Home Office

Data Protection Legislation

Immigration Exemption Policy Document (DRAFT): Use of the immigration exemption under Article 23 of the UK GDPR and Schedule 2 of the DPA 2018

Data and Identity Directorate

v 0.1, December 2021

1. Introduction

This document is the Immigration Exemption Policy Document (IEPD) for the Home Office and is specifically aimed at all staff. It sets out directional guidance on the operational implementation of the Immigration Control Provisions in the Data Protection Act 2018 (DPA) -- set out in Schedule 2, Part 1, para 4 -- commonly referred to as the 'immigration exemption' which will be used for ease of reference in this document. Any person who intends to use the immigration exemption must have regard to this policy document.
It explains how the limited restrictions to the provisions of the UK General Data Protection Regulations 2018 (UK GDPR) must be operationally applied – and for how long data rights might be exempted.

The immigration exemption in the DPA 2018 seeks to ensure that the Home Office is able to maintain the integrity of UK immigration controls, protect the public and the border. It is potentially available where full compliance with the usual data protection rights in respect of an individual data subject would be likely to prejudice:

- the maintenance of effective immigration control, or
- the investigation or detection of activities that would undermine the maintenance of effective immigration control.

(referred to in this IEPD as the "immigration purposes").

The provisions work within the framework of data protection principles set out in the UK GDPR (further detail is provided on these principles in Section 10). It is **not** a blanket exemption, and its use **must** be considered on a case by case basis. The sensitivity of information can change over time. So, an initial decision to refuse to release information should be reviewed if a later request is made and where circumstances have or may have changed.

The IEPD sets out the safeguards the Home Office has in place to protect any personal data if and when the immigration exemption is applied. It has been produced in accordance with Home Office obligations under UK data protection legislation so as to ensure that the exemption can only be used in a way that protects the public and affords adequate safeguards to the data subject.

The key topics that this guidance will cover are:

- The policies and processes for determining the extent to which the application of certain UK GDPR provisions would be likely to prejudice the immigration purposes;
- where it is determined that any of those provisions do not apply in relation to personal data processed for any of those purposes, preventing—
    - the abuse of that personal data, and
    - any access to, or transfer of, it otherwise than in accordance with the UK GDPR.
- Scope of the immigration exemption;

- When the immigration exemption should be used;
- What the prejudice test is including the rights and obligations that are affected;
- How a restriction may be applied;
- The rationale for applying the exemption;
- The need for it to be applied on an individual case by case basis;
- The time constraint on any such use; and
- Retention schedules[1].

[1] https://www.gov.uk/government/publications/home-office-retention-and-disposal-standards/what-to-keep-home-office-guide-to-managing-information

https://horizon.homeoffice.gov.uk/file/466961/download/how-to-determine-retention-and-disposal-schedules.docx

2. Scope

Any person considering applying the immigration exemption must have regard to the IEPD. The IEPD applies to all staff that perform immigration functions for the Home Office who have a role in the collection, processing, sharing and retention of any personal data collected for the purpose of maintaining effective immigration control. This includes all categories of personal information that relate to an identifiable individual, regardless of format, obtained by the Home Office from any source.

3. Legal obligations

Under paragraphs 4(1A) and (1B) of Schedule 2, the Secretary of State is required to have in place this IEPD, which:

- explains the Secretary of State's policies and processes for determining the extent to which the application of certain rights under the UK GDPR would be likely to prejudice any of the immigration purposes; and
- where it is determined that any of those provisions do not apply in relation to personal data processed for any of the immigration purposes, preventing—
    - the abuse of that personal data, and
    - any access to, or transfer of, it otherwise than in accordance with the UK GDPR.

Para 4A(1) of Schedule 2 to the DPA states that:

- the Secretary of State must determine the extent to which the application of the relevant UK GDPR provisions would be likely to prejudice any of the immigration purposes on a case by case basis and
- the Secretary of State must have regard, when making such a determination, to this IEPD.

Para 4A(2) of Schedule 2 states that the Secretary of State must also review this IEPD and keep it updated, and publish it, and any update to it, in such manner as the Secretary of State considers appropriate.

