Home Office

ODPO URN: 70.19

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. Stage 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 in particular 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

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.

Does the processing activity include any of the following?

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.

Yes

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

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

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

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

Yes

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).

No

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

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

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

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).

Stage 2

Section 1

1.1 Proposal/ Project/Activity title:

DPIA – Criminal Casework Radio Frequency/Global Positioning System Dual Tag Transition

1.2 Information Asset title (s):

GPS Satellite Tracking Dataset, owned by Ministry of Justice

1.3 Information Asset Owner/s (IAO):

Email: [REDACTED]
Name: [REDACTED]
Telephone Number:
Information Asset title: GPS Satellite Tracking Dataset

Email:
Name:
Telephone Number:
Information Asset title:

Email:
Name:
Telephone Number:
Information Asset title:

1.4 Officer completing DPIA:

Email: [REDACTED]
Name: [REDACTED]
Telephone Number: [REDACTED]
Business Unit/ Team: Satellite Tracking Services Programme - Business Change

1.5 Date completed:

29.08.2020

1.6 Data Mapping reference:

TBC

1..07 Version:

003

1.8 Linked DPIAs:

N/A

1.9 Publication date:

The Home Office does not routinely publish DPIAs, as there is no legislative requirement to do so. This does not mean we would not make it available to the regulatory authority should the need arise – that being the Information Commissioners Office. We will also consider any request for publication received 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?

Daily Monitoring of individuals subject to immigration control who meet the criteria for wearing a GPS tag - each tag wearer will be uniquely identified by virtue of a HO reference number or Person Identification Number, and supplier tag reference number. Original data monitoring request will include individuals Name, DOB, Nationality, Photograph.

Individuals will be tracked 24/7 allowing trail monitoring data to be recorded. This is in line with Schedule 10 (4) Immigration Act 2016. Individuals can be identified by the supplier and HOIE as the data is linked to them as the person being monitored.

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

Yes - Nationality, Home Office reference number, Person Identification Number, Case ID number, PNC number, Criminal History. Multi Agency Public Protection Arrangements harm and management levels. Vulnerable adult details (of a physical or non-physical nature which have a bearing on the decision to impose a tag. IE a skin condition that is

not compatible with a fitted tag. Risk assessment details for STS purposes and HARM Score details (*This list is not exhaustive and will be further governed by specific details relevant to each individual on a case by case basis contained within the Electronic Monitoring Order form*). Criminal Conviction data will be provided to Electronic Monitoring Services (EMS) the existing supplier, for the protection of supplier employee's and public at large, especially when fitting/removing devices from FNOs.

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

No (if no move to 2.5)

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

N/A

2.5 Will data subjects be informed of the processing?

Yes (if yes move to 2.7)

2.6 (If no) Why not?

N/A

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

They will be notified at induction and given a Home Office letter that will explain, in full, their rights responsibilities and requirements. This will be in the form of a standard induction letter handed in person to the wearer by the supplier field officers. The information will also be available online. However the wearer will have to sign a statement to say they have had the induction notice explained and that they understand.

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

Electronic Monitoring Hub caseworkers and manager. This data may in turn be shared to appropriate HO departments under part 2 data sharing, upon evidence of a Breach of Immigration Bail Conditions. Essentially this will be Roles Based Permissions Access.

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

Password and 'Permissions' controlled access to data systems and shared folders. These will be maintained in compliance with current data storage and retention policies.

2.9 Where will the data be stored?

Immigration Enforcement encrypted data storage and EMS data storage as the existing third-party supplier under the contract awarded by MOJ.

The data is stored by EMS on their internal servers and HOIE do not have access to their systems. Immigration Bail Condition Breach data is forwarded to HOIE on a daily basis for us to be able to manage the breaches. It is received in PDF format and data is transferred to the Case Information Database (CID) and dually onto the Atlas system service until CID is de-commissioned in 2021 whereupon the data will be transferred soley onto the Atlas system on the Immigration Bail Condition Breach screens of the individual.

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 including, erasure, portability, suspension, rectification etc.?

Yes

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

EMS is the existing supplier and the requirements have not changed for the Transition exercise. The data can be manually accessed, extracted , archived accordingly.

2.13 How will data be deleted in line with the retention period and how will that be monitored?

Both MOJ and Home Office will adhere to their individual organisation's information security policies and procedures in regards to handling data.

Records management and retention shall be in line with agreed protocols already in place for radio frequency tagging. Records will be archived every 3 months.

This will be monitored by data assurance audit.

