

Data Protection Impact Assessment (DPIA) Template

URN 77.19 (Updated)

Proposal/ Project/Activity title	Immigration Enforcement (IE) Data & Innovation
Information Asset Owner(s)	

Version 1.23

Data Protection Impact Assessment (DPIA) Template

Document Control

	Name	Job Title	Date
DPIA Drafted by		HEO Business Rules	30/10/2023
Reviewed by		G6 Programme Manager	30/10/2023
Lead DPP for business area	N/A		
Lead business owner /project manager/policy owner		IE Business Rules Programme Manager	30/10/2023

Version/Change history

Version	Date	Comments
Final 0.17	Jan 2021	Signed off by IAO and ODPO.
Draft 0.18	March 2021	First draft. Content transferred over to new template.
Draft 0.19	07/10/2021	Final version to G6 for comment.
Final 1.20	12/10/2021	Final version for IAO.
Final 1.21	11/11/2021	Final version for ODPO.
Draft 1.22	15/06/2022	Sent to IAO for clearance
Final 1.22	20/09/2022	Final version for ODPO.
Draft 1.23	09/02/2023	Review and sent to G6 for clearance
Final 1.23	17/03/2023	Final version for IAO.
Draft 1.24	30/10/2023	

Approved by (Information Asset Owner (IAO) or person acting on behalf of the IAO):

IAO approval is only required if Stage 2 of this template is completed. Project manager sign off is sufficient if the questions outlined in Stage 1 are answered in negative.

Name	Title	Date
	Strategic Services & Transformation (SST) Director & IAO	20/03/2023

Data Protection Impact Assessment (DPIA) Template

Contents

Data Protection Impact Assessment (DPIA) Template.....	1
Document Control.....	2
DPIA Stage 1	4
DPIA Stage 2.....	7
Section 1: Background and contacts	7
Section 2: Personal Data.....	9
Section 3: Purpose of the Processing.....	15
Section 4: Processing activity	18
Section 5: Risks of the Processing	20
Section 6: Data Sharing/Third party processing	21
Section 7: International transfers	23
Section 8: Referral to ODPO	25
Section 9: Referral to Data Board.....	26

Data Protection Impact Assessment (DPIA) Template

Guidance on when and how to complete this template is provided in the Data Protection Impact Assessment (DPIA) Guidance on Horizon – **this guidance should be read before completing the DPIA.**

DPIA Stage 1

Summary of the processing

1. Does the proposal/project/activity involve the processing¹ of personal data, or is new legislation which relates to the processing of personal data being considered?²

☒ Yes

☐ No

If the answer to this question is 'No', then the rest of the form does not need to be completed. If the answer is 'Yes', please continue.

2. Does the proposal/project/activity involve any of the following?

- a new way of processing personal data
- the use of a new form of technology for a new or existing process
- new legislation which relates to the processing of personal data being considered
- substantial changes to an existing project/programme/processes involving personal data, which would include a significant increase in the volume or type (category) of data being processed

☒ Yes

☐ No

If the answer to this question is 'No', then the rest of the form does not need to be completed. If the answer is 'Yes', please continue.

3. What is the purpose of the processing? Provide a brief (up to 100 words) description of the processing activity e.g. sharing with a third party; storing data in a new way; automating a data processing activity; developing a new policy that requires new legislation or amendments to existing legislation etc.)

[NB: this question is repeated at 3.1 at which point you can add more detail/background.]

¹ In relation to personal data, means any operation or set of operations which is performed on personal data or on sets of personal data (whether or not by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).

² Data protection legislation applies to 'personal data' which is defined as any information which relates to a living identifiable person who can be directly or indirectly identified by reference to an identifier. The definition is broad and includes a range of items, such as name, identification number, location data, or on-line identifier etc.

Data Protection Impact Assessment (DPIA) Template

The IEBR Programme will enable the IE workforce by identifying cases, triaging them, and then recommending them as suitable for a particular intervention or service in a consistent, holistic way. This will be delivered via a digital tool called IPIC (Identify & Prioritise Immigration Cases).

The TRAM and Define data sets provide data for IPIC but will also be used for analytical purposes.

Screening questions

4. Does the processing activity include the evaluation or scoring of any of the following?

- profiling and predicting (especially from “aspects concerning the data subject's performance at work”)
- economic situation
- health
- personal preferences or interests
- reliability or behaviour
- location or movements.

☐ Yes

☒ No

5. Does the processing activity include automated decision-making with legal or similar significant effect? i.e. processing that is intended to take decisions about data subjects which will produce “legal effects concerning the natural person” or which could “significantly affect the natural person”.

☐ Yes

☒ No

6. Does the processing activity involve systematic monitoring? i.e. processing used to observe, monitor or control data subjects, including data collected through networks or “a systematic monitoring of a publicly accessible area” e.g. CCTV.

☒ Yes

☐ No

7. Does the processing activity involve mostly sensitive personal data? This includes special categories of personal data, data about criminal convictions or offences, or personal data with the security marking of Secret or Top Secret.

