GC 2023/0008

GDPR and LED Implementing Regulations 2018

Immigration Exemption Policy Document:

Use of the immigration exemption under paragraph 6A of Schedule 9 to the GDPR and LED Implementing Regulations 2018

Contents

Part 1: Introduction

This Immigration Exemption Policy Document (IEPD) explains how the limited restrictions to the Data Protection (Application of GDPR) Order 2018[1] (the "applied GDPR") permitted under the immigration exemption must be operationally applied; and for how long data rights might be exempted.

The immigration exemption in the GDPR and LED Implementing Regulations 2018[2] (the "Implementing Regulations") is designed to ensure that the Immigration Service can maintain the integrity of Isle of Man immigration controls, as well as 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 "immigration purposes", which are—

- the maintenance of effective immigration control; and
- the investigation or detection of activities that would undermine the maintenance of effective immigration control

The provisions work within the framework of data protection principles set out in the applied GDPR. 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. An initial decision to refuse to release information should therefore be reviewed if a later request is made.

The IEPD sets out the safeguards the Immigration Service has in place to protect personal data if the immigration exemption is applied. It has been produced in accordance with obligations under Isle of Man data protection legislation so as to ensure that the immigration exemption is only used where necessary while affording adequate safeguards to the data subject.

The key topics covered by this guidance are—

- The policies and processes for determining the extent to which the application of certain applied 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;
    - any access to, or transfer of, it otherwise than in accordance with the applied GDPR;
- scope of the immigration exemption;
- when the immigration exemption may 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.

[1] See the Data Protection (Application of GDPR) Order 2018 in the collapsible column underneath the "Data Protection Act 2018".
[2] See the GDPR and LED Implementing Regulations 2018 in the collapsible column underneath the "Data Protection Act 2018".

Part 2: Scope

Any person considering applying the immigration exemption must have regard to this IEPD. The IEPD applies to all staff that perform immigration functions for the Immigration Service 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 Immigration Service from any source.

Part 3: Legal Obligations

Under paragraphs 6A(2) and (3) of Schedule 9 to the Implementing Regulations, the Minister is required to have in place an IEPD, which:

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

Para 6B(1) of Schedule 9 to the Implementing Regulations states that:

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

Paragraph 6B(2) of Schedule 9 to the Implementing Regulations states that the Minister must also review this IEPD and keep it updated, and publish it and any update to it, in such manner as the Minister considers appropriate.

Paragraph 6B of Schedule 9 to the Implementing Regulations states that where the Minister determines in any particular case that the application of any of the relevant applied GDPR provisions would be likely to prejudice any of the immigration purposes, the Minister must keep a record of that decision and inform the data subject. However, the Minister is not required to inform the individual if doing so may be prejudicial to the immigration purposes.

Part 4: When the immigration exemption should be used

The immigration exemption is only applicable when data is being processed under the Island's GDPR regime. It therefore cannot be applied where processing is taking place under other parts of data protection legislation including the Law Enforcement Directive.

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

The Immigration Service 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) or any other provisions of the applied GDPR.

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 applied GDPR. It can only be used in respect of the following rights under applied GDPR—

- information to be provided when personal data is collected from data subject (Article 13(1) to (3) of the applied GDPR);
- information to be provided when personal data is collected other than from the data subject (Article 14(1) to (4) of the applied 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 applied GDPR);
- the right to erasure of data (Article 17(1) and (2) of the applied GDPR);
- the right to restrict processing of data (Article 18(1) of the applied GDPR);
- the right to object to data processing (Article 21(1) of the applied GDPR);
- the general principles of processing data under Article 5(1)(a) to (f) of the applied 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

In accordance with paragraph 6A(1) of Schedule 9 to the Implementing Regulations, 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.

Part 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 applied 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 Immigration Service's ability to take any planned enforcement action, then the immigration exemption would permit for disclosure of this data to be restricted;
- if the data requested would reveal details of the Immigration Service's 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 immigration exemption would permit for disclosure of this data to be restricted;
- 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 immigration 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. The immigration 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 may otherwise have to notify the data subject under Article 14 of the applied GDPR.

For example, there may be situations where, as part of an investigation into a data subject, the Immigration Service receives 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.

Part 6: The extent of the immigration exemption

In instances where the application of the immigration provision appears to be justified, consideration must be given to whether there are any elements that, notwithstanding the applicability of the immigration 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 Treasury 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 DPO who will advise on escalation routes if necessary.

The DPO 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.

Part 7: The need for a restriction to be applied on an individual case by case basis

The immigration exemption 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 applied 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 immigration exemption, the likelihood of prejudice to immigration control must be re-examined to determine if it remains appropriate to apply the immigration exemption.

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 immigration 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 has been exempted.

Part 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.

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 immigration exemption you must ensure that all security protocols are in place to prevent unlawful access. This should include role-based access controls so only those that have a genuine need to access the data are allowed to do so. This should include password protected access to data sets, ensuring that all logging requirements are complied with and where permissions are needed that they are evidenced as having been obtained.

No redacted information should be transferred if the immigration exemption has been applied. If questions on this arise, please consult your DPO.

The Immigration Service has internal retention policies in place and the use of the immigration exemption does not affect any such retention periods.