2.14 (a) (If physically moving/ sharing/ transferring data) How will the data be moved/ shared?

See 2.9

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

Both MOJ and Home Office will make themselves aware of, and adhere to, their organisation's information security policies and procedures in regards to handling data in a manner appropriate to the assigned HMG Security Classification tier;

Make themselves aware of, and adhere to, their organisation's record management policies and procedures specifically in relation to collecting, processing and disclosing personal information;

Store and dispose of information, whether in hardcopy or electronic format, in line with their Department's retention and disposal policies;

Take responsibility for preserving the integrity of the information they hold and take reasonable steps to prevent the corruption or loss of the data. This will be monitored by data assurance audit.

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

Yes. New data will be GPS trail Data.

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

Official (including official sensitive)

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

What is the current position:

There is an existing, and has been for 10+ years, tagging process whereby Foreign National Offenders are placed on a tag and are subject to curfews. Any breaches of those curfews are considered a breach of Immigration Bail and sanctions can be taken against the FNO. The Ministry of Justice are the contract owners and Electronic Monitoring Services are the service suppliers. Criminal Casework manage their FNOs through tagging and EMS provide data direct to CC to respond to any Immigration Bail Condition breaches. It is a smooth process and has been in place a long time. Legal challenges of different forms have come and gone and the tagging process continues.

What is changing now (Current DPIA):

The supplier remains the same. The service remains the same. The criteria for tagging is considered on a case by case basis. The type of device that we are using is changing from Radio Frequency to GPS. The existing policy has been changed to allow this and Policy and Home Office Legal Advisors have confirmed our approach. The new device allows us to retain current curfews should the case still require it but also and/or separately provide HOIE with GPS tracking data (known as trail monitoring). GPS tracking will trace and record the locations of all wearers at all times and will be held by the supplier. We believe the use of GPS including 'Trail Data' is in line with the original intent of Electronic Monitoring referred to within Schedule 10 (4) of the Immigration 2016 and that it's use is compatible with the overall aims of effective immigration control. Data detailing the number of 'tagged' cases will be presented on a report known as the Police Dashboard. It will only show high level data Name Nationality DOB Address. It will not show any trail data or breach data. This data can be accessed by MOJ, IE and Police via permissions operated by MOJ. (see Accessing Data) The sharing of this data to police colleagues is not new. IE currently share these details with police on a Police Risk Notification Form in all cases where an FNO is released from detention into the community. It is just that it will also be presented to police in this new format. This will provide a clearer picture for data analysis for IE MOJ and Police, given that the number of tag wearers is expected to rise from 280 to 4500.

Accessing the Data

Data informing MOJ HO and the Police of 'tagged' cases will be presented on a report known as the Police Dashboard on 'Power BI'.
Power BI – is a data visualisation tool by Microsoft, hosted on cloud platform (Microsoft Azure).

The MOJ operate and maintain the Police dashboard.It will display all details of evey IE tag wearer in UK and will be updated weekly by MOJ, after receipt of data from the third party supplier ‘EMS’.
Details include Name, Nationality, DOB, Full Address and type of tag. The sharing of this data to police colleagues is not new.
IE currently share these details with police on a Police Risk Notification Form when an FNO is released from detention into the community.
Its just that the data can now be centralised, collated and analysed easier. It is also anticipated that as the new legislation is enacted the number of tag wearers will rise significantly from 280 to approximately 4500.
MOJ do not create exported reports and circulate. IE STS staff and Police colleagues will have direct access to the dashboard, which is done via permissions. This means no unauthorised personals with the link is able to view the dashboard until MOJ have approved this. However, please note that IE and Police colleagues can export the dashboard in PDF / PowerPoint format if desired once granted access.
The GPS Trail data will not be routinely monitored at all.
However authorised Home Office staff may request access to GPS trail Data for a specified period (not limited) and review that data in the event of either of the following occurances :-

- **Breach of Immigration Bail Conditions**

In the event of a notification of a qualified breach of Immigration Bail conditions from the supplier, authorised Home Office Staff may perform a full review of the bail conditions and ask the individual wearer for any mitigation for the breach. The review consideration may be informed by the mitigation supplied and the review of the full trail monitoring data records where proportionate and justified.
If, during the course of the review of the trail data, it becomes apparent that further breaches of immigration bail conditions may have been/ are being committed (e.g. Trail data provides a strong indication that subject is working in breach – showing them at a specific location other than home between 08:00 – 17:00 hours) then that data may be shared within the Home Office e.g. Immmigration Intel where proportionate and justified to investigate for further possible immigration breaches, under Part 2.
If, during the course of the review of the trail data, by the HO, there is any other indication that criminal activity is or has taken place then that data may be processed and shared with Law Enforcement agencies under Part 3.

