

Data Protection Impact Assessment (DPIA) Template

Proposal/ Project/Activity title	Satellite Tracking Services (STS) GPS Electronic Monitoring Full DPIA.
Information Asset Owner(s)	

Document Control

	Name	Job Title	Date
DPIA Drafted by			19/08/21
Reviewed by			
Lead DPP for business area			
Lead business owner /project manager/policy owner			

Version/Change history

Version	Date	Comments
Draft 0.1		First draft
Draft 0.2		
Draft 0.3		
Draft 0.4		
Final 1.0		
Final 1.1		
Final 1.2		

Approved by (Information Asset Owner (IAO) or person acting on behalf of the IAO):

IAO approval is only required if Stage 2 of this template is completed. Project manager sign off is sufficient if the questions outlined in Stage 1 are answered in negative.

Name	Title	Date

Contents

Data Protection Impact Assessment (DPIA) Template..... Error! Bookmark not defined.

Document Control	2
DPIA Stage 1	4
DPIA Stage 2	7
Section 1: Background and contacts	7
Section 2: Personal Data	8
Section 3: Purpose of the Processing.....	13
Section 4: Processing Activity.....	18
Section 5: Risks of the Processing	21
Section 6: Data Sharing/Third party processing	21
Section 7: International transfers	24
Section 8: Referral to ODPO.....	26
Section 9: Referral to Data Board	27

Guidance on when and how to complete this template is provided in the Data Protection Impact Assessment (DPIA) Guidance on Horizon – **this guidance should be read before completing the DPIA.**

DPIA Stage 1

Summary of the processing

- 1. Does the proposal/project/activity involve the processing¹ of personal data, or is new legislation which relates to the processing of personal data being considered?²**

☒ Yes

☐ No

If the answer to this question is 'No', then the rest of the form does not need to be completed. If the answer is 'Yes', please continue.

- 2. Does the proposal/project/activity involve any of the following?**

- a new way of processing personal data
- the use of a new form of technology for a new or existing process
- new legislation which relates to the processing of personal data being considered
- substantial changes to an existing project/programme/processes involving personal data, which would include a significant increase in the volume or type (category) of data being processed

☒ Yes

☐ No

If the answer to this question is 'No', then the rest of the form does not need to be completed. If the answer is 'Yes', please continue.

- 3. What is the purpose of the processing?** Provide a brief (up to 100 words) description of the processing activity e.g. sharing with a third party; storing data in a new way; automating a data processing activity; developing a new policy that requires new legislation or amendments to existing legislation etc.)

[NB: this question is repeated at 3.1 at which point you can add more detail/ background.]

Daily Monitoring of individuals subject to immigration control who meet the criteria for wearing/carrying a GPS Electronic Monitoring Device. This device can be in the form of a Fitted Ankle Tag or a Non Fitted Device – a smartwatch that the

¹ In relation to personal data, means any operation or set of operations which is performed on personal data or on sets of personal data (whether or not by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).

² Data protection legislation applies to 'personal data' which is defined as any information which relates to a living identifiable person who can be directly or indirectly identified by reference to an identifier. The definition is broad and includes a range of items, such as name, identification number, location data, or on-line identifier etc.

individual shall be expected to carry with them at all times. Each individual who is issued with one of these devices will be uniquely identified by virtue of a HO reference number or Person Identification Number, and supplier tag reference number.

Original data monitoring request (The Bail 206) 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.

Screening questions

4. Does the processing activity include the evaluation or scoring of any of the following?

- profiling and predicting (especially from “aspects concerning the data subject’s performance at work”)
- economic situation
- health
- personal preferences or interests
- reliability or behaviour
- location or movements.

☒ Yes

☐ No

5. Does the processing activity include automated decision-making with legal or similar significant effect? i.e. processing that is intended to take decisions about data subjects which will produce “legal effects concerning the natural person” or which could “significantly affect the natural person”.

☐ Yes

☒ No

6. Does the processing activity involve systematic monitoring? i.e. processing used to observe, monitor or control data subjects, including data collected through networks or “a systematic monitoring of a publicly accessible area” e.g. CCTV.

☐ Yes

☒ No

7. Does the processing activity involve mostly sensitive personal data? This includes special categories of personal data, data about criminal convictions or offences, or personal data with the security marking of Secret or Top Secret.