Para 4B of Schedule 2 states that where the Secretary of State determines in any particular case that the application of any of the relevant UK GDPR provisions would be likely to prejudice any of the immigration purposes, the Secretary of State must keep a record of that decision and inform the data subject. However, the Secretary of State is not required to inform the individual if doing so may be prejudicial to the immigration purposes.

4. When the immigration exemption should be used

The exemption is **only** applicable when data is being processed under the UK GDPR regime or the applied UK GDPR regime set out in Part 2 of the DPA. It therefore **cannot** be applied where processing is taking place under other parts of the DPA including the Law Enforcement processing regime which is covered in Part 3 of the DPA.

The immigration exemption is used to restrict certain data subject rights, for example when individuals make subject access requests to the Home Office to provide the personal data the Department holds on them. This can include special category and criminal convictions data (as they are described in Articles 9 and 10 of the UK GDPR).

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 Home Office, as a matter of policy, treats data concerning nationality as sensitive data.

Rights and obligations that may be disapplied or restricted under the immigration exemption

The immigration exemption does **NOT** apply to all the rights and obligations in the UK GDPR. It can only be used in respect of the following rights in the UK GDPR as follows:

- Information to be provided when personal data is collected from data subject (Article 13(1) to (3) of the UK GDPR);
- Information to be provided when personal data is collected other than from the data subject (Article 14(1) to (4) of the UK GDPR);
- Confirmation of how the data is being processed, access to the data and safeguards for third country transfers (Article 15(1) to (3) of the UK GDPR);
- The right to erasure of data (Article 17(1) and (2) of the UK GDPR);
- The right to restrict processing of data (Article 18(1) of the UK GDPR);
- The right to object to data processing (Article 21(1) of the UK GDPR);
- The general principles of processing data under Article 5 a-f of the UK GDPR.

These will be referred to as the “Restricted Rights” in this IEPD.

What the prejudice test is, including the rights and obligations that are affected

- Under Schedule 2, paragraph 4(1) of the DPA, the Restricted Rights may only be disapplied or restricted in situations where giving effect to those rights would be likely to **prejudice** either or both of the immigration purposes.

Therefore in order to disapply a Restricted Right, you must be able to demonstrate a reason why giving effect to that right in the normal way would cause the prejudice set out above, with particular reference to the right that you wish to restrict. In other words you cannot disapply **all** rights just because **one** right might fit the test. **It must be necessary and proportionate**.

5. How a restriction may be applied

Upon receiving information requests from a data subject or their appointed representative, decision makers should follow the following sequence of considerations:

- Are you satisfied as to the identity of the applicant for the data? Personal data should only be disclosed where you are satisfied that the applicant is the data subject, or has authorised the release of their personal data to a third party;
- Are there any grounds to believe that the release of the information requested would be likely to prejudice the maintenance of effective immigration control or the investigation or detection of activities that would undermine the maintenance of effective immigration control? If not, then the presumption is that the data requested must be released, unless other exemptions are applicable.
- If you have any outstanding concerns about fulfilling the request, and there are no other applicable caveats in the UK GDPR, only then should you consider if it is appropriate to apply the immigration exemption. The risk of prejudice to immigration control should be based on evidence. Examples might be:

    - If we receive a Subject Access Request (SAR) from an individual who is suspected to have committed an immigration offence, or their representative, and disclosure of certain personal data would be likely to prejudice the Home Office's ability to take any planned enforcement action, then the exemption would permit for disclosure of this data to be restricted until the cause for concern has ended;

    - If the data requested would reveal details of the Home Office security checks and systems used for the investigation of immigration offences, and it is believed that this would be likely to prejudice the effective operation of immigration controls, then the exemption would permit for disclosure of this data to be restricted; or

    - If the data requested reveals certain system sensitivities which could be exploited by potential immigration offenders, undermining the effective operation of immigration controls, then the exemption would permit for disclosure of this data to be restricted.

This sequence works on the assumption that each data request is a valid and eligible application, until it can be demonstrated otherwise and until all other considerations (as above) aside from the immigration provision have been tested.

Not all rights will be actioned by a SAR and the exemption applies to a range of rights and obligations which may not involve providing data to the data subject on request – for example it may apply where we receive new information from another department which relates to the data subject and where we would otherwise may have to notify the data subject under Article 14.