- **Individual Absconds**

If the individual wearer loses contact and effectively ‘absconds’. Authorised Home Office staff may access the full trail data in order to try and ascertain the current whereabouts of the individual in order to arrange possible arrest and detention under immigration powers. Data processed under Part 2.

- **EAR Requests**

Where a legitimate and specific request is made for access to specific data by a Law Enforcement Agency. We may process and share under Part 3.

- **Article 8 Representations / Further Submissions**

In the event of the receipt of Article 8 representations or further submissions from the individual, authorised Home Office staff dealing with those submissions may request access to the full trail data to support or rebut the claims. This will hopefully negate the need to request 'substantiating' evidence from third party's which can cause unnecessary delays in considering the claims.

- **Allegations of EM Breaches or Intelligence of Immigration Bail Condition Breaches Received**

In the event of Home Office staff receiving either of the above, Home Office staff may request details of full trail data to cover a specific period relating directly to the allegations or intelligence.

- **Subject Access Requests or Legal Challenge**

In the event of either of above being implemented Home Office staff will comply with legal process and timelines for provision of data.

What is changing in 2021 (future DPIA):

We will be introducing new tag types and volumes. An updated DPIA will be required and one that links back to the manifesto pledge. New legislation is to be enacted in 2018. It is anticipated that is going to go live in Mid 2021.

3.2 What is the lawful basis for the processing? (choose an option from the drop-down menu opposite)

Performance of a public task

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

Substantial Public Interest

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

Yes, however we retain the right to pass on information under part 3 of the Act for public protection purposes. See section 4.11 (If no) What was the original purpose and legal basis? Original purpose: (see above) Performance of a public task Legal basis: (see above) Public Interest

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 (if the answer is yes move to 4.3)

4.2 Is the processing a new activity?

N/A

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

Unknown at this stage but at least 250 individual records, although transactions is a variable based on the compliance and breach levels of the 250. It will be a minimum of 250 but will likely be higher.

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

Regular daily tracking of individuals who satisfy the criteria for inclusion in the programme.

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

4.6 Is the other party another part of the HO group which the Secretary of the State for the Home Department is the controller? If yes provide details

Yes - in some instances when shared with IE (including Prosecutions Team)/ UKVI/ Border Force Intel Team and the police.

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

Yes – Ministry of Justice

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

Yes – EMS as the existing supplier for MOJ

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 4.11)

4.10 (If yes) Provide brief details of the country (ies) and also complete section 7 (International transfers)

N/A

4.11 Is the processing for law enforcement purposes?

The primary purpose of the processing is to track and record the location of individuals in order to support immigration control.

In developing this project we are clear from the outset that there is likely to be the following types of processing:

- In all cases, processing to track and record the location of individuals in order to support immigration control. This includes monitoring of Immigration Bail Condition Compliance. Such processing is done by the HO under Part 2 DPA 2018.
- In a subset of the above cases where the individual breaches their Immigration Bail conditions a Breach Report Review will be created and prosecution for the criminal offence of breach of Immigration Bail will be considered by HOIE, and where the threshold is met a prosecution will be conducted in a timely manner. All such processing will be done by the HO under Part 3 DPA 2018.
- In another subset of the first group in some cases the collection of the data for the Part 2 purposes will incidentally reveal potential criminal activity (other than Immigration Bail breaches). Once this becomes apparent then the information may be made available

to or shared with Intel units or Law Enforcement agencies for the prevention or detection of crime. At this point the information will be shared under Part 3.

The operational processes have included a step to ensure that a consideration must be given to the purposes of the processing on each case and whether it has moved from Part 2 to Part 3.

The HO publication Determining the Right Regime (v2.0 Januray 2019), owned by the Data and Identity Directorate, sections 2.5 to 2.9 refer.

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

No

4.13 Does the proposal involve automated decision making?

No

4.14 Does the processing involve using new technology?

Yes – moving to the use of dual enabled RF/GPS devices

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

GPS Tracking capability to monitor movements of wearer 24/7. EMS as the existing supplier will provide the new dual enabled devices as used by MOJ.

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

No

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

Individuals who meet the criteria for tagging will be informed explicity regarding the use of the data collected and how it will be processed. During a formal induction process.

Benefits

4.18 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): Benefits Realisation Package/ Report underway

How will they be measured? Data will inform Strategic thinking of breach and compliance activities.

