Home Office

Data Protection Legislation

Appropriate Policy Document: processing special categories and criminal convictions data under UK GDPR and Part 2 DPA (2018)

Data and Identity Directorate

v 3.0, March 2021

1. Introduction

This document is the appropriate policy document for the Home Office. It sets out the safeguards the HO has in place to protect special category and criminal convictions data that it processes in accordance with Article 9 and 10 UK GDPR, and has been produced in accordance with Home Office obligations under UK data protection legislation (Schedule 1 DPA 2018). It should be read alongside the Home Office's Data Protection Policy, its Record of Processing Activities, (maintained in accordance with Article 30 UK GDPR), and its Personal Information Charter. The Home Office's Information Asset Register also contains more detailed information about its data processing.

Scope

This policy applies to the processing of special category data – which is defined in Article 9(1) – processed in accordance with the UK GDPR/Part 2 of the DPA 2018. Home Office processing of special category data for law enforcement purposes is not covered in this document. Processing for law enforcement purposes is carried out by the HO in its capacity as a competent authority and falls under Part 3 of the DPA 2018.

The purpose of this policy is to explain:

1. Home Office procedures that are in place to secure compliance with the UK GDPR data protection principles when relying on 'substantial public interest' conditions in Part 2 of Schedule 1 DPA 2018, or for the purposes of 'employment, social security or social protection' in accordance with Part 1 of Schedule 1 DPA 2018 when processing special category data;
2. Home Office retention and erasure policies concerning the processing of special categories of data on grounds of substantial public interest or for the purposes of employment, including an indication of how long such data is to be kept.

Legal obligation

Special categories of personal data

Article 9(1) of the UK GDPR creates a general prohibition on the processing of special categories of personal data. This prohibition is disapplied if a condition in Article 9(2) is met in relation to the proposed processing. Article 9(4) allows the conditions in Article 9(2) to be subject to further requirements, in particular it is worth noting that in relation to– Article 9(2)(b), 'necessary for the purposes of performing or exercising obligations or rights in connection with employment, social security or social protection', and Article 9(2)(g), 'necessary for reasons of substantial public interest' – these will only be met if the

controller also has an appropriate policy document in place (paragraphs 1 and 5 of Schedule 1 DPA).

Home Office staff must therefore have regard to this policy when carrying out processing of special category data on behalf of the Department, when it is acting in its capacity as controller.

The Home Office has considered whether in the course of its official functions there are additional types of data that might be treated as special category data although not prescribed under Article 9(1) UK GDPR or Part 2 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 data. Where other data (such as nationality data in some specific cases) is processed in such a way as to reveal characteristics amounting to special category data (e.g. of race and/or ethnicity) the other data will, as appropriate, be processed subject to the enhanced safeguards for sensitive data.

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 special category data (even when it is not legally necessary or required to be processed as such).

Criminal convictions data

Article 10 of the UK GDPR provides that the processing of personal data about criminal offences and convictions can only be carried out either where it is done under the 'control of official authority' or where the processing is authorised under Union or Member State law providing appropriate safeguards. Section 10(4-5) of the DPA 2018 sets out the requirements for the processing of such data where it is done other than under the control of official authority (i.e. it is only permitted if it meets an additional condition set out in Part 1, 2 or 3 of Schedule 1 DPA 2018).

The HO's processing of criminal convictions data as a controller is done under the control of official authority in accordance with Article 10.

2. Conditions for processing Special Category data

The lawfulness of the Home Office's processing is in most cases derived from its official functions as a government department, and its corporate functions as an employer, and by ensuring that all such processing is necessary and proportionate to the identified purpose. Details of the HO's functions are set out in the department's Personal Information Charter.

When the Home Office processes special category data it does so in accordance with the requirements of Article 9 and 10 of the UK GDPR and Schedule 1 of the DPA 2018. The majority of the HO's processing of special category data is for the following permitted purposes in Article 9:

- 9(2)(b) 'employment';
- 9(2)(g) 'substantial public interest'

The HO is therefore required to have this Appropriate Policy Document in place, and to meet the additional conditions prescribed in schedule 1 DPA.

