Data Protection Impact Assessment (DPIA) Screening Checklist & Template

Xchange Platform

Preamble

Police forces are required to comply with Data Protection legislation – (i) the Data Protection Act 2018 (DPA) when they processes personal data for any of the Law Enforcement Purposes, and (ii) the UK GDPR, as supplemented by the DPA, when the processing is for General Purposes (anything that does not fall under the Law Enforcement Purposes definition).

One of the obligations arising from the Data Protection legislation is the requirement for police forces to conduct a Data Protection Impact Assessment (DPIA) where the prospective processing of personal data is likely to result in a '**high risk to the rights and freedoms of individuals**'.

Even if that 'high risk' threshold is not reached, it is good practice to complete a DPIA, particularly when developing a Data Sharing Agreement.

The DPIA must be undertaken prior to the processing starting and, in some cases, cannot commence without the prior authorisation from the Information Commissioner's Office (ICO) once they have reviewed the DPIA.

The relevant parts of the Data Protection legislation concerning DPIAs can be found at:

- Section 64 of the DPA and Section 65 of the DPA for processing for Law Enforcement Purposes; and,
- Article 35 of the UK GDPR and Article 36 of the UK GDPR for processing for General Purposes.

The ICO has produced extensive guidance on DPIAs for processing for Law Enforcement Purposes and General Processes.

Screening

In order to determine whether a DPIA is required it is necessary to first conduct a screening exercise to assess whether the prospective processing of personal data is likely to result in a 'high risk to the rights and freedoms of individuals.

The screening should occur where there is any new or significant changes to existing processing of personal data.

Even if the screening does not result in a requirement to conduct a DPIA it is often beneficial to conduct one.

A DPIA Screening Checklist appears on the next page which should be used to determine if a DPIA is required.

DPIA Screening Checklist

If you intend to process any types of the personal data set out in List 1 **and** the processing appears in List 2 a DPIA must be conducted.

List 1 **Types of Personal Data processed**	**List 2** **Types of high-risk Processing**
Racial or ethnic origin	Innovative use or new technology or solutions
Political opinions	Denial of service or rights
Religious or philosophical beliefs	Large-scale profiling, evaluation or scoring
Trade union membership	Biometrics or genetic data
Genetic data	Automated decision-making
Biometric data	Combining or matching datasets
Health data	Invisible processing
Sex life	Tracking or monitoring
Sexual orientation	Targeting of children or other vulnerable individuals
Criminal activity	Risk of physical or mental harm
Allegations	
Investigations	
Proceedings	

Confirm which (if any) of the above apply:

List 1
Racial or ethnic origin
Biometric data
Criminal activity
Investigations
Allegations

List 2
Large-scale profiling, evaluation or scoring
Biometrics or genetic data

Screening undertaken by: ****name redacted without exemption as stated within request****

Date undertaken: 21/02/2023

Outcome of Screening:

A DPIA is required for this processing.

If the Screening Checklist identifies a requirement to undertake a DPIA (or you choose to undertake one) please move on to the next page. If there is no requirement, please email this document with the fields above completed to dpo@npcc.police.uk

NPCC DPIA Template

The template, starting on the next page, has been derived from the ICO's and can be completed to record details of the DPIA process and outcome.

Steps 1 to 5 and parts of 7 should be completed by an appropriate person with the necessary knowledge of the processing of personal data being considered (normally the Business Subject Matter Expert (SME) and/or Business Lead[1]).

The NPCC DPO will assist completion of the template where required and in any case will complete Step 6 and parts of Step 7.

The fields requiring completion can readily be identified through appearing with a pale blue/green background when a cursor is hovered over them.

[1] Business Lead is likely to be the Portfolio Lead or Head of National Unit. Subordinates with necessary knowledge and authorisation can participate in the completion of this document

Data Protection Impact Assessment (DPIA)

Xchange Platform

Freedom of Information Act & Information Security

This document (including attachments and appendices) may be subject to an FOI request and the NPCC FOI Officer & Decision Maker will consult with the author on receipt of a request prior to any disclosure. For external Public Authorities in receipt of an FOI request concerning this document, please consult with npcc.foi.request@npfdu.police.uk.

In compliance with the Government's Security Policy Framework's (SPF) mandatory requirements, please ensure any onsite printing is supervised, and storage and security of papers are in compliance with the SPF. Dissemination or further distribution of this document is strictly on a need-to-know basis and in compliance with other security controls and legislative obligations.

Purpose

This DPIA document has been used to:

- identify any privacy or information risks concerning the processing of personal data
- determine any mitigations necessary to bring those risks down to an acceptable level
- provide a record of those mitigations and the decision by Business Lead whether to accept and adopt them
- provide a record of the NPCC's Data Protection Officer's views on the initiative.

Document Administration

Government Security Classification:	**OFFICIAL.**
If OFFICIAL-SENSITIVE set out any handling instructions below:	
N/A.	
For inclusion in FOI Publication Scheme?	**No.**
Version:	**v1.4**
Author(s):	****name redacted without exemption as stated within request****
Date Issued:	**03/08/2023.**
Date to be next reviewed:	**06/09/2023.**
Information Asset Owner (IAO) for this document:	**Nick Dean – NPCC portfolio lead for forensics - National SRO.**

Leads' Details

NPCC Coordination Committee overseeing initiative:

National Crime Coordination Committee.

NPCC Portfolio overseeing initiative:

Forensics.

National Unit overseeing initiative:

Cambridgeshire Constabulary.

Information Asset Owner(s) for information involved in this initiative:

Force Chief Constables are IAOs for the information they process. The NPCC national portfolio lead will act as an agent on behalf of other forces for the Xchange project.

Business SME(s) involved in creation of this DPIA:

****name redacted without exemption as stated within request****

Data Protection Advisor:

****name redacted without exemption as stated within request****

Comments:

N/A.

Step 1: Introduction

This section is intended to provide a concise introduction to the initiative, how it arose and the processing of personal data it involves.

1a. Provide a short introductory summary of the intended processing, including the purpose(s) of the processing and the desired outcome of the processing.

PDS owns and manages the Xchange, a cloud (Amazon Web Services) hosted platform with a suite of forensic applications.

Police forces are independent controllers for the personal data they upload onto the platform. There is no connection or sharing mechanism between forces for this data.

PDS is a processor and engages several sub-processors, which include Amazon who provide their cloud hosting platform and CACI who provide UK based technical support for the system.

PDS owns and manages the Xchange, a cloud hosted platform with a suite of forensic applications. The Xchange platform was developed under the Transforming Forensics programme and is supported by the PDS IT Support Management (ITSM) capability. The service is now called Digital Fingerprint Capability (DFC).