☒ Yes

☐ No

Data Protection Impact Assessment (DPIA) Template

- 8. Does the processing activity involve data processed on a large scale?** If sharing with a third party external to the Home Office large scale is defined as 1,000 plus pieces of personal data in a single transaction or in multiple transactions over a cumulative 12 month period.

☒ Yes

☐ No

- 9. Does the processing activity involve matching or combining datasets that are being processed for different purposes?** e.g. data originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject. *NB:* This does not include matching or combining datasets from different IT systems that are processed for the same purpose and legal basis e.g. CID and CRS.

☐ Yes

☒ No

- 10. Does the processing activity involve mostly data concerning vulnerable data subjects or children?**

☐ Yes

☒ No

- 11. Does the processing activity involve the innovative use or application of new technological or organisational solutions?** e.g. combining use of fingerprints and facial recognition for improved physical access control, etc.

☐ Yes

☒ No

- 12. Will the processing activity in itself prevent data subjects from exercising a right (under Data Protection Legislation and the UK GDPR) or using a service (provided by) or a contract (with) the Department?**

☐ Yes

☒ No

- 13. Is the introduction of new legislation or a legal regulatory measure which relates to the processing of personal data being considered?**

NB: If yes, this may require consultation with the Information Commissioner.

☐ Yes

☒ No

If you have answered 'yes' to more than one of the above screening questions (Q 3 to 12), a DPIA must be completed. If you have answered 'no' to each of the screening questions but feel the planned policy/process/activity is significant, or carries reputational or political risk, you should complete the full DPIA. If you are not sure whether a DPIA should be completed, please consult the Office of the Data Protection Officer (ODPO).

If you have completed Stage 1 and do not need to complete Stage 2, send your Stage 1 assessment to the ODPO.

Data Protection Impact Assessment (DPIA) Template

DPIA Stage 2

Section 1: Background and contacts

1.1 Proposal/Project/Activity title:

Immigration Enforcement (IE) Business Rules Programme (IEBR)

1.2 Information Asset title(s) (if applicable):

Define

TRAM – Triage & Manage

IPIC – Identify & Prioritise Immigration Cases

1.3 Information Asset Owner(s) (IAO):

Email:

Name:

Telephone Number:

Information Asset title: Define, TRAM and IPIC

Email:

Click or tap here to enter text.

Name:

Click or tap here to enter text.

Telephone Number:

Click or tap here to enter text.

Information Asset title:

Click or tap here to enter text.

Email:

Click or tap here to enter text.

Name:

Click or tap here to enter text.

Telephone Number:

Click or tap here to enter text.

Information Asset title:

Click or tap here to enter text.

1.4 Person completing DPIA on behalf of the IAO named at 1.3 above):

Email:

Name:

Telephone Number:

Business Unit/Team: Business Rules, Strategic Services
&Transformation (SST), Immigration Enforcement
Directorate

1.5 Date DPIA commenced:

01/03/2021

Data Protection Impact Assessment (DPIA) Template

1.6 Date processing activity to commence (if known):

NB: if the processing activity is already ongoing, please explain why the DPIA is being completed retrospectively.

The IE Business Rules Programme initiated back in 2016 and the 3 projects were tested before entering a live state. IPIC (the digital service) was piloted in October 2018 and has since been rolled out further across Immigration Enforcement (IE). Several versions of the DPIAs have been completed in line with changes to how the data is being processed, or when new services have been launched, such as the ISD Phase 2 service.

1.7 Information Asset Register reference (if applicable):

Define – [REDACTED]

TRAM – [REDACTED]

IPIC – [REDACTED]

1.8 DPIA version:

Version 1.23

1.9 Linked DPIAs NB: attach word versions, do not provide links.

[REDACTED]

[REDACTED]

[REDACTED]

1.10 DPIA proposed publication date (where applicable, and if known):

NB: Provide below information about whether the DPIA will be published in part or in full, and the reason why it will be published.

There is no intention to proactively publish this DPIA as the processing of data is not high risk, nor is it controversial and we have not sought input from the Information Commissioners Office (ICO); therefore, there is a limited public interest in its publication. However, we may publish later a summary of this and

Data Protection Impact Assessment (DPIA) Template

other DPIAs to aid transparency. We will also consider any request for publication under a Freedom of Information Act (FoIA) request or on advice received by the Office of the Data Protection Officer (ODPO) and/ or the ICO.

Section 2: Personal Data

NB: These questions relate to the personal data being processed in the processing activity described within this DPIA only. It is acknowledged that in many instances the personal data being processed will originate from other HO sources and therefore be subject to their own set of rules governing access, retention and disposal.

2.1 What personal data is being processed?

Name

Date of Birth

Gender

Nationality

Travel Document

Immigration references - HO Reference, Personal Identity reference

Contact Details – Phone Number, Email Address, Addresses

Travel Details

Immigration Case types and outcomes

Detention details

Return details

CID Special Conditions – including markers of potential vulnerability or health markers

Reporting Details

Barriers

Criminality including offences and multi-agency public protection arrangements

Associations

Electronic Monitoring Data

2.2 Which processing regime(s) applies: general processing regime (UK GDPR/Part 2 DPA), and/or law enforcement processing regime Part 3 DPA?

