Using Cloud Services for Law Enforcement Data Guideline

ABSTRACT

This guideline in conjunction with the National Policing Community Security Policy Framework and associated documents sets out National Policing requirements for the secure and compliant use of Cloud Service Providers for processing and storing law enforcement information.

APPENDIX
A: Cloud Guidance DUAA v2.1

ISSUED:	24 JAN 2026
PLANNED REVIEW DATE:	24 JAN 2027
DOCUMENT OWNER:	National Chief Information Security Officer
DISTRIBUTION:	Members of the Policing Community of Trust
COPYRIGHT:	All content – copyright Police Digital Service
DOCUMENT HANDLING:	OFFICIAL – FOR PUBLIC RELEASE

POLICY VALIDITY STATEMENT

This guideline is due for review on the date shown above. After this date, policy and process documents may become invalid.

Readers should ensure that they are consulting the currently valid version of the documentation.

Contents

Community Security Policy Commitment 3

Introduction 3

Purpose 4

Audience 4

Scope 5

Guidance 6

Communication approach 16

Document Compliance Requirements 16

Equality Impact Assessment 16

Appendices 17

Appendix A: Cloud Guidance DUAA v2.1 17

Appendix B: NCSC Cloud Security Principles 25

Review 27

Related documents 27

Document Information 28

Document Location: 28

Version History 28

Approvals 28

Community Security Policy Commitment

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National Policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This guideline, in conjunction with the National Policing Community Security Policy Framework and associated documents, sets out National Policing guidance for the use of Cloud Service Providers. This guidance seeks to specifically address situations where the use of such services may not be explicitly limited to the United Kingdom. This may be because the Cloud Service Provider is headquartered overseas, or the model of support needed to run the service is provided globally, providing 24-hour support, 365 days a year.

Introduction

This document provides detailed guidance to support the use of Cloud Service Providers for law enforcement purposes.

A Cloud Service Provider (CSP) can be defined an organisation that delivers cloud computing services - such as infrastructure, platforms, and software - over the internet. CSPs operate large-scale environments that allow customers to access shared computing resources without maintaining their own physical infrastructure. These services typically fall under three models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). CSPs may be UK-based or globally headquartered and often use international support models, which can introduce additional compliance and security considerations for law enforcement data processing and storage.

Law enforcement data can be defined as data which is processed or stored 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[1]

It has been produced in response to the challenges posed by international data transfers – particularly to US-based[2] CSPs – under Part 3 of the Data Protection Act 2018, which governs law enforcement processing. The document provides actionable guidance around the implications of the Schrems II judgment, the limitations of the UK-US Data Bridge for law enforcement data, and references the forthcoming changes introduced by the Data Use and Access Act 2025. It aims to help members of the policing community of trust to understand

[1] Law enforcement processing: Part 3 DPA 2018; and sharing with competent authorities under the GDPR and Part 2 DPA 2018 | ICO

[2] CLOUD Act 2018 (§2713)

and navigate complex compliance requirements, while maintaining access to modern cloud technologies essential for public protection.

Purpose

The purpose of this guideline is to:

- Support compliance with the National Community Security Policy Framework, Principles, and Policy, when using a CSP for law enforcement data processing and storage.
- Provide subject matter expert guidance to personnel who are responsible for the screening, design, procurement, implementation, and management of a CSP within policing organisations.
- Offer a set of recommended security controls and mitigations to manage specific risks arising from the use of a CSP.

Audience

This guidance is aimed at:

- Senior Information Risk Owners, Information Asset Owners, and Platform Asset Owners.
- Project Managers
- Information and Cyber Security Professionals
- Data Protection Officers and Data Protection professionals
- Technical personnel responsible for system design and implementation
- Commercial and procurement professionals

Scope

In scope:

- Solution Analysis (includes demonstrating that the use of a CSP is necessary to achieve the required business objectives and outcomes)
- Data Protection Impact Assessment
- Procurement
- Design (including control selection)
- Management
- Risk & compliance activities

Caveats:

- The use of a CSP to store and process data which may be considered illegal to possess by a third-party that is not automatically covered by exemptions in law. Furthermore, using CSPs in this way may be in breach of the CSPs own use policies. Additional legal considerations may apply under acts, such as:
    - Protection of Children Act 1978 and Sexual Offences Act 2003 (e.g. indecent images of children)
    - Terrorism Act 2000 and Online Safety Act 2023 (e.g. terrorism-related material)
    - Obscene Publications Act 1959 (e.g. obscene martial deemed to deprave and corrupt)
    - Copyright, Designs and Patents Act 1988 (e.g. large-scale possession of licensed software, films, or music)
    - Official Secrets Act 1989 (e.g. classified documents stored as part of an investigation)

This list is not exhaustive. Organisations must store and process certain types of data covered by these acts in highly controlled environments, with strict legal and technical safeguards. Such controls are often specific to the individual circumstances. Therefore, it is not possible to produce a single piece of guidance covering all possible scenarios. Specific legal and technical guidance must be commissioned in these circumstances.

