



Data Protection Impact Assessment (DPIA) Guidance

Contents

Data Protection Impact Assessment (DPIA) Guidance	1
Overview	2
Scope	2
Introduction	2
What this means for the Home Office.....	3
Roles and responsibilities.....	3
DPIA screening document: Stage 1	3
Full DPIA: Stage 2.....	3
Joint controllers	4
When is a DPIA required?	4
Balancing the risk.....	5
When is a DPIA Not Required?	5
How to complete a DPIA including the screening document	6
The assessment of 'high risk'	6
Reviewing the DPIA and screening document	8
DPIA Content	8
Identifying and recording the benefits of the proposal.....	9
Publishing the DPIA	9
Scope of the DPIA.....	9
Timing of a DPIA	10
Evaluation and Approval	10
Approval and beyond	10
HO SIRO referral.....	11
Annex A.....	13
Stage 2 Section 1	13

Section 2 (personal data)	14
Section 3 (purpose)	17
Section 4 (Processing activity)	18
Benefits	20
Risks	21
Section 5 (Processing for law enforcement purposes)	21
Section 6 (Data Sharing)	23
Technical impact and viability.....	24
Security Checklist.....	25
Section 7 (International transfers)	25
Section 8	26
Section 9	27

Overview

This document provides guidance on how to determine whether a full Data Protection Impact Assessment (DPIA) is required for an activity involving the general processing (including sharing) of personal data, including that for law enforcement and national security purposes and if it does, how to undertake one. It will also take you through the process to complete a DPIA screening document. The Information Commissioners Office (ICO) has produced some [guidance on DPIAs](#), that you may wish to view.

Scope

This guidance relates to the assessment and management of risks to privacy arising from activities within the Home Office (HO), its executive agencies, and is recommended for adoption by Arms-Length Bodies (ALBs). It replaces the existing Privacy Impact Assessment (PIA) and Data Sharing Toolkit (DST) process.

Introduction

Under new data protection legislation ('legislation'), controllers must carry out DPIAs to “evaluate, in particular, the origin, nature, particularity and severity” of the “risk to the rights and freedoms of natural persons” before processing personally identifiable information. Controller replaces the term Data Controller as referred to in the Data Protection Act 1998 (DPA). For the HO, the controller is the Secretary of State – or Home Secretary – for the Home Department. The DPIA “should include the measures, safeguards and mechanisms envisaged for mitigating” the identified risks.

The penalties for non-compliance in fulfilling DPIA requirements are severe. Violations can result in administrative fines of up to 20 million euros or up to 4 percent of the organisation’s total worldwide annual turnover.

What this means for the Home Office

In the past, the HO has operated under dual process whereby a PIA is completed, where required, for large scale projects involving the processing of personal data and a DST is completed where large scale (1000+ records) data sharing with an external (HO) party/body is taking place. For the movement of large (1000+ records) data sets within the HO a Data Movement Application (DMA) is required. The new DPIA will replace all existing processes.

The HO has produced a DPIA template that must be completed every time any part of the Department (not including ALBs and/ or public enquires who must operate their own DPIA process) introduces new personal data processing processes, including sharing, storing, decision making, deleting and outsourcing. Completion of the document will allow the author to establish whether or not a full DPIA is required.

Annex A of this document includes the DPIA template with additional guidance material included to aid the user. This version is not intended to be used operationally as it is a guide only, please use the separate DPIA template linked to this guidance.

The DPIA process is made up of two stages. The first stage is screening to identify the severity of the risk. The second stage is a full impact assessment. Projects will only proceed to the second stage if the risk is assessed as high.

Roles and responsibilities

The legislation states that it is the responsibility of the controller to commission a DPIA although the controller must also seek the advice of the Departmental Data Protection Officer (DPO), and this advice, and the decisions taken, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA.

For the HO this means that it will be for the Information Asset Owner (IAO) and/or the respective Director General to commission the DPIA process and engage with the DPO and HO Senior Information Risk Owner (SIRO) as required, or as directed by the DPIA.

In some instances, the HO will engage with a Third-Party provider/supplier (external to the HO) and in doing so commission that party to undertake some or all of the data processing on behalf of the HO. In these instances, that Third Party is legally defined as a 'processor'. In these circumstances, the HO remains the controller for the data being processed by the Third Party. If the processing is wholly or partly performed by the processor, the processor should assist the controller in carrying out the DPIA and provide any necessary information.

DPIA screening document: Stage 1

Those completing this section on behalf of the IAO/ DG must have a suitable understanding of the potential risks posed by the processing activity and have the authority of the IAO/ DG to answer the questions listed. All questions must be addressed and answered definitively. Where any doubt remains, consultation may be required directly with the respective IAO/DG and/ or with the office of the DPO before completing this stage.

