This publication was archived on 28 November 2023

This publication is no longer current and is not being updated.

Home Office

URN 287.20

The Data Protection Impact Assessment (DPIA) Template

Contents

The DPIA Process

The DPIA process is designed to ensure that the Department meets its statutory obligations under new Data Protection legislation (legislation). This process replaces the Privacy Impact

Assessment (PIA) and Data Sharing Toolkits (DST) processes. This process will assist the Department in the identification and management of data protection risks (and any other risks to fundamental rights and freedoms) caused by the processing of personal data and to achieve privacy by design.

This process is only engaged when a new project/ programme/ processing activity (including data sharing) that will involve the processing of personal data is planned. However, it should also be used where changes are being made to an existing project/ programme/ processing activity that may impact on the personal data being processed. In these cases, it is recommended that a DPIA is completed.

The DPIA process is made up of two stages. The first stage is the screening stage to identify whether or not personal data is being processed and if so, the severity of the risk involved in that processing. The second stage is a full impact assessment. Those completing this document will only proceed to the second stage if personal data is identified as being processed and the risk to that processing is assessed as high. Please refer to the Home Office DPIA guidance for more information including a guide on how to complete the template.

Who is responsible for the screening?

The Senior Responsible Owner for the project/ programme/ processing activity, or the Information Asset Owner for the data set is responsible for ensuring the screening is done, but the document can be completed by another officer with suitable knowledge of the proposed processing activity. It is important that all directly affected and interested parties are identified and consulted where appropriate during this process.

When does the screening take place?

It is mandatory to complete the screening for all proposed projects/ programmes/ activities that involve processing personal data; and where a substantial change is being made to existing projects/ programmes/ activities. The screening must be completed before the data processing commences unless, in exceptional circumstances such as where it is imperative to act quickly to protect the public, in which case an assessment can be completed retrospectively, but as soon as is practically possible.

Pre-screen check list

Depending on the type of data being processed and the activity that is being proposed, you may need to complete different parts of this document. Please complete this pre-screen checklist as you go along to aid completion of the document.

1. DPIA Stage 1

URN 287.20

1. Does the proposal/ project/ activity involve processing personal data? (Data Protection applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier).

   x Yes ☐ No

   ***NB:* If the answer to the previous question is no, then no further questions need to be answered and the form is complete. If the answer is yes, please continue.**

2. 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.

   x Yes ☐ No

3. Automated decision-making with legal or similar significant effect:
   Processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person".

   ☐ Yes x No

4. Systematic monitoring:
   Processing used to observe, monitor or control data subjects, including data collected through networks or "a systematic monitoring of a publicly accessible area" i.e. CCTV.

   x Yes ☐ No

   Monitoring occurs for the 42 day duration as a result of infection reduction control.

5. Mostly sensitive data or data of a highly personal nature:
   This includes special categories of personal data as well as personal data relating to criminal convictions or offences.

   NB: this also includes personal data with the security marking of SECRET or TOP SECRET.

   x Yes ☐ No

6. Data processed on a large scale (in excess of 1000 records in either a single transaction or over a 12-month period).

   x Yes ☐ No

7. Matching or combining datasets, for example 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. (This would not apply to matching or combining datasets from different IT systems, but processed for the same purpose and legal basis e.g. CID and CRS).

☐ Yes x No

8. Mostly data concerning vulnerable data subjects including children. (This only applies where the entirety (or high percentage) of the data being processed relates to this category).

☐ Yes x No

9. The innovative use or applying new technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc.

☐ Yes x No

10. When the processing in itself “prevents data subjects from exercising a right (under Data Protection Legislation and the GDPR) or using a service (provided by) or a contract (with) the Department”.

