Home Office

Data Protection Legislation

Policy on sensitive processing for Law Enforcement Purposes, under Part 3 DPA (2018)

Data and Identity Directorate

v 3.0, March 2021

1. Introduction

This is the appropriate policy document (APD) for the Home Office produced in accordance with its obligations under sections 35(4) and 35(5) of Part 3 of the Data Protection Act 2018 ("DPA 2018"). This policy meets the requirements in section 42 DPA 2018 to set out the safeguards the Home Office has in place for sensitive processing carried out for a law enforcement purpose when acting in its capacity as a competent authority. It should be read alongside the Home Office's Data Protection Policy, its Record of Processing Activities (maintained in accordance with section 61 DPA 2018), and its Personal Information Charter, and APD for sensitive processing under UK GDPR/Part 2**.** The Home Office's Information Asset Register (IAR) also provides more detailed information about its processing.

Scope

This policy applies to sensitive processing – as defined in section 35(8) DPA – undertaken by the HO in accordance with Part 3 of the DPA 2018. Home Office processing of special category data for general purposes is covered in a separate document APD for sensitive processing, UK GDPR/Part 2.

The purpose of this policy is to explain:

- Home Office procedures which are in place to secure compliance with the data protection principles set out in Part 3 of the DPA 2018 when sensitive processing is carried out by the Home Office (in its capacity as controller) on the basis of 'strict necessity' in reliance on one of the conditions set out in Schedule 8, or (in rare cases) on the basis of 'consent'; and
- Home Office policies about the retention and erasure of such personal data, including an indication of how long such data is to be kept.

Legal obligation

Section 35(3) of the Data Protection Act 2018 (the first data protection principle: law enforcement processing) provides sensitive processing (as defined in section 35(8) DPA) for any of the law enforcement purposes is permitted only in the two cases set out in sections 35(4) and (5):

- 35(4): where the data subject has given consent to the processing for the law enforcement purpose; or,
- 35(5): the processing is strictly necessary for the law enforcement purpose and it meets at least one of the conditions in Schedule 8.

An additional requirement for both conditions is that the controller must, at the time the processing is carried out, have an appropriate policy in place.

Home Office staff must therefore have regard to this policy when carrying out sensitive processing on behalf of the Department, when it is acting in its capacity as the competent authority and controller of the personal data. When the Home Office is acting in the capacity of a processor it will do so in accordance with the instructions and policies set by the controller in each case.

The Home Office has considered whether in the course of its official functions there are additional types of data that should be treated as sensitive processing although not prescribed as such under the Law Enforcement Directive and Part 3 of the Data Protection Act 2018. One such occurrence is that of nationality. The HO will always treat data revealing racial and ethnic background as sensitive processing. Where other data (such as nationality data in some specific cases) is processed in such a way as to reveal characteristics amounting to sensitive data (e.g. of race and/or ethnicity) the other data will, as appropriate, be processed subject to the enhanced safeguards for sensitive processing.

Additionally, the HO may in practice voluntarily decide on a case-by-case basis to apply the enhanced safeguards to other data that it processes – this will include any cases where it is more practical for the department to treat all data as sensitive processing (even when it is not legally necessary or required to be processed as such).

2. Conditions for sensitive processing

Organisations that have a law enforcement function and are designated as competent authorities can process personal data for law enforcement purposes – defined in section 31 DPA, which includes processing for the purpose of the prevention, detection, investigation or prosecution of criminal offences – and when they do, such processing must be in accordance with Part 3 DPA 2018. As a ministerial government department, the Home Office is a competent authority in accordance with schedule 7, para 1, DPA 2018 in respect of the law enforcement activities it carries out as part of its official functions.

The Home Office is most likely to carry out 'sensitive processing' for a law enforcement purpose on the basis of 'strict necessity' under s.35(5). It is also able to rely on consent under s.35(4), but we are not aware of this being relied upon in the context of law enforcement processing. The HO is therefore required to have this Appropriate Policy Document in place for both scenarios, and when relying on the s.35(5) condition to permit such processing to also meet at least one of the additional conditions prescribed in schedule 8 DPA.