☒ Yes

☐ No

- 8. Does the processing activity involve data processed on a large scale?** If sharing with a third party external to the Home Office large scale is defined as 1,000 plus pieces of personal data in a single transaction or in multiple transactions over a cumulative 12 month period.
- ☐ Yes ☒ No
- 9. Does the processing activity involve matching or combining datasets that are being processed for different purposes?** e.g. data 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. *NB:* This does not include matching or combining datasets from different IT systems that are processed for the same purpose and legal basis e.g. CID and CRS.
- ☐ Yes ☒ No
- 10. Does the processing activity involve mostly data concerning vulnerable data subjects or children?**
- ☐ Yes ☒ No
- 11. Does the processing activity involve the innovative use or application of new technological or organisational solutions?** e.g. combining use of fingerprints and facial recognition for improved physical access control, etc.
- ☒ Yes ☐ No
- 12. Will the processing activity in itself prevent data subjects from exercising a right (under Data Protection Legislation and the UK GDPR) or using a service (provided by) or a contract (with) the Department?**
- ☐ Yes ☒ No
- 13. Is the introduction of new legislation or a legal regulatory measure which relates to the processing of personal data being considered?**
- NB: If yes, this may require consultation with the Information Commissioner.*
- ☐ Yes ☒ No

If you have answered 'yes' to more than one of the above screening questions (Q 3 to 12), a DPIA must be completed. If you have answered 'no' to each of the screening questions but feel the planned policy/process/activity is significant, or carries reputational or political risk, you should complete the full DPIA. If you are not sure whether a DPIA should be completed, please consult the Office of the [Data Protection Officer](#) (ODPO). **If you have completed Stage 1 and do not need to complete Stage 2, send your Stage 1 assessment to the [ODPO](#).**

DPIA Stage 2

Section 1: Background and contacts

1.1 Proposal/Project/Activity title:

STS GPS Electronic Monitoring

1.2 Information Asset title(s) (if applicable):

GPS Satellite Tracking Data Set – HO are Sole Data Controller.

1.3 Information Asset Owner(s) (IAO):

Email:

Name:

Telephone Number:

Information Asset title:

Email:

Name:

Telephone Number:

Information Asset title:

1.4 Person completing DPIA on behalf of the IAO named at 1.3 above):

Email:

Name:

Telephone Number:

Business Unit/Team: STS

1.5 Date DPIA commenced:

19/08/2021

1.6 Date processing activity to commence (if known):

Ongoing

NB: if the processing activity is already ongoing, please explain why the DPIA is being completed retrospectively.

A transition DPIA is already registered this DPIA is to coincide with the full launch of the legislation. We stated within the transitional DPIA that we would be producing a full DPIA to reflect that from 31/08/21 new legislation will be enacted that means all FNO's subject to deportation must be considered for Electronic Monitoring – previous to this date it is only FNO's who satisfy certain criteria.

1.7 Information Asset Register reference (if applicable):

FNORC IAR Electronic Monitoring.

1.8 DPIA version:

0.1

1.9 Linked DPIAs *NB:* attach word versions, do not provide links.

STS EM Transition DPIA

1.10 DPIA proposed publication date (where applicable, and if known):

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.

NB: Provide below information about whether the DPIA will be published in part or in full, and the reason why it will be published.

[Click or tap here to enter text.](#)

Section 2: Personal Data

NB: These questions relate to the personal data being processed in the processing activity described within this DPIA only. It is acknowledged that in many instances the personal data being processed will originate from other HO sources and therefore be subject to their own set of rules governing access, retention and disposal.

2.1 What personal data is being processed?

Daily Monitoring of individuals subject to immigration control who meet the criteria for wearing/carrying a GPS Electronic Monitoring Device. This device can be in the form of a Fitted Ankle Tag or a Non Fitted Device – a smartwatch that the individual shall be expected to carry with them at all times. Each individual who is issued with one of these devices will be uniquely identified by virtue of a HO reference number or Person Identification Number, and supplier tag reference number. Original data monitoring request (The Bail 206) will include individuals Name, DOB, Nationality, Photograph offending history and any vulnerabilities identified that the third party supplier may need to be aware of.

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.

