Home Office

URN 100.19

N 1The Data Protection Impact Assessment (DPIA) Template

Contents

The DPIA Process

URN 100.19

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 100.19

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

   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.

   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".

   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.

   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.

   No

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

   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). URN 100.19

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).

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.

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”.

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).

DPIA Stage 2

URN 100.19

Section 1

1.1 Proposal/ Project/Activity title:
Animals in Science Procedures E-Licensing - ASPeL

1.2 Information Asset title (s):
ASPeL

1.3 Information Asset Owner/s (IAO):

Email:	william.reynolds10@homeoffice.gov.uk
Name:	Will Reynolds
Telephone Number:	020 7035 5650
Information Asset title:	ASPeL

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:	Phoebe.stannard@homeoffice.gov.uk
Name:	Phoebe Stannard
Telephone Number:	020 7035 5650
Business Unit/Team:	ASRU

Email:	ben.stevens@digital.homeoffice.gov.uk
Name:	Ben Stevens
Telephone Number:	Click or tap here to enter text.
Business Unit/Team:	DDaT

1.5 Date completed:
28/09/2020

1.6 Data Mapping reference:
N/K

1.7 Version:
Version 1

1.8 Linked DPIAs:

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

We will publish this DPIA on the ASRU website and have it linked from the footer of ASPeL

Section 2 (personal data)

2.1 What personal data is being processed?

Names, dates of birth, email addresses, phone numbers, places of work, positions held, professional training and qualifications

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

No

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

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

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?

Privacy notice (last updated 17th May 2018) on the system where they enter the data

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

ASRU staff, including licensing officers, inspectors, and other support and management toles within the team. Some security cleared staff/contractors from DDaT who are building and supporting the new system.

2.8 (b) How will that access be controlled?

ASRU staff will only be able to access the system through an account that can only be setup using a POISE machine. Admin users of the system will control access level permissions.

Any DDaT access to the data will be limited, and only accessible through a VPN.

2.9 Where will the data be stored?

The electronic data will be stored in AWS (London). Some paper copies will be stored under lock and key in Lunar House.

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)?

Yes

If 'No' state, why below and move to 2.12

All users will be able to make these requests. Any mistakes will be rectifiable, and, on request, data can be exported into a portable format. Users who are named on licences won't be able to have their data erased, unless ten years have passed since the data was last accessed – as per the requirements of ASPA (1986).

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

Users will contact ASRU through the established channels, then ASRU will raise a ticket with the Live support team to take any action that they are unable to complete through the system. There is a user-facing interface through which rectifications can be made.

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

Users that have never held a licence can have their data removed. Users who have been named on a licence, will, as per ASPA, be removed from the database once ten years have passed since the record was last accessed. We would also keep refused licences for 10 years.

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

There will be no physical moving of data. It will only be done electronically between micro services. Communication between these services is conducted through SSL using TLS1.2. All data is encrypted during transit.

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

Strict kubernetes network policies have been put in place to ensure that services are only open to incoming connections from known clients, and that secure transport layers are enforced.

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

No

(If the answer is yes, provide details)

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

OFFICIAL/OFFICIAL-SENSITIVE

URN 100.19

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)

Information from licence holders and prospective licence holders will be assessed to make decision about whether or not licence applications and amendment requests should be granted. Aggregate data will be used for management information, for answering FOI requests and Parliamentary questions. It will also be used so ASRU can fulfil its obligations to publish certain statistics.

A digital system with an ASRU-facing front end and a licence holder facing front end is being built to provide access to and management of the licensing data.

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? **Not relevant**

Consent	☐
Employment/Social Security	☐
Vital Interest	☐
Non-profit making organisation	☐
In the pubic 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

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.

No

If the answer is yes move to 4.3

4.2 Is the processing a new activity?

No

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

3,500 transactions are expected to be made annually.

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

The new system is expected to be available 365 days per year, 24 hours per day, so a transaction could occur at any time. There are seasonal spikes with certain transaction types. Extraction of data for reporting or responding to a particular question may also happen at any time.

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

The supplier does not process or hold the personal data they have only created the structure of the system

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. URN 100.19

☐ Yes ☐ 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?

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?

☐ Yes ☒ No

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?

No

If yes, provide details

Click or tap here to enter text.

4.12 Does the proposal involve automated decision making?

No

If yes, provide details

Click or tap here to enter text.

4.13 Does the processing involve using new technology?

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.

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 ☐ **No**

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

All processing activities of personal data at the data subject, or their representative's request.

We did seek the views of the representatives, via regular stakeholder engagement, research and user testing.

a) If no, what is the justification for not seeking the views of data subjects and/ or their representatives? URN 100.19

Click or tap here to enter text.

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):	Fewer instances of accidental non compliance
How will they be measured?	Known issues are logged
Benefit(s) Owner (in HO):	Martin Whiting, service owner
Beneficiaries:	Establishments, and ASRU
Benefit(s):	Quicker reporting
How will they be measured?	Anecdotally
Benefit(s) Owner (in HO):	Martin Whiting, service owner
Beneficiaries:	Business support team (ASRU)
Benefit(s):	Reduced admin burden on licence holders
How will they be measured?	Various measurements around project licence drafting time
Benefit(s) Owner (in HO):	Martin Whiting, service owner
Beneficiaries:	Establishments
Benefit(s):	System build in-line with service standard
How will they be measured?	Pass service assessments
Benefit(s) Owner (in HO):	Martin Whiting, service owner
Beneficiaries:	All licence holders and ASRU users

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?

Yes

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

The biggest risk we have is that the system is breached and identifiable information relating to licence holders is compromised – putting them at risk of harm. There is also the risk of IP being compromised.

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

A clear and well-structured permissions model. Secure system architecture that has been properly risk-assessed and been through an IT Health check.

Section 5 (Processing for law enforcement purposes)

Not applicable

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: Ben Marvell
Grade: Click or tap here to enter text.
Organisation: Marvell
Business Unit/Area: Click or tap here to enter text.
Contact email: Ben Marvell <ben@marvell-consulting.com>
Contact telephone: Click or tap here to enter text.

Name: Ben Stevens
Grade: Click or tap here to enter text.
Organisation: Home Office
Business Unit/Area: DDAT
Contact email: Stevens Ben (Digital) <Ben.Stevens@digital.homeoffice.gov.uk>
Contact telephone: Click or tap here to enter text.

NB: The supplier does not process or hold and personal data, they have only created the structure of the system

6.2 How long will the data be retained by the receiving organisation?
***See 2.8 and 2.9**

6.3 How will it be destroyed by the receiving organisation once it is no longer required?
***See 2.8 and 2.9**

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

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

NB: The contract is to only create the structure of the system

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.

Click or tap here to enter text.

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:

Choose an item.

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?

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

18/07/2019

8.2 Comments/recommendations
Please address the comments above and resubmit

8.3 Completed by
Ian Morris

8.4 Date returned to the business owner listed in Section 1
19/07/2019

8.5 Date re-referred to the DPO
24/09/2020

8.6 Comments/ recommendations
Please confirm the current/ new author of the DPIA at question 1.4 and the identity of 'admin users' at 2.12 and then resubmit

8.7 Completed by

Ian Morris

8.8 Date returned to the business owner listed in Section 1

25/09/2020

8.9 Date re-referred to the DPO
28/09/2020

8.10 Comments/ recommendations
Review complete – no further comments

8.11 Completed by

Ian Morris

8.12 Date returned to the business owner listed in Section 1

29/09/2020

Section 9

9.1 Date referred to the SIRO

9.2 Referred by

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.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**