Ministry of Justice

Data Protection Impact Assessment – report template

Introduction

Whenever personal data is being processed, the processing should be compliant with data protection legislation. Completing a data protection impact assessment (DPIA) before you start the data processing will help you to identify and minimise risks as well as demonstrate compliance with data protection legislation. It is mandatory to complete a DPIA for proposals that have a high risk of causing individuals harm.

The legislation consists of the Data Protection Act (DPA) 2018 and Regulation (EU) 2016/679: the General Data Protection Regulation (GDPR).

HMG security policy also requires that an initial assessment of the privacy risks to individuals in the collection, use and disclosure of information is made for all new policies or projects that include the use of personal information.

Any planned policy, project or initiative should be assessed to identify potential privacy risks, it'll be easier to make changes at the start than later on. If you have any questions or comments in relation to this assessment please contact the Information Governance and Data Protection team mailbox in the first instance at data.compliance@justice.gov.uk.

Who is responsible for the DPIA?

The Senior Responsible Owner for the project or programme or the Information Asset Owner for the personal data that will be processed is responsible for ensuring the DPIA takes place. They are also responsible for approving the finalised DPIA. A DPIA is a collaborative exercise and cannot be completed by one individual on their own. Contributions will be required from all those involved in the policy change, project or proposal. Those who will be affected by the proposal should be consulted whenever possible and also other teams that may be required to deliver the proposal such as commercial or technology.

On completion, the DPIA report should be approved by your Information Asset Owner (IAO), Business Owner or Project Senior Responsible Owner (PSRO). Proposals that involve the processing of a significant amount of personal data or are high risk should be signed off by your Senior Information Risk Owner (SIRO).

A DPIA should be a living process and the assessment should be reviewed regularly, preferably annually and certainly if any changes to the project are proposed. The completed DPIA must be submitted to the Data Protection Officer for review at data.compliance@justice.gov.uk.

Key individuals

Role	Name	Email	Tel:
Senior Information Risk Owner (SIRO)			
Information Asset Owner			
Business IA Lead			
Digital Assurer (if relevant)			
Product Manager (if relevant)			

Section 1: Outline of the proposal and personal data to be processed

What kind of processing and data does this proposal involve?	
1.1 Explain broadly what the proposal aims to achieve.	In conjunction with the Home Office's Joint Security and Resilience Centre (JSARC), HMPPS have embarked on the Visitors Verification Project. The aim of the project is to trial biometric solutions that enables Prisons to verify who a person is. In December 2018 three separate biometric suppliers will test their technology in three prisons in the Yorkshire region. • **Technology A:** Is an identity document verification solution that will be tested in HMP Hull.

	• **Technology B:** Is a facial recognition technology that will be tested in HMP Humber. • **Technology C:** Is an iris scanning technology that will be tested in HMP Lindholme. The trials will be testing which supplier(s) can provide an effective and efficient solution for prisons to verify who a person is. As per 1.5, the capture and retention of biometric data by government is a high profile issue and subject to public scrutiny. The trial will gather this data. However the participants will be aware and give their consent. In addition we will not retain the data at the end of the trial or use it in any operational work. Performance metrics will be captured during the six weeks which will seek to identify quantitative data, such as, system outputs, user feedback and visitor feedback. 1.1 has been redacted under section 31 exemption.
1.2 Does the proposal replace an existing policy, process or system?	Currently, there are two systems which are used for the booking and verification of visitors into Prisons across England and Wales. Redacted under section 31 exemption The trial will run parallel to the existing visitor verification process that the three prisons have in place. The initial enrolment process with each supplier varies, it can take up to approximately one minute per visitor. Once the initial enrolment has been completed when the visitor next attends the establishment the verification process should take up to ten seconds. With how visits sessions are currently delivered it is not expected that with running two processes running parallel to one another will hinder visiting times. All visitors will have the right to refuse partaking in the trial.
1.3 How will data processing support this objective?	The processing of biometric data will allow HMPPS to better identify and verify who visitors are. Visits is an area that is exploited for the conveyance of illicit items, therefore biometric technology will support prisons with the detection and prevention of crime. Redacted under section 31 exemption