NB: this question is repeated at Q.3.1.a.

General processing (UK GDPR/Part 2 DPA) ☒

IEBR data is processed under general processing for immigration purposes only.

Law enforcement (Part 3 DPA) ☐

Data Protection Impact Assessment (DPIA) Template

2.3 Does the processing include any of the following special category, or criminal conviction data?

Criminal conviction data	<input checked="" type="checkbox"/>	Yes	<input type="checkbox"/> No
Race or ethnic origin (including nationality)	<input checked="" type="checkbox"/>	Yes	<input type="checkbox"/> No
Political opinions	<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/> No
Religious or philosophical beliefs	<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/> No
Trade union membership	<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/> No
Genetic data or biometric data for the purpose of uniquely identifying individuals	<input checked="" type="checkbox"/>	Yes	<input type="checkbox"/> No
Health	<input checked="" type="checkbox"/>	Yes	<input type="checkbox"/> No
Sexual orientation or details of the sex life of an individual	<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/> No

2.4 Does it include the processing of data relating to an individual aged 13 years or younger?

☒ Yes

☐ No

2.5 (If 'yes') What additional safeguards are necessary for this processing activity? If none, explain why.

No additional safeguards are required. All processing is undertaken within the secure HO network and we will use data and assurance mechanisms already in use on the HO systems.

2.6 Will data subjects be informed of the processing?

☐ Yes

☒ No

If 'yes' go to Q2.7 If no, explain why.

There is no requirement to specifically inform data subjects. All individuals will be informed their data may be used for certain purposes when they apply for an immigration service, this is done via our HO [Privacy Information Notice \(PIN\)](#) contained on some HO application forms and can be accessed on the Gov.uk website.

In cases when processing data on certain categories of individuals such as illegal migrants or a Foreign National Offenders (FNO), it may not be appropriate to notify them that their data is being processed. In these instances we may apply

Data Protection Impact Assessment (DPIA) Template

the exemptions set out in Schedule 2 Part 1 of the Data Protection Act 2018 if deemed appropriate.

2.7 (If 'yes') How will they be informed/ notified?

Click or tap here to enter text.

2.8. Which HO staff and/or external persons will have access to the data?

Data will only be available to HO staff using the Business Rules workflow tools TRAM (Triage and Manage) and IPIC (Identify and Prioritise Immigration Cases (IPIC), [REDACTED]

[REDACTED] staff processing the requests on behalf of the HO staff who have requested the data. Data from all three products will also be available to the SST users who require access to enable them to monitor trends and issues within the data.

Please note – All HO staff and contractors will be security cleared to the appropriate level, typically SC.

There are 3 levels of security clearance.

The level of clearance a new starter needs, depends on the nature of their role and how much they need access to.

The security levels are:

- 1. Counter Terrorism Check (CTC):** The minimum requirement for staff working at HO buildings.
- 2. Security Check (SC):** For staff that need regular, unsupervised access to Secret or occasional supervised access to Top Secret material or information.
- 3. Developed Vetting (DV):** For staff who need long-term, frequent, and unsupervised access to Top Secret material or information.

2.8a. How will access be controlled?

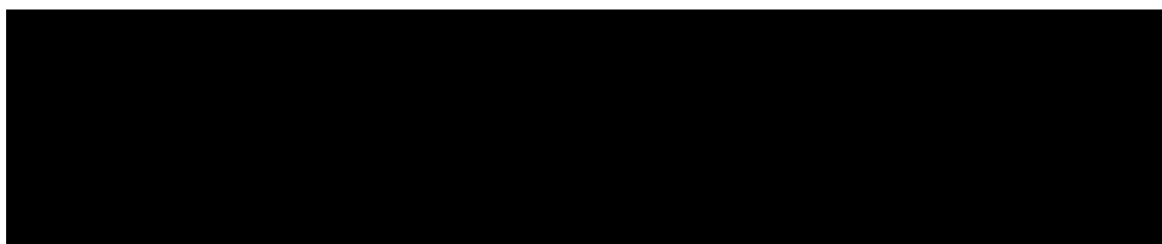
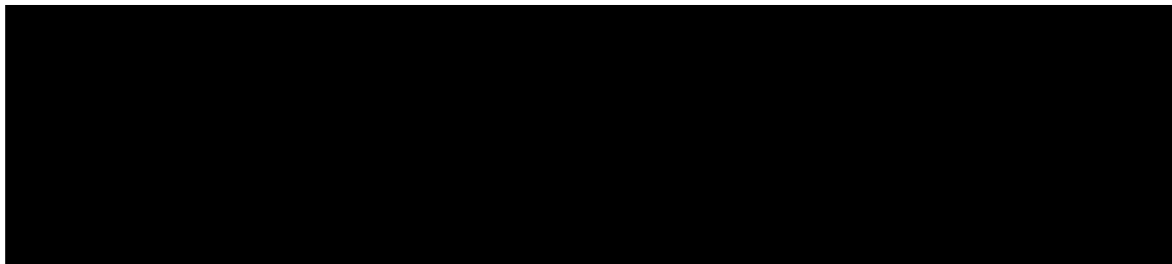
The business will restrict access in line with its own policies. DSA has a restricted working environment which is controlled internally via restricted access rights and password protection protocols.