- For those individuals who are given a non fitted device – smartwatch- to carry/ wear, they will have to complete random monitoring checks throughout the day by virtue of taking a photograph of themselves using the smartwatch which will be cross checked against a system held Biometric Facial Image template (This template, is a series of dots produced by an algorithm applied to an original Biometric Image – ‘The Enrolment Image’ taken during the induction process, held on the suppliers database. The monitoring checks – up to 5 per day are matched against the Template Image only not the Enrolment Image produced at the induction.). If the image verification fails then then the check is made manually against the Enrolment image that is stored on the database.
- **Enrolment template** - Created from the enrolment image and is stored on BioID (Suppliers database). Used for intelligent matching using an algorithm.
- **Enrolment image** - Captured once at start of order and saved as image on Chronos(Suppliers Database). Used for manual verification in the event of Template Image verification failure.
- The field officer taking / approving the original Biometric Facial Image Enrolment Image is acting solely on the instructions of the HOIE authorising officer who completed the Bail 206 Monitoring Order. This demonstrates a clear relationship link between the two parties.

2.2 Which processing regime(s) applies: general processing regime (UK GDPR/Part 2 DPA), and/or law enforcement processing regime Part 3 DPA?

NB: this question is repeated at Q.3.1.a.

General processing (UK GDPR/Part 2 DPA) ☒

Law enforcement (Part 3 DPA) ☒

2.3 Does the processing include any of the following special category, or criminal conviction data?

Criminal conviction data	☒	Yes	☐ No
Race or ethnic origin (including nationality)	☒	Yes	☐ No
Political opinions	☐	Yes	☒ No
Religious or philosophical beliefs	☐	Yes	☒ No
Trade union membership	☐	Yes	☒ No

Genetic data or biometric data for the purpose of uniquely identifying individuals	☒	Yes	☐ No
Health	☒	Yes	☐ No
Sexual orientation or details of the sex life of an individual	☐	Yes	☒ No

2.4 Does it include the processing of data relating to an individual aged 13 years or younger?

☐ Yes ☒ No

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

Click or tap here to enter text.

2.6 Will data subjects be informed of the processing?

☒ Yes ☐ No

If 'yes' go to Q2.7 If no, explain why.

Click or tap here to enter text.

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

Data subjects will be informed of the use of data in Electronic Monitoring information session delivered face to face in IRC's /Prisons. They will also be given an information booklet about the processing of data and sharing of data. They will also be informed by the supplier field officer who fits their tag during the induction process. This booklet and the information share verbally, includes all right to be informed conditions.

2.8. Which HO staff and/or external persons will have access to the data?

Electronic Monitoring Hub caseworkers and manager through role based access control. This data may in turn be shared to appropriate HO Departments, upon evidence of a Breach of Immigration Bail Conditions.

2.8a. How will 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 solely onto the Atlas system on the Immigration Bail Condition Breach screens of the individual. The original breach report is stored under normal HOIE storage and retention.

2.10 If the data is being stored electronically, does the storage system have the capacity to meet data subject rights (e.g. erasure, portability, suspension, rectification etc)?

☒ Yes

☐ No

If 'No' explain why not below and go to Q2.12

Click or tap here to enter text.

2.11 If 'Yes' explain how these requirements will be met.

EMS is the existing supplier and the requirements have not changed for the launch of the full. The data can be manually accessed, extracted , archived accordingly. All EM individuals can use provided privacy information to act on rights, either the booklet or gov.uk hosted resources and all requests will be assessed on a case by cases basis.

[2.12 For law enforcement processing only: If the data is being stored electronically, does the system have logging capability (as per s.62 DPA)?

☒ Yes

☐ No

If 'no', what action is being taken to ensure compliance with the logging requirement?]

Click or tap here to enter text.

[2.13 For law enforcement processing only: Will it be possible to easily distinguish between different categories of individuals (e.g. persons suspected of having committed an offence, victims, witnesses etc.) as well as between factual and non-factual information (as per s.38 DPA)? e.g. criminal record (fact); allegation (non-factual)

☒ Yes

☐ No

If 'no', what action is being taken to ensure compliance with s.38 DPA?]

Click or tap here to enter text.