Out of scope:

- Information assets classified at 'SECRET' and above under the Government Security Classification (GSC) scheme.

Guidance

Reference	Minimum requirement	Control reference	Compliance Metric
Step 0	Conduct a Business Impact Assessment of the Information Assets in scope. Use this information to develop an understanding of the business impacts resulting from a compromise of information confidentiality (resulting from unauthorised disclosure). Agree a Risk Appetite with the Information Asset Owner (and Senior Information Risk Owner if necessary). Associated documents: • *National Police Information Security Risk Management Guidance* • *National Police Information Security Risk Framework*	NIST CSF 2: GV.OC-04, GV.RM-02, GV.SC-05	Completed Business Impact Assessment defining the business impacts of compromise, considering the following areas of impact: • Financial • Operational • Legal & Regulatory Compliance • Reputational • People • Strategy Defined Risk Appetite statement, aligned to the National Police Information Security Risk Management Framework.
Step 1	Develop a detailed understanding of the type of agreement that your organisation is seeking to enter into with a CSP. Examples may include: • UK-based, UK-only support • UK-based, non-UK – with EU support • UK-based, non-UK – with US support	Annex A: Cloud Guidance DUAA v2.1 NIST CSF 2: GV.OC-03	A documented assessment, detailing the type of cloud arrangement, that has been produced by someone with suitable knowledge and experience of cloud hosting. A comprehensive understanding of the environment should form part of an assessment against the NCSC's 14 Cloud Security Principles.

Reference	Minimum requirement	Control reference	Compliance Metric
	• Non-UK based – EU hosted • Non-UK based – US hosted • Non-UK based – rest of world (excluding high-risk countries[3])		
Step 2	Read and apply the Cloud Guidance DUAA v2.1 provided in Annex A according to the type of CSP agreement. Ensure that all of the required Data Protection obligations have been aligned to the type of activity undertaken.	Annex A: Cloud Guidance DUAA v2.1 NIST CSF 2: GV.OC-03	Data Protection Impact Assessment (DPIA). The DPIA demonstrates a detailed understanding of the type of arrangement (see *Step 1*). The DPIA specifically addresses the required points set out in the Cloud Guidance DUAA v2.1.
Step 3	Implement additional safeguards following a risk-based approach. Risks to mitigate may include: Risks to rights and freedoms of data subjects Unlawful processing of personal information Access by non-UK authorities (e.g. US CLOUD Act)	Annex A: Cloud Guidance DUAA v2.1 NIST CSF 2: GV.OC-03, GV.RM-02	Cyber risk assessment which includes a specific focus on the additional risks of CSP use and how they are mitigated. A developed set of Non-Functional Requirements (NFRs) that can be issued as part of a tender pack or formalised to be incorporated as contractual requirements. Contract with CSP, which includes Data Processing amendments (see Cloud Guidance DUAA v2.1) and enhanced buyer security requirements – proportionate to mitigate the risks identified.
Implement additional mitigating controls or safeguards to protect personal information that may be stored or processed outside of the UK. **Important Note:** All cloud services should be designed and built in a manner consistent with the NCSC's guidance on Cloud Security Principles, regardless of data storage and processing locations. This will include the implementation of additional controls – set out within the National Community Security Policy Framework and Standards.			

[3] Form an assessment based on the use of a number of intelligence sources, e.g., NMC Threat Intelligence, UK Foreign Office, NCSC, local organisational intelligence.