☐ Yes x No

11. If you have answered yes to one or more of the above questions, then a DPIA must be completed. If you have answered no to all of the questions, but you feel the planned policy/ process/ activity is significant, or carries reputational or political risk, then please complete the DPIA. If you are unsure or have any doubts about whether a DPIA should be completed, please consult with the office of the Data Protection Officer (DPO).

x Yes ☐ No

Section 1

1.1 Proposal/ Project/Activity title:
Public Health Passenger Locator Form (Digital) & Pre-Departure Testing

1.2 Information Asset title (s):
Public Health Passenger Locator Form
MG11 Form

1.3 Information Asset Owner/s (IAO):

Email:	<redacted>
Name:	Michael Stepney
Telephone Number:	<redacted>
Information Asset title:	Public Health Passenger Locator Form
Email:	<redacted>
Name:	<redacted>
Telephone Number:	<redacted>
Information Asset title:	Public Health Passenger Locator Form

1.4 Officer completing DPIA:

Email:	<redacted>
Name:	<redacted>
Telephone Number:	<redacted>
Business Unit/Team:	Access UK 1
Email:	<redacted>
Name:	<redacted>
Telephone Number:	<redacted>
Business Unit/Team:	DID, Data Policy

1.5 Date completed:
25/03/2021

1.6 Data Mapping reference:
N/A

1.7 Version:
V1

1.8 Linked DPIAs:
DPIAs will be entered into with the transport regulators, Maritime and Coastguard Agency (MCA) , the Civil Aviation Authority (CAA) and the Office of Rail and Road (ORR) to facilitate data sharing for a public interest / health purposes. It is as a result of non-compliance with the health functions, that passengers and (through CAA, MCA and ORR

enforcement action) airlines, coastal operators and rails operators will be made subject to law enforcement action under this DPIA which will require law enforcement processing with the CAA, MCA and ORR. There are already existing DPIAs with Public Health England, the Department of Health and Social Care, the Police forces and the UK devolved administrations concerning other health related measures at the border.

1.9 Publication date:

NB. If the intention is not to publish the completed DPIA either in full, or in part, record the reason why here

It is not Home Office (HO) policy to routinely publish DPIAs. This is a niche Border Force (BF) provision and assessment in conjunction with transport regulators, which is fully disclosed to data subjects. Publication would therefore not massively enhance the transparency of this process. Consideration will be given however, to disclosure under FOI or on advice received by the Home Office Data Protection Officer or the ICO.

Section 2 (personal data)

2.1 What personal data is being processed?

Passenger's Personal Data

Contact Information: Email, Telephone number, Address
Biographic Information: Name, Date Of Birth, Passport Information
Travel Plans: Dates Travelling to UK, Details of Transiting the UK, Flight details
Confirmation that user understands Covid testing policies

2.2 Does it include any of the following special category or criminal conviction data?

- Race or ethnic origin (including nationality)
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data or biometric data for the purpose of uniquely identifying individuals
- Health
- Sexual orientation or details of the sex life of an individual

x Yes ☐ No

2.3 Will any personal information be processed or collected relating to an individual age 13 years of age or younger?

x Yes ☐ No

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

- Should Border Force Officers or Immigration Enforcement have access to data on a minor, existing safeguarding policy will be followed to ensure data remains secure;
- PLF Information will be shared via a secure email by security cleared staff;

- CAA, MCA and ORR must ensure that additional safeguards are in place of processing of child data and this will be covered within their DPIA with the expectation that as another public sector body they are stringent with Data Protection Act compliance.

2.5 Will data subjects be informed of the processing?

x Yes ☐ No

If yes move to 2.7

2.6 (If no) Why not?

Click or tap here to enter text.

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

Links to the Border Immigration and Citizenship: Privacy Information Notice and the Coronavirus (Covid 19) Passenger Privacy Notice on gov.uk and guidance, included on the form used to input data. If a printed form is used at the border a print out of the privacy information notice will be attached to the form.

2.8 (a) Which HO staff will have access to the data?

Authorised Border Force Operatives

Border Force officers will carry out on the spot checks of arriving passengers at the UK border in order to check that a PLF had been completed and that satisfactory evidence had been produced of a negative Covid test taken in the 3 days prior to departure. Where the passenger has not complied with these requirements, that will be evidence relevant to consideration of whether the operator has complied with its obligations under the Carrier Regulations.