1.4 What are the benefits of the data processing to MoJ and more broadly?	There are several potential benefits to improving on how HMPPS verify who visitors are: Redacted under section 31 exemption • By using biometrics, such as, facial recognition HMPPS can confirm who is entering the establishment. Also enabling an efficient and secure service to visitors. • Facial recognition will support the detection and prevention of crime in prisons across England and Wales. Where necessary, HMPPS will work with Law Enforcement Agencies.
1.5 Are the any current issues of public concern that should be factored in?	Yes. The capture and retention of biometric data by government is a high profile issue and subject to public scrutiny. The trial will gather this data. However the participants will be aware and give their consent. In the event they don't give consent they will still be able to continue the visit using the current processes in place. In addition we will not retain the data at the end of the trial or use it in any operational work.
1.6 Will the processing be under the GDPR or part 3 of the Data Protection Act?	Part 3 of DPA
Part 3 of the DPA (2018) covers personal data processing for 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.	
1.7 What personal data will be processed as part of the proposal?	Currently prisons in England and Wales record the following pieces of data for each visitor: • Full name. • Date of Birth • Address In addition to this, the following data will be recorded by each of the suppliers: • **Technology A:** Facial imagery and documentation, such as, passport or drivers licence • **Technology B:** Facial imagery • **Technology C:** Iris imagery

Personal data *means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes opinions expressed about an individual.*	
1.8 Does the proposal involve information about individuals of a kind particularly likely to raise privacy concerns or expectations?	As per 1.5. The capture and retention of biometric data by government is a high profile issue and subject to public scrutiny. The facial recognition trial will naturally gather data on someone's gender and race. However the participants will be aware and give their consent. . In the event they don't give consent they will still be able to continue the visit using the current processes in place. In addition we will not retain the data at the end of the trial or use it in any operational work.
The data protection laws identify a number of categories of personal data that require special care. These include racial and ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life, offences and court proceedings. You should also flag other sensitive personal data use, including financial data, data about vulnerable individuals and data which can enable identity theft.	
1.9 How many individuals' personal data will be processed?	The trial will be running for approx. six weeks in three prisons, HMP Hull, HMP Humber and HMP Lindholme. We are unable to provide exact numbers for how many individual's data will be processed, the information below can be used as a guide. • **HMP Hull:** They currently run ten social visits sessions across six days. • **HMP Humber:** They currently run nine social visits sessions across seven days. • **HMP Lindholme:** They currently run five social visits sessions across five days. It should be noted that during the six week trial it is likely that each prison will receive visits from the same individuals as some visit on a weekly basis. One of the anonymised performance metrics will be to measure how many visitors pass through the systems. These will be quantitative measures that will seek to identify the accuracy and efficiency of the system. In addition to this, each prison will run visit sessions for professional and legal visitors. These are either held on separate days or concurrent to social visit sessions. Redacted under section 31 exemption

1.10 What is the proposal's relationship with the individuals?	The visitors to the prison are data subjects
1.11 What is the source of the information?	The information that will be recorded will be personal biometric and identity data, such as, name and date of birth, official documentation imagery and facial imagery. This data will be checked against the images and data contained within the system in order to verify who the visitor is, and the documentation provided is accurate.
1.12 Does the proposal involve the use of personal data MoJ currently processes for new purposes?	HMPPS currently holds personal bio data of all social visitors which is recorded on either PNOMIS or standalone biometric systems. The verification of visitors and the recording of information is managed in accordance with PSI 15/2011 Management and Security at Visits.
1.13 How frequently will data be collected?	As per question 1.9. We are unable to provide exact numbers for how many individual's data will be processed, the information below can be used as a guide. • **HMP Hull:** They currently run ten social visits sessions across six days. • **HMP Humber:** They currently run nine social visits sessions across seven days. • **HMP Lindholme:** They currently run five social visits sessions across five days. Redacted under section 31 exemption
1.14 What geographical area will data be collected from?	The trial is going to run across HMP Hull, HMP Humber and HMP Lindholme. These three prisons all form part of the Yorkshire Prison Group. These prisons have been selected for the trial as they have been identified as a priority prison through the Ministerial commissioned drugs works.
1.15 Will it be collected directly from the individuals?	Data will be collected from all individuals (except children under the age of 18 years of age) during the trial period who give their consent to be involved in the trial. Individuals under the age of 18 cannot visit without an adult.