Full DPIA: Stage 2

Those completing the DPIA on behalf of the IAO/DG must engage with relevant Units within the Department including (as necessary) DDaT, KIMU, HO Security, HO SIRO and the DPO. The DPIA will direct those completing it to the relevant business areas.

As part of the DPIA process those completing the DPIA must consider seeking the views of data subjects or their representatives, where appropriate. Those completing the DPIA

should also document its justification for not seeking the views of data subjects, if it is decided that this is not appropriate.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult with the ICO as to whether the processing operation complies with the legislation.

Consultation with the ICO will only be required after full internal consideration and consultation with the HO DPO and SIRO has taken place and in instances where risks cannot be mitigated and remain high - such as where individuals may encounter significant or even irreversible consequences, or when it is obvious that a risk may occur. For more information about how to liaise with the ICO contact DPO@homeoffice.gsi.gov.uk

Joint controllers

When two or more controllers jointly determine the purposes, and means of processing, they will be joint controllers. In such cases, the joint controllers must, in a transparent manner, define their respective obligations precisely by means of an arrangement between them. Their DPIA should set out which controller will be the point of contact for data subjects and responsible for the various measures designed to treat risks and to protect the rights of the data subjects.

When is a DPIA required?

Wherever possible DPIAs should be carried out prior to the processing in order to identify and assess any potential privacy risks. This will allow the business to make an informed decision on whether or not to proceed with the processing and if necessary, develop and implement appropriate mitigation.

There is an obligation on controllers to carry out a DPIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA (screening document) must be completed:

- when using new technology,
- developing new projects,
- when planning revisions to existing practices,
- when sharing/ moving large amounts (1000 or more records or transactions) of personal data internally or externally.

If in doubt, carry one out

Once the screening stage is complete, a full DPIA will only be required where the risk is assessed as high.

Examples of some instances where a full DPIA may be required include:

- matching or combining datasets, in a way not anticipated by individuals (data subjects)
- data concerning vulnerable individuals (which extends to employees; children; vulnerable groups; any case where there is an imbalance)
- daily transfers of data outside the EU,
- processing which has the effect of refusing people access to a contract or service

The ICO states:

“It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term ‘data protection by design and by default’. It also makes PIAs – referred to as ‘Data Protection Impact Assessments’ or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

Not only is completion of a DPIA now mandatory in certain circumstances, taking a privacy by design approach is essential in minimising privacy risks and building trust and designing projects, processes, products or systems with privacy in mind at the outset. This can lead to benefits which include:

- potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- increased awareness of privacy and data protection across an organisation.
- actions are less likely to be privacy intrusive and have a negative impact on individuals.
- provides evidence that the Department took privacy issues seriously when undertaking a project in the event that something goes wrong once it has been implemented.

Balancing the risk

While the GDPR does not provide guidance on how to evaluate and assign weight to the various risks and harms in the context of the DPIA requirements, it does provide that any evaluation must take into account the proportionality between risk/ harm and the purposes, interests or benefits that are being pursued. Thus, the same risk may be scored differently when compared to a low benefit or a high benefit.

When is a DPIA Not Required?

DPIAs are only required for general processing initiated after the new Data Protection legislation comes into force (25 May 2018).

A DPIA is not required in the following cases:

- where the processing is not likely to result in a high risk to the rights and freedoms of natural persons;
- when the nature, scope, context and purposes of the processing are very similar to the processing for which a DPIA has previously been carried out. In such cases, results of a DPIA for similar processing can be used;
- in circumstances as stipulated by the [ICO](#)

How to complete a DPIA including the screening document

The assessment of 'high risk'

The actual risk level (i.e. the "likelihood" and "severity" of any harm) and whether a given processing is, in fact, "high risk" must be determined in light of the specific circumstances at hand by taking into account:

- (a) the nature, scope, context and purposes of the processing and
- (b) the ability to mitigate a "high risk",

There is limited guidance on what constitutes high risk processing, but the Article 29 Working Party has provided a list of processing activity that they consider to be high risk and as such that will be the starting point for any assessment made by the Home Office. To begin to assess whether or not the processing activity is high risk you will need to consider whether or not that processing includes one or more of the following:

1. The evaluation or scoring, including 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. The Home Office would view this as any form of profiling.
2. 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". This covers fully automated decision making only and not automated processing, or what could be constituted as semi-automated decision making. If there is any form of human interaction with the decision then the process will not be considered as automated decision making.
3. 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". The primary example of this would be the use of CCTV.
4. 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. The Home Office would interpret this as the processing activity constituting of mostly all sensitive data and not simply where the processing activity includes some sensitive data. The Home Office would also include any personal data with the security marking of Secret or Top Secret in this definition.
5. Data processed on a large scale. The Home Office takes the view that large scale processing of personal data occurs where records in excess of 1000 records in either a single transaction or over a 12-month period are being processed. This is in line

with the existing DST process and is based on the ICO's definition of large scale processing.