The checking Border Force officer will prepare a MG11 form containing the personal data of the arriving passenger derived from the PLF and passenger interview. That MG11 form will also contain personal data confirming whether Border Force has issued the passenger with a fixed penalty notice relating to their failure to complete (or provide evidence of) a PLF or to complete (or provide evidence of) a negative Covid test. Border Force Officer's will also be using a central operations platform to record anonymised data. Once completed, the MG11 form will be securely emailed by the Criminal Justice Unit (CJU) within the Home Office, to security cleared staff in the CAA, MCA, and ORR via secure email addresses. The sharing of data is anticipated to be on a daily basis.

Authorised Ops Engineers

Only Home Office authorised engineers operating the PLF database will have access to the system.
There will be access control policies on this data store that only allow 'the minimum number of Security Cleared people as necessary to maintain and operate the system', on a 'need to know basis'. There will be audit logs that show access and actions performed on this data store.

2.8 (b) How will that access be controlled?

Access will be only be available to authorised personnel following the process outlined above.

2.9 Where will the data be stored?

Within the Home Office IT infrastructure.

2.10 If the data is being stored by electronic means - as opposed to hard copy paper records - does the system have the capacity to meet data subject rights (e.g., erasure, portability, suspension, rectification etc)?

x Yes ☐ No

If 'No' state why below and move to 2.12

Click or tap here to enter text.

2.11 If you have chosen yes for 2.10, provide details of how these requirements will be met

Any of the data rights requests made in 2.10 can be actioned by the Home Office subject to business approval and following a case by case assessment. When requirements for the data change is approved, appropriate actions will be taken to implement requests. Individuals know how to act on these rights from the privacy information published. Data shared beyond Home Office's responsibility and managed by CAA, MCA and ORR is subject to an expected equivalency of data rights management. Communication will occur between affiliates to deliver data rights when required.

2.12 What is the retention period, how will data be deleted in line with the retention period and how will that be monitored?

The 42 day retention period for PLF data was agreed to allow sufficient time for both the Home Office and other data sharing partners to access the data in relation to any further action such as enforcement of non-compliance.

Data will be deleted to be in line with the retention period stated. PLF data may be held further for legitimate reasons based on the original purpose for processing and on a case by case basis where processing is not incompatible for the purpose for which personal data was originally collected. For example if Home Office received a legal challenge from an individual in respect of the processing, an individual is prosecuted, or appeals enforcement action or personal data was further processed by the Home Office to make a health-related immigration decision. The Privacy Information Notice contains examples of when data may be retained. This retention will at no time be indefinite and will remain subject to ongoing review.

In the limited instances where a paper form is used a designated Border Force Officer will be responsible for ensuring that the form is only kept until the data can be inputted into the online form. The officer will also be responsible for destroying all forms once the data has been inputted. Destruction will be through shredding or secure waste facilities. Copies will not be made of completed forms.

2.13 If physically moving/sharing/transferring data, how will the data be moved/ shared?

PLF Data shared with the CAA, ORR and MCA will be done through secure email to security cleared and recognised staff contacts. URN 287.20

2.14 What security measures will be put in place around the / movement/ sharing/ transfer?

Data is not physically transferred when shared. Digital transfer of data is secured through the Home Office IT network. Emails are secured by enforcing TLS in the data transfer. MoUs have been put in place with authorities which receive PLF data.

2.15 Is there any new/additional personal data being processed (obtained from either the applicant or a third party) for this activity?

x Yes ☐ No

(If the answer is yes, provide details)

Where the passenger has not presented a negative test result, we would record this on the MG11 form. In this scenario we will be collecting health related data from individuals.

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

OFFICIAL/OFFICIAL-SENSITIVE	x
SECRET	☐
TOP SECRET	☐

Section 3 (purpose)

3.1 What is the purpose for the processing? (Provide a brief description of what the purpose is for the processing activity e.g. sharing with a third party; storing data in a new way; automating a data processing activity etc.)

What resources are needed to build the model? (e.g. FTEs, skills, software, external resource)

Infectious diseases such as COVID-19 present a serious and ongoing threat to the nation's health. If not controlled, they can infect large numbers of people and, depending on the disease and other factors, can result in ill-effects ranging from relatively minor symptoms to early death. Data is captured by HO through a digital form and through paper for the protection of a public health purpose, by having the requirement to complete the PLF and have pre-departure testing to help control the spread of infectious diseases.

