for an offence under this Act may be instituted only—*

*(a) by the Commissioner, or*

*(b) by or with the consent of the Director of Public Prosecutions for Northern Ireland.*

*(3) Subject to subsection (4), summary proceedings for an offence under section 173 (alteration etc of personal data to prevent disclosure) may be brought within the period of 6 months beginning with the day on which the prosecutor first knew of evidence that, in the prosecutor's opinion, was sufficient to bring the proceedings.*

*(4) Such proceedings may not be brought after the end of the period of 3 years beginning with the day on which the offence was committed.*

*(5) A certificate signed by or on behalf of the prosecutor and stating the day on which the 6 month period described in subsection (3) began is conclusive evidence of that fact.*

*(6) A certificate purporting to be signed as described in subsection (5) is to be treated as so signed unless the contrary is proved.*

*(7) In relation to proceedings in Scotland, section 136(3) of the Criminal Procedure (Scotland) Act 1995 (deemed date of commencement of proceedings) applies for the purposes of this section as it applies for the purposes of that section.*

**Commentary** – [DPA Part 7 Section 197](http://www.legislation.gov.uk/ukpga/2018/12/section/197) sets out which enforcement agencies are responsible for prosecuting offences under the Act.

Subsections (1) and (2) provides that in England and Wales, prosecutions can be brought by the ICO or by, or with the consent of, the Director of Public Prosecutions, and that prosecutions in Northern Ireland can be brought by the ICO or by, or with the consent of, the Director of Public Prosecutions for Northern Ireland. In Scotland, the Procurator Fiscal handles all prosecutions in the public interest. Consequently there is no need for an equivalent provision in the Act for Scotland.

The remaining subsections concern periods allowed for commencement of prosecutions for an offence under [DPA Part 6 Section 173](http://www.legislation.gov.uk/ukpga/2018/12/section/173) alteration etc. of personal data to prevent disclosure.

### Liability of Directors etc (DPA Part 7 Section 198)

[DPA Part 7 Section 198 Liability of directors etc offences](http://www.legislation.gov.uk/ukpga/2018/12/section/198) states:

*(1) Subsection (2) applies where—*

*(a) an offence under this Act has been committed by a body corporate, and*

*(b) it is proved to have been committed with the consent or connivance of or to be attributable to neglect on the part of—*

*(i) a director, manager, secretary or similar officer of the body corporate, or*

*(ii) a person who was purporting to act in such a capacity.*

*(2) The director, manager, secretary, officer or person, as well as the body corporate, is guilty of the offence and liable to be proceeded against and punished accordingly.*

*(3) Where the affairs of a body corporate are managed by its members, subsections (1) and (2) apply in relation to the acts and omissions of a member in connection with the member's management functions in relation to the body as if the member were a director of the body corporate.*

*(4) Subsection (5) applies where—*

*(a) an offence under this Act has been committed by a Scottish partnership, and*

*(b) the contravention in question is proved to have occurred with the consent or connivance of, or to be attributable to any neglect on the part of, a partner.*

*(5) The partner, as well as the partnership, is guilty of the offence and liable to be proceeded against and punished accordingly.*

**Commentary** – [DPA Part 7 Section 198](http://www.legislation.gov.uk/ukpga/2018/12/section/198) allows proceedings to be brought against a director, or someone in or acting in a similar position, as well as the body corporate where it is proved that breaches of the Act have occurred with the consent, connivance, or negligence of that person.

It is unclear as to what extent this provision applies to police forces.

### Recordable Offences (DPA Part 7 Section 199)

[DPA Part 7 Section 199 Recordable offences](http://www.legislation.gov.uk/ukpga/2018/12/section/199) states:

*(1) The National Police Records (Recordable Offences) Regulations 2000 (S.I. 2000/1139) have effect as if the offences under the following provisions were listed in the Schedule to the Regulations—*

*(a) section 119;*

*(b) section 132;*

*(c) section 144;*

*(d) section 148;*

*(e) section 170;*

*(f) section 171;*

*(g) section 173;*

*(h) section 184;*

*(i) paragraph 15 of Schedule 15.*

*(2) Regulations under section 27(4) of the Police and Criminal Evidence Act 1984 (recordable offences) may repeal subsection (1).*

**Commentary** – [DPA Part 7 Section 199](http://www.legislation.gov.uk/ukpga/2018/12/section/199) only applies to England and Wales. It makes that offences under the Act recordable on the Police National Computer by extending them to come under the scope of [The National Police Records (Recordable Offences) Regulations 2000 (Statutory Instrument 2000/1139.](http://www.legislation.gov.uk/uksi/2000/1139/contents/made)

Offenders who are arrested for a recordable offence may have their fingerprints and DNA samples taken.

Separate provisions exist for both Northern Ireland and Scotland.