Benefit(s) Owner (in HO): [REDACTED]

Beneficiaries: Criminal Casework/ Immigration Enforcement, Public Protection

Risks

4.19 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?

No

4.20 (If required) What steps have been taken to mitigate the risks listed at question 4.19 above? We have ensured the presence of strict security protocols and have monitoring systems in place to test compliance.

Section 5 (Processing for law enforcement purposes)

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

Y/N (if the answer is no move to 5.4) No

5.2 (If yes) What was that purpose?

Y/N (if the answer is no move to 5.4) N/A

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

Y/N ((if yes provide details) N/A

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

Y/N (if no move to 5.6) Y

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

New data: GPS Daily Monitoring/ movement of individuals subject to immigration control
Source: GPS Tracking Device/Tag
Lawful basis: (*see 3.2 above)

5.6 Where will the data be stored/retained?

(*See 2.8 and 2.9) Within current Home Office encrypted storage systems and EMS/MOJ systems.

5.7 (If being stored electronically) Does the system have logging capability?

Yes, HO systems and EMS/MOJ systems.

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

N/A

5.9 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

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

N/A

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

Yes, Full movement monitoring to allow for effective control to removal.

Section 6 Data Sharing

6.1 External contact details for data exchange

Name: [REDACTED]

Grade: [REDACTED]

Organisation: Electronic Monitoring Services (EMS)
Business Unit/ Area: Special Cases
Contact email: [REDACTED]
Contact telephone: [REDACTED]

Name: [REDACTED]
Grade: [REDACTED]
Organisation: Electronic Monitoring Services (EMS)
Business Unit/ Area: Special Cases
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) For 6 years from the point the individual is removed from the tag.

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

(*See 2.8 and 2.9) In line with existing EMS/MOJ data destruction policies as referred to in 13.1 of the MOU

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

Y/N (If no, provide details why a formal written agreement is not required and move to 6.6) An MoU is already in place dated 16/3/18 as agreed by [REDACTED] and [REDACTED]. This is now under review and will be signed off between HO STS Director and HO Senior Commercial Manager. The new MOU is expected to be completed by November 2020.

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: See 6.4
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?

Y/N (If yes, please provide the identity of the processor and confirm details of that arrangement will be included in the data sharing agreement) No

Technical impact and viability

6.7 Which of the following reflects the data exchange?

Data Extract	Yes
Data Matching	Yes
Data Reporting	Yes
Data exchange/ feed	Yes
Direct Access	Yes

6.8 Has any analysis or feasibility testing been carried out?

Y/N (If yes, provide details, if no, explain why it is not required). No – process has existed for over 10 years.

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

(a) Y/N (If yes provide details including time frame) No
(b) Y/N (If yes provide cost details) No

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

No (If no move to 6.14)

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

N/A

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

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

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

N/A

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)

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

7.3 (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.

7.4 (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?

7.5 (If no) Provide details of when one will be completed and by whom?

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

Y/N (If no, go to 7.9)

7.7 (If yes) Does the agreement cover the purpose(s) for which you need to share data?

Y/N (If no, you will need to consider reviewing the existing agreement to include the new processing activity)

7.8 (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?

Y/N (If yes move to section 8)

7.9 (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

10/09/2020

8.2 Comments/ recommendations

Please review comments and resubmit for a further review.

8.3 Completed by

[REDACTED]

8.4 Date returned to the business owner listed in section 1

10/09/2020

8.6 Date referred to the DPO

10/09/2020

8.7 Comments/ recommendations

Review complete subject to the recommendation that HOLA are re-engaged re: Part 3 processing reference at section 4.11.

8.8 Completed by

[REDACTED]

8.9 Date returned to the business owner listed in section 1

10/09/2020

8.6 Date referred to the DPO

18/09/2020

8.7 Comments/ recommendations

Review complete with no further comment.

8.8 Completed by

[REDACTED]

8.9 Date returned to the business owner listed in section 1

18/09/2020

8.10 Date referred to the DPO

22/09/2020

8.11 Comments/ recommendations

Review complete with no further comment.

8.12 Completed by

[REDACTED]

8.13 Date returned to the business owner listed in section 1

22/09/2020

Section 9

9.1 Date referred to the SIRO

9.2 Referred by

9.3 Reason for referral to the SIRO

9.4 Comments/ questions/ recommendations from SIRO

9.5 Completed by (SIROs' details)

9.6 Date returned to the business owner listed in section 1

9.7 Action taken by business owner listed in section 1

Any suggestions for improvements or comments on this template should be directed to [REDACTED]

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**