Reference	Minimum requirement	Control reference	Compliance Metric
The additional controls below are aimed at mitigating additional risks which may be present in a CSP which is non-UK based and/or where non-UK processing may occur (through the use of global support models or country-specific laws and regulations).			
1.	**Physical Auditing** Physical facilities and third parties that may process and/or store law enforcement information must undergo suitably scoped third-party and physical assurance – regardless of their physical location. Organisations should naturally prefer third parties who hold independently assessed industry standards (such as ISO27001, or SOC 2 Type II). However, where there is a requirement for a physical audit of a third party outside of the UK, this will help to provide confidence that a good security baseline exists before committing resources to any assessment. Associated documents: • *Third Party Assurance for Policing (TPAP) Standard* • *Physical & Environmental Security Management Standard*	Annex A: Cloud Guidance DUAA v2.1: Section 6.5 PASF (Storage) TPAP (Processing) NIST CSF 2: ID.RA-01, GV.SC-03	Completed PASF audit. Completed TPAP audit.

Reference	Minimum requirement	Control reference	Compliance Metric
2.	**Vetting** Local vetting leads must be consulted to determine the appropriate level of vetting to be conducted, prior to undertaking the activity. The outcome of this assessment should also form the basis of commercial agreements, ensuring that personnel security requirements are maintained for the duration of the storage/processing. A compliance assessment should be undertaken to establish the types of data and access and the controls implemented to maintain compliance with the vetting requirements. Associated documents: • *People Security Management Standard*	Annex A: Cloud Guidance DUAA v2.1: Section 6.5 National Vetting APP NIST CSF 2: ID.RA-01, GV.SC-03, GV.RR-04	Documentation detailing the level of access to data by CSP personnel. Evidence of a formal position reached by local/national police vetting leads. Inclusion of personnel security requirements within commercial agreements. Design decisions captured within the low-level design documentation to restrict access to vetted personnel only.
3.	**Information Protection** If the CSP is compelled to provide customer data to its country's authorities, the CSP should not be able to supply intelligible data. This should be achieved through a number of layered methods, which include data protection methods and technical methods.	ICO Guidance Annex A: Cloud Guidance DUAA v2.1: Section 6.5 NIST CSF 2: GV.OC-02, GV.OC-03, PR.AA-01, PR.DS-01, PR.DS-02	DPIA and/or other documentation explains how the information processed/stored by the CSP is minimised. Cyber/Information risk assessment covering the risks of unauthorised access to data to determine if object-level encryption is necessary and therefore if the key management should be under the control of the data controller. Low-level system design documentation.

Reference	Minimum requirement	Control reference	Compliance Metric
	Data Protection Methods: Data minimisation Only the minimum amount of information necessary is stored/processed by the CSP. Data pseudonymisation Where possible, replace, remove or transform information that identifies people, keeping that information separate and inaccessible to the CSP. Data anonymisation Consider rendering personal information anonymous so the data subject cannot be identified. **Technical Methods:** A risk assessment must be performed to determine if all law enforcement information must be encrypted using cryptographic keys that are generated, stored, and managed solely under the control of the data controller (policing organisation). Where an assessment identifies unacceptable risks of unauthorised data access, the cloud service provider should not have the ability to generate, store, access, or manage these keys, nor should		

Reference	Minimum requirement	Control reference	Compliance Metric
	they hold any copy or escrow of them. In this instance, the data controller should always retain exclusive authority to grant, revoke, or rotate encryption keys. Associated documents: • *Cyber Procurement Standard*		
4.	**Cryptography** To mitigate against unauthorised access or disclosure of law enforcement information, objective-level / application-level encryption should be used to mitigate against misconfiguration or compromise of other layers of controls. Full-Disk Encryption (FDE) is usually only viable with platform-managed encryption – for which the CSP maintains control. This only mitigates against physical data centre compromise, where the threat actor lacks access to the encryption keys. Encrypting files, databases, and applications may be done at the platform level, using provider-managed or customer-managed encryption keys. However, this only	Annex A: Cloud Guidance DUAA v2.1: Section 6.5 NIST CSF 2: PR.AA-01, PR.DS-01, PR.DS-02	Cyber/Information risk assessment to determine if encryption keys should be platform managed or customer supplied. Assessment of cyber risk considers the business impact of information in the future, as well as the present. Low-level system design documentation. Register of cryptographic solutions in use (e.g. asset register). This should include records of cipher suites in use.