It is important to note that the Immigration Exemption cannot be used to withhold any personal data where an individual is establishing a legal case or where the courts are acting in their judicial capacity. When applying the immigration exemption, care must be given to ensure compliance with human rights obligations.

Part 9: Checklist for users to be assessed when determining the extent to which the application of the Restricted Rights would be likely to prejudice the immigration purposes

When considering using the immigration 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 immigration 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 likelihood of prejudice to the immigration purposes;
- use of the immigration exemption should not be done to restrict all rights, but must be limited to only those rights for which likely prejudice has been identified and evidenced;
- this means there should be a rebuttable assumption to inform the data subject of the use of the immigration exemption and only not do so where it would be prejudicial to the immigration purposes;
- always have regard to the potential need for reasonable adjustments for a person with a disability;
- the best interests of a child, whether that child is the applicant or a dependant of the data subject, must be taken into account as a primary, although not the only, consideration in considering the application of the immigration exemption. 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 of the applied GDPR and ensure compliance where we need to;
- where you consider that the immigration exemption does apply, keep a record of that decision and the reasons for it. The data subject should be informed of that decision, unless informing them may be prejudicial to any of the immigration purposes;
- review any decision when the data subject subsequently seeks to exercise their data rights again, taking into account all available and relevant information;
- if you remain unsure on any aspect regarding the immigration exemption's use, then you must seek advice from your DPO in the first instance or policy leads.

Part 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 applied GDPR. 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 Implementing Regulations can be used to restrict the restricted rights. However, even when rights are being restricted under the immigration 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 are set out in full in Article 5 of the applied GDPR, but broadly set out 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;
- protected to ensure integrity and confidentiality.

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 immigration 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.

Accountability principle

The Treasury and Immigration Service has put in place appropriate organisational measures to meet the requirements of accountability, as required by Article 5(2) of the applied GDPR. These include—

- the appointment of a DPO who has a key assurance, compliance and advisory role on data protection matters within the Treasury;
- the development and regular review of a privacy notice[3], setting out how personal data provided may be processed;

[3] The privacy notice is available on the immigration home page in the "Downloadable Documents" box.

Principle 1: 'lawfulness, fairness and transparency'

The legal basis for the processing of your data will, in most cases, be Article 6(1)(e) of the (GDPR), namely that the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The specific conditions under which data may be processed for reasons of substantial public interest are set out in Schedule 2 of the Implementing Regulations. Most of the processing by the Immigration Service 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 Schedule 2, para 6(2)—

- the administration of justice;
- the exercise of a function of Tynwald and its branches;
- the exercise of a function conferred on a person by an enactment;
- the exercise of a function of the Crown, a Department or a Statutory Board

The Immigration Service meets the further requirements of Schedule 2 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 Immigration Service. 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 working for the Immigration Service are required to complete the mandatory data protection training, which includes up-to-date information on how to comply with privacy and data protection legislation;
- using the Data Processing Impact Assessment ("DPIA") process to ensure our collection and subsequent processing of data is appropriate;
- taking the further steps set out in the 'Principle 3: data minimisation' section below.

The Immigration Service may, on occasion, relay on other conditions in Schedule 2, such as—

- paragraph 8, preventing or detecting unlawful acts;
- paragraph 22, safeguarding of children and of natural persons at risk;

Principle 2: 'purpose limitation'

The Immigration Service 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 visas, securing the Isle of Man 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 by the Immigration Service, unless that processing is permitted by law. Where the Immigration Service 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.

Principle 3: 'data minimisation'

The Immigration Service 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. The Immigration Service has bespoke application forms or digital services 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: 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.

Where processing is for research and analysis purposes, wherever possible this is done using anonymised or de-identified/pseudonymised data sets.

Principle 4: 'accuracy'

Providing complete and accurate information is required when applying for a visa. Data subjects are required to notify the Immigration Service of relevant changes in their circumstances, where relevant for their bespoke visa, such as a change in employment circumstances, for the holder of a work visa.

Details of how to do this will be provided at the point of data collection and/or via the Immigration Service website, and its privacy information notices. Immigration Service 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.

Where permitted by law, and when it is reasonable and proportionate to do so, Immigration Service processes may include cross-checking information provided by a data subject with other organisations to ensure accuracy.

If the Immigration Service 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 immigration exemption applies, inform the data subject of this outcome.

Principle 5: 'storage limitation'

The Immigration Service has an internal retention policy 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.

All special category data processed by the Immigration Service for the purpose of substantial public interest is, unless retained longer for archiving purposes, retained in accordance with these internal retention policies.

Principle 6: 'Integrity and confidentiality'

Relevant Immigration Service IT systems are designed to ensure to the greatest extent possible personal data cannot be corrupted when it enters or is processed within them.

All staff handling Immigration Service or using an official system must have the appropriate security clearance.

Monitoring, review and version control

This Government Circular 2023/0008 revokes and replaces Government Circular 2023/0001

The Immigration Service will formally review this document not less than 6 months after its initial introduction and keep under regular review thereafter.

Effective date of this version: 16 January 2024
Last revision: 16 January 2024
Next revision date: 16 January 2025

Table of versions of this document

Document version number	In place
Immigration Exemption Policy Document: version 1	9 May 2023
Immigration Exemption Policy Document: version 2	16 January 2024