1.16 Does the proposal require individuals to be contacted in ways which they might find intrusive? If so, justify this approach.	No
1.17 Will it be collected by another organisation on behalf of MoJ?	The data will be collected by the three providers Technology A, Technology B and Technology C on the behalf of HMPPS. Following the completion of the trial, all the data collected will be deleted. Redacted under section 31 exemption
1.18 If so, what is the relationship and authority/control the MoJ has over the organisation?	These are three private companies but we will have an MoU with each for the trials
1.19 Which organisation is the data controller, which is a data processor?	HMPPS – Data Controller Private Companies – Data Processor
1.20 How will the project/policy/initiative use personal data?	The project involves the trialling of three pieces of commercial technology that capture certain biometric information about an individual, specifically a visitor to a prison. The biometric information includes images of faces, fingerprints or Iris. This biometric information will be used to verify whether a visitor is who they say they are. This is just a trial so while in the long term it could be used in concert with existing facial images and other databases, for now it will just be used to capture the images themselves.
1.21 Does the proposal involve using new technology which might be perceived as being privacy intrusive? If so, justify the approach.	The trial is to test facial recognition technology on visitors to prisons. Capturing facial images of visitors is something that already occurs in some prisons across England and Wales. An exception to this, will be Technology C which collects facial and iris data. This may be something that some individuals find intrusive. The collection of this data is essential for the visitor verification project in order to establish which solution is the most effective and suited to a prison environment.
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 video recording, profiling, data mining, and logging of electronic traffic.	

1.22 Are there any prior concerns of this type of processing or security flaws? If so, justify why you are using this approach.	Yes. Facial recognition has not been used in HMPPS before. The trials will be conducted to verify the accuracy of this technology

Section 2: Consultation

You should consult individuals whose data you are processing in some form. This process can reassure individuals that you are protecting their interests and have reduced any negative impact on them as much as you can. In some cases, the consultation process for a DPIA gives them a chance to have some say in the way their information is used.

You should also consult other stakeholders, including data processors (if applicable), legal, digital and/or information security experts.

You may also need to consult the ICO if the proposal is particularly high-risk. Any approach must be agreed with the Data Protection Officer, whom you can contact at data.compliance@justice.gov.uk.

Consultation with relevant stakeholders	
2.1 When and how will other individuals' views be sought? If you are not consulting, explain why.	We will assess the outcomes of the project by identifying by identifying specific performance metrics which considers data such as, time for processing visitors, how many visitors passed through, etc… as well as the views of both prisoner (user) staff and visitors. During the trial period, literature will be displayed and available for visitors which will detail what the project is about. The first will be an open letter to visitors which will detail why the trial is taking place, and the second will be posters to be displayed in the visitor's areas.
2.2 Who else within MoJ (including its Executive Agencies and ALBs) will be involved in the project/policy/initiative?	The Visitor Verification Project is a joint initiative between the Joint Security and Resilience Centre (JSARC) of the Home Office and the Security, Order and Counter Terrorism Directorate of HMPPS. MoJ Digital & Technology and Data Science teams will also be involved in the trials.

2.3 Will you have a data processor for the policy/programme/initiative. If so, will you consult accordingly?	Yes this will be the private companies
2.4 Will information or other security experts be consulted?	Yes, MoJ Information Assurance are engaged, as well as HMPPS Information Security.

Section 3: Data Flow Analysis

Set out in a diagram or table the data flows. You should include details of where the data comes from; how it moves within the MOJ and how it moves to and from other organisations.

*You should also include details of the collection, use storage and deletion of the data; and the mechanisms used to move the data (e.g. internet, courier, email).***Data Flow**

Redacted under section 31 exemption

Section 4: Legislative requirements

This will assess the compliance of your proposal against the requirements various privacy legislation and policies.

Section 4.1 relates to the requirements of the GDPR and DPA (2018) for the processing of personal data.

Section 4.2 relates to the requirements of Part 3 of the DPA (2018), which has **some** different requirements to the GDPR and Parts 1 and 2 of the DPA (2018)

Section 4.3 relates to the requirements of other privacy legislation and policies. This section is **compulsory**.

