Home Office

OPDO DPIA URN: 167.19

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

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).

   ☒ 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.

   ☐ 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 ☒ 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.

   ☐ Yes ☒ No

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.

   ☐ 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).

   ☒ 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 ☒ 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 ☒ 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 ☒ 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 ☒ 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).

☒ Yes ☐ No

DPIA Stage 2

Section 1

1.1 Proposal/ Project/Activity title:

Asylum Support Payments

Secure transfer of eligible asylum seeker's information to PFS who will issue Aspen payment cards and add credit to the cards as requested by the Home Office. This DPIA relates to data sharing as part of BAU activity after the PFS contract start date of 27/5/21.

The Aspen card is a Mastercard pre-paid debit card, which is nameless and is registered per user. Each applicant will receive a card which they will have to activate via an automated telephone line. The security of the card is managed by chip and PIN. This DPIA covers the transfer of information between the Home Office and PFS and relates to expected activities during BAU.

1.2 Information Asset title (s): Asylum Support data

3 files are transferred

1) Applicant details

NASS_REF

First Name

Last Name

DOB

Address

Daily Rate

Weekly Rate

Payment Start Date

2) Payment Instructions

NASS_REF

Instruction

Effective Date

Payment Amount

3) Aspen Response File

NASS_REF

Change Type

Card issue date

Payment start date

Payment Initial Value

Payment Regular Value

Card Ref

1.3 Information Asset Owner/s (IAO):

Email:	<REDACTED>
Name:	Ann Smith

Telephone Number: <REDACTED>
Information Asset title: Aspen Card Service (Asylum Support)

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 Officer completing DPIA:

Email: <REDACTED>
Name: <REDACTED>
Telephone Number: <REDACTED>
Business Unit/Team: Project Business Lead

1.5 Date completed:
21/09/2021

1.6 Data Mapping reference:
N/A

1.7 Version:
1

1.8 Linked DPIAs:
Sodexo Data Sharing Toolkit (2017)

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

There is no intention to proactively publish this DPIA in its current form as the processing is not high risk, is not for publication, is solely being used to enable service user payment - which they (service users) consent to the sharing of that data for that purpose, is not controversial and we have not sought ICO input. Therefore, there is limited public interest in publication. However, we may publish at a later date a summary of this and other DPIA's to aid transparency. We will also consider any request for publication 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?
Name, Address, DOB

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

☐ Yes ☒ No

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

☐ Yes ☒ No

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

Click or tap here to enter text.

2.5 Will data subjects be informed of the processing?

☒ 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?

A GDPR paragraph within the declaration on the Asylum Support Application (ASF1) form which references the PIN and includes a link. It is on both declarations – S4 & S95 and reads, “The Home Office will use the personal information you provide to consider your application. We may also share your information with other public and private sector organisations in the UK and overseas. For more detail please see the Privacy Notice for the Border, Immigration and Citizenship system at: www.gov.uk/government/publications/personal-information-use-in-borders-immigration-and-citizenship. This also sets out your rights under the Data Protection Act 2018 and explains how you can access your personal information and complain if you have concerns about how we are using it.”

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

Aspen Operations Team

2.8 (b) How will that access be controlled?

- System only accessible from company machine which is maintained with security patches and regularly checked for viruses
- Access is only granted to staff with security clearance and need to know
- User accounts are personally identifiable and have strong passwords
- Role based access controls to limit access to only the information needed

2.9 Where will the data be stored?

S3 bucket. An S3 bucket is a data storage location within the AWS (Amazon Web Services) environment. S3 refers to the Amazon Simple Storage Services. Amazon S3 can be used to securely store any type of object (documents, images, audio, backup files, log files etc.) with guaranteed availability levels. The objects can be encrypted and access to the object can be controlled and audited to protect the integrity and confidentiality of the information.

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 (eg, erasure, portability, suspension, rectification etc)?