Xchange (the Platform) offers a fingerprint analysis toolset which supports at-scene transmission of fingerprints (as well as palm, toe and sole prints) and other scene of crime images into forensic bureaux (Bureaux) for analysis. The Platform has been designed to be modular and open in its build and design, including using microservices and using the design principle of infrastructure as code, ensuring the Platform build is as future proofed as possible and owned by Policing.

The Platform will collect and process personal data about two main categories of data subject:

a) Force employees/contractors (crime scene investigators (CSIs), other officers, allocators, fingerprint examiners, reviewers etc.) who use the Platform to log and transmit information and to use/access/maintain the Platform (Users); and

b) "Persons of interest" relevant to the crime, such as suspects, witnesses, victims, homeowners, other eliminations (e.g. visitors to the property) and other individuals considered relevant to the crime scene (Persons of Interest).

Personal data held about Users within the Platform will be limited to User login details and basic User information (name, employee number, force/Bureau). Personal data about Persons of Interest will be more extensive and will include name, date of birth, exhibits (including vehicle registration numbers, digital device identification and IP addresses), and fingerprint/other biometric marks (biometric) and identifications, if made. There is no specific area designated for suspect information addition by CSI's or FEL officers. There are however free text fields, and a 'Submission notes' section within the Platform for Users to submit notes. It is unlikely that Users will submit personal data into these fields, but incidental processing in this field is possible.

The Platform will also hold information about the crime itself, such as the crime reference number, type and date, which will not, in itself, be "personal data" but may become personal data if the crime is then linked to a particular Person of Interest (most notably a suspect). There will also be free text fields within the Platform for Users to submit notes. It is highly unlikely that Users will submit personal data into these fields, but it is possible.

1b. Describe where the intention for the processing arose from i.e. who decided to progress this initiative, in response to what?

This processing is not novel within forces. The Xchange platform further digitizes and centralises the process of obtaining and processing marks taken from crime scenes. This project was developed and funded by the Home Office as part of 'transforming forensics programme'.

1c. Confirm whether the processing is for Law Enforcement Purposes or General Purposes. (within policing if the processing is not for Law Enforcement Purposes it will be for General Purposes). Processing could be for both Law Enforcement and General Purposes.

The majority of the processing will be for the Law Enforcement Purposes. This includes information about "persons of interest" and logging/audit data relating to staff processing the data.

There will be limited General Purposes processing where policing staff/contractors are added/removed from the Platform as well as training for the platform.

Legal basis: DPA18 s.35(2)(b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority. This is to collect information from a crime scene for use in criminal investigations.

There will be sensitive processing including biometric information, which requires a DPA18 Schedule 8 condition – statutory purposes. This processing is strictly necessary for statutory purposes, in this case by the exercise of a function conferred on a person by enactment (Chief Constables).

There will be limited processing for general purposes to manage force employees/contractors access to the system and provide support/training. This processing is required for running the platform and is necessary for the performance of a task carried out in the exercise of official authority vested in the controller (UK GDPR Article 6 1(e)).

1d. If relevant, describe what non-Data Protection legislative framework supports or requires the processing i.e. is the processing mandated or required by an Act of Parliament?

This processing is not mandated or required by an Act of Parliament. However, the processing must also be compliant with the Protection of Freedoms Act 2012.

Step 2: Describe the processing

This section is intended to provide details of the personal data involved and how it will be processed throughout its lifecycle.

Processing Operations

2a. Describe how the personal data involved will be obtained or created, including from where, by whom, by what means, when, and how frequently.

In Release 5 further functionality was added to assist an organisation to conform to retention and weeding requirements. Every case created is given a retention review date on creation, and this review date is based on the MOPI classification of the offence type. E.g., for volume crime 6 years after the case is created. Privileged users can run reports that will extract cases that have passed their retention date. They can then review the case, and then retain or weed via a fully auditable on-screen process.

The sources of data are as follows:

- **User information: User login details will be provided by the force during the onboarding process and logins allocated to each User by the PDS Technology Enhancement and Support (TES) provider. Users will be given training during which they will be required to set a new password. After the initial onboarding, new Users will need to complete a form for line manager approval, which is then sent to the force's IT helpdesk and to the PDS TES provider for the User to be set up. Other User information attached to a docket will be uploaded to the Platform by the User themselves.**
- **Crime scene marks: (the vast majority of which are presumed to contain biometric data) will originate from both the scene, as well as from evidence recovered from the scene and submitted to the FEL for examination. This will take the form of digital images. CSIs and other officers (who have had a user account created) can also add intelligence into the PDS Xchange manually at the scene, such as contextual images of the scene (containing the context of where the images were found) and information about potential eliminations. There is no specific area designated for suspect information addition by CSI's or FEL officers. There are however free text fields, and a 'Submission notes' section within the Platform for Users to submit notes. It is unlikely that Users will submit personal data into these fields, but in theory, it is possible. Other information can be uploaded by Users, for example officers and CSI's can upload details of eliminations for marks to be checked against. Details of suspects can be uploaded by Bureau staff following other forensic evidence, such as a DNA match, or if a suspect is later arrested and linked to the crime at that arrest. Data originating from persons of interest – both biometric (e.g. fingerprint and palmprint forms) as well as demographic will again be variable, but is likely to be significant. Forms will either originate from requests to IDENT1 from Bureau end users or submitted to the bureau by other means (e.g. hand-delivered by officers)**
- **Crime scene evidence: The CSI at the crime scene will collect marks either at the scene itself, or by recovering property from the scene that has marks on it, in which case the property will be sent to a lab to develop the marks to be sent to the Bureaux. CSIs can also add intelligence into the PDS Xchange manually at the scene, such as contextual images of the scene (containing context of where the images were found) and information about potential eliminations.**
- **FEL Data: Data developed by the forensic lab.**
- **People information sources: Other information can be uploaded by Users, for example lab officers and CSIs can upload details of eliminations for marks to be checked against. Details of suspects can be uploaded by Bureau staff following other forensic evidence,**

such as a DNA match, or if a suspect is later arrested and linked to the crime at that arrest. Both FEL and CSIs have free-text fields where suspect/any data could be added.

- **IDENT1: If there is a match on IDENT1, a form will need to be specifically requested for export from HOB to the Platform by the bureau user.**

The Platform, and therefore the data, will be hosted on AWS. Live data will only be held in the production environment. Data held within the development environment is synthetic data. Data held within the pre-production, training and test environments will be "ground truth" data, which comprises fingerprints taken from individuals working within the TF programme and other donors who have agreed for their fingerprints to be used in conjunction with fake names and details for testing and training purposes. The ground truth database from which ground truth data is taken is held elsewhere and contains live data, and is subject to a separate DPIA.