If you are processing data under Part 3 of the DPA (2018) you should complete:

- **Most** of Section 4.1: requirements of the GDPR and DPA (2018) – you don't need to complete question 4.1.11;
- Section 4.2: requirements of Part 3 of the DPA (2018); and
- Section 4.3: other privacy legislation and policies.

If you are **not** processing data under Part 3 of the DPA (2018), you should complete:

- Section 4.1 **in full**: requirements of the GDPR and DPA (2018); and
- Section 4.3: other privacy legislation and policies.

Section 4.1: Requirements of the GDPR and DPA 2018 Part 2

Requirement		Comments
Data Protection Impact Assessment **GDPR Article 35** **or** **The Act Section 64**	**4.1.1 Data Protection Impact Assessment (DPIA):** • Has a DPIA screening process for the proposal/project/system been completed? If yes, please attach the DPIA screen form. • Has a DPIA/PIA that relates to the proposal/project/system been completed? If yes, please attach the assessment.	No. We have been directed by MoJ Data Protection Team to complete the full assessment.
The Principles **GDPR Articles 5, 6** **or** **The Act Section 34** • **Lawful** • **Specific** • **Limited** • **Accurate** • **Time-Bound** • **Secure**	**Lawful:** complete separate section below	
	4.1.2 Specific: complete Q1.1	
	4.1.3 Adequate: • What assessment has been made on the adequacy of the data being processed in relation to the purpose?	The trafficking of illicit items through visits halls is a significant threat to prison security. The collection of biometric data is considered an adequate response to this
	4.1.4 Limited: • What assessment has been made on the relevance of the data being processed to the purpose? *An important aspect of privacy protection is not to collect excessive personal data. There must be clear justification for the necessity of all data processing*.	Biometric data will help us verify the identity of a visitor and better identify those who are potentially visiting to commit crime. For the purposes of these trials the data will be limited to the time of the trial and deleted afterwards. It will not be used for other purposes during the trial

	• Will the data be used for any other purpose? *Data controllers must be clear and specific about the purposes for which personal data is to be used and not use it for purposes incompatible with those for which it was initially collected*.	
	4.1.5 Accurate: • How will the accuracy of the data be checked? • How will inaccurate data be corrected? • How will it be kept up to date? • What processes will be in place to manage requests for rectification?	Part of the trial will be to test the accuracy of the data collected by the equipment. Any inaccuracies will be flagged and deleted during the trial
	4.1.6 Time-Bound: • How will the data be stored? • How long will the data be stored? • Is the data covered by an existing retention and deletion schedule? If not, will one be agreed with the Departmental Records Officer? • Will you be able to delete the data when you no longer need it? • If you can't delete it, can you anonymise it partly or wholly? • What processes will be in place to ensure the data is securely destroyed/deleted? • Will an audit be put in place of the retention and disposal activity?	The data will be secured within the equipment's own memory and also within HMPPS data systems. The data will be retained during the trial and deleted at its conclusion. This will be overseen by an HMPPS member of staff and written confirmation received of the destruction to agreed HMG defined standards.
	Secure: complete question 4.1.18 below	

Transparent **GDPR Article 12, 13, 14** **or** **The Act Section 44, 45**	**4.1.6 Transparent / Duty to Inform:** • Will you have a privacy notice for data subjects when you collect data from them? If not, explain why. • How will data subjects (e.g. customers, staff) be made aware of what is happening to their data if you have received it from another source i.e. not collected it from the data subjects themselves? • Do individuals have an opportunity and/or right to decline to disclose or share their information? Provide a copy or link to any privacy notices.	Yes. Each visitor will be informed of what we are collecting and for what purpose during the trial. It will only be collected from the data subject. No operational watch lists will be used during the trial Visitors will be given the right to refuse to take part in the process. This will be clearly stated in the letter issued to each visitor when they arrive on site.
Subject Access **GDPR Article 15** **or** **The Act Section 45**	**4.1.7 Subject Access Requests:** • Will the personal data be extracted and provided to the data subject through usual business processes? • If not, how will subject access requests be managed?	Yes
Data Transfers **GDPR Article 44, 45** **or** **The Act Section 72 to 78**	**4.1.8 Data Transfers:** • Will the data be held or transferred outside the UK? If yes, where will it be held or transferred to? • Will the data be held or transferred outside the EEA? If yes, where will it be held or transferred to? • What processes will be in place to ensure it any data stored outside the EEA is adequately protected?	No, it will be retained in the UK
Lawfulness **GDPR Article.6** **or**	**4.1.9 Lawfulness:** What lawful basis will apply to how the data is processed? *The bases are:*	Performance of a public task.