The schedule 8 conditions for sensitive processing that the Home Office is most likely to rely on are:

- para 1, ‘statutory etc purposes’, where the sensitive processing is necessary to fulfil one of its official law enforcement functions and/or is in accordance with its responsibilities under legislation, such as those listed below as well as other relevant law (including under common law), and where the processing is necessary for reasons of substantial public interest:
    - Immigration Act 1971
    - Proceeds of Crime Act 2002;
    - powers or duties conferred under amendments to the Police and Criminal Evidence Act 1984;
    - Crime and Courts Act 2013
    - any duty or responsibility arising from the royal prerogative, common or statute law in relation to immigration, border, customs or terrorism offences, or any of the HO’s other law enforcement functions;
- para 2, administration of justice’, for example, for processing in relation to the handling of mutual legal assistance (MLA) claims;
- para 4, ‘safeguarding of children and of individuals’, for example, where the sensitive processing is necessary to protect an individual, such as a child or a person at risk -- for example, identified as a victim of human trafficking;
- para 5, ‘personal data already in the public domain’, for example if considering information available via the internet when deciding whether to proceed with an investigation;
- para 6, ‘legal claims’, also for processing data in relation to MLA claims.

The Home Office may on occasion also rely on other conditions in Schedule 8, such as:

- para 3, ‘protecting individual’s vital interests’;
- para 8, preventing fraud;
- para 9, ‘Archiving etc.’.

This list is not exhaustive. Further details of the HO’s processing activities and the conditions it relies upon are set out in its record of processing, and in its Information Asset Register.

3. Compliance with data protection principles

Section 34 of the DPA sets out the data protection principles which apply to the processing of personal data by a competent authority for a law enforcement purpose. The procedures the Home Office has in place to ensure compliance with these when carrying out sensitive processing is set out below.

a) Accountability principle

The Home Office has put in place appropriate technical and organisational measures to meet the requirements of accountability (as required by s.34(3)). These include:

- the appointment of a Data Protection Officer (DPO) who has a key assurance, compliance and advisory role on data protection matters within the Home Office;
- a direct reporting line from the DPO to our highest management levels;
- the development and regular review of corporate data protection policies and guidance for staff setting how the Home Office meets its data protection obligations – such as how to ensure new projects, applications or systems meet the technical requirements set out within UK data protection legislation;
- the development of more detailed local guidance relevant to the processing taking place within each business area, such as Immigration Enforcement, UKCA etc;
- the Home Office Data Board – which reports directly to the HO's Executive Committee on the management of data related risks – providing top-level oversight of data protection strategy, policy, and governance across the Home Office;
- the Data Protection Board (DPB, acting as a sub-board to the Data Board) being responsible for driving and monitoring compliance across the Home Office, including approving departmental data protection policies and guidance, other data protection measures that affect the whole department, and facilitating a data protection information-sharing forum to communicate the latest updates and good practice;
- the appointment and training of Information Asset Owners (IAOs) (at SCS level where appropriate) to be responsible for the management of assigned information assets, including the identification and mitigation of risks arising from the processing of personal data, and that the appropriate documentation is maintained for each of our processing activities;
- the establishment, management and on-going training of a Data Protection Practitioner (DPP) network across the department, comprising staff who provide advice on data protection matters and take steps to ensure compliance within their local business area;
- Home Office Security directorate being responsible for advising the business on the organisational measures and controls required to protect the security and integrity of personal data processed by the Home Office;
- HO Cyber Security (HOCS) directorate being responsible for advising system developers and managers to ensure that risks to Home Office data and the systems on which it is processed, stored and transmitted are identified and mitigated;
- implementing appropriate security measures in relation to the personal data we process by using the above networks, guidance, and processes (such as the DPIA) to ensure staff access to personal data and/or to systems containing such are limited and monitored;

- using the above networks to regularly review our accountability measures, and update or amend them when required, and to ensure we take a 'data protection by design and default' approach to our activities, including the design of HO systems.

Further information can also be found in our Data Protection Policy which sets out the ways in which the HO complies with data protection legislation (including integrating data protection by design and default), and in the APD for processing special category data, UK GDPR/Part 2.

b) Principle 1 - 'lawful and fair'

Lawful

The lawfulness of the Home Office's processing for law enforcement purposes is in most cases derived from its official functions and statutory/common law powers, and by additionally ensuring all processing is necessary and proportionate to the identified law enforcement purpose (see 'data minimisation' below).

The Home Office's law enforcement functions include supporting and having the policy responsibility for the prevention, detection, investigation and prosecution of organised crime and terrorist offences; and safeguarding against, and the prevention of, threats to public safety. This includes the prevention and combating of money laundering and the financing of terrorism; and the conduct of criminal and financial investigations which may include the use of mobile data extraction. It is also responsible for undertaking investigations and prosecutions relating to immigration enforcement, border and customs control, and, through its UK Central Authority (UKCA), for processing mutual legal aid requests for HM Government.

Its exercise of powers to investigate criminal offences relating to immigration offences are set out within the Immigration Act 1971 and subsequent Acts. Designated members of staff may also investigate both civil and criminal cases under the relevant powers in the Proceeds of Crime Act 2002 (POCA). The Home Office also sometimes relies on the Royal Prerogative, for example, as the legal authority for the UKCA to respond to MLA requests and transmit evidence overseas.