2.14 What is the retention period for the data?

Audit trail data will be retained for up to 6 years after the monitoring order has ceased. This is the standard retention for audit trail data held by MOJ. Biometric facial image checks will retained for 2 years after production of check, this is to

allow for any prosecution period resulting from fraudulent image submission or false positive checks.

2.15 How will data be deleted in line with the retention period and how will the deletion 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.

2.16 If physically moving/sharing/transferring data outside the Home Office, how will it be moved/shared?

See 2.9

2.17 What security measures will be put in place to ensure the transfer is secure?

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.

Email Transfer: All HO emails to the MoJ are sent via the Home Office O365 email address. All HO email communications are secured via TLS (version 1.2). A risk assessment on the email transfer has been presented to senior leadership for awareness and approval.

2.18 Is there any new/additional personal data being processed? This includes data obtained directly from the data subject or via a third party.

☒ Yes

☐ No

If 'yes', provide details below:

Yes new GPS Trail data and Biometric Facial image data.

The Enrolment Image -a Biometric Facial Image is 'transferred to an image template' via a system algorithm that transfers the image into a series of image facial feature dots and these dots the 'Template Image' are then stored on the database for cross referencing against daily Facial Image request checks sent to and supplied by the wearer. These checks are performed up to 5 times per day at random intervals. This process is completed in an attempt for HOIE to be assured that the individual is carrying the Non Fitted Device with them at all times.

If the verification fails against the Template image then we may use the Enrolment image for manual checks

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

OFFICIAL/OFFICIAL-SENSITIVE	☒
SECRET	☐
TOP SECRET	☐

2.20 Will your processing include the use of Cookies?

☐ Yes ☒ No

If 'no' go to section 3.

If 'yes', what sort of Cookies will be used? Tick the correct categories:

1) Essential (no consent required)	☐	Yes	☐	No
2) Analytical (consent required)	☐	Yes	☐	No
3) Third party (consent required)	☐	Yes	☐	No

2.20.a. If cookies fall into categories 2) & 3) how will you ensure data subjects are aware and can give active consent to the use of cookies?

Click or tap here to enter text.

Section 3: Purpose of the Processing

3.1 What is the purpose of the processing? Provide a detailed description of the purpose for the processing activity. This section needs to provide an overview (in plain English) that can be read in isolation to understand the purpose and reasons for the processing activity.

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.

What is changing now

The supplier remains the same. The service remains the same. The criteria for tagging will change from 31/08/21 when the new legislation is enacted. From that date all FNO's subject to Deportation Proceedings have to be considered for Electronic Monitoring (EM). Other cases may be considered on a case by case basis. That EM will be in the form of Fitted devices (Ankle Tag) or Non Fitted Devices (a Smartwatch). The existing policy has been changed to allow this and Policy and Home Office Legal Advisors have confirmed our approach. The new devices allow 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.

Biometric Facial Image check

The Enrolment Image – a Biometric Facial Image is 'transferred to an image template' via a system algorithm that transfers the image into a series of image facial feature dots and these dots the 'Template Image' are then stored on the database for cross referencing against daily Facial Image request checks sent to and supplied by the wearer. These checks are performed up to 5 times per day at random intervals. If verification fails using the Template Image – we can check the monitored image against the Enrolment Image manually. This process is completed in an attempt for HOIE to be assured that the individual is carrying the Non Fitted Device with them at all times. 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 every 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 and has been subject to assessment.

IE currently share these details with police on a Police Risk Notification Form when an FNO is released from detention into the community.

It's 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 persons 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, from where they would be expected to use only in line with business need and to an equivalency of security.

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 occurrences :-

- **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. Immigration 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. Rights will be assessed on a case by case basis and delivered in conjunction with supplier or other government/public bodies as required.

3.1.a Which processing regime(s) applies: general processing regime (UK GDPR/Part 2 DPA), and/or law enforcement processing regime Part 3 DPA?

General processing (UK GDPR/Part 2 DPA) ☒ - go to question 3.2.a.

Law enforcement (Part 3 DPA) ☒ - go to question 3.2.b.

3.2.a. General processing only: What is the (UK GDPR Article 6) lawful basis for the processing? Choose an option from the list:

Consent ☐

- | | |
|---|-------------------------------------|
| Contract | ☐ |
| Legal obligation [see 3.3(a)] | ☐ |
| Vital Interest | ☐ |
| Performance of a public task [see 3.3(a)] | ☒ |
| Legitimate Interest | ☐ |

NB: Legitimate Interest cannot be relied upon by the Home Office for processing carried out in order to fulfil or support a public task.