The Act Section 35, 36	• Consent (which is clear, informed and feely given). • Contract (which stipulates the data processing is required). • Legal obligation (Act of Parliament, SI, common law). • Vital (health) Interests (of data subject or another). • Performance of a public task, (including administration of justice, exercise of a function of either House of Parliament, exercise of a function conferred on a person by an enactment or rule of law, or exercise of a function of the Crown, a Minister of the Crown or a government department). Does this legal basis require you to process the data or simply gives you coverage to process it?	Health interests of serving prisoners. Visitors will have to give consent to taking part in the trial. An open letter will be given to each visitor detailing that the trial is taking place. Should a visitor decline to take part, their visit will not be hindered in any way. Required to process for the prevention, investigation, detection or prosecution of crime, and for security of the prison.
Consent **GDPR Article 7** **or** **The Act Section 35, 42**	**4.1.10 Consent:** • If you will be relying on consent, will it be given by a confirmation or action by the individual? How will this be recorded? • Will plain language be used? • What processes will be in place to manage withdrawal of consent?	Data will be recorded and retained for the duration of the trial only unless an individual refuses after being informed of the trial and its purposes. The letter informing them of collection will be in plain English. In the event of a visitor withdrawing their consent, their data will be removed from the database and confirmed as such by an HMPPS employee.
Special categories of Personal Data **GDPR Article 9, Schedule 1**	**4.1.11 Special categories:** *For completion if processing under GDPR **not** Part 3 of the DPA (2018).* Will you process any of the following special categories of personal data: • Race; • Ethnicity; • Health; • Religion,	N/A

	• Sex life; • Sexual orientation; • Political views; • Trade union membership; or • Genetic or biometric data? *If you are processing sensitive personal data under the GDPR (rather than Part 3 of the DPA (2018)), you need to establish a specific lawful basis to do so, which are:* a) Explicit Consent; b) Necessary in compliance with legal obligation; c) Vital (health) Interests; d) By a legitimate, not-for profit body with a political, philosophical, religious or trade union aim; e) Data which has manifestly been made public by the data subject; f) Establishing / defending a legal claim or Courts acting in a judicial capacity; g) Substantial public interest; h) Preventative occupational medicine, or occupational health; i) Public interest in the public health (serious); and j) Archiving in the public interest or for historical/scientific research. Indicate which basis you will use to process any special categories of personal data. *If you are processing sensitive data under Part 3 of the DPA (2018), this processing is called 'sensitive processing' and requires different lawful bases. Please respond to the question about this processing at the end of this section.*	

Criminal Convictions & Offences **GDPR Article 10** **or** **The Act Section 11**	**4.1.12 Criminal Convictions:** *The GDPR sets out requirements for processing criminal conviction data outside the context of Part 3 of the DPA (2018) i.e.* ***not*** *for 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.* • Will you process personal data about offences/convictions? • Do you have a legal basis to hold and process it i.e. are you an official body or required by law to process criminal conviction data? The processing will also need to meet a condition in Part 1, 2 or 3 of Schedule 1 of the DPA 2018.	No.
Right to Erasure **GDPR Article 17** **or** **The Act Section 47 and 48**	**4.1.13 Erasure:** • What processes will be in place to manage requests for erasure?	At the end of the trial all data will be deleted from all systems used. If an individual requests their data to be deleted before the end we will make this happen and it will be confirmed by onsite HMPPS staff. The open letter to visits will contain the contact details for MoJ Data Protection Officer.
Right to Restriction **GDPR Article 18** **or** **The Act Section 47 and 48**	**4.1.14 Restriction:** • What processes will be in place to manage requests to restrict processing?	Refusal by the visitor to take part in the trial. This will have no detrimental impact on their visit. If they withdraw their consent their data will be removed as soon as possible and confirmed by an onsite HMPPS employee.