6. 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. The Home Office view is that 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.
7. Data concerning vulnerable data subjects including children. The Home Office view is that this only applies where the entirety (or high percentage) of the data being processed relates to this category and will not apply where the processing simply includes data concerning vulnerable data subjects including children.
8. 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. The Home Office view is that this only applies where processing biometric information in a new way such as combining existing or collecting new biometric data.
9. When the processing in itself "prevents data subjects from exercising a right or using a service or a contract". The Home Office view is that this will only apply where the processing directly prevents the data subject exercising rights under Data Protection or Human Rights Legislation, or the processing actively prevents the data subjects using a service provided by or subject to a contract with the Home Office.

In the absence of any clearer guidance being available the Department's judgement of whether the specific circumstances give rise to high-risk processing will be a deciding factor. This may necessitate a referral to the HO SIRO for comment. (See section HO SIRO Referral below for more guidance on the circumstances in which a referral to the HO SIRO may be necessary).

Consultation with all relevant partners is an essential part of this process. A DPIA is not complete unless it contributes to the decision-making process, as a DPIA will lead to findings on the risks of the project, which will aid the decision maker to make a more informed judgement whether any risk can be mitigated or accepted.

A DPIA is an iterative process, and the report that you produce should be revisited throughout the project's/ policy lifecycle and at key milestones (see reviewing the DPIA section below).

Those completing a DPIA on a proposed activity, project, programme, policy or strategy may decide in some circumstances to build the issues into the regulatory impact assessment and include the partner consultation in the public consultation process. If a DPIA is carried forward in this way it needs to be noted as such in the final report and accompanied with the appropriate reasoning.

The DPIA is designed as a self-assessment process, and those conducting a DPIA, require a strong understanding of the activity itself, knowledge of privacy and an understanding of

risk assessment generally. It will be unlikely that one person will have the diversity of expertise and interests required to complete a DPIA. Hence the project, programme manager or key policy lead should gather together expertise from a number of areas, depending on the specific programme/project, policy or process.

In some circumstances, particularly where large programmes of work are planned, it may be necessary to carry out a number of DPIAs to ensure that all privacy issues associate with the programme are considered in sufficient detail. In this instance, the recommendation would be for a single DPIA to be completed for the programme, with specific process/ issue level DPIAs also undertaken and attached to the primary document. An example of this would be, if the E-Borders programme was being introduced now, there would be a single DPIA for the entire programme and separate DPIAs to cover issues including things like the collection and processing of data from carriers (new processing); the introduction of E-gates (new IT) and the sharing of personal data outside the HO (large scale data sharing).

Where programmes, projects, policies or processes overlap in terms of privacy, discussion should take place with other activities. However, the scope of any DPIA should be clear and its component parts should be listed.

As part of the DPIA process you must ensure that the activity being assessed complies with all relevant laws including the Human Rights Act. Where there is an international aspect to the policy you should also consider the privacy effect of the activity with regard to foreign and/or international law.

Reviewing the DPIA and screening document

As a matter of good practice, a DPIA should be continuously reviewed on existing processing activities. However, it should at least be re-assessed after 3 years, perhaps sooner, depending on the nature of the processing and the rate of change in the processing operation and general circumstances. Such assessment is also recommended for data processing which had taken place before May 2018 and was therefore not subject to a DPIA, to make sure that 3 years after this date or sooner, depending on the context, the risks for the rights and freedoms are still mitigated.

DPIA Content

A DPIA must include, at minimum:

- details of the business unit completing the document
- a description of the personal data being processed
- a description of the purpose for processing, including the lawful basis
- a description of the processing activity, including details of other parties involved (if appropriate)
- an assessment of the processing's necessity and proportionality.
- an assessment of risks to data subjects.
- measures to address the risks and demonstrate compliance with the legislation.

Optional for completion (as appropriate)

- a section on processing for law enforcement purposes
- a section on large scale data sharing
- a section on International transfers

Identifying and recording the benefits of the proposal

All risk assessments must include a consideration of the benefits of processing, including the benefits to individuals, the organisation, third parties and society, to enable the preservation of the desired benefits when implementing any necessary mitigations to address the identified risks. Benefits should be considered at the outset of the risk assessment as they are related to the purpose of the processing. The benefits and purposes of the processing must be kept in mind when devising mitigations to avoid unnecessary reduction of the benefits or undermining of the purposes.

Publishing the DPIA

While publishing a DPIA is not legally required, the guidelines strongly urge controllers to consider publishing all or part of their DPIAs to help foster trust in the processing operations and demonstrate transparency. This is particularly useful in cases where members of the public are affected by the processing operation, such as when public authorities carry out DPIAs.

Regardless of whether or not DPIAs are externally published, an internal record of all DPIAs must be retained, which will include instances where a DPIA was considered but not completed in full and the reasons for that. It is responsibility of each IAO and/ or DG to retain that record and make it available on request to others including the HO DPO and, if required the ICO.