Reference	Minimum requirement	Control reference	Compliance Metric
	mitigates against compromise of the cloud environment when a threat actor does not have access to the encryption keys. Where there is a risk that a CSP may be compelled to provide client information under country-specific laws, encrypting files, databases, and applications should be achieved using Customer-Supplied Encryption Keys (CSEK). This is sometimes also referenced as Bring Your Own Key (BYOK). CSEK should be held in a cryptographic module or service located within the UK and under the sole control of the policing organisation. This will support a wider range of due diligence activity and protection guarantees provided in law. Key lifecycle must be under the policing organisation's control. Organisations should favour solutions that are agile to emerging cryptographic vulnerabilities and technology advancements (crypto agility). Cryptographic algorithms that are		

Reference	Minimum requirement	Control reference	Compliance Metric
	resistant to quantum computing attacks should be used in all cases. Organisations should consider the business impact of information compromise in the future, as well as the present. Future quantum cryptography attacks may result in encrypted data being compromised in the future, leading to unauthorised disclosure. Associated documents: • *Cryptography Standard*		
5.	**Logging & Monitoring** Consideration should be given to exporting all access logs from the platform/application to a Security Incident and Event Monitoring (SIEM) solution to monitor for CSP access attempts to law enforcement data. This may help to identify if a CSP compelled to provide data to authorities is attempting to do so. It may also identify where a CSP is not complying with certain contractual obligations. It may also help by providing an opportunity to review the risk of processing/storage	Annex A: Cloud Guidance DUAA v2.1: Section 6.5 NIST CSF 2: PR.PS-04, DE.CM-01, DE.CM-03, DE.CM-06	Cyber/Information risk assessment entry covering unauthorised access risks and mitigations. Low-level system design documentation.

Reference	Minimum requirement	Control reference	Compliance Metric
	activities where this has triggered an alert.		
6.	**Data-Loss Prevention** There may be a need for CSP personnel to access law enforcement information (e.g. when shadowing a customer during a support call). CSP Data-Loss Prevention (DLP) policies should be reviewed to understand the risks of CSP personnel exfiltrating decrypted information from the system (e.g. in screen captures and log files). Active DLP policies that prevent an activity from taking place should be preferred over passive policies, that may only provide a record of potential data loss.	Annex A: Cloud Guidance DUAA v2.1: Section 6.5 NIST CSF 2: DE.CM-09, PR.DS-01	Cyber/Information risk assessment entry covering data-loss risks and mitigations. Low-level system design documentation.
7.	**Enhanced Management, Monitoring, and Governance** Higher risk information processing and storage activities should naturally drive more robust risk management, monitoring, and governance. Organisations should ensure that the prioritisation of these activities recognises the additional challenges posed by using a CSP for processing law enforcement data.	Annex A: Cloud Guidance DUAA v2.1: Section 6.5 NIST CSF 2: GV.OC-03, GV.OC-05, GV.PO-02, GV.SC-01, GV.SC-02, GV.SC-03, GV.SC-04, GV.SC-05, GV.SC-07, GV.SC-09, GV.SC-10, ID.AM-02, ID.AM-05, ID.AM-07	SyAP maturity, specifically controls covering governance, risk management, and supply-chain security. Evidence of a Data Protection function with strong knowledge, skills, and experience. Information Asset Register (or similar) detailing the affected Information Assets and CSPs, enabling easy identification and assessment of changes. Commercial prioritisation of higher-risk third-party contracts and agreements. Security Working Group minutes, with agenda items that

Reference	Minimum requirement	Control reference	Compliance Metric
	Data Protection leads should maintain a detailed understanding of regulatory requirements and assess the impact of any changes. To assist with impact assessments, organisations should ensure that a register of services affected by this guidance is maintained. This ensures that services affected by changes in regulation or risk can be easily identified. Commercial leads should maintain a heightened awareness of commercial agreements with CSPs and sub processors. Where there are contractual changes, these changes should be reassessed in accordance with this guidance. Security Working Groups and attendees should prioritise regularly reporting on and discussing key topics, such as: • Changes to the threat landscape; • Security events and incidents; and • Changes in regulation.		sufficiently address the ongoing risks of non-UK CSP processing/storage.

Communication approach

This document will be communicated as follows:

- Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.
- Presentation to the National Cyber Policy & Standards Board (NCPSB) for approval.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

Measurables generated by adopting this standard can also form part of regular cyber management reporting.

(Describe how this standard should communicated & implemented by the target audience.)

Document Compliance Requirements

(Adapt according to local policy needs.)

Equality Impact Assessment

(Adapt according to local policy needs.)