Data Portability* **GDPR Article 20**	**4.1.15 Portability:** • Will the data be extractable in a machine-readable format? • What processes will be in place to manage requests to port the data? *NB: This does not apply to data processed on the legal basis of legal obligation (e.g. an enactment or legislation).	Yes. The data will remain within the environment of the trial
Automated Decision Making **GDPR Article 22** **or** **The Act Section 49 and 50**	**4.1.16 Automated Decision Making:** • Will the processing involve automated decision making affecting a person? If yes, please explain the circumstances of the processing and the impact of it on the individual. • What processes will be in place to manage objections to automated decision-making?	No, while facial recognition will use machine learning to match faces it will not decide whether the person has access to the prison. No operational decisions will be taken from this data during the trial
Joint Controllers & Processors **GDPR Articles 26 to 30** **or** **The Act Section 58 to 61**	**4.1.17 Data Sharing / Contracts:** • Will the data be shared with other business units/teams/parts of the Department? If yes, how will the data be shared/disclosed? • Will the personal data be shared with an external organisation? Please list and identify whether it is another government department or agency, a supplier or third party. • What kind of arrangement will be in place to covers this? - Contract? - Data Sharing Agreement? - Memorandum of Understanding? - Other? • How will the data be shared/disclosed with the other organisations?	Data will be processed and shared with the three triallists companies but only on the machine based locally. An MOU has been agreed with each of these.
Security **GDPR Article**	**4.1.18 Security:** • How will the data be secured and kept safe? What technical / operational security features and/or policies protect it? Consider risk	Information will be retained on trial equipment which has appropriate security accreditation or in accredited third party cloud storage.

32 **or** **The Act Section 66**	of data loss, corruption and confidentiality breaches. • What is the state of technology in this area? • Will the data encrypted at rest and in transit? If not, explain why. • How and when will the data be pseudonymised? If not, explain why. • Will back-ups be taken? • What processes will be in place to determine who will have access to the data/system? • What level of security clearance will be required to access the system/data? • What data protection/security training will users of the data/system be required to have? • Will the security of the system be required to have any formal accreditation or independent certification (e.g. ISO27001)? • Are the organisations processing the data signed up to any approved codes of connection or certificate schemes? • Will the security of the system/premises be tested regularly? • What information asset register and/or risk register will the data be recorded on?	Biometric technology is new to HMPPS however all three technologies chosen are already in use in HMG settings (policing) or in secure locations (airports) All data is encrypted both at rest and in transit for all three trial machines. Security certification (including cyber essentials) has been provided to MoJ accreditors. Access to the data will be restricted to those HMPPS staff who have been trained to operate the machines being trialled. These staff have the vetting to work in a prison and access other personal data we retain. As this is a 4-6 week trial there will be no ongoing testing and as the equipment is on loan there will be no information asset register. Redacted under section 31 exemption

Section 4.2: Part 3 of the DPA (2018)

You should only complete this section if your proposal will process data under Part 3 of the DPA (2018).

Requirement		Comments
Sensitive processing **The Act Sections 35 (3) – (5), (8) 42, Schedule 8**	**4.2.1 Sensitive processing:** Are you processing sensitive data under Part 3 of the DPA (2018): • Race; • Ethnicity; • Health; • Religion, • Sex life; • Sexual orientation; • Political views; • Trade union membership; or • Genetic or biometric data? If so, have you identified your legal basis for doing so: • Explicit consent: • Additional schedule 8 conditions: a) Judicial and statutory purposes. b) Protecting the individual's vital interests. c) Personal data already in the public domain. d) Legal claims and judicial acts. e) Preventing fraud. f) Archiving, research and statistics.	Biometric Data. Legal basis is preventing fraud Also explicit consent for the trial Protecting individual's vital interests Archiving research and statistics

Auditable Logging **The Act Section 62**	**4.2.2 Logging:** • Will the system / process have a logging function to track changes and access to the data so that a record (or log) is created each time a user does something with the data, such as; (a) adding / collecting it; (b) altering or amending it; (c) viewing or reviewing it; (d) sharing, disclosing or transferring it (including to whom) (e) combining it with other data (e.g. to identify / prove something) (f) deleting or archiving it.	All systems are fully auditable
Data Distinction **The Act Section 38(3)**	**4.2.3 Distinction (of data subjects):** • Will the system / process make a clear distinction between personal data relating to different types of data subject, and why it is being processed for criminal law enforcement purposes? This should include: (a) persons suspected of committing a criminal offence; (b) persons convicted of a criminal offence; (c) persons who are or may be victims of a criminal offence; (d) witnesses or other persons with information about offences The distinction should prevent the confusion of the above individual's data.	During the trial the systems will only be collecting the data from the participants. Redacted under section 31 exemption