Scope of the DPIA

A DPIA may concern a single data processing operation. However, ¹that “single assessment may address a set of similar processing operations that present similar high risks” (Article 35(1) of the GDPR).

Recital 92 states “here are circumstances under which it may be reasonable and economical for the subject of a DPIA to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity”.

This means that a single DPIA could be used to assess multiple processing operations that are similar in terms of the risks presented, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing. This might mean where similar technology is used to collect the same sort of data for the same purposes. A DPIA can also be useful for assessing the data protection impact of a technology product, for

example a piece of hardware or software, where this is likely to be used by different Controllers to carry out different processing operations. Of course, the Controller deploying the product remains obliged to carry out its own DPIA with regard to the specific implementation, but this can be informed by a DPIA prepared by the product provider, if appropriate.

A DPIA screening document will be necessary when sharing/ moving large amounts (1000 records or transactions) of personal data with an external body to the HO, or within the HO between Directorates. Completion of this document will ensure the appropriate level of HO sign-off for the exchange/ movement is obtained and if necessary, that a data sharing agreement is signed between parties. There is more information available on Horizon about data sharing agreements, also known as Memoranda of Understanding (MoU) and examples of a template.

Timing of a DPIA

Wherever possible the DPIA (including the screening document) should always be carried out prior to the processing.

The DPIA process should be started as early as practical in the design of the processing operation even if some of the processing operations are still unknown. As the DPIA is updated throughout the lifecycle, it will ensure that data protection and privacy are considered and promote the creation of solutions which promote compliance. It can also be necessary to repeat individual steps of the assessment as the development process progresses because the selection of certain technical or organisational measures may affect the severity or likelihood of the risks posed by the processing.

The fact that the DPIA may need to be updated once the processing has actually started is not a valid reason for postponing or not carrying out a DPIA. In some cases, the DPIA will be an on-going process, for example where a processing operation is dynamic and subject to ongoing change. Carrying out a DPIA is a continual process, not a one-time exercise.

Evaluation and Approval

Once you have identified privacy-related risks, you should evaluate their potential impact, as well as the costs and benefits of privacy enhancing options. There is, of course, a great deal of complexity to evaluating risks, costs and benefits, and it is important to remember to use both qualitative and quantitative research. Once you have clarified the risks, options, costs and benefits, you will be better situated to recommend the best way forward.

Approval and beyond

Once completed, DPIAs and screening documents should be signed off at the appropriate level. Screening documents, where no high risks are identified can be signed off by a suitably senior officer within the project or programme. Full DPIAs will always need to be signed off by the IAO (or IAOs is appropriate), seen and commented on by the DPO and in some instances by the HO SIRO, HO Data Board, or other internal Departmental

governance bodies. It is important to note that any feedback/ comment/ or recommendation made by the HO Data Board or other governance body must be shared with the DPO to ensure the DPO's advice remains accurate and relevant.

The DPO is able to provide advice on:

- whether you need to do a DPIA;
- how you should do a DPIA;
- whether to outsource the DPIA or do it in-house;
- what measures and safeguards you can take to mitigate risks;
- whether you've done the DPIA correctly; and
- the outcome of the DPIA and whether the processing can go ahead.

The DPO's advice will be recorded on the DPIA. If you don't follow their advice, you should record your reasons and ensure you can justify your decision.

DPOs must also monitor the ongoing performance of the DPIA, including how well you have implemented your planned actions to address the risks.

Completed DPIAs must be retained in line and alongside the originating project documentation, business case or other relevant documentation.

HO SIRO referral

In some circumstances, it may be necessary to refer a completed DPIA to the HO SIRO to seek guidance and comment. This must be done after the DPO has commented on the completed DPIA, because it is important that the SIRO is aware of any data protection or privacy issues that the DPO has raised.

Circumstances where the SIRO should be consulted include:

- where the DPO has raised significant data protection, or privacy issues
- where the decision has been taken by the IAO or DPO (or both) to approach the ICO for advice/ comment
- where the proposed initiative impacts on other areas of the Home Office and after consultation, those areas have raised data protection, or privacy concerns
- where the proposed initiative involves the processing of entire data processing strands, or significantly high volumes of personal data
- where the IAO (or DPO) has identified the proposed initiative as being politically, socially or economically sensitive
- where the IAO has data protection, or privacy concerns not covered by those listed above (these must be articulated fully in the SIRO referral section of the DPIA)

Effective Date	05/18
Last Review Date	25/06/18
Next Review Date	24/06/18
Owner	DID
Approved by	Head of DID
Audience	All HO Staff

Annex A – How to complete your assessment

Stage 2 Section 1

1.1 Proposal/ Project/ activity title:

Provide the name of the project, or if the activity is not a formal project, a short descriptor of what the activity consists of

1.2 Information Asset title (s):

This can be obtained from your Information Asset Register or your Data Mapping Return. If in doubt, contact your Data Protection Practitioner (DPP)

1.3 Information Asset Owner (IAO):

Provide the name, email and telephone number for the IAO, along with the title of the asset or data strand owned.