The sharing of personal data by Home Office with the CAA, MCA and ORR to review, and where appropriate enforce by issuing fixed penalty notices and prosecute is considered a necessary and proportionate measure to achieve the substantial public interest of preventing danger to public health and thereby ensuring public health, safety and security. **For more information on the Border Force management of enforcement powers, see DPIA URN 86.20.**

The Home Office has a controller/controller relationship with affiliated parties:

- We all have different roles and use and process personal data for different purposes.

- We do not dictate the extent to which health authorities carry out track and trace functions, nor what enforcement action police force partners carry out. URN 287.20
- We each hold separate copies of the personal data in discrete data stores.

- This is a health matter and as such is a devolved mater to all countries of the UK and we are operating under their relevant health regulations and so are not in a position to direct them as to how they would process the data we transfer to them.

3.2 What is the lawful basis for the processing? (Choose an option from the list)

Consent	☐
Contract	☐
Legal obligation	☐
Vital Interest	☐
Performance of public task	x
Legitimate Interest	☐

3.3 If processing special category data (see 2.3 above), what is the condition for processing?

Consent	☐
Employment/Social Security	☐
Vital Interest	☐
Non-profit making organisation	☐
In the public domain	☐
(Exercising/defending) legal rights	☐
Public Interest	x
Personal healthcare	☐
Public healthcare	☐
Research	☐

"Public Interest" as laid out in The Health Protection (Coronavirus, International Travel) (England) Regulations 2020 and The Health Protection (Coronavirus, Pre-Departure Testing and Operator Liability) (England) Regulations 2021

Appropriate Policy Document: Special Category Data

3.4 Is the purpose for processing the information the same as the original purpose for which it was obtained?

x Yes ☐ No

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

Original purpose: Click or tap here to enter text.

Original Lawful basis:	Consent	☐
	Contract	☐
	Legal obligation	☐
	Vital Interest	☐
	Performance of public task	☐

Legitimate Interest ☐

NB: Legitimate interest is not available for the performance of a public task

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 x No

If the answer is yes move to 4.3

4.2 Is the processing a new activity?

x Yes ☐ No

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

Unknown. This is a new activity with no precedent. Business as usual statistics of travel suggest this may be 150 million per year (for indicative purposes only) however the policy will be regularly reviewed, and data sharing will be ceased should it be deemed no longer necessary. Provisions have been put in place for the system to deal with these volumes of form completions.

4.4 Is this a one-off activity, or will it be frequent, or regular?

Ongoing until further notice.

4.5 Does the processing activity involve another party?

(This includes another internal HO Directorate, as well external HO parties both public and private sector)

x Yes ☐ No

If the answer is "No" move onto 4.9

4.6 Is the other party another part of the HO Group for which the Home Secretary of is the data controller? If yes, provide details

x Yes ☐ No

Border Force and Immigration Enforcement will review an individual's data at the border (in form of PDF) to confirm they have completed the PLF and have a negative Covid 19 test result . This will be in the form of a visual spot check to ensure that an individual has a negative test result, that the PLF has been completed, that the traveller has somewhere to self-isolate (unless exempt) and that the name and travel document numbers on the form match the traveller's documents.

Border Force and Immigration Enforcement can also enforce self-isolation and issue fixed penalty notices at the border if a passenger refuses to complete the form and fails to present a negative test result. CJU will also use the data to carry out enforcement activity under the Regulations, and may issue fixed penalty notices and/or prosecute as appropriate.

4.7 Is the other party another public authority in the UK? If so, provides details AND complete questions in Section 6.

URN 287.20

x Yes ☐ No

CAA, MCA and ORR will use the data to carry out law enforcement activities for the purpose of Regulation 11 under the 2021 Regulations above by levying a fine on the operator for bringing in a passenger in breach of the regulations.

Provide brief details here and then ensure Section 6 is also completed

4.8 Is the other party a private sector organisation in the UK? If so, provide details AND complete questions in Section 6.

☐ Yes x No

Provide brief details here and then ensure Section 6 is also completed

Click or tap here to enter text.