The tactical process (for TRAM) involves use of the dataset *without* service level business rules applied. Access to the tactical (short-term) process is limited to those in the [REDACTED]

Data Protection Impact Assessment (DPIA) Template

TRAM has an access-management process in place and usage of the data is monitored and audited periodically by SST. For access to TRAM, users of the datasets will need to sign a declaration before access is granted.

The strategic process (for IPIC) involves use of the dataset with service level business rules applied to it.



To qualify for access to specified 'groups' the first part of the process is to submit an [REDACTED] request for access and the second stage is then granting those actual permissions in IPIC which is handled currently via the IPIC Admin access team (within the business). The permissions in IPIC ensure users only have access to the relevant service and interventions applicable to them / their business area.

At the second stage, the IPIC Admin team will ensure there is a requisite business need for access. Once a need is recognised, the relevant IPIC access will be provided.

2.9 Where will the data be stored?

For Define: password protected excel outputs stored in a secure Home Office shared drive. This folder is locked down and requires specific access to access. Define is also stored on the secure [REDACTED] platform and within [REDACTED]

For TRAM: stored in the secure DSA platform. For the tactical (short term) process TRAM is stored within the secure HO secure network for Poise users and in addition, secure folders with restricted access or via Sharepoint to named users with varying, controlled access levels depending on business need.

Data Protection Impact Assessment (DPIA) Template

For IPIC: The data will be hosted on [REDACTED] and relies on [REDACTED] security standards such as:

1. Simple Storage Services (S3): This provides cloud storage for various types of web development and through [REDACTED] and architecture approvals. [REDACTED] is a web service 'running in the cloud' and is designed to simplify the set-up, operation and scaling of a relational database for use in applications

2. Data at rest is encrypted and is in transit: This takes place over HTTPs (Hyper Text Transfer Protocols).

3. The Operational Acceptance Testing (OAT): This process is used to conduct operational readiness (pre-release) of a product, service, or system as part of a quality management system providing a security input into the architecture.

Platforms containing business data (including sensitive rulesets within IEBR) are strictly controlled as set out below:

1. SC Clearance is required
2. Regular audit of access and privileges by Business Rules team
3. [REDACTED] wide governance and monitoring processes apply

2.10 If the data is being stored electronically, does the storage system have the capacity to meet data subject rights (e.g. erasure, portability, suspension, rectification etc)?

☒ Yes

☐ No

If 'No' explain why not below and go to Q2.12

Click or tap here to enter text.

2.11 If 'Yes' explain how these requirements will be met.

All data held is derived from Home Office systems such as: the [REDACTED]

These systems have the means to meet these data subject rights where appropriate.

Data Protection Impact Assessment (DPIA) Template

IPIC has a memory function to enable navigation of historical cases for review purposes. This includes being able to historically review recommended interventions on a case, but all further personal data will be erased. See 2.14 on retention and erasure of data.

[2.12 For law enforcement processing only: If the data is being stored electronically, does the system have logging capability (as per s.62 DPA)?

☐ Yes

☐ No

If 'no', what action is being taken to ensure compliance with the logging requirement?]

Click or tap here to enter text.

[2.13 For law enforcement processing only: Will it be possible to easily distinguish between different categories of individuals (e.g. persons suspected of having committed an offence, victims, witnesses etc.) as well as between factual and non-factual information (as per s.38 DPA)? e.g. criminal record (fact); allegation (non-factual)

☐ Yes

☐ No

If 'no', what action is being taken to ensure compliance with s.38 DPA?]

Click or tap here to enter text.

2.14 What is the retention period for the data?

IEBR Retention Period Policy, notes that data will be stored for 5 years from when a decision is made in IPIC or data is processed for Define and TRAM.

2.15 How will data be deleted in line with the retention period and how will the deletion be monitored?

The HO has put in place the Moratorium of Destruction. This is a Statutory requirement, and it covers all information; however, this does not mean retention periods cannot be set. In IPIC, users will be able to go back and historically review what intervention was recommended for an individual, via an archive functionality, but not for any other data.

If personal data is required to be retained for longer than 5 years, decisions taken will be in line with official guidance to extend those periods and advice will be sought from the ODPO and the KIMU (Knowledge and Information Management Unit) to ensure Data Protection Legislation (DPL) compliance.

2.16 If physically moving/sharing/transferring data outside the Home Office, how will it be moved/shared?

N/A

Data Protection Impact Assessment (DPIA) Template

2.17 What security measures will be put in place to ensure the transfer is secure?

N/A

2.18 Is there any new/additional personal data being processed? This includes data obtained directly from the data subject or via a third party.

☐ Yes

☒ No

If 'yes', provide details below:

Click or tap here to enter text.