1.4 Officer completing DPIA:

Provide your name, email address, telephone number, and the unit/team you work for.

1.5 Date completed:

This is the date the DPIA is completed in full, not date completion of this form has begun. There may well be several days between the date this form is started and then completed in full.

1.6 Data Mapping reference:

All new processing activities must be captured on the respective IAOs data mapping return. Wherever possible, it is advisable to make note the relevant entry details including unique number in this section. In some cases, an entry on the mapping return will already exist. However, if this activity is a new purpose for processing, a new lawful basis for that processing, or new personal data is being processed as a result of this activity, then a new entry on the return may be required. If any of these are the case, this must be agreed with your DPP.

1.7 Version:

Ensure all versions of this document are kept until such time as approval to proceed has been obtained (or otherwise). Once approved, only the final version must be retained in line with the retention period for all other documentation relating to the associated project or activity.

1.8 Linked DPIAs:

In the event a significant Programme requires more than one DPIA, you must ensure all associated DPIAs are cross referenced.

1.9 Publication date:

Provide the date of when the DPIA was published.

Wherever possible DPIAs should be made public, unless there is a business/operational reason why not. GDPR guidelines strongly urge controllers to consider publishing all or part of their DPIAs to help foster trust in the processing operations and demonstrate transparency. This is particularly useful in cases where members of the public are affected by the processing operation, such as when public authorities carry out DPIAs.

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

Section 2 (personal data)

2.1 What personal data is being processed?

List all personal data fields that will be processed
E.g.: name, DoB, address etc.

2.2 Does it include 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

Please answer yes or no.

Special category (Article 9 of the GDPR) and criminal conviction (Article 10 of the GDPR) data is personal data which the legislation says is more sensitive, and therefore needs more protection. In order to lawfully process special category data, you must identify both a lawful basis and a separate condition for processing special category data. These do not have to be linked. See section 3 questions 3.2 and 3.3 below.

To process criminality data, you must either be processing the data in an official capacity, or have specific legal authorisation – which means a condition under the Data Protection Act and compliance with the additional safeguards set out in the Act).

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

Answer yes or no. If no, move to 2.5

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

Examples may include seeking explicit consent from the child or legal guardian, anonymisation or redaction, or limiting access to and/or amount of data processed. If no additional safeguards are planned please explain why.

2.5 Will data subjects be informed of the processing?

Please answer yes or no. If yes move to 2.7.

Unless an exemption to the legal requirement under GDPR Article 13 (data gathered directly from the data subject) and Article 14 (data gathered from a third party) to notify data subjects how their data will be used applies, then data subjects affected by the processing described in this document must be informed it is taking place. In most instances for the HO this will have already been done, in the form a Personal Information Notice (PIN) issued to the data subjects at point of original data collection.

You will need to confirm that your current PIN covers the processing activity described in this document and if not, you will need to consider informing the data subjects separately, unless an exemption to that requirement exists.

2.6 (If no) Why not?

In all instances data subjects must be notified how their data is being processed, the only exception to this is where an exemption to that requirement applies. If there is an exemption for this processing activity, details of which exemption applies and how must be detailed here.

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

Provide detail the methods that will be used to inform data subjects on how their data will be processed

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

Please include full details of who within your unit/team/directorate (or wider) will have/obtain access to information processed as a result of the activity described in this document.

2.8 (b) And how will that access be controlled?

Describe what controls are in place to manage that access
e.g. password protection folders, controlled (by permission) access only etc.

2.9 Where will the data be stored?

Please provide details of where the data will be physically stored, including paper and electronic e.g. on an access data base, recorded on a case working system e.g. (for immigration) CID etc.

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)?

Please answer yes or no. (If no, state why and move to 2.12)

Unless an exemption applies to these data subject rights, we must have the physical capacity to erase, rectify, suspend processing of and provide access for individuals to

their personal data. If an exemption to that right applies to the processing detailed in this document, please provide details here.

2.11 (If yes) provide details of how these requirements will be met?

Please provide conformation here that these rights can be met by the Department in respect of this processing activity. Input from a technical expert including DDaT or, if appropriate, external suppliers may be 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?

Please provide details of the retention period for the data. This may be a new retention period designed solely for the processing activity described in the document, or it may be in-line with existing retention periods.

Please also provide information on how the data will be monitored through the rest of its lifecycle through to deletion or transfer for permanent preservation. If software is being used, is that software capable of adhering to existing retention periods (if appropriate)?