4.9 Will the handling of data involve transfer of data to public bodies or private organisations outside the EEA?

☐ Yes x No

If no move to 4.10

a) If yes, provide brief details of the country/ies and also complete Section 7 (International Transfers)

Click or tap here to enter text.

4.10 Is the processing for law enforcement purposes?

x Yes ☐ No

The Home Office will carry out a separate law enforcement purpose pursuant to Part 3 DPA 2018 to enforce the regulations at the border and issuing fixed penalty notices for non-compliance. **For more information on the Border Force management of enforcement powers, see DPIA URN 86.20.**

If the answer is yes, you will need to complete Section 5

4.11 Does the proposal involve profiling operations likely to significantly affect individuals?

☐ Yes x No

If yes, provide details

Click or tap here to enter text.

4.12 Does the proposal involve automated decision making?

☐ Yes x No

If yes, provide details

Click or tap here to enter text.

4.13 Does the processing involve using new technology?

☐ Yes x No

If the answer is no, proceed to question 4.15

4.14 Describe the new technology being used including who is supplying and supporting it.

URN 287.20

Click or tap here to enter text.

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

☐ Yes x No

If yes, explain how that is being achieved and move to 4.18

Click or tap here to enter text.

a) If no, what is the justification for not seeking the views of data subjects and/ or their representatives?

This process relates to maintaining and protecting public health and security during the unprecedented COVID-19 crisis. The emergency nature prevents meaningful prior consultation. Data subjects can access public facing privacy information on the gov.uk website.

Benefits

4.16 List the benefits of undertaking the processing activity, including named business owner of the benefits and how they will be measured. If the beneficiaries include those outside the HO these must be listed as well.

Benefit(s):

- Lowering the risk of a COVID-19 outbreak in the UK for international travel.
- Protect other individuals in the UK from being infected with the virus.

How will they be measured?:

No direct means of measuring since this product is designed to mitigate risk and will be continually reviewed.

Benefit(s) Owner (in HO): Discharge of a duty in the public interest

Beneficiaries:

The health and wellbeing of the general public and reassurance that the Government is acting in those interests

Risks

4.17 Are there any other known, or anticipated risks associated with the processing of personal data that have been identified by the project/ programme/ initiative owner, which have not been captured in this document?

x Yes ☐ No

If yes, provide details and carry on to question 4.17 a)

- Risk 1: There is a risk that the process defined by the Home Office (i.e Passengers should fill out a PLF before arriving at the border) may not be completed prior to travel. This may occur because the user may be unaware of the requirement, and carriers may not have strict means to enforce a check, or the

user may willfully choose to not adhere to the requirement. This may lead to delays at the border. Mitigations for this are listed in 4.17 a. URN 287.20

- Risk 2: There is a risk that users may provide an email address from a provider that does not enforce email transfer securely via TLS. This risk exists because not all email providers have the configuration enabled, and the PLF service relies on providers being able to enforce TLS to send emails securely. This risk means that emailed data may be vulnerable to cyber attacks. Mitigations for this are listed below.
- <redacted>.

If required, what steps have been taken to mitigate the risks listed at question 4.17 above?

- Risk 1 Mitigations: If a form has not been completed prior to travel and the subject does not have a device they can use, tablets will be available at the border for passengers to use to complete the form digitally. The requirement to fill out the PLF is enforced through fixed penalty notices (details in section 3.1).
- Risk 2 Mitigations: The PLF systems are configured to always use TLS if the user's email provider supports it. Furthermore, we ask for the user's consent to send over the completed data (in the form of a PDF) via email. Considerations on multiple options to further mitigate the TLS issue were made (such as encrypting the PDF or requiring the user to login to their account to download the PDF). The decision to implement the consent solution was chosen as it ensures that the PLF process has a low barrier for users to adopt – which further helps to mitigate Risk 1.
- <redacted>.

Section 5 (Processing for law enforcement purposes)

5.1 Was the data previously being processed for a different purpose?

☐ Yes x No

The data is being gathered by HO for the UK health authorities and collecting data for transport operators to carry out enforcement to use for health purposes under Part DPA 2018/GDPR. HO (Border Force) officers will also separately carry out a law enforcement purpose pursuant to Part 3 DPA 2018 and enforce the regulations at the border and confirm users have competed the form, and also enforce self-isolation / issue fixed penalty notices.