☒ 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

There is an existing process in place within Asylum Support Case working to address and deal with data subject access requests. Assessment of digital systems utilised to share data between the Authority (Home Office) and commercial delivery partners is part of that process and able to meet data subject rights accordingly.

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

Currently a moratorium is in place. Sodexo will hold data for the duration of the contract due to end at the latest 27th May 2021 – this data will then remain on a read only database for a period of 12 months before being returned to the responsible Information Asset Owner, either by media or formatted disk as per the provisions of the agreed contract. PFS will receive live data from late April 2021 to allow for transition activity to take place and will retain the data for the duration of the contract (currently up to 27 February 2025).

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

Files will be transferred via MOVEit which is a secure web based system allowing file sharing. It allows files to be reliably transferred between 2 machines over the internet by granting users access to specific folders within a file share area. To initiate the transfer a user logs in to the MOVEit using a secure authentication protocol and the files are encrypted during the transfer over the internet to protect the confidentiality and integrity of the information.

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

Access to MOVEit is via username and password. Data is encrypted in transit and at rest.

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

☐ Yes ☒ No

(If the answer is yes, provide details)

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

OFFICIAL/OFFICIAL-SENSITIVE	☒
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)

The purpose is to be able to share personal data of the service users to enable them to receive payments using Aspen cards provided by PFS.

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	☒
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	☒
Personal healthcare	☐
Public healthcare	☐
Research	☐

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

☒ 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 ☐ No

MoveIT was the primary method of securely sharing data on a daily basis with the service provider. The new MACP system is fed data directly from Atlas although manual payments are still conducted with MOVEit support.

Click or tap here to enter text.

If the answer is yes move to 4.3

4.2 Is the processing a new activity?

☐ Yes ☒ No

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

c31,668,000 per annum

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

Regular activity several times a day

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)

☒ 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

☐ Yes ☒ No

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

☐ Yes ☒ No

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

Click or tap here to enter text.

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

☒ Yes ☐ No

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

Click or tap here to enter text.Will the handling of data involve transfer of data to public bodies or private organisations outside the EEA?

☐ Yes ☒ 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.

4.9 Is the processing for law enforcement purposes?

☐ Yes ☒ No

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

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

☐ Yes ☒ No

If yes, provide details

Click or tap here to enter text.

4.11 Does the proposal involve automated decision making?

☐ Yes ☒ No

If yes, provide details

Click or tap here to enter text.

4.12 Does the processing involve using new technology?

☒ Yes ☐ No

If the answer is no, proceed to question 4.15

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

Master Administration Control Portal (MACP) is the portal used by UKVI staff and Migrant Help staff to manage all the backend functions for Asylum Support Payments. MACP integrates with the Home Office Atlas case working system where it receives payment instructions sent via LA or CP files from Atlas via an SFTP server. The Aspen File Processor handles these payments instructions and translates them into PFS backend operations to manage the daily and weekly deposit batches as well as other operations such as updating cardholder information.

MACP enables cards to be created anonymously and allocated to service users, provides updated card and service user data and enables card funding. The data stored in MACP includes Service User data such as name, address, DOB, regular payment amount as well as providing their card status and a history of all card transactions.

MACP is a web based browser accessed via a Poise desktop/laptop and used by PFS's other clients. The Aspen File Processor was built specifically for the Home Office as a way to process incoming payment instruction files. Both MACP and the File processor are supported by PFS/EML Payments.

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

☐ Yes ☒ 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?

The purpose is to provide eligible Service Users with Asylum Support funds. Support recipients are advised that HO and the payment provider will exchange data relating to the support application in order to ensure the correct support is put in place or to correct any problems arising. They are required to consent to this before the application can be initiated.

Benefits

4.15 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): To prevent destitution by ensuring the correct levels of support are paid.

How will they be measured?: Contractual monitoring of PFS performance as the Payment Provider to ensure payments to SUs arrive on time and are accessible to prevent destitution. Service credits levied based on data returns against KPI.