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

Please provide details of the physical method of data transfer e.g. email, post etc

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

Please provide details of how the data will be secured during the transfer process e.g. encrypted file by email, secure data transfer portal etc. If by post, first class or signed for.

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

Please answer yes or no. If the answer is yes, provide details.

You will need to list what new data is being processed and the source of that data. Also confirm the following:

- If the data is from a third-party other than the data subject, what is the lawful basis for the third party providing that information and does the third party's PIN provide for the provision of that data? (or does an exemption to that requirement exist? if so please list)
- If the new data emanates from the data subject does any existing PIN cover the collection of that data for this purpose, or is a new notice required? In addition
- Whether a new (i.e., different from the original) lawful basis for the processing applies, and if so, what it is?

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

- OFFICIAL (including 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)

Provide a brief but succinct summary of the proposed processing activity, and the resource required.

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

If the lawful basis for processing the data is the consent, please confirm whether the consent already given by the data subject(s) allow for this processing? If not, new explicit consent for this processing will have to be obtained. You will need to look at the terms of the consent provided by the data subject(s) to make this assessment. If the lawful basis for processing is not consent, does the existing PIN cover this form of processing? If not, you will need to consider providing a new PIN to the data subject(s). For more information contact [REDACTED]

3.3 If processing special category data (see 2.3 above), what is the condition for processing? (Choose an option from the list)

Whilst there will still be the initial lawful basis for your processing, there is also a requirement for a second specific lawful basis for the processing of special category data. The initial lawful basis does not dictate which special category condition you must apply, and vice versa. You should choose whichever special category condition is the most appropriate in your particular circumstance.

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

Please answer yes or no.

It is important to understand whether the proposed processing activity is associated to the original purpose for processing to establish whether or not the legal basis for processing has changed, as this is a requirement under DP legislation.

E.g. if the original purpose for processing the data in question was to assess an application for a UK passport and the processing activity described in this document is to assist in the process by introducing a new tool to streamline the application process, or you wish to share information to assist in assessing entitlement to a UK passport, then the purpose for processing is commensurate with the original purpose. You will be able to identify the original purpose for processing and legal basis from your data processing mapping return maintained by your DPP.

(If no) What was the original purpose and legal basis?

Original purpose: (see 3.1 for the description)

Legal basis: (see 3.2 for the description)

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.

Please answer yes or no. If the answer is yes move to 4.3.

Examples of this will include introducing new automated tools or processes to increase efficiencies, or replacing existing automated tools with new ones.

E.g. currently individual (case by case) validation checks are made of another government department, the proposal is to semi-automate that process and increase the volume by sending larger volumes in a single transaction.

4.2 Is the processing a new activity?

Y/N (Is the processing activity brand new? E.g. post EU exit there may be a requirement to collect data on EEA Nationals for the first time in support of a new application process; this will be a new activity with a new legal basis).

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

The higher the volume the higher the risk associated with the processing, therefore it is important to be accurate with the figures provided. If it is envisaged that the volume of personal data being processed will significantly increase

E.g. the activity described is a pilot exercise as a forerunner of more significant activity then this document will need to be updated as necessary.

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

Provide details on the frequency. If the intention is to run a pilot or 'test' on a small amount of data, but then move to larger scale processing in the event the pilot or test exercise was successful, you will need to revisit this document and create a new or updated version with details of the increased volumes and frequency concerned.

Frequent is defined as at least monthly; regular is defined as on an ongoing (e.g., daily/weekly/monthly basis).

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)

Please answer yes or no. If no, move onto 4.9.

The answer will only be no if the unit/team/directorate completing this document is the sole body engaged in the activity outlined in this document.

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

Please answer yes or no.

If another part of the HO is either supplying the data or is a recipient of the data then the respective IAO must participate in the completion of this document and their details includes in section 1.3. The HO Group includes all Directorates but not ALBs

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

Please answer yes or no.

Provide brief details here and then ensure Section 6 is also completed. Public authorities include central and local government, Arm's Length Bodies and Independent Inquiries

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

Please answer yes or no.

Provide brief details here and then ensure Section 6 of this document is completed. Private sector bodies include credit reference and fraud prevention agencies and any other body not directly reporting to, or the responsibility of a government authority

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

Please answer yes or no. If no move to 4.11.

The transfer of data includes data in transit and not just the country of destination and where third-party processors are employed by any of those parties engaged in the processing activity detailed in this document.

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

List all the non-EEA countries engaged in the processing activity detailed in this document.

4.10 Is the processing for law enforcement purposes?

Please answer yes or no. If the answer is yes, you will need to complete Sections 5.

Law enforcement processing is defined as: 'Processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' and for this definition to apply, the primary purpose of processing activity detailed in the document must be for law enforcement only.

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

Please answer yes or no.

On the ICO's website Profiling is defined as: "automated processing of personal data to evaluate certain things about an individual". Under the new legislation there are additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them. More information on [profiling and automated decision making](#) can be found on the ICO's website.