If the answer is no, move to 5.4

5.2 If yes, what was that purpose?

☐ Yes ☐ No

If the answer is no move to 5.4

5.3 At that time was the data being processed by another Controller or HO IAO?

☐ Yes ☐ No

If yes, provide details

5.4 Is any new and/ or additional data being processed for this purpose?

x Yes No

If no move to 5.6

5.5 What is the new/additional data, the source and the legal basis for the processing?

New data:

- Passenger Data: Health data.
- Border Forces' Staff's Personal Data Contact Information: Work Email, Work Telephone number, Name.
- Health data: In response to does the witness have any particular needs?
- Source: MG11 form

Lawful basis (*see 3.2 above):

- Public Task and Public Interest, using The Health Protection (Coronavirus, International Travel) (England) Regulations 2020 and The Health Protection (Coronavirus, Pre-Departure Testing and Operator Liability) (England) (Amendment) Regulations 2021 made under sections 45B and 45F(2) and 45P(2) of the Public Health (Control of Disease) Act 1984

5.6 Where will the data be stored/retained?

Same as 2.8, 2.9

5.7 If being stored electronically, does the system have logging capability?

x Yes ☐ No

If yes, move to 5.9

a) If no, what action is being taken to either address this issue or mitigate the risk of non-compliance with DP legislation?

Click or tap here to enter text.

5.8 Will it be possible to easily distinguish between different categories of individuals (e.g. persons suspected of having committed an offence, victims, witnesses etc.)?

☐ Yes ☐ No

If yes, move to 5.9

a) If no, what action is being taken to either address this issue or mitigate the risk of non-compliance with DP legislation?

5.9 Does the proposal involve using new technology which might be perceived as being privacy intrusive?

☐ Yes x No

Section 6 Data Sharing

6.1 External contact details for data exchange

Name: <redacted>.
Organisation: MCA

Business Unit/Area: Regulatory Compliance Investigations Manager
Contact email: <redacted>

URN 287.20

Name: <redacted>
Organisation: ORR
Business Unit/Area: Deputy Director, Consumers
Contact email: <redacted>

Name: <redacted>
Organisation: CAA
Business Unit/Area: Legal Advisor
Contact email: <redacted>

6.2 How long will the data be retained by the receiving organisation?

Data will be held for 42 days before it is deleted unless still required for a relevant legal purpose that is not incompatible to the original purpose for processing. For example, may be retained beyond 42 days if the HO, CAA, MCA or ORR were made subject to a legal challenge.

6.3 How will it be destroyed by the receiving organisation once it is no longer required?

Data will be deleted after 42 days/7 days by an automated script. See 2.12 for further details

6.4 Does the arrangement require a data sharing agreement (MoU)?

x Yes ☐ No

If no, provide details why a formal written agreement is not required and move to 6.6

6.5 Provide details of the proposed HO MoU signatory and confirm they have agreed to be responsible for the data sharing arrangement detailed in this document.

Name: Oscar Ramudo
Grade: SCS
Business Unit/Area: Border Force
Contact email: <redacted>
Contact telephone: <redacted>

6.6 Will the recipient share any HO data with a third party including any 'processors' they may use?

☐ Yes x No

If yes, please provide the identity of the processor and confirm details of that arrangement will be included in the data sharing agreement

6.7 Has advice been sought from HO Legal Advisers in respect of this data sharing activity?

x Yes ☐ No

If no, explain why HO Legal Advisors have not been consulted

Click or tap here to enter text.

6.8 Provide a summary of the legal advice received

<redacted>.

6.9 Which of the following reflects the data exchange?

Data extract	☐	Yes	x No
Data matching	☐	Yes	x No
Data reporting	☐	Yes	x No
Data exchange/feed	x	Yes	☐ No
Direct access	x	Yes	☐ No

6.10 Has any analysis or feasibility testing been carried out?

x Yes ☐ No

If yes, provide details. If no, explain why it is not required.
The solution is based on exisiting and well-known technologies used within the Home Office. Functional and Performance testing of the solution was completed before the form had been put live.