[3.2.b. Law enforcement processing only: What is the (Part 3 DPA) lawful basis for the processing? Choose an option from the list:

- | | |
|---|-------------------------------------|
| Consent | ☐ |
| Necessary for a law enforcement purpose | ☒ |

3.3. If you have selected 'legal obligation' or 'performance of a public task' for general processing (for Q3.2.a), OR if the processing is for a law enforcement purpose

Indicate below the legal basis and relevant legislation authorising the processing of the data:

Common law (list HO function/objective below) ☐

Click or tap here to enter text.

Royal Prerogative (HMPO only) ☐

Explicit statute/power (list statute below) ☒

Immigration Act 2016 and The Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021

Implied Statute power (list statute below) ☐

Click or tap here to enter text.

3.4.a. General processing only: If processing special category data or criminal convictions data (see Q2.2 above)

What is the (UK GDPR Article 9) condition for processing the special category data?

- | | |
|-------------------------------------|-------------------------------------|
| N/A | ☐ |
| Consent | ☐ |
| Vital Interests | ☐ |
| In the public domain | ☐ |
| (Exercising/defending) legal rights | ☐ |
| Substantial Public Interest | ☒ |
| Public healthcare | ☐ |

Archiving or Research

☐**Appropriate Policy Document: Special Category Data Part 2**

[3.4.b. Law enforcement processing only: If processing sensitive data for a law enforcement purpose: **What is the (DPA Schedule 8) condition for the processing?**

- | | |
|--|-------------------------------------|
| Consent | ☐ |
| Substantial public interest (for a statutory purpose) | ☒ |
| Administration of justice | ☐ |
| Vital Interests (of the subject or another) | ☐ |
| Safeguarding children and individuals at risk | ☐ |
| Data already in the public domain | ☐ |
| Legal claims (seeking advice, legal proceedings, defending rights) | ☐ |
| Judicial acts | ☐ |
| Preventing fraud (working with anti-fraud organisations) | ☐ |
| Archiving | ☐ |

Appropriate Policy Document: Sensitive Processing Part 3

3.5 Is the purpose for processing the information described at 3.1 above the same as the original purpose for which it was obtained by the Department?

☒ Yes☐ No

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

Original purpose: [Click or tap here to enter text.](#)

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

Section 4: Processing activity

4.1 Is the processing replacing or enhancing an existing activity or system?

If so, please provide details of what that activity or system is and why the changes are required.

☒ Yes☐ No

[Click or tap here to enter text.](#)

If the answer is 'yes' go to 4.3

4.2 Is the processing a new activity? This description should include details (if appropriate) of what resources are needed to build the model? (e.g. FTEs, skills, software, external resource)

☐ Yes

☐ No

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

Approx. 4500

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

Regular activity

4.5 Does the processing directly relate to the processing of personal data that includes new legislative measures, or of a regulatory measure based on such legislative measures? If 'no', move onto 4.6.

☒ Yes

☐ No

4.6 If the answer is yes, please explain what that processing activity is, including whether or not the HO will be accountable for the processing of personal data?

Monitoring of individual via biometric facial recognition. The Enrolment Image -a Biometric Facial Image is 'transferred to an image template' via a system algorithm that transfers the image into a series of image facial feature dots and these dots the 'Template Image' are then stored on the database for cross referencing against daily Facial Image request checks sent to and supplied by the wearer. If checks against the Template Image fail we can check against the Enrolment Image manually. These checks are performed up to 5 times per day at random intervals. This process is completed in an attempt for HOIE to be assured that the individual is carrying the Non Fitted Device with them at all times. HO is the Sole Data Controller.

4.7 Does the processing activity involve another party? (This includes other internal HO Directorates, external HO parties, other controllers or processors).

☒ Yes

☐ No

If the answer is "No" go to 4.7.

4.6.a In what capacity is the other party acting?

- Part of the HO ☐
- Controller in their own right (i.e. non HO) ☐
- Joint Controller with the HO ☐
- Processor (public body) on behalf of the HO ☒

- Processor (non-public body) on behalf of the HO ☒

Provide details here:

Moj as processor on behalf of HO and Electronic Monitoring Services EMS as a sub processor non-public body.