AWS hosts the data securely on UK servers, subject to AWS's standard data processing terms and security measures.

The initial capability release (Release 1) enabled the allocation and management of fingerprint analysis work, digital analysis of friction ridge detail, on-screen comparison of images, and the ability to digitally record notes and outcomes. Building on the initial release, the second release included Home Office Biometrics (HOB) integration to allow the automatic import of Tenprint images from IDENT1 into the Platform. IDENT1 is the national automated fingerprint system which collates fingerprints and other crime scene marks in a single database, allowing police forces to search and compare marks. IDENT1 forms part of the Home Office's wider HOB Programme which delivers biometric capabilities across law enforcement and government. Additionally, a mobile application has been developed so that CSIs can directly upload images from a crime scene and additional integration with the National Crime Agency has been implemented. The NCA integration enables the NCA to use the Platform to request and receive images from IDENT1 securely. Images will be stored in a separate S3 bucket and provided to the NCA using a one-time unique url.

Broadly, the Platform allows lab officers in the FEL and CSIs working at crime scenes to submit fingerprints and other identifying marks (e.g. toe, sole, palm prints) found at the scene, together with information about that crime scene, to Bureaux electronically for analysis of the marks. The Platform will package all information submitted by the CSI into a "docket" which is transmitted to the relevant Bureau. The mark is then analysed by the Bureau and identified using IDENT1 or manual methods of identification. Evidence of identification is manually uploaded to the Platform. The Platform also allows further upload of information relevant to the case as the case progresses and secure storage of that information to act as a centralised record of the forensic analysis in relation to the specific case.

2b. Once the personal data has been obtained set out in chronological order and stage-by-stage how it will be subsequently processed. For each stage describe the processing operation involved, including what will occur, who will be involved, when and how frequently it will occur. Processing will include storage, amendment, disclosure, sharing and disposal of the personal data.

Fingerprint marks will be photographed and uploaded by the CSI at the crime scene, together with information about their origin, any other contextual information about the crime scene (E.g., the light switch where the mark was powdered, where the gun was in the room, the bonnet of the car where the blood mark was etc) and the CSI's own User information. Where marks are taken for elimination purposes, details about the relevant Person of Interest (elimination) will also be collected and uploaded along with that person's marks. This information will be packaged into a "docket" by the Platform and will be transmitted to the relevant Bureau. Photographic images of marks developed by FEL officers will be uploaded. Bureau users may also receive images from (external) agencies for examination. Once again, images will be uploaded onto the Platform from these areas and packaged into a "docket" for examination.

An allocator, or other end user at the Bureau will review the docket and check the local crime management system (CMS) for potential suspects, or other POI, whose details can then be

manually added to the docket by the end user. A POI form(s) may be requested and retuned (uploaded) via the HOB gateway to the platform. Before upload to the Platform the examiner should check that the image in IDENT1 is legally held (complying with obligations relating to the regulation of biometric data under the Protection of Freedoms Act 2012 (POFA) by checking against the Police National Computer (PNC). Paper forms can also be digitised for upload onto the Platform.

The examiner assigned to the docket will have the ability to assess the value of mark(s) within it. The examiner has the option of checking marks of value manually (i.e. digitally on-screen, rather than with the aid of a search algorithm) against Persons of Interest, or searching on IDENT1 (if of sufficient quality).

If the mark is unidentified and of sufficient quality to perform a search, the examiner will upload the mark into IDENT1 (via the Generic Mark Camera Interface, which is part of IDENT1) and will search against parameters set by the examiner. IDENT1 will return potential matches and the examiner will manually review the returned candidate list to determine if any of the returned results is, in fact, a match.

If there is no match, the mark is not identified. If there is a match, a POI form(s) may be requested and returned (uploaded) via the HOB gateway to the Platform. Before carrying out the work to confirm the match, the examiner should check that the image in IDENT1 is legally held (complying with obligations relating to the regulation of biometric data under the Protection of Freedoms Act 2012 (POFA)) by checking against the Police National Computer (PNC). If the image is legally held and the examiner identifies a match, the examiner will add the form image(s) to the docket for the relevant case within the Platform. If the image is not marked as being legally held, the image will not be marked as identified and assigned to a case on the Platform. Images that have been returned by HOB will be automatically deleted if they have not been assigned to a case after 90 days. The force is responsible for ensuring it is comfortable that the image is legally held and can be lawfully used and uploaded into the Platform. There is a risk that the examiner could fail to carry out this step which could result in marks and identifications from IDENT1 being assigned to a case on the Platform without a legal justification for that mark being held.

In regard to Persons of Interest whose data is not already known to be held in IDENT1, their prints can be taken by the CSI at the scene (or an officer at a later time). Forms received in this way can be manually uploaded to the system following digitisation (most likely via scanning) and the examiner is able to compare any marks against those prints. If the mark is not of sufficient quality to search on IDENT1, the examiner will manually check the mark against any named Persons of Interest (i.e., Persons of Interest who have been identified by the force as potentially being involved or being an elimination). If a match is discovered related to a paper elimination form given to the bureau, the examiner can digitise the form to allow it to be uploaded onto the Platform.

2c. Confirm whether any of the processing will involve joint controllership with another controller(s). If so, describe when and how the personal data becomes subject of joint controllership.

Forces will be independent controllers.

2d. Confirm whether or not any of the processing will involve the use of a processor to process personal data on behalf of the NPCC. If so, describe when and how the personal data becomes subject of processing by a processor.

PDS is providing the Xchange platform and the Fingerprint application to process the data. A Data Processing Contract will be in place with the processor. Similarly, contracts are in place with sub processors (Amazon and CACI). Amazon will be subject of processing throughout, given that they host the environment for the platform. CACI will only process data when providing technical support for the system and training for staff/contractors.

AWS hosts the data securely on UK servers, subject to AWS's standard data processing terms and security measures. AWS reserves the right, in its terms and conditions, to transfer data to other regions if required in an emergency or otherwise to provide the services. As standard, AWS has appropriate mechanisms in place to govern these transfers if they constitute transfers outside the UK. AWS's terms have been reviewed to confirm the position relating to model clauses for processing personal data. It is noted that since the *Schrems II* judgment in July 2020, there are additional requirements that must be complied with when relying on model clauses. All PDS Xchange data is subject to technical controls including encryption in transit and at rest, with private keys under the control of PDS Xchange. If further measures are required following implementation of final guidance, this will be assessed and implemented as required.