The HO may also occasionally process some special category data in accordance with other Article 9 conditions, such as:

- 9(2)(a) 'consent' – as a government department the HO will very rarely rely on consent as the basis for processing. When it does, the HO ensures that explicit and freely given consent for each special category data item is sought, that the data subject is informed they have the right to withdraw their consent at any time, and that processes are in place to easily facilitate the withdrawal of consent;
- 9(2)(c) 'vital interests' – the HO may rely on this condition under certain circumstances, such as where the processing is necessary to protect asylum seekers or others who may be in the care of the department;
- 9(2)(e) data 'made public by the data subject' – the HO may rely on this if, for example, it checks and further processes data in the public domain to confirm it aligns with a statement submitted in support of an application or claim etc;
- 9(2)(j) 'archiving purposes' – the HO relies upon this condition, for example, to transfer data to The National Archives and the Office of National Statistics for archival research purposes;
- 9(2)(f) 'for the establishment, exercise or defence of legal claims' – the HO may rely on this if, for example, it provides personal data to assist a third party (such as a vulnerable person or claimant against the HO) in relation to their legal claim, or is required to disclose material to a claimant, and where such processing is not strictly in support of the HO's own public tasks;
- 9(2)(h) for the purposes of health – the HO may rely on this, for example, when processing Occupational Health referrals.

These other Article 9 conditions do not require an APD to be in place.

3. Compliance with data protection principles

a) Accountability principle

The Home Office has put in place appropriate technical and organisational measures to meet the requirements of accountability [as required by Article 5(2)]. 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, whose responsibilities include (among other things):
    - providing leadership in raising the profile of data protection compliance across the Home Office;
    - monitoring compliance with data protection legislation, including the assignment of responsibilities, and overseeing departmental training of staff involved in processing operations;
    - the design and implementation of a planned programme of risk-based assurance reviews/audits to test departmental compliance with privacy and UK data protection legislation, and recommend ways of reducing any identified risks;
    - investigating complaints from data subjects and other stakeholders about the department's processing of personal data;
    - acting as the department's main point of contact with the Information Commissioner's Office (ICO) on issues related to the department's processing of personal data.
- a direct reporting line from the DPO to our highest management levels, including to the Accounting Officer and the Audit and Risk Assurance Committee (ARAC) on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control in relation to its data protection obligations;
- 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 when and how a Data Protection Impact Assessment (DPIA) should be completed; and how to ensure new projects, applications or systems meet the legislative, technical and organisational 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 HR, Immigration 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, including reviewing the highest risk data protection impact assessments (DPIAs) referred to it by the DPO or business owner;

- 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 ensuring 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 technical 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). The HO may also produce subject-specific APDs as a supplement to this document if the processing of special category data requires very specific handling or in order to cater for very specific needs of the data subjects.

b) Principle 1 - 'lawfulness, fairness and transparency'

Lawfulness

As noted above, the lawful basis for the Home Office's processing is in most cases derived from its official functions as a government department, and its corporate functions as an employer, and by ensuring all processing is fair, necessary and proportionate to the identified purpose (see 'data minimisation' below) and applicable legal basis.

When processing special category data for the **employment purposes** the HO ensures the processing is **necessary** and **proportionate** to perform its duties and meet its

obligations to the data subject(s) (Part 1 para 1 of Schedule 1 to the DPA 18). This includes processing:

- for compliance with a **legal obligation** in connection with employment and personnel matters (e.g. reporting Trade Union Representative data);
- personal data concerning health in connection with the HO's rights and duties under employment law;
- data relating to criminal convictions in connection with recruitment, discipline or dismissal.

This list is not exhaustive - further details are recorded in the HO's Information Asset Register (IAR) and in our Personal Information Charter, Recruitment Privacy and Employee Lifecyle Privacy Information Notices.

The specific conditions under which data may be processed for reasons of **substantial public interest** are set out in paragraphs 6 to 28 of Schedule 1 of the DPA. As a government department, most of the HO's processing of special category data for a substantial public interest is in support of its public tasks or functions and in accordance with the purposes set out in para 6(2), Part 2, Schedule 1:

- exercise of a function conferred on a person by an enactment or rule of law; and/or
- exercise of a function of the Crown, a Minister of the Crown or a government department.