Appendices

Appendix A: Cloud Guidance DUAA v2.1

Annex A

Using cloud with confidence: data protection guidance for the use of cloud services for law enforcement purposes

1 **Background**

1.1 Modern technology is cloud-based, and the significant majority of cloud infrastructure is ultimately owned by one of a small number of corporations headquartered in America. If policing is to use the best and latest technology available to protect the public, using the US cloud is inevitable.

1.2 Data protection legislation sets out different obligations for general processing (under UK GDPR & Part 2 of the Data Protection Act (DPA 2018)) and law enforcement processing (under Part 3 of the DPA 2018). This includes separate, but similar, obligations for controllers to implement in contracts with processors as well as an entirely different international transfer regime. This also includes different adequacy decisions between general and law enforcement processing. Most relevant here is that the US organisations on the Data Privacy Framework List (DPF List) are, with some stipulations, treated as providing an adequate level of protection for general processing, but not for law enforcement processing. Furthermore, sections of Part 3 of the DPA 2018 were not originally written with cloud, or even processors, in mind. However, with the amendments due to come into effect by the Data Use and Access Act 2025, cloud considerations have now been integrated into law enforcement transfers. Please see **7** for a summary of these changes.

1.3 In addition to these differences there is a spectrum of cloud hosting options that Cloud Service Providers (CSPs) provide. These range from:

- UK centric: a US CSP with a subsidiary UK CSP that hosts the data with technical support located within the UK;
- US centric: to the hosting of policing data within the US CSP hosting in the US with 'follow the sun' support resulting in data potentially being accessed across the world.

1.4 There is also additional context to consider following the 2020 Schrems II judgement from the CJEU regarding US transfers as well as the US legislation that precipitated that judgement (such as US surveillance programmes and the US Cloud Act). As well as the US response that enabled the UK/US Data Bridge to be established. However, the test required by the Schrems II judgement is now set out in the s.74AB of the DPA (2018).

1.5 To address these challenges, the Police Digital Service (PDS) commissioned advice from leading Counsel (Anya Proops KC and Raphael Hogarth of 11KBW), which informs

the following guidance. This document is for data protection professionals working within police forces to provide a practical methodology that forces can use to ensure that the appropriate due diligence is conducted, obligations are met, and risks are appropriately managed.

2 Due diligence

2.1 Beyond the standard approach for new projects, forces will need to be able to demonstrate that they are confident that their relationship with their CSP processor and its supply chain comply with the obligations set out in Part 3 of the DPA 2018. This will consist of:

- Building the right contract;
- Additional Data Protection Impact Assessment (DPIA) considerations;
- A Transfer Risk Assessment (TRA);
- Risk management.

2.2 With this in mind, and taking into account Counsel's advice, we have set out below the process and key steps that forces should take to ensure that their procurement and use of cloud services, when Part 3 DPA is engaged, complies with the legislation. We believe that this is a pragmatic and sensible approach to take that will not lead to any adverse legal or regulatory effects for forces.

3 Contractual structure

3.1 In most cases where policing procures cloud services, Forces will either contract directly with the US CSP or with a UK/EEA based subsidiary. In the later, the UK CSP is likely to sub-contract some data processing to affiliates and other sub-processors in third countries, potentially including the original US CSP. There may also be scenarios where a UK headquartered cloud provider also draws technology and support through sub-contracting to sub-processors in third countries. The processing location of the data also may not be as clear cut where some functionality may be within the UK and others processed externally (such as for "follow the sun support" and business continuity). In any of these scenarios, these large CSPs usually reserve wide rights to transfer personal data to the US and other third countries as required.

3.2 Typically, the legal obligations and instructions for the processor are integrated into the contract with the CSP. There may be some exceptions to this where separate data processing agreements are required, but this should not be the norm.

3.3 The largest CSPs may be reluctant to agree specific amendments to their contracts with forces. However, forces should be able to demonstrate that they have done as much as possible to negotiate required amendments. If relevant amendments cannot be agreed, forces should consider this in the DPIA and set out why the decision has been made to proceed even without relevant amendments.

3.4 Requirements include:

3.4.1 Ensure that the relevant processor provisions in the data protection section of the contract are aligned with s.59 of the DPA 2018 (the optimal approach here is to directly cite those obligations but it may only be possible to make minimal edits to ensure the wording covers off the same requirements);

3.4.2 confirmation/a warranty from the CSP that they have taken all steps required by the legislation, including (importantly) under Part 3 DPA, to ensure that their onward transfers are compliant;

3.4.3 obligations on the CSP to notify the force of third party/government access requests for data received and refuse to respond to them as far as possible (note that some form of this obligation may well be included in the CSP's standard terms, so forces will need to make sure that it covers personal data processed for law enforcement purposes).