2e. Describe the extent to which there is likely to be public, media or pressure group concerns over the processing.

There is not likely to be significant concern around the processing of this data given that biometric processing at crime scenes is widely understood and accepted.

2f. Identify which, if any, of the processing operations could potentially present high risks to the confidentiality of the personal data involved.

There are no outstanding high risks presented by any of the processing operations to the confidentiality of individuals. However, there is a significant sensitive processing and the impact to the confidentiality regarding 'persons of interest' is severe.

2g. Describe the extent to which the processing will be novel, new, or not resembling processing previously occurring.

This is not novel or new processing. Forces are already processing personal data for the same purposes before the Xchange platform is introduced. The only novelty will be that all of these operations will be on one platform with data feeds from the National Crime Agency and Home Office Biometrics (HOB – IDENT-1).

2h. Provide an overview of the measures to be put in place to ensure adequate security/maintenance of confidentiality of the personal data when it is processed. These measures may be technical or organizational ones proportionate to the nature of the personal data involved. Technical measures can be defined as the measures and controls afforded to systems, devices, networks and hardware and encompass cybersecurity, encryption and pseudonymisation, physical security, secure disposal, passwords and access controls. Organizational measures may consist of internal policies, organizational methods or standards, and controls and audits. They can include information security policies, business continuity plans, risk assessments, polices & procedures, awareness & training, reviews & audits, and due diligence.

****Security information redacted as worded within your request****

2i. If the processing involves use of new or altered software or IT infrastructure describe what measures have been put in place or are planned to ensure that software or IT infrastructure has or will be accredited to confirm it is suitable secure to use.

****Security information redacted as worded within your request****

2j. Describe the processes that will ensure the personal data will not be retained longer than is necessary for the purposes set out at 1a.

The expectation is that forces will retain and delete data in accordance with MOPI. Unless otherwise instructed by a force, data (including logs and audits) will be retained within the Platform for up to 100 years.

Data can be deleted before the end of the relevant retention periods by the Data Controller in line with their data retention policies and legal/regulatory obligations. The intention is for this to be "self-service", without Members having to come to PDS to request deletion of data. Deletion usually takes place by deleting a specific case, rather than deleting information about specific individuals. When information is deleted, the docket and associated case will be deleted, but logs and audits will be retained for audit trail/accountability/record-keeping purposes. If a Member needs to delete information about a particular data subject whose data is held across several different cases, the Member will need to identify where (i.e. in relation to which cases) that data is held so that it can be deleted from different cases.

When information is deleted, the docket and the associated case will be deleted, but logs and audits will be retained for audit trail/accountability/record-keeping purposes.

Release 5 delivers the following privileged roles to organisations – Edit Administrator: able to amend or delete certain data including free text in line with requirements. Case deleter: force user able to delete a whole case before the end of the retention date. Case weeder: able to locate casework that has passed its retention review period and delete. Auditor: able to run reports on users and case activity including a key word search.

Nature of the Personal Data

2k. Describe the type of personal data involved, including whether it is Criminal Offence Data[2], Special Category Data[3], or Data Subject to Sensitive Processing[4]. Where appropriate list data fields.

Force staff/contractors:

- **Basic user information (name, employee number, associated force)**

For "Persons of Interest":

- **Images of fingerprints, contextual images and scene images.**
- **Individuals are appropriately categorised by designed (e.g. witness, offender, suspect etc)**
- **Comparison of fingerprints may include an individual's name associated with the images (i.e. 'suspect' and name, 'home owner' and name.**
- **Vehicle registration**
- **Digital device identification**
- **IP Address**

---

[2] Defined where processing is for General Purposes as personal data relating to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

[3] Defined where processing is for General Purposes as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[4] Defined where processing is for Law Enforcement purposes as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data, or of biometric data, for the purpose of uniquely identifying an individual; data concerning health an individual's sex life or sexual orientation.

- **Criminal offence information (reference number, type and date)**
- **Categorisation requirements: witness, victim or suspect etc**

Sensitive processing:

- **Finger, palm, toe, sole prints and other identifying marks (biometric)**
- **Racial or ethnic origin could be extrapolated through some images**

.

2l. Describe the volume of personal data involved, including how many individuals it will relate to.

The volume of data will depend on the number of forces using the Platform, the number of crime scenes and the number of marks collected at each crime scene. It is therefore difficult to say with certainty how much data will be collected and used, but it is likely to be significant number of individuals.

2m. Describe any criteria used to determine what personal data will be processed.

Personal data is limited to "Persons of interest" at a crime scene. Personal data of staff/contractors is limited to those who have access to the platform (or previously had access where recorded in audit logs).

2n. Describe the measures to be put in place to ensure an excessive amount of personal data is not processed. These may be technical and/or organizational ones.

All users will be trained before being given access to the system. The purpose for the use of the system is limited to crime scene investigations and access is limited to those that require it. Additionally, the platform is designed to only input data in specific ways described earlier in this document.

2o. What measures will be put in place to ensure the personal data processed is of the necessary quality (accurate, complete, clear etc). These may be technical and/or organizational ones.

Users have the ability to continuously update the information and all changes are appropriately logged. Staff/contractors using the platform will be appropriately trained before they process personal information on the platform.

Data Subjects

2p. Describe the types/categories of the data subjects whose data will be processed e.g. victims. witnesses, offenders, suspects, officers, staff etc.

"Persons of interest" – individuals whose personal data is captured at a crime scene

Staff/contractors – individuals whose information is captured to provide access to the system and whose processing activities are retained for logging purposes.

2q. Confirm whether the personal data is processed based on data subjects' consent and if so, describe how that consent will be obtained and recorded, and how withdrawals of consent would be managed.

Consent is not the basis for this processing.

2r. Describe the extent to which the personal data involved will relate to children or other vulnerable people.

Data relating to children and other vulnerable people (such as victims) will be processed where their information is related to the crime scene.

2s. Describe the nature of a force's relationship with data subjects, including whether they would expect their personal data to be used in this way, and the extent to which they can influence the processing.

The data subjects are either employed by a police force or their personal information is related to a crime scene (such as victims, witnesses, offenders or other subjects of interest).

Step 3: Consultation

This section is intended to stimulate consideration as to whether the views of internal or external stakeholders should be sought. Initiatives that have the potential to lead to public or media concern may benefit from consultation that could help enhance the processing. Clearly external consultation may be counter-productive if it were to reveal sensitive policing techniques or capabilities. Where the processing is largely consistent with a well-established approach there may be little benefit in consultation.