For example where we seek to carry out investigations concerning a data subject and receive data from a third party, where there is a risk of prejudice to immigration controls, then the need to inform that data subject of third party data sharing or similar actions may be exempted.

A similar approach to that set out above will be required – i.e. to identify the relevant rights and obligations, to establish whether there is a likelihood of the prejudice occurring, to check whether there are any other applicable caveats, and then to decide whether to apply the restricted.

6. The extent of application of the exemption

In instances where the application of the immigration provision appears to be justified, you must consider whether there are any elements that, notwithstanding the applicability of the exemption, might require a compliance with full data rights for the data subject or their representative. For example, in a SAR it may be that disclosing some of the personal data covered by the request would not have any prejudicial effect – in that case the non-prejudicial data should be disclosed. The fact that the immigration exemption applies to some of the data does not mean that all data within the scope of the request can be withheld.

Oversight comes from the Home Office Data Protection Officer (DPO) and externally from the Information Commissioners Office (ICO); all other rights of the data subject will be unaffected by any action taken under the immigration exemption and normal rules on disclosure will apply – for example in any appeal case – data held on the data subject must be released to the data subject to allow for a full and fair hearing.

With reference to the right to correct data redacted/restricted under the immigration exemption, no personal data is withheld or restricted that would prevent someone from establishing a legal defence or case and the normal rules of disclosure will apply.

Where there are other circumstances that may affect your decision, **you must** seek further advice. In the first instance please consult your business area Data Protection Practitioner (DPP) who will advise on escalation routes if necessary.

Business areas have appointed Data Protection Practitioners (DPPs) who will be there to help and advise but also provide oversight on operational matters. This should include self-auditing of your data, how it is collected, stored, processed, retained and destroyed.

7. The need for it to be applied on an individual case by case basis

The immigration exemption must always and can only be applied on a case-by-case basis and only for as long as is strictly necessary. Each case must be carefully considered to identify the extent to which adhering to the provisions of the UK GDPR listed above would be likely to prejudice:

- the maintenance of effective immigration control, or
- the investigation or detection of activities that would undermine the maintenance of effective immigration control.

Accordingly, if subsequent requests are made following the use of the exemption, if the likelihood of that prejudice no longer exists, then the restriction of the applicable UK GDPR rights and obligations must end and rights and obligations should be complied with as usual.

Before applying the immigration exemption, consideration must be given to whether the rights of the individual override the prejudice to immigration control. You must therefore apply the exemption in a way that is proportionate to the circumstances of the individual case. You must also document each instance when the immigration exemption is used. It is for the data controller to be able to evidence, if necessary, why a right (or rights) is to be exempted and to reinstate the right once the issue evidenced no longer satisfies the criteria for either (a) or (b) above.

8. The time constraint on any such use and safeguards in place to prevent unlawful access or transfer

A right can only be disapplied or restricted when the prejudice test is satisfied. If the situation changes over time (for example, because of new evidence) and giving effect to that right would no longer be likely to prejudice the maintenance of effective immigration control, then from that point onwards the relevant right must be given effect as usual.

Use of the immigration exemption should not be seen as a one off test but one of continual monitoring with the objective of restoring any right that has been restricted, as soon as the evidence that supported that restriction has been addressed.

Where there is a continuing operational need for restriction, to prevent the likely prejudice to immigration controls, then the restriction can remain in place.

When looking to rely on the exemption you must ensure that all security protocols are in place to prevent unlawful access. This should include role based access controls, only those that have a genuine need to access it should be allowed and able to do so. This should include password protected access to data sets and ensure that all logging

requirements are complied with and where permissions are needed that they are evidenced as having been obtained.

No redacted documents should be transferred, where the exemption has been applied. If questions on this arise, please consult your DPP.

The Home Office has a corporate retention schedule in place which is published online in its retention and disposal standards page. The use of the exemption does not affect any such storage periods.