3.5 There may be other amendments that are appropriate depending on the circumstances; the DPIA should consider what other amendments might be needed.

In addition to non-cloud obligations contracts must:

- Ideally contain data protection provisions within the main contract, or at least appended to it. As a last resort, rely on a separate Data Processing Agreement (sometimes required for law enforcement obligations).
- Contain the provisions and obligations set out in s.59
- Contain confirmation or warranty that all onward transfers are compliant
- Confirmation and commitment from the processor and any sub-processors to inform the force of any third party/government access and refuse to respond as far as possible

4 Data Protection Impact Assessment (DPIA)

4.1 Forces should carry out a DPIA for the use of any cloud services for law enforcement purposes. In addition to a regular DPIA, this should make some further considerations relevant to cloud processing.

4.2 Section 73 sets out two relevant conditions that must be met:

4.2.1 Condition 1: The transfer is necessary for any of the law enforcement purposes. This requires forces to be confident that there is no realistic alternative solution on the market and that the force could not effectively discharge its law enforcement functions other than by contracting with the relevant CSP.

One point that Counsel made is that legislation must be interpreted in a way that is proportionate and does not produce absurd or unworkable results. Given the ubiquity of cloud services and the need for the technology used by law enforcement bodies to protect the public, Counsel's view and ours is that applying the legislation in a way that prevents forces from using cloud services at all would be disproportionate, absurd and unworkable. Taking a narrow view of the legislation would result in forces being stuck with legacy systems and essentially locking the sector out from new technology. Not using cloud arguably presents a greater risk of prejudice to data subjects,

because alternative technologies carry other risks and do not provide sufficient capabilities.

Necessity: On this basis, forces can construct an argument that there is no alternative solution to cloud that delivers the same benefits to the public that is available, reliable and secure. This must be tested and demonstrated for each cloud solution.

Establishing necessity in the DPIA should account for the following:

(i) Establishing necessity: Demonstrate that the use of this cloud service is necessary for this law enforcement task. This includes that there are no viable non-cloud or pure UK cloud alternatives that provide the same essential capabilities. The processing must also be aligned to a clear law enforcement purpose and the data in scope is proportionate to that task.

(ii) Balancing: Evaluate the public interest in achieving the law enforcement objective (such as preventing serious crime or ensuring public safety). Weigh this against the potential impact on data subject fundamental rights and freedoms (including the risk of inappropriate processing in the receiving country) as well as what safeguards are in place to mitigate these risks.

Condition 2: The transfer is: a) based on adequacy regulations; b)…based on there being appropriate safeguards; or c)…based on special circumstances. There are no current relevant adequacy regulations (as the UK DPF does not cover law enforcement processing) and no relevant "special circumstances" for the regular use of cloud processing beyond the EEA. Therefore, forces must rely on "appropriate safeguards". These could be either:

(iii) A "legal instrument" binding the US CSP which contains appropriate safeguards to protect personal data. In theory, this could be any contract, but Counsel's advice is clear that they do not consider that the IDTA or the EU SCCs plus the UK Addendum could be used in their current form, as they are drafted with UK GDPR, rather than Part 3 DPA, in mind.

The IDTA could be used as a starting point but would need to be amended to reflect law enforcement processing and Part 3 DPA obligations and safeguards. It is also worth noting that where the onward transfers are from an EEA/UK CSP the contracts would need to be in place between the processors doing the transfers; there are likely to be challenges in implementing this with large cloud providers.

Given that this refers to a legal instrument, this will include the contract with the CSP provided that a competent authority (force) is party to it and it meets the requirements set out in the data protection test.

OR

(iv) The controller, acting reasonably and proportionately, considers that the data protection test is met in relation to the transfer. This is simpler than the above option but is not likely to be appropriate where the force is party to a contract ((i) would apply). However, this basis is sufficient for onward processing through the supply chain.

Where there is a **transfer to a processor**, there are no longer any obligations to notify the ICO of the categories of data transfers that may take place. There are also no longer any obligations to record the transfer, beyond that of existing obligations elsewhere in DPA (2018).