Benefit(s) Owner (in HO): Ann Smith and <REDACTED>

Beneficiaries: Service users in receipt of or applying for asylum support.

Risks

4.16 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?

☐ Yes ☒ No

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

Click or tap here to enter text.

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

Click or tap here to enter text.

Section 5 (Processing for law enforcement purposes)

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

☐ Yes ☐ No

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

Click or tap here to enter text.

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

☐ 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: Click or tap here to enter text.
Source: Click or tap here to enter text.
Lawful basis (*see 3.2 above): Click or tap here to enter text.

5.6 Where will the data be stored/retained?

Click or tap here to enter text.

***See 2.8 and 2.9**

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

☐ 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?

☐ Yes ☐ No

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

☐ Yes ☐ No

Section 6 Data Sharing

6.1 External contact details for data exchange

Name: <REDACTED>
Grade: Head of Client Services (UK)
Organisation: Prepaid Financial Services Ltd
Business Unit/Area: Aspen Cards
Contact email: <REDACTED>
Contact telephone: <REDACTED>

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

***See 2.8 and 2.9**

Currently, a moratorium is in place. Data will be held for the duration of the contract. The data will be returned to the responsible Information Asset Owner, either by media or formatted disk as per the provisions of the agreed contract.

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

***See 2.8 and 2.9**

The data will be returned to the responsible Information Asset Owner, either by media or formatted disk as per the provisions of the agreed contract and handled in line the HO returned data policy. Data will be destroyed under the guidance of Knowledge Information Management Unit and in line with HO policy.

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

☐ Yes ☒ No

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

From a commercial perspective no data sharing agreement or MoU are required at present, however, if these required in the future these will be established in accordance with the new legislation.

Responsibilities have been highlighted in the main contract under the data security schedule.

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: Click or tap here to enter text.
Grade: Click or tap here to enter text.
Business Unit/Area: Click or tap here to enter text.
Contact email: Click or tap here to enter text.
Contact telephone: Click or tap here to enter text.

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

☐ Yes ☒ No

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

Click or tap here to enter text.

Technical impact and viability

6.7 Which of the following reflects the data exchange?

Data extract	☒	Yes	☐	No
Data matching	☐	Yes	☒	No

Data reporting	☐	Yes	☒	No
Data exchange/feed	☒	Yes	☐	No
Direct access	☐	Yes	☒	No

6.8 Has any analysis or feasibility testing been carried out?

☒ Yes ☐ No

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

Feasibility testing and system analysis were conducted by DDaT as part of the integration work conducted between November 2020 and May 2021.

6.9 Please confirm whether

a) development work is required

☐ Yes ☒ No

If yes, provide details including time frame

Click or tap here to enter text.

b) there be a fiscal cost?

☐ Yes ☒ No

If yes, provide the cost details

Click or tap here to enter text.

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

☐ Yes ☒ No

If no, move to 6.14

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

Click or tap here to enter text.

Security Checklist

6.12 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?

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

Click or tap here to enter text.

Section 7 (International transfers)

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

☐ Yes ☒ 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.

Click or tap here to enter text.

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

21/10/2019

8.2 Comments/recommendations
Please review comments and re-submit. Updates required at 1.9, 2.7, 2.9, 2.11, 2.13, 4.1 and 6.7.

8.3 Completed by
<REDACTED>, Senior Risk & Assurance Analyst, Office of the DPO.

8.4 Date returned to the business owner listed in Section 1
23/10/2019

8.5 Date re-referred to the DPO
30/10/2019

8.6 Comments/ recommendations
Review complete with no further comment.

8.7 Completed by
<REDACTED>, Senior Risk & Assurance Analyst – Office of the DPO

8.8 Date returned to the business owner listed in Section 1
01/11/2019

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 KIMDirection@homeoffice.gsi.gov.uk

Effective Date **May 2018**
Last Review Date **25/06/18**

Next Review Date	**24/06/19**
Owner	**DID**
Approved by	**Head of DID**
Audience	**All HO Staff**