4.8 Will any personal data be transferred outside the UK?

- ☐ Yes ☒ No

If 'no' go to 4.8. If 'yes', provide brief details of the countries and complete Section 7.

Click or tap here to enter text.

4.9 Does the proposal involve profiling that could result in an outcome that produces legal effects or similarly significant effects on the individual?

- ☐ Yes ☒ No

If yes, provide details

Click or tap here to enter text.

4.10 Does the proposal involve automated decision-making?

- ☐ Yes ☒ No

If yes, provide details

Click or tap here to enter text.

4.11 Does the processing involve the use of new technology?

- ☒ Yes ☐ No

If 'no', go to question 5.1.

4.12 If 'yes': Describe the new technology, including details of the supplier and technical support.

The new Smartwatch device that we will be using for monitoring purposes via inclusion exclusion zones and collection of Biometric Facial Image checks is new technology and is currently still undergoing checks .It will be supported by MOJ and HO DDAT. The Smartwatch devices will not be available until November 2021 and any emerging risk will be included and assessed within this DPIA.

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

- ☐ Yes ☒ No

a) If 'yes', explain how this is being achieved

Click or tap here to enter text.

b) If 'no', what is the justification for not seeking their views?

Legislation dictates that all those subject to deportation must be considered for GPS EM All individuals who are required to wear a device are asked to submit representations as to why they believe they should not have to wear a tag. They also receive frequent physical and verbal privacy information through the process and to which they can continue to refer, so we believe further consultation would not bring further transparency benefits.

Section 5: Risks of the Processing

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

☒ Yes

☐ No

If 'yes' provide details and go to question 5.2.

Disproportionate provision of Offending history and Health issues

- 5.2 What steps have been taken to mitigate these risks?**

Quality Assurance of Monitoring Orders. All Monitoring orders will be subject to random quality assurance checking. This process involves checking what information has been presented on the Bail 206 Monitoring Order. All Offence history and medical information will be checked for proportionality.

- 5.3 Can you demonstrate that the risks to the individuals are sufficiently balanced by the perceived public protection benefits?**

☒ Yes

☐ No

If 'yes' provide details and go to question 5.4.

Critical vulnerability issues and Offending history has to be provided for the safety of the EMS field officers and the safety/protection of the individual

- 5.4 Are these risks included within a risk register?**

☒ Yes

☐ No

Section 6: Data Sharing/Third party processing

Complete this section if you have answered 'yes' to question Q.4.4.

6.1 External contact details for data exchange/ processing

Name:

Grade:

Organisation:

Business Unit/Area:

Contact email:

[Redacted contact details]

Name:
 Grade:
 Organisation:
 Business Unit/Area:
 Contact email:

6.2 What is the legal basis/power/statutory gateway for the processing activity?

Common law (list HO function/objective below) ☐

Royal Prerogative (HMPO only) ☐

Explicit Statute/power (list statute below) ☒

Immigration Act 2016 and The Immigration (Collection, Use and Retention of Biometric Information and Related Amendments) Regulations 2021

Implied Statute/power (list statute below) ☐

Click or tap here to enter text.

6.3 How long will the data be retained by the receiving organisation or processor for the purpose for which it is received?

*See 2.14

All the data contained within the monitoring orders will be retained for 6 years after the Monitoring ceases to be live. All audit trail data will be retained for 6 years after the monitoring order ceases to be live. All biometric images taken and stored as part of the Non Fitted devices monitoring regime will be retained for 2 years after the image is taken apart from the original Enrolment Image which will be retained for 6 years after the Monitoring order has ceased to be live.

6.4 How will it be destroyed by the receiving/ processing organisation once it is no longer required for the purpose for which it has been received?

*See 2.15

- Personal data about offenders will be stored in a number of different systems that support the electronic monitoring operation, some of which are older legacy systems. As a result, a mix of approaches will be taken for erasure from the different systems, as outlined below:
 - o Records within the case management system will be anonymised, and those anonymised records will be moved to a separate business unit accessible only by system administrators, putting them beyond operational use. This approach is taken to ensure system database consistency rather than total erasure.
 - o An erasure approach for records containing personal data will apply to the data warehouse, document management and tasking systems, with only bulk statistics being retained.
 - o Subject images for biometric enrolment and biometric templates captured to support non fitted device operation will be erased once no longer required.
- In all cases, specific automated system administration tools and scripts will be utilised to execute anonymisation or erasure routines to ensure consistency and reliability.