2.19 What is the Government Security Classification marking for the data?

OFFICIAL/OFFICIAL-SENSITIVE

☒

SECRET

☐

TOP SECRET

☐

2.20 Will your processing include the use of Cookies?

☐ Yes

☒ No

If 'no' go to section 3.

If 'yes', what sort of Cookies will be used? Tick the correct categories:

1) Essential (no consent required) ☐ Yes

☐ No

2) Analytical (consent required) ☐ Yes

☐ No

3) Third party (consent required) ☐ Yes

☐ No

2.20.a. If cookies fall into categories 2) & 3) how will you ensure data subjects are aware and can give active consent to the use of cookies?

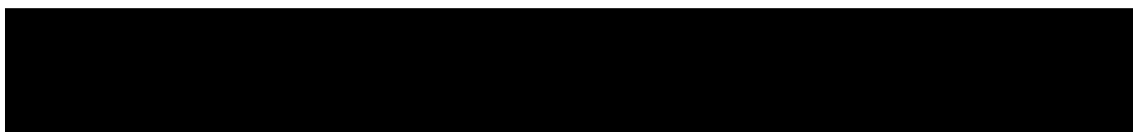
Click or tap here to enter text.

Section 3: Purpose of the Processing

3.1 What is the purpose of the processing? Provide a detailed description of the purpose for the processing activity. This section needs to provide an overview (in plain English) that can be read in isolation to understand the purpose and reasons for the processing activity.

The purpose is to create an easier, faster, and more effective way for Immigration Enforcement (IE) to identify, prioritise and coordinate the services/interventions needed to manage its caseload.

Data Protection Impact Assessment (DPIA) Template



TRAM enriches this data based on set criteria to inform triage options.

IPIC will apply a set of 'business rules' to this data and present cases to internal users in a prioritised way for consideration of an intervention/action.

This provides efficiencies and staff time can then be spent on value-added activity for example, undertaking the interventions recommended and not manually searching for the next case.

Data will also be used for analytical purposes.

3.1.a Which processing regime(s) applies: general processing regime (UK GDPR/Part 2 DPA), and/or law enforcement processing regime Part 3 DPA?

General processing (UK GDPR/Part 2 DPA) ☒ - go to question 3.2.a.

IEBR data is processed under general processing for immigration purposes only.

Law enforcement (Part 3 DPA) ☐ - go to question 3.2.b.

3.2.a. General processing only: What is the (UK GDPR Article 6) lawful basis for the processing? Choose an option from the list:

- | | |
|---|-------------------------------------|
| Consent | <input type="checkbox"/> |
| Contract | <input type="checkbox"/> |
| Legal obligation [see 3.3(a)] | <input type="checkbox"/> |
| Vital Interest | <input type="checkbox"/> |
| Performance of a public task [see 3.3(a)] | <input checked="" type="checkbox"/> |
| Legitimate Interest | <input type="checkbox"/> |

NB: Legitimate Interest cannot be relied upon by the Home Office for processing carried out in order to fulfil or support a public task.

[3.2.b. Law enforcement processing only: What is the (Part 3 DPA) lawful basis for the processing? Choose an option from the list:

- | | |
|---|--------------------------|
| Consent | <input type="checkbox"/> |
| Necessary for a law enforcement purpose | <input type="checkbox"/> |

3.3. If you have selected 'legal obligation' or 'performance of a public task' for general processing (for Q3.2.a), OR if the processing is for a law enforcement purpose

Data Protection Impact Assessment (DPIA) Template

Indicate below the legal basis and relevant legislation authorising the processing of the data:

Common law (list HO function/objective below) ☐

Click or tap here to enter text.

Royal Prerogative (HMPO only) ☐

Explicit statute/power (list statute below) ☐

Implied Statute power (list statute below) ☒

Based on Implied Statute power, information and data gathered for processing is in pursuant with core HO functions and the Immigration Act 1971 legislation

3.4.a. General processing only: If processing special category data or criminal convictions data (see Q2.2 above)

What is the (UK GDPR Article 9) condition for processing the special category data?

- | | |
|-------------------------------------|-------------------------------------|
| N/A | <input type="checkbox"/> |
| Consent | <input type="checkbox"/> |
| Vital Interests | <input type="checkbox"/> |
| In the public domain | <input type="checkbox"/> |
| (Exercising/defending) legal rights | <input type="checkbox"/> |
| Substantial Public Interest | <input checked="" type="checkbox"/> |
| Public healthcare | <input type="checkbox"/> |
| Archiving or Research | <input type="checkbox"/> |

[3.4.b. Law enforcement processing only: If processing sensitive data for a law enforcement purpose: **What is the (DPA Schedule 8) condition for the processing?**

- | | |
|--|--------------------------|
| Consent | <input type="checkbox"/> |
| Substantial public interest (for a statutory purpose) | <input type="checkbox"/> |
| Administration of justice | <input type="checkbox"/> |
| Vital Interests (of the subject or another) | <input type="checkbox"/> |
| Safeguarding children and individuals at risk | <input type="checkbox"/> |
| Data already in the public domain | <input type="checkbox"/> |
| Legal claims (seeking advice, legal proceedings, defending rights) | <input type="checkbox"/> |
| Judicial acts | <input type="checkbox"/> |
| Preventing fraud (working with anti-fraud organisations) | <input type="checkbox"/> |
| Archiving | <input type="checkbox"/> |

3.5 Is the purpose for processing the information described at 3.1 above the same as the original purpose for which it was obtained by the Department?