The HO meets the further requirements of Part 2 Schedule 1 by ensuring it only processes such data where it is in the substantial public interest and the processing is **necessary** and **proportionate** to perform the specific lawful functions of the Home Office. We do this in various ways, including by:

- providing all staff with training on how to comply with the privacy and data protection legislation - all members of staff and contractors working for the HO are required to complete the mandatory **Responsible for information e-learning**, which includes up-to-date information on how to comply with privacy and data protection legislation;
- providing and monitoring additional training for staff involved in processing operations, including training on assessing necessity and proportionality:
    - further privacy and data protection e-learning courses are available via the HO's online learning portal (Metis Learn) for all staff to improve their data protection awareness and understanding;
    - tailored training and advice is also provided by the ODPO across the HO, and via the networks described in the above section on Accountability;
- providing more detailed subject-specific guidance on how to conduct case-by-case assessments of such processing where relevant - for example, the assessment of Mutual Legal Assistance (MLA) requests by the UKCA;

- using the DPIA process to ensure our collection and subsequent processing of data is appropriate;
- ensuring our DPPs are trained to provide advice on individual cases and processing activities including designing privacy into these processes as required;
- ensuring our IAOs are trained to fulfil their responsibilities; and
- taking the further steps set out in the 'data minimisation' section below.

The HO may, on occasion, rely on other conditions in Schedule 1, such as:

- para 8, 'Equality of opportunity or treatment' to ensure compliance with our obligations under legislation such as the Equality Act 2010 and Sex Discrimination Act 1970; or,
- para 10, 'preventing or detecting unlawful acts', if providing information to the police or other law enforcement bodies;
- para 18, 'Safeguarding of children and of individuals at risk', for example, if any of our safeguarding teams identify an at risk individual for referral to social services, a GP, or other relevant professional;
- para 24, 'Providing information to elected representatives' such as Members of Parliament in response to a data subjects requests for assistance.

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 maintained in accordance with Article 30 GDPR, and in its IAR.

Fairness and Transparency

Detailed information about how the Home Office uses personal data, including special category data, is published in the Home Office's Personal Information Charter on GOV.UK and its privacy information notices, such as the following examples:

- Borders, immigration and citizenship privacy information notice
- HM Passport Office privacy information notice
- Passenger locator form privacy information notice
- Recruitment Privacy Information Notice
- Employee Lifecyle Privacy Information Notice

Further information about what the HO does as a Government Department is also published on the HO website.

The Home Office's 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, visa application forms explain information may be shared with sponsors linked to the application.

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 - 'purpose limitation'

The Home Office only processes personal data when permitted to do so by law. Personal data is collected for specific, explicit and legitimate purposes -- such as for issuing passports and visas, securing the UK border and controlling immigration – and will not be further processed for reasons that are incompatible with the purposes for which the data was originally collected for the Home Office, unless that processing is permitted by law. Where the Home Office obtains data on a basis that imposes specific purpose (or other) limitations, then such data will not be processed in any way that is incompatible with those further specific limitations.

Privacy information notices are used to inform individuals of the legitimate purposes for which data will be processed, and the HO uses the networks and processes outlined above to ensure it meets these requirements.

b) Principle 3 - 'data minimisation'

The Home Office will in each case collect only the personal data that is needed for the particular purpose/purposes 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 - 'accuracy'

Providing complete and accurate information is required when applying for a passport or visa or accessing other HO services. Data subjects are required to notify the Home Office of relevant changes in their circumstances, such as changes of address or marital status. Details of how to do this will be provided at the point of data collection and/or via the HO website, and its privacy information notices. Home Office IT systems are designed to allow for changes to personal data to be made, or for data to be erased where appropriate to do so.

If a change is reported by a data subject to one service or part of the Home Office, whenever possible this is also used to update other services, both to improve accuracy and avoid the data subject having to report the same information multiple times. Where permitted by law, and when it is reasonable and proportionate to do so, Home Office processes may include cross-checking information provided by a data subject with other organisations – for example local authorities or sponsors, to ensure accuracy.

If the HO decides not to either erase or rectify the data, for example because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision and, unless an exemption applies, inform the data subject of this outcome.

d) Principle 5 - 'storage limitation'

The Home Office has a corporate retention schedule in place which is published online in its retention and disposal standards page and separate retention policies for its operational records/casefiles based on relevant legislation and the period for which information is needed for a justified business process. Also some types of information have specific policies – for example, where information relates to court proceedings or contractual arrangements. All of these policies are set in line with HO guidance on 'How to Determine Retention and Disposal Schedules' produced by the Knowledge and Information Unit. They can be accessed via the above links, and relevant policies are also published in the Home Office's Privacy Information Notices, some of which can be accessed via our Personal Information Charter.

All special category data processed by the Home Office for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in these policies. HO retention schedules are reviewed regularly and updated when necessary.

Sensitive data processed on the basis of consent is also 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.

e) Principle 6 - 'integrity and confidentiality'

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 for example 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 to the Information Commissioner on request, in accordance with s42(3)(c) of the DPA.

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