6.5 Is the data sharing process underpinned by a non-binding arrangement (Memorandum of Understanding (MoU) or equivalent) or binding agreement (Treaty or contract)?

☒ Yes

☐ No

If no, provide details why a formal written arrangement is not required and move to 6.7

Click or tap here to enter text.

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

Name:

Grade:

Business Unit/Area:

Contact email:

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

☒ Yes

☐ No

If yes, please provide the identity of the processor and confirm details of that arrangement will be included in the formal written arrangement between the HO and the receiving/processing organisation.

MOJ may share details with police and agreement is covered in the approved MOU and with the awareness of the Home Office.

Technical impact and viability

6.8 Which of the following reflects the data processing? The process may meet several of these descriptions.

Data extract: *Are you working through and assessing data to secure relevant information?*

☒ Yes

☐ No

Data matching: *Are you comparing several sets of data?*

☐ Yes

☒ No

Data reporting: *Are you processing data to produce accurate analysis?*

☒ Yes

☐ No

Data exchange/feed: *Are you sharing the data between programmes?*

☒ Yes

☐ No

Direct access: *Are you obtaining data by going directly to where it is physically located?*

☐ Yes ☒ No

Other

☐ Yes ☐ No

a) If 'Other, please provide details

[Click or tap here to enter text.](#)

6.9 Has any analysis or feasibility testing been carried out? For example, through a proof of concept or pilot exercise?

☐ Yes ☒ No

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

A pathfinder exercise is expected for the Non Fitted Devices.

6.10 Confirm if:

development work is required to ensure systems are DP compliant?

☐ Yes ☒ No

If yes, provide details including time frame

[Click or tap here to enter text.](#)

Security Checklist

6.11 Given the security classification of the data, are you satisfied with the proposed security of the data processing/transfer arrangements detailed at 2.16 and 2.17 above?

☒ Yes ☐ No

6.12 Confirm you have read the associated [guidance](#) and, if necessary, consulted with HO Security and the relevant DDaT teams, including the Office of the CISO:

NB: If your processing activity involves any use of IT systems or physical documentation being sent outside of the Home Office to a non-governmental organisation, you *must* consult with the Office of the CISO, prior to your DPIA being submitted.

I confirm I have read and understood associated guidance.

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

[Click or tap here to enter text.](#)

6.14 Will the data be stored and be accessible off-site?

☒ Yes ☐ No

6.15 If 'yes', have you considered the security arrangements that need to be in place to prevent the data from being accidentally or deliberately compromised? Please provide details.

☒ Yes

☐ No

- Standard security protocols of 2 factor authentication, firewalls, penetration testing, encryption in transit/at rest and regular risk assessments.
- The data is stored on the MoJ Azure platform which provides data encryption in transit and at rest.
- Dependent on the MoJ's security risk assessment guaranteeing security of the Home Office's data and information.
- All signed off by Technical Assurance Board.

Section 7: International transfers

Only complete this section if you have answered yes to question 4.7.

7.1 Does the activity involve transferring data to a country outside of the UK (including Crown Dependencies, Overseas Territories and Sovereign Base Areas)?

☐ Yes

☒ No

If 'yes', specify the country. If 'no', go to Section 8.

[Click or tap here to enter text.](#)

7.2 Does the country have a positive adequacy decision?

☐ Yes

☐ No

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

i) General processing only:

- Pursuant to a legally binding Treaty which contains appropriate safeguards for 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 binding rules providing 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 (and set out in a non-binding MoU) ☐

ii) **Law enforcement processing only:**

- Pursuant to a legally binding Treaty which contains appropriate safeguards for the rights of data subjects and effective legal remedies for those rights
☐
- On the basis that the transfer is necessary for 'in individual cases for any of the law enforcement purposes' which are recognised in statute ☐

7.3 Does the HO already have a binding or non-binding data sharing arrangement with this country?☐ Yes☐ No**If no, skip 7.4 a)****a) If 'yes', does the arrangement cover the purpose(s) for which you need to share data?**☐ Yes☐ No**If you have selected no for 7.3, you will need to consider reviewing the existing agreement to include the new processing activity**

- I. **If 'yes', does the arrangement 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; or set out why the transfer is necessary in individual cases for a law enforcement purpose?