3a. Describe the extent to which you intend to consult, or already have consulted, with stakeholders on their views of the processing described in response to 2c. Stakeholders can include externally - data subjects, members of the public, campaign groups, partner organizations; internally – information security experts, ethics committees etc.

This DPIA is being completed centrally by the TF programme. Each force will be a data controller for the personal data input into the Platform in relation to that force's investigations and each force may produce its own DPIA if it considers appropriate. This has been recommended as part of the force onboarding process.

- **Force DPOs have been engaged through existing national data protection governance**
- **It is not considered necessary to consult with the cloud infrastructure provider. These types of providers would not generally be consulted, and it is unlikely to be appropriate to share extensive information regarding Xchange with such providers.**
- **We do not consider that public consultation is necessary in respect of the use of the Xchange Platform or the wider PDS Xchange solution. As detailed above, the collection and processing of fingerprint data for these purposes is not new and the effect on individuals of using the Platform will not differ significantly from the effect of the previous, manual processing of fingerprint data.**

3b. If consultation is not intended or is to be limited set out a rationale for adopting that position.

N/A.

Steps 4 & 5: Identify risks, assess risks, and determine measures to reduce risks

The table overleaf sets out in Column 1 generic information risks that could apply to the processing of personal data under any initiative.

Columns 2 and 3 should be used to record the results of a risk assessment that should be carried out on each potential risk, the numerical result of which should then be added to Column 4.

Once the risk assessment has been conducted the Business Lead for the initiative covered by this DPIA should determine, against their risk appetite, whether the risk should lead to termination of the initiative, or alternatively can be tolerated, or transferred or treated. These terms are described below:

- Terminate - Some risks are so far beyond the tolerance identified by the risk appetite or are assessed as having such a severe impact on the business that the initiative should not be progressed.
- Tolerate – some risks are of a sufficiently low level that no actions need to be taken.
- Transfer – on rare occasions it could be possible to transfer the risk to third-parties.
- Treat – many risks can be treated or mitigated to reduce them to a level that is acceptable to the Business Lead.

Where the decision is to treat the risk the treatment to be applied should be added to Column 7 – Column 6 provides potential risk treatments which can be used as prompts for the completion of Column 7.

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	5. Decision (Terminate, Tolerate, Transfer or Treat)	6. Potential Risk Treatment	7. Risk Treatment to be adopted, or comments
Confidentiality-related						
IR1. The information is accessible by people who should not have access to it	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Restrict access to the information through appropriate technical, physical or procedural means so that only those with a legitimate justification can access it Anonymise or pseudonymise the information where possible	**Access is appropriately restricted to those that require access. Forces do not have access to the same datasets within the platform.** ****Security information redacted as worded within your request****
IR2. The system is hosted on an insecure infrastructure or premises. • Insufficient security could lead to unauthorised access internally or externally. This would lead to unauthorised data breaches which could lead to fines by the Information Commission Office (ICO). • There will be a personal impact experienced by the individuals who are subject to the data breach. • Reputational damage would occur within the Police Forces.	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	The system must be hosted on a secure IT infrastructure, either on police premises or hosted	****Security information redacted as worded within your request****
IR3. People who should have access to the information have inappropriate levels of access to it	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Review technical, physical or procedural measures controlling access to the information on a regular basis and amend where necessary	****Security information redacted as worded within your request****
IR4. The information is accidentally disclosed inappropriately	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Educate users on how to prevent the accidental inappropriate disclosure of the information Implement appropriate technical, physical or procedural measures to prevent accidental disclosure of the information	**There is no disclosure mechanism within the platform. To disclose information would require extracting the data from the platform and actively pursuing a disclosure process.** **Users are trained before they have access to the platform.**
IR5. The information is deliberately accessed or disclosed inappropriately	**2 Possible**	**3 Severe**	**2 Medium**	**Treat**	Educate users on the criminal offences relating to deliberate access or disclosure of personal data (Section 170 Data Protection Act 2018) Educate users on the criminal offences within the Computer Misuse Act 1990	**Users will all be appropriately trained before being provided access. Force and support staff will also have received relevant mandatory training.** ****Security information redacted as worded within your request****

					Implement auditing or validation of users' access and/or use of the information	
IR6. The information is held or used in an insecure environment	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Conduct a risk assessment on the environment and implement appropriate technical, physical or procedural measures to protect the information	****Security information redacted as worded within your request****
IR7. The information can be damaged or inappropriately deleted	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Review technical, physical or procedural measures concerning deletion or amendment of the information on a regular basis and amend them where necessary	****Security information redacted as worded within your request****
Integrity-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR8. The integrity of the information is jeopardised	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Review technical, physical or procedural measures concerning the integrity of the information on a regular basis and amend them where necessary	****Security information redacted as worded within your request****
Availability-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR9. The information is inaccessible to those who should have access to it	**1 Remote**	**2 Significant**	**1 Low**	**Tolerate**	Review technical, physical or procedural measures controlling access to the information on a regular basis and amend them where necessary	****Security information redacted as worded within your request****
IR10. The information is not shared when it could be	**1 Remote**	**2 Significant**	**1 Low**	**Tolerate**	Review potential information sharing opportunities and adopt them where appropriate	**Sharing of data is intended to be managed outside of the system**
IR11. The information is not exploited when it could be	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Identify and implement other appropriate potential uses of the information	**The Xchange platform was, in part, developed to avoid this risk by combining many functions that were previously separate or manual.**
IR12. The information cannot be found (e.g. physical documents or searching of IT)	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Ensure the Register of Processing Operations and/or Information Asset Register is completed to record the location of the information Conduct periodic audits to test whether information can be found and undertake any necessary activities to improve the situation	**The information is all on one platform, where users will be able to find data that their role requires access for. Where information cannot be found, access can be managed where required.**
Legality-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR13. The purpose(s) for processing the information is unclear	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Determine and record the precise reason(s) for processing the	**The purpose for this processing and why data is added to the platform is very clear. Training has been developed to ensure that the platform is used correctly and individuals added to the**