Section 4.3: Other privacy legislation and policies

Requirement		Response	If yes, provide details
Privacy & Electronic Communications Regulations 2003	**4.3.1 Technology** Does the project/policy/initiative involve new or inherently privacy-invasive electronic communications technologies? *For the avoidance of any doubt, 'communication' means any information exchanged or conveyed between finite parties by means of a public electronic communications service, but does not include information conveyed as part of a programme service, except to the extent that such information can be related to the identifiable subscriber or user receiving the information.*	☐ Yes ☒ No	
	4.3.2 Communication providers *Does the project/policy/initiative involve new or existing communication providers?* *For the avoidance of doubt, 'communication providers' means a person or organisation that provides an electronic communications network or an electronic communications service.*	☐ Yes ☒ No	
	4.3.3 Communication subscribers / users *Does the project/policy/initiative involve new or existing communication subscribers / users?* *For the avoidance of doubt, 'communication subscriber' means a person who is a party to a contract with a provider of public electronic communication services for the supply of such services. 'User' means an individual using a public*	☐ Yes ☒ No	

	electronic communications service.		
Human Rights Act 1998	***4.3.4 Article 2: Right to Life*** *Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to life, subject to any limitations as may be defined in Article 2(2)?* *For the avoidance of any doubt, the limited circumstances are that in peacetime, a public authority may not cause death unless the death results from force used as follows:* • *Self defence or defence of another person from unlawful violence;* • *Arresting of someone or the prevention of escape from lawful detention; and* • *A lawful act to quell a riot or insurrection*	☐ Yes ☒ No	
	4.3.5 Article 3: Prohibition of Torture *Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not subjected to torture or inhuman or degrading treatment?* *For the avoidance of doubt, this is an absolute right.*	☐ Yes ☒ No	
	4.3.6Article 4: Prohibition of Slavery or Forced Labour *Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not held in servitude or*	☐ Yes ☒ No	

	forced to perform compulsory labour? *For the avoidance of doubt, this is an absolute right; the following are excluded from being defined as forced or compulsory labour:* • *Work done in ordinary course of a prison or community sentence;* • *Military service;* • *Community service in a public emergency; and* • *Normal civic obligations.*		
	4.3.6 Article 5: Right to Liberty and Security *Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not deprived of their liberty subject to certain limitations?* *For the avoidance of doubt, the following limitations apply when a person is:* • *Held in lawful detention after conviction by a competent court;* • *Lawfully arrested or detained for non-compliance with a lawful court order or the fulfilment of any lawful obligation;* • *Lawfully arrested or detained to effect the appearance of the person before a competent legal authority;* • *Lawfully detained to prevent the spreading of infectious diseases;* • *Lawfully detained for personal safety (applies to persons of unsound mind, drug addicts etc); and* • *Lawfully detained to prevent unlawful entry into the country or lawful deportation from the country.*	☐ Yes ☒ No	

	4.3.7 Article 6: Right to a Fair Trial *Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to have a public hearing within a reasonable time by an independent and impartial tribunal established by law?* *For the avoidance of doubt, the hearings included are both civil and criminal proceedings that are not specifically classified as hearings that must be heard 'in camera', i.e. closed to the public.*	☐ Yes ☒ No	
	4.3.8 Article 7: Right to no Punishment without Law *Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to not be prosecuted for a crime that was not, at the alleged time of commission, constitute a criminal offence under national or international law?* *For the avoidance of doubt, this is an absolute right.*	☐ Yes ☒ No	
	4.3.9 Article 8: Right to Respect for Private and Family Life *Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to respect for privacy in terms of their private and family life subject to certain qualifications?* *For the avoidance of doubt, the qualifications are:* • *Legal compliance;* • *National security;* • *Public safety;*	☐ Yes ☒ No	