4.12 Does the proposal involve automated decision making?

Please answer yes or no. If yes, provide details.

Automated decision making is a decision made solely automatically with no human intervention. In the [profiling and automated decision making](#) guidance, the ICO states: You can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract,
- authorised by Union or Member state law applicable to the controller, or
- based on the individual's explicit consent

4.13 Does the processing involve using new technology?

Please answer yes or no. If the answer is no, proceed to question 4.15.

New technology means totally new technology and not reusing or extending the use of existing technology

e.g. introducing a new tool to capture and record biometric information

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

In the event that new technology is being deployed, you will need to confirm that the appropriate accreditation for its use has been obtained and the HO Security has been consulted. In addition, if a third-party supplier is being used, a formal written contract is required.

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

Please answer yes or no. If yes, explain how that is being achieved and move to 4.18.

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

The legislation requires controllers to consider consulting directly with data subjects on issues relating to the processing of their personal data that may constitute a risk to that data. If, as a controller, the HO opts not to consult, the reasons for not doing so must be recorded

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.

Benefits:

How will they be measured?

Benefit(s) Owner (in HO):

Beneficiaries

This could include efficiency and/or resource savings, improved customer service, compliance with a legal obligation etc. It is important that the business benefits associated with the processing detailed in this document and that you also have a robust method to record and report on those benefits. You will need to list all those who will benefit from the activity both internal and external to the HO. In some cases, this will help to justify that the activity is proportionate.

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?

Please answer yes or no. If yes, provide details and carry on to question 4.18.

While it is expected that the majority of risks to personal data that may be associated with the processing described in the document will have been identified, it is possible that some might not, therefore it is important to list any other risks that have been identified by the project/programme/initiative owner at this stage.

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

Section 5 (Processing for law enforcement purposes)

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

Please answer yes or no. If the answer is no, move to 5.4.

Where the purpose for processing has changed from the original purpose for processing, the justification for that must be documented, as quite often the change in purpose, will also mean a change in other aspects including lawful basis, retention periods and Information Asset Owner.

5.2 (If yes) What was that purpose?

In this section please also include details of previous legal basis. This information will be available on the data mapping return held by your DPP, or the DPP operating for the previous IAO.

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

Please answer yes or no. If yes, provide details.

If the data was previously being processed by another part of the HO, this information will be available on the data mapping return held the DPP operating for the previous IAO. It is important that if more than one IAO has responsibility for - or a vested interest in - an information asset, that they are engaged in the DPIA completion process to ensure their respective roles and responsibilities in terms of retention periods, access control and provision of subject access rights are clear.

Where data is being processed for law enforcement purposes, exemptions to some data subject access rights may apply and it is therefore important that data, subject to exemptions is clearly identifiable to those responsible for servicing those rights. If the data was previously being processed by another Controller, it is important to be clear on what (if any) responsibility that Controller retains in respect of that data. It may be that in processing the data for the purposes detailed in this document, the HO becomes the sole controller for the data in question. Equally, the HO may become a joint Controller. This relationship must be clarified and articulated in any formal written agreement that is created to manage the transfer of the data in question.

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

Please answer yes or no. If no, move to 5.6.

If any new data is being processed as a result of the processing activity detailed in this document, it is important to ensure that any PIN already provided to the data subject(s) covers the processing of this 'new' data. If not, a new PIN may be required unless an exemption to the legal requirement to notify the affected data subjects exists.

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

New data: Provide full details of what the new data consists of.

Source: Confirm the source of the data

Lawful basis: What is the lawful basis (*see 3.2 above) for processing the data for this purpose? If the data includes special category information a condition for processing must also be listed (*see 3.3 above).

5.6 Where will the data be stored/retained?

(*See 2.9 and 2.10)

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

Please answer yes or no. If yes, move to 5.8.

When processing personal data for law enforcement purposes it is a legal requirement of the new DP legislation that any electronic system used to process data must have a logging capability. This means that provision must be made to audit the following activity, with specific reference to personal data: Create; Read; Update; Delete; Export; Reporting; Search and Transfer,

For systems in use since May 2016 that logging requirement is immediate. For systems in use prior to May 2016, the logging requirement is deferred until May 2023. If all records are being maintained in hard copy paper form, this obligation does not apply.

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

See above. Full details must be provided on what action is planned to address this issue, including time frames or if none is scheduled and the mitigation for non-compliance.

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)

Please answer yes or no. If yes, move to 5.9.

When processing personal data for law enforcement purposes it is a legal requirement of the new DP legislation to have the ability distinguish between categories of personal data.

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

Full details must be provided on what action is planned to address this issue, including time frames or if none is scheduled, and any mitigations for potential non-compliance.

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

Please answer yes or no. If yes, provide details of what the risks of that intrusion are and how that intrusion is justified.