					information, updating as is necessary	**system are clearly categorized as required by data protection legislation (such as victims, witness etc).**
IR14. There is no lawful basis to process the information	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Stop processing the information until a lawful basis for processing it is found Identify, record and regularly review the lawful basis for the processing	**The Xchange platform is only for storing forensic information related to crime scene investigation.** **Where there is any change to the lawful basis of processing this DPIA and related contracts will be updated to reflect these changes.** **The completion of this DPIA (and/or subsequent completion by each force of its own DPIA (which forces are entitled to undertake if they think it necessary) and records of processing will resolve this risk or identify further steps to be taken to resolve this risk.**
IR15. The information is being used unfairly or without transparency to data subjects	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Implement physical or procedure measures to ensure transparency requirements are met – including consideration of a Privacy/Transparency Notice(s)	**Forces will need to implement appropriate privacy notices and appropriate policy documents to cover this processing. Given that this processing is not novel, it is up to forces to update those documents to align with their use of Xchange.**
IR16. The information is being used for a purpose incompatible with the reason it was first used/collected	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Document the approved uses that the information may be put to Audit the use of the information to identify any incompatible use, which should be stopped	****Security information redacted as worded within your request****
IR17. Pseudonymised versions of the information can be altered to identify individuals	**1 Remote**	**1 Minimal**	**1 Low**	**Terminate**	Ensure any pseudonymisation information meets the requirements of appropriate published standards	**Pseudonymisation is not used.**
Data Quality-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR18. The information is inaccurate	**2 Possible**	**3 Severe**	**2 Medium**	**Treat**	Implement quality assurance processes when the information is first recorded Correct inaccurate data as soon as possible after it is apparent it is inaccurate	**Training on the use of the platform will reduce the risk of inaccurate information being entered and educate users on how to make corrections.** ****Security information redacted as worded within your request****
IR19. The information is incomplete	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Implement quality assurance processes when the information is first recorded	**See above. Additionally, information will be entered about a crime scene and may be updated as a case progresses.**
IR20. The information cannot be amended when it needs to be	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Adopt processes to append new 'correct' information to the information requiring amendment Implement technical measures to allow the information to be amended	**Forces are able to amend information were required via role based access. This does not apply to logging information.**

IR21. Duplicate versions of the information exist	**2 Possible**	**1 Minimal**	**1 Low**	**Tolerate**	Adopt technical and procedural measures to prevent the creation of duplicate copies of the information Run audits to identify duplicate copies of the information Merge the duplicate copies of the information Educate users on the issues arising from duplicated information and the measures they must adopt to prevent the creation of duplicated information	**Each force is responsible for ensuring that the data they record on the platform is not duplicated. Forces also have the ability to correct data where necessary.** **Training on the use of the platform will reduce the risk of duplicate information being entered and educate users on how to make corrections.**
Records Management-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR22. Excessive information is held	**1 Remote**	**2 Significant**	**1 Low**	**Tolerate**	Review the scope of the information held and reduce the scope so that it is restricted to that necessary for the purpose it is held Train users on the scope of information that should be collected	**The Xchange platform has MOPI retention and review policies built in. Additionally, staff will be trained on the scope of information that should be collected.**
IR23. The information is held longer than is necessary	**1 Remote**	**2 Significant**	**1 Low**	**Tolerate**	Implement review, retention and deletion (RRD) processes (technical and/or non-technical) so that the information is held no longer than is necessary Implement review, retention and deletion (RRD) processes (technical and/or non-technical) so that the information is held no longer than is necessary Implement review, retention and deletion (RRD) processes (technical and/or non-technical) so that the information is held no longer than is necessary Document the RRD processes Educate users as to their responsibilities in connection with the RRD processes	**See above.**
IR24. The information cannot be disposed of when no longer required	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Implement technical measures to allow the information to be disposed of	**Forces have control over the data they add to the platform.** **Forces are to ensure that they keep accurate records of where personal data is held within the Platform and reflect this in instructions to delete data to ensure that all relevant data is deleted.** **Forces will be responsible for having policies and procedures in place to respect and comply with data subjects' rights. The Platform offers forces ways to comply with data subject rights**

						requests, for example mechanisms to search for and delete data in response to a right to be forgotten request.
Training-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR25. Users of the information are inadequately trained	**2 Possible**	**3 Severe**	**2 Medium**	**Treat**	Implement appropriate training for all users	**All users must receive training for the platform before they are provided with access.**
Governance-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR26. There is inadequate policy or procedure surrounding the access or use of the information	**1 Remote**	**2 Significant**	**1 Low**	**Tolerate**	Implement and maintain necessary policy or procedure concerning the access or use of the information	**Forces are very familiar with how this data needs to be processed and the necessary policies and procedures are already in place. For the use of the platform, staff will be trained to use it before accessing to it.**
IR27. There is an absence of an adequate information sharing agreement (where one is required)	**Choose an item.**	**Choose an item.**	**Choose an item.**	**Choose an item.**	Implement and maintain necessary information sharing agreements and review these on at least an annual basis	**The HO and NPCC have a data sharing agreement in place that covers IDENT-1.**
IR28. There is an absence of a data processing contract (where one is required)	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Implement and maintain necessary data processing contracts	**All data processing contracts will be in place before live data processing begins. This includes between NPCC (acting as an Agent on behalf of forces) and PDS (processor) as well as PDS to its sub processors (Amazon and CACI).**
IR29. Generally there is inadequate governance for the information	**1 Remote**	**2 Significant**	**1 Low**	**Tolerate**	Designate, train and task an information asset owner for the information	**Force Information Asset Owners and DPOs will be aware of this processing and ensure that the existing governance is update to reflect the use of Xchange.**
Ethical-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR30. The information is inappropriately discriminatory	**1 Remote**	**3 Severe**	**1 Low**	**Tolerate**	Implement measures to ensure that the collection and use of the information does not inappropriately discriminate against certain groups, in particular children	**Information is only entered for specific purposes and individuals are appropriately categorized to avoid discrimination. These can be revised as an investigation develops.**
IR31. Data Subjects are unaware of their rights regarding the information	**3 Probable**	**2 Significant**	**2 Medium**	**Treat**	Ensure that Privacy/Fair Processing Notices provide details of data subjects' rights and how to exercise them	**Forces will need to ensure that their privacy notices and appropriate policy documents are updated to reflect their use of Xchange compared to the previous use of other processes.**
Miscellaneous	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR32. Lawful, fair and transparent –when examiners identify marks by checking them against images in IDENT1, there is a risk that examiners will not check that the image in IDENT1 is legally held. This could result in marks and identifications from IDENT1 being added to cases on the	**2 Possible**	**3 Severe**	**2 Medium**	**Treat**		**Forces will be given clear instructions regarding the processes that they must follow to ensure images are legally held. This will include clear obligations on the examiner to check the mark from IDENT1 against the PNC to ensure it is legally held; only if the mark is legally held should the mark then be added to a case on the Platform.**