6.11 Please confirm whether

a) development work is required

x Yes ☐ No

If yes, provide details including time frame

2 weeks for initial development of the form, and upgrade of database to handle higher loads. Development work will be ongoing for maintenance, further functionalities and updates.

b) there be a fiscal cost?

x Yes ☐ No

If yes, provide the cost details

Standard costs for the delivery of form infrastructure and services within the Home Office.

6.12 Would the increased volumes result in any degradation of an existing service?

☐ Yes x No

If no, move to 6.14

6.13 Provide details and how that risk to the business is being mitigated

Click or tap here to enter text.

Security Checklist

6.14 Given the security classification of the data, are you satisfied with the proposed security of the data processing/ transfer arrangements detailed at 2.14 above?

x Yes ☐ No

NB: Please also confirm that you have read the associated guidance and, if necessary, consulted with HO Security:
Yes, I have read the guidance and/or consulted with HO Security

a) 6.15 (If the answer is no) What needs to happen to ensure that adequate security arrangements are achieved?

Click or tap here to enter text.

Section 7 (International transfers)

URN 287.20

7.1 Does the activity involve transferring data to a country outside of the EEA?

☐ Yes x No

If yes, specify the country and continue with this section. If no, do not complete the rest of this section, and go to Section 8.

N/A

7.2 Does the country have a positive adequacy decision from the European Commission?

☐ Yes ☐ No

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

- Pursuant to a legally binding Treaty which recognises 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 data subjects and includes 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 ☐

7.3 If relevant, have you carried out an Overseas Security and Justice Assistance (OSJA) assessment to determine if there are any human rights or legal/reputational risks?

☐ Yes ☐ No

a) Provide details of when one will be completed and by whom?

Click or tap here to enter text.

7.4 Does the HO already have a data sharing agreement (MoU) with this country?

☐ Yes ☐ No

If no, skip 7.4 a)

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

☐ Yes ☐ No

If you have selected no for 7.4, you will need to consider reviewing the existing agreement to include the new processing activity

I. If yes, does the agreement 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?

☐ Yes ☐ No

If yes move to Section 8

II. If no, how do you propose to document the terms of the understanding with the other country (including mitigations for risks identified in the OSJA assessment)?

Section 8

8.1 Date referred to the DPO
14/01/2021

8.2 Comments/recommendations
- Strong document, minor comments made for clarification and some elements currently outstanding.

8.3 Completed by
<redacted>.

8.4 Date returned to the business owner listed in Section 1
14/01/2021

8.5 Date re-referred to the DPO
15/01/2021

8.6 Comments/ recommendations
- ODPO review process complete.

8.7 Completed by
<redacted>.

8.8 Date returned to the business owner listed in Section 1
17/01/2021

8.9 Date re-referred to the DPO
01/04/2021

8.10 Comments/ recommendations
- ODPO resubmission review complete.

8.11 Completed by
<redacted>.

8.12 Date returned
07/04/2021

8.13 Date re-referred to the DPO
06/05/2021

8.14 Comments/ recommendations
- Small number of comments on the PDT pause.

8.15 Completed by
<redacted>.

8.16 Date returned
10/05/2021

8.17 Date re-referred to the DPO
10/05/2021

8.18 Comments/ recommendations
- ODPO resubmission review complete.

URN 287.20

8.19 Completed by
<redacted>.
8.20 Date returned
10/05/2021

Section 9

9.1 Date referred to the SIRO
Click or tap to enter a date.

9.2 Referred by
Click or tap here to enter text.

9.3 Reason for referral to the SIRO
Click or tap here to enter text.

9.4 Comments/questions recommendations from SIRO
Click or tap here to enter text.

9.5 Completed by (SIROs' details)
Click or tap here to enter text.

9.6 Date returned to the business owner listed in section 1
Click or tap to enter a date.

9.7 Action taken by business owner listed in section 1
Click or tap here to enter text.

Any suggestions for improvements or comments should be directed to hodpbillteam@homeoffice.gov.uk

Effective Date **May 2021**
Last Review Date
Next Review Date
Owner **DID**
Approved by
Audience **All HO Staff**