Examples include, but are not limited to: radio frequency identification (RFID) tags, biometrics, facial recognition, locator technologies (including mobile phone location), applications of global positioning systems (GPS) and intelligent transportation systems, visual surveillance, digital image and recording, profiling, data mining, and logging of electronic traffic.

Section 6 (Data Sharing)

6.1 External contact details for data exchange

Name:

Grade:

Organisation:

Business Unit/ Area:

Contact email:

Contact telephone:

Name:

Grade:

Organisation:

Business Unit/ Area:

Contact email:

Contact telephone:

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

(*See 2.9 and 2.10)

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

(*See 2.9 and 2.10)

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

Please answer yes or no. If no, provide details why a formal written agreement is not required and move to 6.6.

You must include confirmation that the relevant team responsible for MoUs in your area has been consulted and their agreement has been obtained that no new data sharing MoU is required.

Teams to be consulted include:

- Domestic Data Sharing – [REDACTED]
- International Data sharing [REDACTED]
- BF Intelligence – Border Force
- HMPO – [REDACTED]
- An example of a data sharing MoU can be found on Horizon

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:

Grade:

Business Unit/Area:

Contact email:

Contact telephone:

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

Please answer yes or no. If yes, please provide the identity of the processor and confirm details of that arrangement will be included in the data sharing agreement.

Where another body is engaged with the processing of data supplied by the HO, as the originating controller we retain an obligation to ensure that activity remains compliant with the legislation.

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

Please answer yes or no. If no, explain why HO Legal Advisors have not been consulted.

6.8 Provide a summary of the legal advice received

The information entered should provide a sound overview of the advice given.

Technical impact and viability

6.9 Which of the following reflects the data exchange?

Data Extract	Y/N
Data Matching	Y/N
Data Reporting	Y/N
Data exchange/ feed	Y/N
Direct Access	Y/N

6.10 Has any analysis or feasibility testing been carried out?

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

6.11 (a) Is development work is required and (b) will there be a fiscal cost?

(a) Please answer yes or no. If yes, provide details including time frame.

(b) Please answer yes or no. If yes, provide cost details.

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

Please answer yes or no. If no, move to 6.14.

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

Please ensure that your answer is clear and easy to understand

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?

Please answer yes or no. If yes, move to Section 7.

In this section confirm that you have read the associated guidance and consulted with HO Security if necessary).

a) If the answer is no, what needs to happen to ensure that adequate security arrangements are achieved?

Please ensure that your answer is clear and easy to understand

Section 7 (International transfers)

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

Please answer yes or 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.

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

Please answer yes or no. The list of countries is available on the [European Commission](#) website.

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

Options:

- 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 of 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?

Please answer yes or no. If yes provide details and move to 7.4.

Advice on how to carry out an [OSJA assessment](#) is available on the Gov.UK website.

a) If no, provide details of when one will be completed and by whom?

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

Please answer yes or no. If no, skip 7.4 a).

If the HO transfers personal data to a third country which does not have the benefit of an adequacy decision, the MoU must contain safeguards, and the MoU will need to be authorised by the ICO – see A46(3) of the GDPR.

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

Please answer yes or no. If no, you will need to consider reviewing the existing agreement to include the new processing activity.

I) If yes, 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?

Please answer yes or 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

This is the date the completed DPIA was sent to the DPO.

8.2 Comments/ recommendations

Full comments and any recommendations by the DPO.

8.3 Completed by

Name of the person in the ODPO who made the comments/recommendations.

8.4 Date returned to the business owner listed in Section 1

This is the date the DPOs comments and recommendations are returned to the business owner listed in Section 1.

8.5 Date re-referred to the DPO

To be completed and repeated as necessary.

8.6 Comments/ recommendations

8.7 Completed by

Name of the person in the ODPO who made the comments/recommendations

8.8 Date returned to the business owner listed in Section 1

Provide the date that it was sent to the business owner

Section 9

9.1 Date referred to the SIRO

This is the date the completed DPIA was sent to the SIRO.

9.2 Referred by

Name of the person making the referral.

9.3 Reason for referral to the SIRO

Full reason for referral to SIRO, this must include a summary of the issues and any specific questions being asked of/ advice being sought from the SIRO. This includes directions to relevant parts/section of the DPIA if required.

9.4 Comments/ questions/ recommendations from SIRO

Full comments and any questions from/ recommendations by the SIRO

9.5 Completed by (SIROs' details)

Details of officer completing 9.3 including if the SIRO, or someone else commenting on behalf of the SIRO (e.g. a Deputy)

9.6 Date returned to the business owner listed in Section 1

This is the date the SIROs comments and recommendations are returned to the business owner listed in Section 1.

9.7 Action taken by business owner listed in Section 1

Full details of any actions taken as a direct result of the comments made/ questions raised/ recommendations proposed by the SIRO including re-referral to the SIRO if necessary.