Platform when there was no lawful justification for holding that data in IDENT1 in the first place.						
IR33. **Accuracy** – there is a risk that Persons of Interest are inaccurately identified by fingerprint examiners as matches are based on the examiner's opinion as to whether a mark is a close enough match to an image returned from IDENT1. This is a risk inherent in any fingerprint analysis work.	2 Possible	2 Significant	2 Medium	Treat		Mitigated by examiners' expert knowledge and experience of fingerprint analysis and matching. This risk is not exclusive to the use of the Platform and exists in any fingerprint analysis work.
IR34. **Accuracy** – the Platform is reliant on matches from IDENT1 being returned with accurate data. There is a risk that IDENT1 could return a match that is associated with inaccurate information about an individual, which could result in that individual being incorrectly linked to a crime.	2 Possible	3 Severe	2 Medium	Treat		Mitigated by processes within IDENT1 (Home Office Biometrics) to ensure correct identification of individuals within database.
IR35. **Minimisation** – there is a risk that personal data submitted by Users, particularly in free text fields, could include more personal data than is necessary in order to investigate the case.	2 Possible	1 Minimal	1 Low	Treat		Data fields will be considered to ensure that only data fields that are relevant to the crime/investigation are included. Forces will train their Users not to include personal data in free text fields.
IR36. **International data transfers** – Although data is hosted on AWS UK servers, AWS reserves the right in its terms to transfer data to other regions in an emergency or if required to provide the services (for example in a failover scenario).	2 Possible	2 Significant	2 Medium	Treat		Transfers will be limited, only in certain scenarios. Data is encrypted in transit and at rest and only PDS has access to the encryption keys in the UK. This means that if the data is transferred to the US it will be fully encrypted and individuals cannot be identified. This is in line with EDPB and ICO recommendations. This is a key safeguard. Guidance to be reviewed when finalised and position to be discussed with AWS to establish what measures AWS is taking to ensure compliance. NCA DPIA has been reviewed for completeness.
IR37. **International data transfers** – inappropriate access by international surveillance or law enforcement authorities (such as US signals operations or law enforcement via the Cloud Act)	1 Remote	3 Severe	1 Low	Tolerate		Transfers will be limited to fallback scenarios. Data is encrypted in transit and at rest and only PDS has access to the encryption keys, stored in the UK. This means that if the data is transferred to the US, it will be fully encrypted and individuals cannot be identified. This is in line with EDPB and ICO recommendations. There are compliant and simpler international routes US authorities can legitimately use to exchange information for law enforcement and national security purposes. The US' signals Executive Order helpfully restricts the activities of US surveillance organisations. The data privacy framework has now been approved at an EU level and confirms that there are appropriate safeguards in place to protect against US government access. While this framework

						is not yet the case in the UK, it is indicative of the reassurance EU states have taken from the US' evolving data privacy stance.

.

Step 6: Assess Data Protection Compliance

The NPCC Data Protection Officer will complete this step with assistance from the Business SME, Business Lead and other associated Data Protection professionals, as is necessary.

Processing for Law Enforcement Purposes

Law Enforcement 1st Principle (Lawful & Fair)
(DPA Part 3 Section 35)

Requirement	Compliant?
LE1. No rule of law prohibiting the processing is transgressed (including that arising from the application of any rights of rectification, erasure or restriction under the DPA)	**Overtype here.**
LE2. The processing is authorised by either statute, common law, royal prerogative or by or under any other rule of law	**Overtype here.**
LE3. Either of the following two processing conditions under DPA Part 3 Section 35(2) apply: Consent has been obtained, in compliance with ICO Guidance, or Processing is necessary for task carried out by a competent authority;	**Overtype here.**
LE4. Where **Sensitive Processing** occurs either of the two following cases exist: DPA Part 3 Section 35(4) - Consent has been obtained, in compliance with ICO Guidance and an appropriate policy document exists as per DPA Part 3 Section 42. or DPA Part 3 Section 35(5) - Processing is strictly necessary, an Appropriate Policy Document exists as per DPA Part 3 Section 42, and one of the following DPA Schedule 8 conditions is met: 1 Statutory etc. purposes 2 Administration of justice 3 Protecting individual's vital interests 4 Safeguarding of children and of individuals at risk 5 Personal data already in the public domain 6 Legal claims 7 Judicial acts	**Overtype here.**

8 Preventing fraud 9 Archiving etc;	
LE5. The processing is in accordance with data subjects' reasonable expectations (fair); measures to provide privacy information are in place; Privacy Notices adequately describes the purpose and provide information about specific categories of processing including retention periods and transfers.	**Overtype here.**

Law Enforcement 2nd Principle (Specific, Explicit & Legitimate Purpose)
(DPA Part 3 Section 36)

Requirement	Compliant?
LE6. The purpose for collecting the personal data is specified, explicit and legitimate	**Overtype here.**
LE7. Processing is compatible with the purpose it was collected for	**Overtype here.**
LE8. Personal data collected for the law enforcement purpose is not otherwise processed unless it is authorised by law to do so	**Overtype here.**

Law Enforcement 3rd Principle (Adequate, Relevant & Not Excessive)
(DPA Part 3 Section 37)

Requirement	Compliant?
LE9. Adequate for the purpose	**Overtype here.**
LE10. Relevant to the purpose	**Overtype here.**
LE11. Not Excessive for purpose	**Overtype here.**

Law Enforcement 4th Principle (Accurate & Kept-up-to-date where necessary)
(DPA Part 3 Section 38)

Requirement	Compliant?
LE12. Is accurate with distinction between fact-based and opinion-based	**Overtype here.**
LE13. Is kept up-to-date where necessary	**Overtype here.**
LE14. Distinguishes between suspects, offenders, victims, witness & others where relevant	**Overtype here.**

LE15. Is erased or rectified if inaccurate without delay	**Overtype here.**
LE16. Is not transmitted or made available if inaccurate, incomplete or out-of-date	**Overtype here.**

Law Enforcement 5th Principle (Kept no longer than is necessary)
(DPA Part 3 Section 39)

Requirement	Compliant?
LE17. Personal data is not kept longer than is necessary	**Overtype here.**
LE18. It is possible to justify the retention in relation to the purpose of the processing	**Overtype here.**
LE19. A written retention, review and deletion policy exists for the personal data	**Overtype here.**
LE20. Personal data is subject to periodic review and is anonymized, erased or disposed of when no longer needed	**Overtype here.**

Law Enforcement 6th Principle (Processed Securely)
(DPA Part 3 Section 40)

Requirement	Compliant?
LE21. Appropriate measures are in place or planned to prevent the personal data being accidentally or deliberately compromised	**Overtype here.**
LE22. Those measures are commensurate to the nature of the personal data and the nature of harm that could result from a compromise or data breach	**Overtype here.**
LE23. Those measures include physical, technical, and procedural types and have been developed in consideration of the reliability and training of staff involved in the processing	**Overtype here.**
LE24. Appropriate measures are in place to swiftly and effectively identify, respond to and manage information security incidents and data breaches (including notification to the Commissioner and data subject) (DPA Part 3 Sections 67 and 68) involving the personal data	**Overtype here.**
LE25. DPA Part 3 Section 66 Security of processing requirements are met	**Overtype here.**

Law Enforcement Accountability Requirement
(DPA Part 3 Section 34)

Requirement	Compliant?