# Case Studies

## Under development – to be included in a future edition of this Manual.

# Appendices

## Appendix A: Role & Position of DPO Letter (see [2.6](#_Data_Protection_Officer))



## Appendix B: Role & Position of DPO Report (see 2.6)



## Appendix C: Personal Data Breaches (see [4.2.7.2](#_Data_Breach_Management) and [6.2.7.1](#_Data_Breach_Reporting))

****

## Appendix D: Appropriate Policy Template (see [4.2.2.7](#_Appropriate_Policy_Document) and [6.7](#_Toc510348039))



## Appendix E: Request to external organisation for the disclosure of personal data to the Police (Version 1.1.3) (see [6.9](#_Request_to_external))



## Appendix F: Joint Controllers Definitions & Arrangements (see [4.5.3](#_Joint_Controllers_(GDPR) & [6.4.3](#_Toc510348027))

****

## Appendix G: High-Level Privacy Notice [see [4.4.3.1](#_Toc505013791)]



## Appendix H: Lower-Level Specific Privacy Notice for GDPR (see [4.4.3.2](#_Lower-Level_Specific_Privacy))

****

## Appendix I: Information Management IT System Requirements (see [4.5.2](#_Data_Protection_by))

****

## Appendix J: Standards (see [1.2](#_Terminology_Used,_Manual))

****

## Appendix K: DPIA ICO Derived Template (see [4.5.2.1](#_Data_Protection_Impact))



## Appendix L: National Data Processing Contract Template (see [4.5.4](#_Obligations_on_Processors))



## Appendix M: Information Sharing Under the GDPR Guidance & Template (see 4.9)

## 

## Appendix N: Lower-Level Specific Privacy Notice for Law Enforcement Processing (see 6.3.3)

## 

## Appendix O: Collaborative Units - Project management-based approach to deliver Data Protection compliance (see 4.5.3.1)

## 

# Version Control

## Significant changes to previous version

Draft version 0.1 published for review on 24th November 2017

Draft version 0.2 circulated on POLKA 26th December 2017

Draft version 0.3 circulated with simple markup on POLKA on 31st January 2018

Draft version 0.4 circulated with simple markup on POLKA on 25th February 2018

Draft version 0.5 circulated with simple markup on POLKA on 1st April 2018

Draft version 0.6 circulated with simple markup to National Subject Rights Group on 17th April 2018

Draft version 0.7 circulated with simple markup on POLKA on 9th May 2018

Draft version 0.8 not circulated (May 2018)

Draft version 0.9 circulated on POLKA on 30th January 2019

Draft version 0.10 circulated on POLKA on 27th February 2019

Draft version 0.11 circulated on POLKA on 29th March 2019

Draft version 0.12 circulated on POLKA on 3rd January 2020

Draft version 0.13 presented to the National DP/FOI Group of 6th August 2020

Version 1.0 published to the Knowledge Hub 14th August 2020.

Version 1.1 published to the Knowledge Hub 21st August 2020. Correction of minor typos.

Version 1.2 published to the Knowledge Hub 22nd March 2021. Addition of Appendix O.

1. The first of these was the ACPO Code of Practice for Police Computer Systems in 1987, which was followed by the ACPO Code of Practice on Data Protection in 1995 and 2002. Next came the two-part ACPO Data Protection Manual of Guidance covering Standards and Audit. Part 1 Standards was published in seven editions from 2006 to 2013. The Manual of Guidance was superseded by the College of Policing’s Data Protection Authorised Professional Practice from 2014 and that remains in place for non-data protection professionals. [↑](#footnote-ref-1)
2. Via a letter to Chief Officers from the Chair of the NPCC’s IMORCC dated 8th May 2018) [↑](#footnote-ref-2)
3. Law Enforcement Processing refers to processing of personal data competent authorities (broadly the police and other criminal justice agencies) “for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security.” [↑](#footnote-ref-3)
4. Technically the scope of the GDPR does not actually extend to all non-Law Enforcement or non-Intelligence Services processing, so the DPA Part 2 Chapter 3 (Sections 21 to 28) extends GDPR equivalent provisions to fill any remaining gaps between the GDPR and Law Enforcement and Intelligence Services processing. These extensions are known as the “Applied GDPR Scheme.” [↑](#footnote-ref-4)
5. As adapted by UK law by virtue of GDPR Article 6(3) [↑](#footnote-ref-5)
6. As adapted by UK law by virtue of GDPR Article 6(3) [↑](#footnote-ref-6)
7. The sixth condition – (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child – is not available to the police by virtue of a sentence appended to the condition: “Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.” [↑](#footnote-ref-7)
8. As adapted by UK law by virtue of GDPR Article 6(3) [↑](#footnote-ref-8)
9. As adapted by UK law by virtue of GDPR Article 6(3) [↑](#footnote-ref-9)
10. Rather confusingly different sets of “Listed GDPR Provisions” exist for DPA Schedule 2 Parts 1, 2, 4, 5 & 6 relevant only to those parts respectively. [↑](#footnote-ref-10)
11. Rather confusingly different sets of “Listed GDPR Provisions” exist for DPA Schedule 2 Parts 1, 2, 4, 5 & 6 relevant only to those parts respectively. Within DPA Schedule 2 Part 6 differing sets appear under Paragraphs 27 and 28. [↑](#footnote-ref-11)
12. Rather confusingly different sets of “Listed GDPR Provisions” exist for DPA Schedule 2 Parts 1, 2, 4, 5 & 6 relevant only to those parts respectively. Within DPA Schedule 2 Part 6 differing sets appear under Paragraphs 27 and 28. [↑](#footnote-ref-12)
13. By way of comparison police forces do not have to respond to requests for information for which the retrieval of the information would take more than 18 man-hours [↑](#footnote-ref-13)
14. The other is GDPR Recital 70 (“Right to object to Direct Marketing”) [↑](#footnote-ref-14)
15. By way of comparison police forces do not have to respond to requests for information for which the retrieval of the information would take more than 18 man-hours [↑](#footnote-ref-15)