The above lists are not exhaustive – further details of the HO's work can be found in its Personal Information Charter , on its website, and in local guidance, for example, such as the following produced by HO teams, UKCA and the Criminal Financial Investigation Team (part of Immigration Enforcement):

- **Criminal and Financial Investigation IE Guidance**
- **Mutual Legal Assistance (MLA) Guidelines**

The HO uses the networks, training and guidance outline above (in the section on 'accountablity') to ensure the lawful purpose for and necessity of its processing activities is always identified and documented in its Record of Processing, its Information Asset Register, Privacy Information Notices, and in guidance for staff.

Strictly necessary

When the Home Office carries out sensitive processing it will mainly be in reliance on the 'strictly necessary' criteria (s.35(5)), and must meet at least one of the permitted conditions set out in Schedule 8 DPA – the ones the HO is most likely to rely on are listed in section 2 above.

Before carrying out sensitive processing HO staff must undertake an assessment to determine whether the proposed processing is strictly necessary for and proportionate to the specified law enforcement purpose being pursued and schedule 8 condition, and whether it will serve a substantial public interest. If the aim could be achieved by other means -- such as by not processing the data, or limiting the processing to data that is not sensitive, or by using an anonymised version – the sensitive processing will not take place. The outcome of the assessment must be documented in line with local policies and guidance and retained for a period of at least six months after the processing has ceased.

We ensure staff who might carry out sensitive processing are trained to understand their obligations when processing personal data, and provided with local guidance specific to the area of law enforcement work they are engaged in on how to assess and record their decision-making on a case-by-case basis about whether the processing is strictly necessary etc. Further details of how we ensure this are set out in the HO's APD for UK GDPR/Part 2 DPA.

Consent

The Home Office is also able to rely on consent as permitted by section 35(4) as the basis for its sensitive processing. While we are not aware of this being relied upon in the context of law enforcement processing, were it necessary to do so we would ensure data subjects are provided with a Privacy Information Notice and that explicit consent for each data item is sought, data subjects are informed they have the right to withdraw their consent at any time, are provided with details of how they can do this, and that the HO has processes in place to easily facilitate any withdrawal of consent.

Further details of when the Home Office relies on specific conditions are set out in its Record of Processing Activities and in its Information Asset Register.

Fairness

High-level information about how the Home Office uses personal data, including sensitive processing, is published in the Home Office's Personal Information Charter (PIC) on

GOV.UK and its privacy notices. Home Office application forms signpost the Personal Information Charter, provide high-level information about how the Home Office uses personal data, and refer to any processing that is particularly relevant. For example, UK visa and immigration forms explain that information may be shared with other public and private sector organisations in the UK and overseas including for the purposes of detecting fraud or the proceeds of crime etc, and that further information can be obtained from the BICS Privacy Information Notice published on the Home Office website.

As a government department the HO is also bound by the public sector equality duty and HM Government's Data Ethics Framework. Both are followed to ensure appropriate and responsible data use. The HO conducts Equality Impact Assessments (EIAs) where appropriate to assess the fairness and likely impact of policy decisions on particular groups and to ensure it develops policies and delivers services which are fair and just and uses the Ethics Framework to ensure ethical considerations are addressed within HO projects.

a) Principle 2 – 'specified, explicit and legitimate'

The Home Office only carries out sensitive processing when permitted to do so by law. Such personal data is collected for specific, explicit and legitimate purposes -- such as medical data for the issuing of prohibited firearms licensing -- and will not be further processed for reasons that are incompatible with the purposes for which the data was collected (unless allowed for under s.36(2)).

The HO uses the networks and processes outlined above (and expanded on in the APD for the processing of Sensitive Data under UK GDPR/Part 2) to ensure it meets these requirements.

b) Principle 3 - 'adequate, relevant and not excessive'

The Home Office will in each case collect only the personal data that is needed for the particular law enforcement purpose(s) of its processing, ensuring it is necessary, proportionate, adequate and relevant. Each Home Office service will have a bespoke application form or digital service to ensure it collects only the information necessary to determine entitlement, deliver services, or meet one of its stated purposes for processing.

Each form or process will not prompt data subjects to answer questions and provide information that is not required, nor (as far as possible) will they require data subjects to provide the same information, such as date of birth or address, repeatedly to the department: application forms will instruct data subjects to skip questions that either do not

apply, or which they have already answered, and digital processes will be designed in the same way.

Additionally, Home Office internal guidance, training and policies require staff to use only the minimum amount of data required to enable specific tasks to be completed.
Where processing is for research and analysis purposes, wherever possible this is done using anonymised or de-identified/pseudonymised data sets.

c) Principle 4 - 'accurate and up to date'

When the Home Office becomes aware that personal data is inaccurate or out-of-date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, the reason for that decision will be documented.

