Cabinet Office

Government Security Classifications

FAQ Sheet 3: Working with Personal Information

v1.0 – April 2013

This FAQ sheet addresses practical aspects of working with personal information and data using the Government Security Classifications Policy (December 2012). It is intended to support a consistent approach to implementation that can ensure trust, interoperability and effective sharing.

Will all personal information be handled in OFFICIAL?

Almost all personal information/data will be handled within OFFICIAL without any caveat or descriptor. In very limited circumstances, specific sensitivity considerations may warrant additional (generally procedural) controls to reinforce the 'need to know' for access to certain personal data at OFFICIAL.

Personal information / data should only be managed in the SECRET classification where the context warrants defending against a heightened threat profile, e.g. data identifies a person as being in an exceptionally sensitive position or situation (e.g. an employee of the Security and Intelligence Agencies).

What about sensitive personal data as defined by the Data Protection Act (DPA)?

In most cases (apart from where other particular sensitivity considerations apply) personal information and sensitive data, as defined by the DPA, will be handled within OFFICIAL without any caveat or descriptor. This also applies to information previously marked protected personal data as defined in HMG Information Assurance Standard 6.

Will personal information in the OFFICIAL level be widely accessible?

No. All information must be subject to appropriate protection. There is no presumption of unbounded access at any level of the classification policy; though the principles of openness, transparency and information reuse need to be considered. As with current arrangements, organisations should use ICT access control measures, supported by procedural and personnel controls, to manage their information assets and enforce the 'need to know' principle.

All personal data / information is subject to the 'need to know' principle and it is the responsibility of Information Asset Owners (IAOs) to ensure that this is enforced in respect of personal data / information for which they are responsible.

Will the OFFICAL level provide the adequate/proper protection for personal data?

Everyone working with government information, staff, contractors and service providers, has a personal responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked or not.

IAOs need to consider the sensitivity and threats to their information and to identify those instances where access to personal information must be no wider than necessary for the efficient conduct of an organisation's business. The 'need to know' principle must be used wherever personal information is collected, stored, processed, destroyed or shared within government and when dealing with external public or private sector organisations, and effective procedural controls put in place.

The recommended technical controls for the OFFICIAL classification set out in the GSC Security Controls Framework provide an appropriate level of protection for most personal information and data held on ICT systems. However, the onus remains on IAOs and business leads to properly understand the value, sensitivity and threats to their information when determining the Confidentiality, Integrity and Availability requirements for specific ICT solutions.

Technical controls at OFFICIAL utilise 'good' commercial ICT products and services. Whilst these controls cannot absolutely assure against the most sophisticated highly capable, determined and well resourced threats, they will provide for robust and effective protections that make it very difficult, time consuming and expensive to illegally access this information. This is no different from current arrangements for the lower classification level systems.

Is there a single set of baseline security controls that will protect all personal data?

No, as currently the controls will vary according to a range of factors, for example the value and sensitivity of the information, the threats to that information, how it is used, by whom and where. Organisations need to undertake an holistic risk assessment to determine the appropriate controls necessary to meet the confidentiality, integrity and availability requirements.

What about meeting the Data Protection Act requirements?

The DPA requirement to provide appropriate and proportionate protection for personal data is unchanged. Senior Information Risk Owners (SIROs) and IAOs need to assure themselves that they have taken reasonable steps to comply with the DPA principles. Organisations must ensure that staff are trained in the handling of any personal data they process or manage and that tailored guidance is available about specific local processes. Security Classifications are designed to be used in parallel with any DPA controls but will not in themselves provide the requisite protection for information covered by DPA.

What type of personal information might qualify as OFFICIAL-SENSITIVE?

The OFFICIAL-SENSITIVE caveat should be applied where the 'need to know' must be most rigorously enforced, particularly where information may be being shared outside of a routine or well understood business process. For example, where the loss or compromise of information could have severely damaging consequences for an individual or group of

individuals - there is a clear and justifiable requirement to reinforce the 'need to know principle' particularly rigorously across the organisation.

To maintain its currency the threshold for marking information OFFICIAL-SENSITIVE should be kept quite high. It is certainly not intended that because an OFFICIAL document or data contains personal information it should be routinely marked OFFICIAL-SENSITIVE, it should meet the criteria set out above.

Aggregation of large amounts of personal data has no bearing on the application of classification markings, but it can change the threat to the information and also enhance the impact of any compromise. Where large data sets of personal information exist in the OFFICIAL classification, effective procedural, and in some cases technical, controls may be appropriate to reinforce the 'need to know' principle and provide enhanced protection. However the data should not be marked OFFICIAL-SENSITIVE.

Who decides what information is OFFICIAL-SENSITIVE?

Organisations' SIROs and IAOs, need to make their own judgements about the value and sensitivity of the information that they manage, and decide the instances where it is appropriate to use the OFFICIAL-SENSITIVE caveat. This will vary depending on the subject area, context and in some cases, any statutory or regulatory requirements; however, to facilitate information sharing across organisations a consistent approach should be adopted.

Can I use a descriptor to identify information or data that contains personal information?

Only in very specific circumstances to identify certain categories of information that have already been assessed OFFICIAL-SENSITIVE.

The descriptor should be applied in the format: 'OFFICIAL-SENSITIVE [DESCRIPTOR]'

Where descriptors are permitted they must be supported by local policies and business processes and staff training provided.

Can I identify particular processes that involve personal information or data?

If there are business or transactional processes with specific personal information or data related to them, for example a "Court Report" or "Tax Record", then organisations may choose to identify the documents or data in some way to link them to that particular business process and associated handling rules. Such identifiers are not related to the security classification.

Can I send OFFICAL documents containing personal information across the Internet or email them to people on the Internet?

Current rules continue to apply. By default personal information should be protected in transit, i.e. personal information may be sent over the GSi or encrypted across the Internet.

However there are circumstances where it may be appropriate to send unencrypted personal data over the Internet. Before unencrypted personal information is sent across unsecured

networks a risk assessment should be undertaken to assess the consequences of compromise. This assessment should also consider the operational or valid business reasons for this requirement, for example an individual has given permission for their information to be sent via the Internet in order to access or receive a service.

Aggregated datasets of personal information should never be sent unprotected across unsecured networks.

Can personal information be off shored?

Any organisation planning to store or process personal information / data outside the UK/EEA must first consult the Office of the Government SIRO (OGSIRO).

Does OFFICIAL-SENSITIVE personal information have to be registered and tracked?

Where large volumes of OFFICIAL-SENSITIVE personal information or data are regularly shared between organisations, the respective SIROs and IAOs may wish to agree specific handling arrangements and transfer protocols in line with the policy.

How should organisations deal with personal information losses or breaches?

Just as they do now. Organisations must ensure that staff are trained to understand that they have a duty of confidentiality and a personal responsibility to safeguard any HMG information that they are entrusted with. This includes ensuring that they comply with the legal and regulatory requirements and standards, for example the encryption of personal data on removable media.

Incident management policies and procedures should be readily accessible and training supported by common sense local business processes that make it easier for staff to follow the rules (e.g. clear desk policies, guidance on the transmission of personal data, proper disposal, etc). The potential sanctions (criminal or disciplinary) for inappropriate behaviours should be clearly explained to staff and where inappropriate behaviours or security breaches occur they should be dealt with. HR policies and procedures should complement security policies and any disciplinary sanctions should be applied in a measured and proportionate way.