☐ Yes☐ No**If yes go to Section 8**

- II. **If 'no', how do you propose to document the terms of the understanding with the other country?**

Click or tap here to enter text.

Note: You should consult guidance on Overseas Security and Justice Assistance (OSJA) to determine whether an assessment of human rights, International Humanitarian Law, political and reputational risks is required.

Section 8: Referral to ODPO**8.1 Referral to the ODPO**

Date referred to the ODPO	Reviewed by:	Date returned to the Author	Comments/ recommendations
19/08/2021		20/08/2021	Comments throughout require clarification

Click or tap to enter a date.		Click or tap to enter a date.	

8.2 ODPO Review complete

NB: Any subsequent changes made to the DPIA by the business must be done clearly and transparently and in accordance with accepted version control convention. In the event of changes being made, earlier versions of this DPIA must be retained for auditing purposes and in-line with your agreed retention period.

If substantive changes are made to this DPIA, you must re-refer to the ODPO for a new review.

Date referred to the ODPO	Reviewed by	Date returned to the Author	Comments/recommendations
24/08/2021		27/08/2021	ODPO review process complete

8.3 IAO sign-off

Date referred to IAO	Name of IAO or person signing on behalf of	Date returned to the Author	Comment (including approved to proceed Y/N)
Click or tap to enter a date.		Click or tap to enter a date.	

Section 9: Referral to Data Board

This section is only required if one or more of the criteria for referral to the HO Data Board is met (see DPIA guidance). Referral to the HO Data Board will be completed by the ODPO after consultation with the business owner(s) listed in part 1 of this DPIA. [Guidance](#) is available on Horizon.

9.1 Criteria for referral to the HO Data Board:

Criteria	Met
ODPO have identified a risk that, in its opinion, requires escalation to the ICO (regardless of risk severity; guidance will be produced in due course once	

examples indicate how this might be revealed). The view of the Chair of the Data Board will be sought in advance of any such escalation.	
ODPO reason for referral if not one listed below: [ODPO insert detail]	
There is a significant impact, either qualitative and/or quantitative, upon individual rights, this may be one or more of the following:	
An instance where the proposal will not meet the Home Office obligations to meet the individual rights and protections of data subjects as defined in UK GDPR and DPA18.	
An instance where the proposal is likely to result in any person(s) individual privacy/data protection rights being compromised.	
A particular concern is identified having regard to the purpose, method of processing and location of processing that in combination warrants further escalation or consideration.	
High sensitivity – the nature of the personal data itself is so sensitive, even though the rest of the risks around processing were low. The board could be asked to scrutinize but equally the Board could determine that it did not need to do so.	
It is not possible to implement all recommended controls/mitigations. (Where controls and mitigations have been identified but result in a short period of heightened risk this would not warrant escalation).	
High likelihood of challenge or regulatory enforcement being brought, or a high likelihood of such a challenge or action being successful against the HO.	
Where a proposal resulted in advice that the processing would be unlawful, and the project has since revised (tweaked) the proposal this should be referred to the Board.	
Specific referral circumstances:	
Data processing has been promised by a Minister/ the Cabinet, but there are questions as to whether there is a sufficient legislative/technical /administrative framework in place to enable this.	
A decision has been made to prefer specific safeguards over others or a riskier approach.	
An issue that is business critical emerges e.g. essential work to a business-critical system, that may mean that data subjects rights may not be met.	
Where processing is likely to attract significant controversy.	
Other: [add detail]	

9.2 Referred to the HO Data Board Secretariat

Date referred to the Secretariat	Referred to HO Data Board	Date of Data Board (if appropriate)	Date returned to the Author
Click or tap to enter a date.	Yes ☐ No ☐	Click or tap to enter a date.	Click or tap to enter a date.
Recommendations/ findings/ comments from the HO Data Board/ Secretariat			

--

9.3 Action taken by the respective IAO(s)

Effective Date 2021

Last Review Date

Next Review Date

Owner

Approved by

Audience



All HO Staff