Providing complete and accurate information is required when applying for a firearms or other licence, or other services provided by the Home Office. Data subjects are required to notify the Home Office of relevant changes in their circumstances, such as changes of address. Where permitted by law, and when it is reasonable and proportionate to do so, the Home Office may check this information with other organisations – for example local authorities or sponsors – before amending details on our records.

If a change is reported by a data subject to one service or part of the Home Office, whenever possible this will also be used to update other services, both to improve accuracy and avoid the data subject having to report the same information multiple times.

Categorisation of data

The Home Office will, as far as possible, distinguish between personal data based on facts and personal data based on personal assessments or opinions by marking the file/information to reflect the distinction.

Where relevant, and as far as possible, we will also distinguish between personal data relating to different categories of data subject in order to fulfil our obligations under section 38(3) DPA, such as:

- People suspected of committing an offence or being about to commit and offence
- People convicted of a criminal offence
- Known or suspected victims of a criminal offence
- Witnesses or other people with information about offences.

This will be done by marking the file/information in accordance with guidance specific to the system/type of file on which the data is being recorded, and by ensuring new systems are designed with this functionality.

The Home Office only does the above where the personal data is relevant to the law enforcement purpose being pursued.

Verification of data before transmission

The Home Office will take reasonable steps to ensure that personal data which is inaccurate, incomplete or out-of-date is not transmitted or made available for any of the law enforcement purposes. Where possible and practicable, we do this by verifying any data before sending it externally or otherwise making it available, and by providing the recipient with the necessary information we hold to assess the accuracy, completeness and reliability of the data, including how up-to-date it is.

The Home Office will document all decisions to make personal data available for any of the law enforcement purposes and, if we discover after transmission that the data was incorrect or should not have been transmitted, we will inform the recipient as soon as possible.

The HO uses the networks and processes outlined above (and expanded on in the APD for the processing of Sensitive Data under UK GDPR/Part 2) to ensure it meets these requirements.

d) Principle 5 - 'kept no longer than is necessary'

The Home Office has a corporate retention schedule in place which is published online in its retention and disposal standards page. Most applications and some types of information have separate tailored retention policies, as the period for which information is necessary for the purpose for which it is processed will differ – for example, where information relates to court proceedings. Separate retention policies are also in place for Home Office operational records and casefiles. These policies can be accessed via the above links, and are published in the Home Office's Privacy Information Notices, some of which can be accessed via our Personal Information Charter.

The Home Office will usually retain information processed for the purposes of law enforcement for 6 years from closure of the matter unless there is a legitimate reason to retain it for longer, as set out in the above polices. Where consent is used as the basis for the sensitive processing, such data will be retained for the periods set out in these policies unless consent is revoked before then: details of how to revoke consent are provided when the data is collected, and details of how to contact the HO's DPO are published on our website.

All retention schedules are set in accordance with HO guidance on 'How to Determine Retention and Disposal Schedules', and are to be reviewed at least every 3 years or sooner if legal or statutory requirements, systems or processes change.

f) Principle 6 - 'processed in a secure manner'

Relevant Home Office IT systems are designed to ensure to the greatest extent possible personal data cannot be corrupted when it enters or is processed within them; this includes ensuring adequate security to guard against hackers who might try to corrupt the data, and a method for monitoring the ongoing integrity of inputted data, for example, by the production of regular data quality reports.

The Home Office has a range of security standards and policies based on industry best practice and government requirements to protect information from relevant threats. We apply these standards whether Home Office data is being processed by our own staff, or by a processor on our behalf. The security policy framework for government is published on gov.uk.

All staff handling Home Office information or using an official system must have the appropriate security clearance and are required to complete annual training on the importance of security, and how to handle information appropriately.

In addition to having security guidance and policies embedded throughout HO business, the HO also has specialist security, cyber and resilience staff to help ensure that information is protected from risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. The managing framework and the roles and responsibilities of lead officials for security is set out in the Home Office's Security Roles and Responsibilities Policy.

4. Monitoring and Review

The Home Office will formally review this document not less than six months after its introduction (not later than the end of October 2018) and yearly thereafter.

This document will be made available on request to the Information Commissioner pursuant to s42(3)(c) of the DPA.

This guide is managed by the Home Office Data and Identity Directorate. Any suggestions for improvements or comments should be directed to DPPolicyHub@homeoffice.gov.uk.

Effective Date	25/05/2018
Last Revision Date	04/08/2021
Next Revision Date	29/03/2022
Approved by	DP P&G Working Group, Director Data & Identity
Audience	All Staff