☒ Yes ☐ No

Data Protection Impact Assessment (DPIA) Template

If 'no', what was the original purpose and lawful basis?

Original purpose: Click or tap here to enter text.

Original Lawful basis:

Consent	<input type="checkbox"/>
Contract	<input type="checkbox"/>
Legal obligation	<input type="checkbox"/>
Vital Interest	<input type="checkbox"/>
Performance of public task	<input type="checkbox"/>
Legitimate Interest	<input type="checkbox"/>

Section 4: Processing activity

4.1 Is the processing replacing or enhancing an existing activity or system?

If so, please provide details of what that activity or system is and why the changes are required.

☒ Yes ☐ No

Previously existing data sets have been improved [REDACTED]
[REDACTED]
[REDACTED] provides a more holistic view of the whole population.

New processing brings consistency to decision making and restricts access based on use case.

If the answer is 'yes' go to 4.3

4.2 Is the processing a new activity? This description should include details (if appropriate) of what resources are needed to build the model? (e.g. FTEs, skills, software, external resource)

☐ Yes ☒ No

How many individual records or transactions will be processed (annually) as a result of this activity?

Click or tap here to enter text.

4.3 Is this a one-off activity, or will it be frequent and/or regular?

Regular activity

4.4 Does the processing directly relate to the processing of personal data that includes new legislative measures, or of a regulatory measure based on such legislative measures? If 'no', move onto 4.6.

☐ Yes ☒ No

Data Protection Impact Assessment (DPIA) Template

4.5 If the answer is yes, please explain what that processing activity is, including whether or not the HO will be accountable for the processing of personal data?

Click or tap here to enter text.

4.6 Does the processing activity involve another party? (This includes other internal HO Directorates, external HO parties, other controllers or processors).

☒ Yes

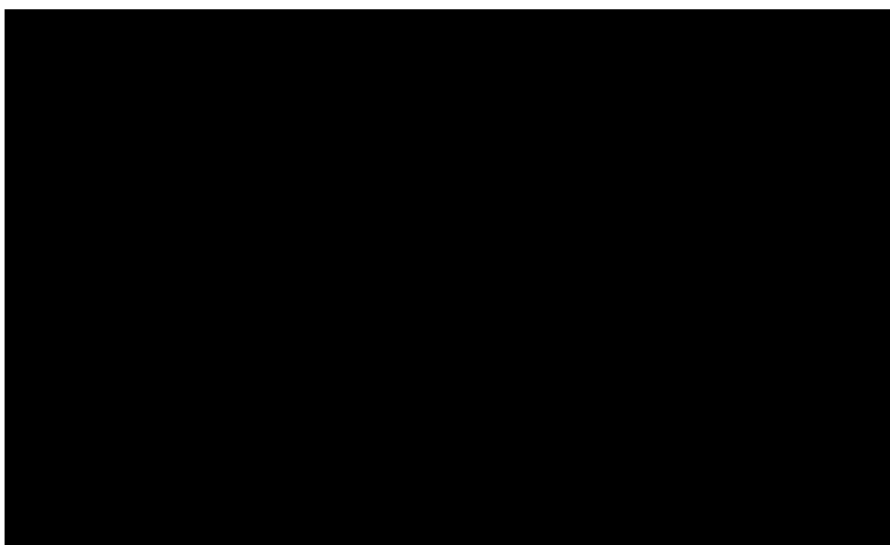
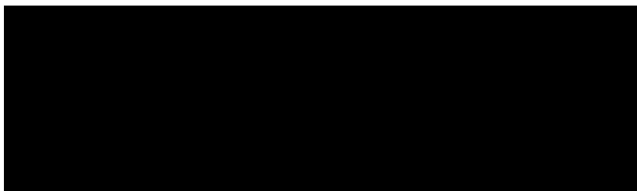
☐ No

If the answer is “No” go to 4.7.

4.6.a In what capacity is the other party acting?

- Part of the HO ☒
- Controller in their own right (i.e. non HO) ☐
- Joint Controller with the HO ☐
- Processor (public body) on behalf of the HO ☐
- Processor (non-public body) on behalf of the HO ☐

Provide details here:



4.7 Will any personal data be transferred outside the UK?

☐ Yes

☒ No

Data Protection Impact Assessment (DPIA) Template

If 'no' go to 4.8. If 'yes', provide brief details of the countries and complete Section 7.

Click or tap here to enter text.

4.8 Does the proposal involve profiling that could result in an outcome that produces legal effects or similarly significant affects on the individual?

☒ Yes

☐ No

If yes, provide details

[REDACTED]

[REDACTED] The scoring does not predict any future behaviour.

Business areas using IPIC will be recommended cases to take action on. For example, [REDACTED]

[REDACTED]

4.9 Does the proposal involve automated decision-making?

☐ Yes

☒ No

If yes, provide details

Click or tap here to enter text.