4.2.2 Unless and until a law enforcement addendum to the IDTA exists, which is implemented between UK CSPs and their international affiliates, it seems most sensible for Forces to rely on the contract or data processing agreements to utilise a legal instrument for the processing. The DPIA should record the consideration and decision made.

A DPIA must:

- Demonstrate that the transfer is necessary for the law enforcement purposes; necessity can be assessed by weighing the need for the processing against the risks to the rights and freedoms of data subjects
- Where adequacy regulations cannot be relied upon, appropriate safeguards are required. Any contract a force is party to can rely on it as a 'legal instrument' (s.75(1A)). The data protection test is required
- However, processor to sub-processor (and beyond) contracts must rely on the 'assessment' alternative safeguard. The data protection test is required

5 Transfer Risk Assessment (TRA), Schrems II & the Data Protection Test

5.1 The Data Protection Test implements the changes implied by Schrems II's effect on UK GDPR. In cloud processing, the most common use of the Data Protection Test (s.74AB) will be as a consequence of utilising appropriate safeguards. In addition to this, the Data Protection Test also formalises due diligence work to understand the risks associated with the transfers.

5.2 Forces should ask CSPs for copies of any TRAs and any supplementary measures they have put in place for their own transfers. These are likely to be UK GDPR focused and may need some adaptation to apply to law enforcement processing. But they will provide useful insights. Additionally, forces should closely review any information published by the CSP on any government access requests received and responded to or ask the CSP for this information if it is not published.

5.3 The Data Protection Test sets out what must be considered before transfers to a third country can be carried out. These largely supplant previous responsibilities implied

from UK GDPR for a TRA. Each of these must be demonstrated in the DPIA or TRA, which if used, should be read with a DPIA. This includes:

- respect for the rule of law and for human rights in the country or by the organisation,
- the existence, and powers, of an authority responsible for enforcing the protection of data subjects with regard to the processing of personal data in the country or by the organisation,
- arrangements for judicial or non-judicial redress for data subjects in connection with such processing,
- rules about the transfer of personal data from the country or by the organisation to other countries or international organisations,
- relevant international obligations of the country or organisation, and
- the constitution, traditions and culture of the country or organisation.

5.4 These must be carefully balanced against the rights and freedoms of the data subjects and the particular personal data that is being transferred.

Data Protection Test:

- Where a force relies on an appropriate safeguard a Data Protection Test must be conducted, ideally this would be completed with the, or annexed to, the DPIA, so they can be read together
- This is an assessment that must cover the risks to the rights and freedoms of data subjects regarding:
  - respect for the rule of law and for human rights in the country or by the organisation,
  - the existence, and powers, of an authority responsible for enforcing the protection of data subjects with regard to the processing of personal data in the country or by the organisation,
  - arrangements for judicial or non-judicial redress for data subjects in connection with such processing,
  - rules about the transfer of personal data from the country or by the organisation to other countries or international organisations,
  - relevant international obligations of the country or organisation, and
  - the constitution, traditions and culture of the country or organisation.

6 Understanding and Managing risk

6.1 It is impossible to fully understand the risk without understanding the unintended oddities in the legislation that emerge around US transfers. There is a limited adequacy decision in place for US firms participating in the Data Bridge. In some instances, this could include personal data that is processed with greater risk to the data subjects but is not subject to any additional scrutiny relating to international transfers. This is because, both the UK and EU have assessed the US and found that personal data processed under UK/EU GDPR is afforded essentially equivalent protections. However, law enforcement processing in the same CSP, or even on the same platform, is not. Therefore, identical risks between both regimes are treated entirely differently depending on where they sit in the legislation and not primarily on the actual risk to the rights and freedoms of data subjects.

6.2 To bring further context, the majority of the international transfer risks would only crystallise in the event of a legal challenge. Provided that forces develop effective approaches to managing cloud compliance, challenge seems unlikely to arise or be successful given that:

6.2.1 Any judicial challenge would need to be brought by someone who had been damaged by such transfers, and a judicial review claim would similarly need to demonstrate that the claimant had sufficient interest in the decision being reviewed; and

6.2.2 The ICO made a publicly available statement in the development of previous legislation, that it does not consider these transfers to be unlawful (and the ICO itself uses cloud solutions for law enforcement purposes).