9. Checklist for users to be assessed when applying an exemption.

When considering using the exemption you should consider all of the below issues to ensure you have allowed for the least restriction possible and have fully considered the case on its individual merits:

- The use of the exemption must be necessary and proportionate in each case and takes into account the individual circumstances of the data subject;
- It should only be used where there is a risk to immigration matters and other relevant restrictions should be considered if they are more appropriate;
- Use of the exemption should not be done to restrict all rights, but must be targeted at a specific right which evidences where the likely prejudice has been identified.
- This means there should be a rebuttable assumption to inform the data subject of the use of the exemption and only not do so where it would be prejudicial to the immigration purposes;
- Always have regard to our Public Sector Equality duty and the potential need for reasonable adjustments for a person with a disability;
- Particular care should be employed when dealing with safeguarding issues of any child or vulnerable adult, a restriction should never be applied where its use could impact on such positive duties of care;
- You will need to identify and evidence what the risk is of prejudice to the immigration purposes and recognise that any restriction can only be applied where such prejudice still persists;
- The risk of prejudice must be a real one that is likely to cause the prejudice identified, it is not enough to think it might lead to such prejudice;
- Have full regard to the data protection principles as listed in Article 5 UK GDPR and ensure compliance where we need to;
- Where you consider that the immigration exemption does apply, keep a record of that decision and inform the data subject of that decision, unless informing them may be prejudicial to any of the immigration purposes in which case you should not inform them that the immigration exemption has been applied;
- Review any decision when new information is made available to ensure any restriction is only applied for as long as is necessary;

- If you remain unsure on any aspect regarding the exemption's use, then you must seek advice from your DPP in the first instance or policy leads.

10. Compliance with data protection principles

It is important to understand the data protection principles – they are at the centre of how we operate with respect to personal data. The default position is that a data subject has all the rights guaranteed in the DPA. That position can only be altered where the test laid down in the Act is satisfied and only for as long as that same test continues to have validity.

The immigration exemption in the DPA can be used to restrict the Restricted Rights. However, even when rights are being restricted under the exemption, we still need to be aware of and comply with the Data Protection Principles, except in those limited circumstances where the principles can be disapplied / restricted.

The Data Protection Principles broadly are that personal data:

- Shall be processed lawfully, fairly and in a transparent manner;
- Should be collected for specific and lawful purposes and not further processed in a manner incompatible with those purposes;
- Should be adequate, relevant and limited to what is necessary (data minimisation);
- Shall be accurate, kept up to date, and rectified or erased, if appropriate;
- Kept for no longer than is necessary, and
- Protected to ensure integrity and confidentiality.

For the full transcript see UK GDPR Article 5.

The Principles can be restricted/disapplied, where they correspond with one of the other rights that is being restricted as a result of the application of the immigration exemption in a particular case. For example, where we are restricting the right to access data under Article 15, the principle of fair and transparent processing would also be relevant – so the exemption allows us to disapply the principle of fair and transparent processing as well as Article 15 (as otherwise we could be in breach of this principle) but only in so far as that principle relates to Article 15.

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 Home Office'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 and Information 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;
- Home Office 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 Home Office systems.

Further information can also be found in our Data Protection Policy which sets out the ways in which the Home Office complies with data protection legislation (including integrating data protection by design and default). The Home Office 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

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.

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 Home Office'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 Home Office 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 Home Office 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 Home Office'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 Home Office, 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 Home Office 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 Home Office'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 in Borders, immigration and citizenship privacy information notice

Further information about what the Home Office does as a Government Department is also published on the Home Office 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 Home Office 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 Home Office 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 Home Office 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 Home Office 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 Home Office 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 Home Office 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 Home Office 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 Home Office 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. Home Office retention schedules are reviewed regularly and updated when necessary.

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 Home Office business, the Home Office 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.

11. Terms and definitions

- 'Data application', 'data request', 'information application' and 'information request' are interchangeable in this guidance. They all relate to the exercise of a specific right under the relevant provisions of the UK GDPR;

- 'Data subject' means the individual to whom any particular personal data relate;

- ‘Data controller’ means the person, public authority, agency or other body which, determines the purposes and means of the processing of personal data;

- ‘Data processor’ means the person, public authority, agency or other body which processes personal data on behalf of the controller;

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

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

12. 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 July 2022) and yearly thereafter.

Effective Date	31/01/2022
Last Revision Date	N/A
Next Revision Date	31/07/2022
Approved by	Director, Data & Identity Directorate
Audience	All Staff