4.10 Does the processing involve the use of new technology?

☐ Yes

☒ No

If 'no', go to question 5.1.

4.11 If 'yes': Describe the new technology, including details of the supplier and technical support.

Click or tap here to enter text.

4.12 Are the views of impacted data subjects and/or their representatives being sought directly in relation to this processing activity?

☐ Yes

☒ No

a) If 'yes', explain how this is being achieved

b) If 'no', what is the justification for not seeking their views?

There is no need to seek the views of such individuals as the data is being processed for the same purposes as for which it was collected.

Section 5: Risks of the Processing

5.1 Are there any other known, or anticipated risks associated with the processing of personal data that have been identified by the project/

Data Protection Impact Assessment (DPIA) Template

programme/initiative owner, which have not been captured in this document?

☒ Yes

☐ No

If 'yes' provide details and go to question 5.2.

5.2 What steps have been taken to mitigate these risks?

All IEBR products display information derived from core HO systems. IPIC makes recommendations only for interventions. The final decision always rests with a user.

5.3 Can you demonstrate that the risks to the individuals are sufficiently balanced by the perceived public protection benefits?

☒ Yes

☐ No

If 'yes' provide details and go to question 5.4.

Ongoing review and testing mitigates the risk of individuals being incorrectly recommended for interventions, additionally any action to an individual's case rests with the end user who can reject any recommendation made. This is then used to further mitigate future referrals.

5.4 Are these risks included within a risk register?

☒ Yes

☐ No

Section 6: Data Sharing/Third party processing

Technical impact and viability

6.8 Which of the following reflects the data processing? The process may meet several of these descriptions.

Data extract: *Are you working through and assessing data to secure relevant information?*

☒ Yes

☐ No

Data matching: *Are you comparing several sets of data?*

☒ Yes

☐ No

Data reporting: *Are you processing data to produce accurate analysis?*

☒ Yes

☐ No

Data exchange/feed: *Are you sharing the data between programmes?*

☐ Yes

☒ No

Direct access: *Are you obtaining data by going directly to where it is physically located?*

☒ Yes

☐ No

Data Protection Impact Assessment (DPIA) Template

Other

☐ Yes

☒ No

a) If 'Other', please provide details

Click or tap here to enter text.

6.9 Has any analysis or feasibility testing been carried out? For example, through a proof of concept or pilot exercise?

☒ Yes

☐ No

If yes, provide details. If no, explain why it is not required.

The following testing has been completed to ensure rollout is workable:

1. Regression testing
2. Usability testing
3. Performance testing
4. Functional testing
5. Compatibility testing (on different browsers)
6. Accessibility testing
7. Security testing (the vulnerability scanner runs daily)

6.10 Confirm if:

development work is required to ensure systems are DP compliant?

☐ Yes

☒ No

If yes, provide details including time frame

Click or tap here to enter text.

Security Checklist

6.11 Given the security classification of the data, are you satisfied with the proposed security of the data processing/transfer arrangements detailed at 2.16 and 2.17 above?

☒ Yes

☐ No

6.12 Confirm you have read the associated guidance and, if necessary, consulted with HO Security and the relevant DDaT teams, including the Office of the CISO:

NB: If your processing activity involves any use of IT systems or physical documentation being sent outside of the Home Office to a non-governmental

Data Protection Impact Assessment (DPIA) Template

organisation, you *must* consult with the Office of the CISO, prior to your DPIA being submitted.

Yes, I have read the guidance and/or consulted with HO Security

6.13 If the answer is 'no': What needs to happen to ensure that adequate security arrangements are achieved?

Click or tap here to enter text.

6.14 Will the data be stored and be accessible off-site?

☒ Yes

☐ No

6.15 If 'yes', have you considered the security arrangements that need to be in place to prevent the data from being accidentally or deliberately compromised? Please provide details.

☒ Yes

☐ No

Section 7: International transfers

Only complete this section if you have answered yes to question 4.7.

7.1 Does the activity involve transferring data to a country outside of the UK (including Crown Dependencies, Overseas Territories and Sovereign Base Areas)?

☐ Yes

☒ No

If 'yes', specify the country. If 'no', go to Section 8.

Click or tap here to enter text.

7.2 Does the country have a positive adequacy decision?

☐ Yes

☐ No

a) If 'no', under what legal basis do you propose to transfer the data?

i) General processing only:

- Pursuant to a legally binding Treaty which contains appropriate safeguards for the rights of data subjects and includes effective legal remedies for those rights ☐
- Pursuant to an administrative (non-binding) arrangement approved by the UK Information Commissioner which recognises the rights of

Data Protection Impact Assessment (DPIA) Template

data subjects and includes binding rules providing effective legal remedies for those rights ☐

- On the basis that the transfer is necessary for 'important reasons of public interest' which are recognised in statute or common law (and set out in a non-binding MoU) ☐

ii) Law enforcement processing only:

- Pursuant to a legally binding Treaty which contains appropriate safeguards for the rights of data subjects and effective legal remedies for those rights ☐
- On the basis that the transfer is necessary for 'in individual cases for any of the law enforcement purposes' which are recognised in statute ☐

7.3 Does the HO already have a binding or non-binding data sharing arrangement with this country?

☐ Yes

☐ No

If no, skip 7.4 a)

a) If 'yes', does the arrangement cover the purpose(s) for which you need to share data?