6.3 Ultimately, the lack of symmetry between UK GDPR and DPA 2018 Part 3 processing adequacy regulations is unfortunate. However, there is nothing to suggest that the intention of the legislation was to restrict the use of cloud services for law enforcement purposes, and interpreting the legislation in this way would be disproportionate, absurd and unworkable.

6.4 The ICO's TRA tool provides a useful guide to risk and mitigations around cloud and international transfers as well as extra steps and Protections set out in the Appendix.

Using data security

6.5 A significant portion of the risks associated with US CSPs are around inappropriate access to the data, either through government surveillance or through a US force's use of the US Cloud Act. Therefore, a great deal of mitigation against this risk can be accomplished through robust cyber security controls. These are not covered by this paper.

7 Key Data Use and Access Act changes to law enforcement cloud processing

7.1 Transfers to processors in third countries are now exempt from s.77 requirements.

- Change will add s.73(4)(aa) which adds a 'home' for processors, which does not require s.77 conditions to be met. Previously, processors would have fallen under s.73(4)(b) (for entities that are not relevant authorities, which require additional safeguards (s.77)).

7.2 Transfers to processors using 'appropriate safeguards' no longer require the ICO to be informed and no longer have additional documentation requirements. The data protection test from Schrems II has now been formally added and is required where appropriate safeguards are applied.

- S.75 (transfers on the basis of appropriate safeguards) processors will be exempt from informing the ICO and documentation requirements (s.75(2) & (3)). Data protection test to be added in (1A)(b).

7.3 Subsequent transfers rules now exempt transfers to processors, instead there is reference to the section relating to processors (s.59) & the general principles (s.73).

- S.78 will be largely re-written, s.78(A1) exempts processors from almost all obligations, except the new s.78(7), which is exclusively for transfers to processors and just points to pre-existing obligations s.59 & s73(1).

7.4 The data protection test has been formally added to the legislation, there is little change here to existing Schrems II requirements.

- Test must consider about 3rd country:
    - Respect for rule of law
    - Existence, powers and authority of their data protection authority
    - data subjects' opportunities for judicial or non-judicial redress
    - their international transfer rules
    - their international obligations
    - their constitution, traditions and culture (country and/or relevant sectors/organisations)

Appendix B: NCSC Cloud Security Principles

Overview: https://www.ncsc.gov.uk/collection/cloud

NCSC Principle	Information
Principle 1: Data in transit protection	Please consult the NCSC website content for the most up-to-date guidance: https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-1-data-in-transit-protection
Principle 2: Asset protection and resilience	https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-2-asset-protection-and-resilience
Principle 3: Separation between customers	https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-3-separation-between-customers
Principle 4: Governance framework	https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-4-governance-framework
Principle 5: Operational security	https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-5-operational-security
Principle 6: Personnel security	https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-6-personnel-security
Principle 7: Secure development	https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-7-secure-development
Principle 8: Supply chain security	https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-8-supply-chain-security

Principle 9: Secure user management	https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-9-secure-user-management
Principle 10: Identity and authentication	https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-10-identity-and-authentication
Principle 11: External interface protection	https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-11-external-interface-protection
Principle 12: Secure service administration	https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-12-secure-service-administration
Principle 13: Audit information and alerting for customers	https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-13-audit-information-and-alerting-for-customers
Principle 14: Secure use of the service	https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-14-secure-use-of-the-service

Review

This document will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed and that the policy continues to meet the objectives and strategies of the police service.

Related documents

DOCUMENT NAME	VERSION AND DATE
NPCC National Policing Digital Strategy 2025-2030	2025
NPCC National Policing Cyber Security Strategy	2024
ISF - Standard of Good Practice (for Information Security)	2024
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	02/2022
CIS Controls	V8.1 06/2024
NIST Cyber Security Framework v2.0	V2.0 02/2024
CSA Cloud Controls Matrix v4.0	V4.0 08/05/2025
NCSC Cyber Assessment Framework v4.0	V4.0 2025
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page
NCSC 14 Cloud Security Principles – NCSC.GOV.UK	Web Page

Document Information

Document Location:

National Policing Policies & Standards Platform - https://knowledgehub.group/web/national-standards

Version History

VERSION	AUTHOR	REVISION	DATE
0.1	PDS Cyber	Initial draft – input from local forces and PDS stakeholders	11/2025

Approvals

VERSION	BODY	TITLE	DATE
1.0	NCPSWG	National Cyber Policy & Standards Working Group	14/01/26