	• *National economy;* • *Prevention of crime and disorder;* • *Protection of public health and morals;* • *Protection of rights and freedom of others.*		
	4.3.10 Article 9: Right to Freedom of Thought, Conscience & Religion *Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to freedom of thought, conscience and religion subject to certain qualifications?* *For the avoidance of doubt, the qualifications are:* • *Unless prescribed by law;* • *In interest of public safety;* • *Protection of public order, rights or morals;* • *Protection of rights and freedoms of others.*	☐ Yes ☒ No	
	4.3.11 Article 10: Right to Free Expression *Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to hold opinions and express their views singly or in dialogue subject to certain qualifications?* *For the avoidance of doubt, the qualifications are as set out in Article 9 above.*	☐ Yes ☒ No	

	4.3.12 Article 11: Right to Freedom of Assembly & Association *Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to freedom of peaceful assembly and association with others subject to certain qualifications.* *For the avoidance of doubt, the qualifications are as set out in Article 9 above.*	☐ Yes ☒ No	
	4.3.13 Article 12: Right to Marry *Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to marry and found a family subject to certain restrictions?* *For the avoidance of doubt, the restrictions are regulated by law so long as they do not effectively take away the right, e.g. age restrictions apply.*	☐ Yes ☒ No	
	4.3.14 Article 14: Right to Freedom from Discrimination *Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be treated in a manner that does not discriminate the individual from others subject to certain restrictions?* *For the avoidance of doubt, this right is restricted to the conventions as set out in the European Convention of Human Rights 1950; the grounds for discrimination can be based on:*	☐ Yes ☒ No	

	• Sex • Race • Colour • Language • Religion • Political persuasion • Nationality or social origin • Birth • Other status.		
	Articles: 16 / 17 / 18 *Not relevant for the purpose of this questionnaire*		
Regulation of Investigatory Powers Act (RIPA) 2000	***4.3.15*** *Does the project/policy/initiative involve new or inherently privacy invasive electronic technologies to intercept communications? For the avoidance of doubt, 'communications' is defined in RIPA Part V, section 81(1).* *Does the proposal involve new or inherently privacy invasive electronic technologies pertaining to the acquisition and disclosure of data relating to communications?* *Does the proposal involve new or inherently privacy invasive electronic technologies pertaining to the carrying out of surveillance?* *Does the proposal involve new or inherently privacy invasive electronic technologies pertaining to the provision of the means by which electronic data protected by encryption or passwords may be decrypted or accessed?* *Does the proposal undertake any of the functions of the Security Service, the Secret Intelligence Service or the Government Communications*	☐ Yes ☒ No	

	Headquarters?		

Section 5: Risk management

Risks to individuals can be categorised in different ways and it is important that all types of risk are considered. These range from risks to physical safety of individuals, material impacts (such as financial loss) to less tangible impacts (for example, distress caused).

You should consider:

- Risks to individuals, e.g. inappropriate data sharing, transparency and privacy
- Corporate, e.g. sanctions, fine and reputational damage and cost to later mitigations; and
- Compliance risks with the GDPR, DPA (2018), Privacy and Electronic Communications Regulations, human rights legislation and other privacy legislation.

You should use the MoJ five-point risk assessment scale to calculate the risk by combining scores for impact and likelihood of the risk. For example, a risk with an impact of 3 and likelihood of 4 would provide a combined risk rating of 12 (medium). More information is available in the guidance.

Risk(s) identified in the assessment *(for example risks to individuals, corporate risks, compliance risks)*	***Solution(s)***	***Result:*** *is the risk eliminated, reduced, or accepted?*	***Evaluation:*** *is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project/policy/initiative?*	***Impact***	***Likelihood***	***Rating (IxL)***
Distress to visitors from undergoing more rigorous checks	*Visitors given option to opt out of the trials*	*Reduced*	*Yes*	*3*	*1*	*4*
Risks that equipment, as new technology will not be secure	*Undertaking closed trials* *Validation of accreditation*	*Reduced*	*Yes*	*4*	*1*	*4*

	before trials take place					

Contributors and approvals

Stakeholders/Participants. What organisations and individuals contributed to this assessment (include their role/function)? You should record the input of the Data Protection Officer, internal and external stakeholders, including any difference of opinion.			
Name	***Role***	***Organisation***	***Nature of Input (including any difference of opinion)***

Approved by:	**Date:**