☐ Yes

☐ No

If you have selected no for 7.3, you will need to consider reviewing the existing agreement to include the new processing activity

- I. If 'yes', does the arrangement recognise the rights of data subjects? Does it include effective legal remedies for data subjects' rights; or set out important reasons of public interest and how those reasons are legally founded; or set out why the transfer is necessary in individual cases for a law enforcement purpose?

☐ Yes

☐ No

If yes go to Section 8

- II. If 'no', how do you propose to document the terms of the understanding with the other country?


Click or tap here to enter text.

Note: You should consult guidance on Overseas Security and Justice Assistance (OSJA) to determine whether an assessment of human rights, International Humanitarian Law, political and reputational risks is required.

Data Protection Impact Assessment (DPIA) Template

Section 8: Referral to ODPO



8.1 Referral to the ODPO

Date referred to the ODPO	Reviewed by:	Date returned to the Author	Comments/ recommendations
12/11/2021		16/11/2021	Review complete; no further comment
Click or tap to enter a date.		Click or tap to enter a date.	

8.2 ODPO Review complete

NB: Any subsequent changes made to the DPIA by the business must be done clearly and transparently and in accordance with accepted version control convention. In the event of changes being made, earlier versions of this DPIA must be retained for auditing purposes and in-line with your agreed retention period.

If substantive changes are made to this DPIA, you must re-refer to the ODPO for a new review.

Date referred to the ODPO	Reviewed by	Date returned to the Author	Comments/recommendations
20/09/2022		22/09/2022	ODPO review is now complete with no further comment.
31/03/2023		05/04/2023	ODPO review is now complete with no further comment.

8.3 IAO sign-off

Date referred to IAO	Name of IAO or person signing on behalf of	Date returned to the Author	Comment (including approved to proceed Y/N)

Data Protection Impact Assessment (DPIA) Template

Click or tap to enter a date.		Click or tap to enter a date.	
-------------------------------	--	-------------------------------	--

Section 9: Referral to Data Board

This section is only required if one or more of the criteria for referral to the HO Data Board is met (see DPIA guidance). Referral to the HO Data Board will be completed by the ODPO after consultation with the business owner(s) listed in part 1 of this DPIA. [Guidance](#) is available on Horizon.

9.1 Criteria for referral to the HO Data Board:

Criteria	Met
ODPO have identified a risk that, in its opinion, requires escalation to the ICO (regardless of risk severity; guidance will be produced in due course once examples indicate how this might be revealed). The view of the Chair of the Data Board will be sought in advance of any such escalation.	
ODPO reason for referral if not one listed below: [ODPO insert detail]	
There is a significant impact, either qualitative and/or quantitative, upon individual rights, this may be one or more of the following:	
An instance where the proposal will not meet the Home Office obligations to meet the individual rights and protections of data subjects as defined in UK GDPR and DPA18.	
An instance where the proposal is likely to result in any person(s) individual privacy/data protection rights being compromised.	
A particular concern is identified having regard to the purpose, method of processing and location of processing that in combination warrants further escalation or consideration.	
High sensitivity – the nature of the personal data itself is so sensitive, even though the rest of the risks around processing were low. The board could be asked to scrutinize but equally the Board could determine that it did not need to do so.	
It is not possible to implement all recommended controls/mitigations. (Where controls and mitigations have been identified but result in a short period of heightened risk this would not warrant escalation).	
High likelihood of challenge or regulatory enforcement being brought, or a high likelihood of such a challenge or action being successful against the HO.	
Where a proposal resulted in advice that the processing would be unlawful, and the project has since revised (tweaked) the proposal this should be referred to the Board.	
Specific referral circumstances:	
Data processing has been promised by a Minister/ the Cabinet, but there are questions as to whether there is a sufficient legislative/technical /administrative framework in place to enable this.	
A decision has been made to prefer specific safeguards over others or a riskier approach.	

Data Protection Impact Assessment (DPIA) Template

An issue that is business critical emerges e.g. essential work to a business-critical system, that may mean that data subjects rights may not be met.	
Where processing is likely to attract significant controversy.	
Other: [add detail]	

9.2 Referred to the HO Data Board Secretariat

Date referred to the Secretariat	Referred to HO Data Board	Date of Data Board (if appropriate)	Date returned to the Author
Click or tap to enter a date.	Yes <input type="checkbox"/> No <input type="checkbox"/>	Click or tap to enter a date.	Click or tap to enter a date.
Recommendations/ findings/ comments from the HO Data Board/ Secretariat			

9.3 Action taken by the respective IAO(s)

Effective Date

Last Review Date

Next Review Date

Owner

Data and Identity Directorate (D&ID)

Approved by

DP Policies and Guidance Group, & Head of D& ID

Audience

All HO Staff