LE26. It is possible to demonstrate compliance with all the Law Enforcement Principles	**Overtype here.**

Other DPA Part 3 Controller & Processor Obligations
(DPA Part 3 Section 40)

Requirement	Compliant?
LE27. Compliance with Controller's general duties (DPA Part 3 Section 44)	**Overtype here.**
LE28. Appropriate technical & organisational measures, including policy as required by DPA Part 3 Section 56 are implemented;	**Overtype here.**
LE29. Data Protection by Design & Default requirements set out in DPA Part 3 Section 57 are met	**Overtype here.**
LE30. Where joint controllership exists that each parties' respective obligations under DPA Part 3 Section 58 to comply with the UK GDPR are documented	**Overtype here.**
LE31. Where a processor is employed DPA Part 3 Section 59 and 60 obligations are met including the requirement for a data processing contract to be place	**Overtype here.**
LE32. Records of processing activities are maintained in accordance with DPA Part 3 Section 61;	**Overtype here.**
LE33. Logs are maintained in accordance with DPA Part 3 Section 62;	**Overtype here.**
LE34. Data Protection Impact Assessments (DPIA's) are conducted in accordance DPA Part 3 Section 64 and 65 where required	**Overtype here.**

Law Enforcement International Transfers
(DPA Part 3 Section 37)

Requirement	Compliant?
LE35. Where the transfer is to competent authorities it is in compliance with DPA Part 3 Section 73 General principles for transfers of personal data, including where a third country is 'adequate' (DPA Part 3 Section 74) or where there are appropriate safeguards (DPA Part 3 Section 75), or special circumstances apply (DPA Part 3 Section 76). or Where the transfer is other than to competent authorities it is compliance with DPA Part 3 Section 77;	**Overtype here.**

LE36. Conditions regarding subsequent transfers are set as required by DPA Part 3 Section 78.	**Overtype here.**
LE37. Where the transfer is to competent authorities it is in compliance with DPA Part 3 Section 73 General principles for transfers of personal data, including where a third country is 'adequate' (DPA Part 3 Section 74) or where there are appropriate safeguards (DPA Part 3 Section 75), or special circumstances apply (DPA Part 3 Section 76). or Where the transfer is other than to competent authorities it is compliance with DPA Part 3 Section 77;	**Overtype here.**

Processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes
(DPA Part 3 Section 41)

Requirement	Compliant?
LE38. Where this applies this is compliant with DPA Part 3 Section 41.	**Overtype here.**

Processing for General Purposes

UK GDPR 1st Principle (Lawful, Fair & Transparent)
UK GDPR Article 5(a)

Requirement	Compliant?
G1. No rule of law prohibiting the processing is transgressed (including that arising from the application of any rights of rectification, erasure or restriction under the DPA/UK GDPR)	**Overtype here.**
G2. One of the five available UK GDPR Article 6(1) **Processing Conditions** exists for all of the personal data including Special Category Data and Criminal Offence Data *(Note: The Police are unable to use (f) Legitimate Interests)*: (a) Consent; (b) Contract; (c) Legal Obligation; (d) Vital Interests; (e) Public Task (see DPA Part 2 Section 8 for examples)	**Overtype here.**
G3. If **Consent** is used it complies with definition at UK GDPR Article 4(11), requirements at UK GDPR Article 7 (Conditions for Consent), and ICO Guidance (subject to	**Overtype here.**

exemption for **Special Purposes** at DPA Schedule 2 Part 5 Paragraph 24);	
G4. For any **Special Category Data** being processed, in addition to a UK GDPR Article 6(1) **Processing Condition** being met, one of the following UK GDPR Article 9(2) **Special Processing Conditions** applies: (a) Explicit Consent; (b) Employment, Social Security & Social Protection; (c) Vital Interests; (d) Political, Philosophical, Religious or Trade Union (e) Made Public by Data Subject; (f) Defence of Legal Claims; (g) Substantial Public Interest; (h) Health and Social Care; (i) Public Health; (j) Archiving, Research & Statistics **And** in the case of (b) Employment, Social Security and Protection, or (h) Health and Social Care, or (i) Public Health, or (j) Archiving, Research and Statistics, a condition in DPA Schedule 1 Part 1 applies; or in the case of (g) Substantial Public Interest, a condition in DPA Schedule 1 Part 2 applies And An **Appropriate Policy Document** is created and maintained in accordance with DPA Schedule 1 Part 4 if a condition in DPA Schedule 1 Part 1 or 2 is used	**Overtype here.**
G5. If the purpose of the processing differs from the initial purpose when the data was collected, and the processing is not based on consent or law, compatibility of the new use is tested using UK GDPR Article 6(4)	**Overtype here.**
G6. For any **Criminal Offence Data** being processed, in addition to a UK GDPR Article 6(1) **Processing Condition** being met; compliance with UK GDPR Article 10 is achieved; a DPA Schedule 1 Part 1, 2 or 3 is condition is met, an **Appropriate Policy Document** is created in accordance with DPA Schedule 1 Part 4; and the processing is authorised by law as a clear and foreseeable application of a common law task, function or power, a statutory provision, or statutory guidance	**Overtype here.**

G7. Fairness & Transparency requirements under UK GDPR Articles 12 13 14 are met	**Overtype here.**
G9. Consideration is given to the appropriate use DPA Schedule 2 exemptions where justified.	**Overtype here.**

UK GDPR 2nd Principle (Purpose Limitation)

UK GDPR Article 5(b)

Requirement	Compliant?
G10. Processing is in a manner that is compatible or where is for archiving in public interest, scientific or historical research or statistical purposes is exempt from that requirement by virtue of UK GDPR Article 89(1)	**Overtype here.**
G11. Consideration is given to the appropriate use DPA Schedule 2 exemptions where justified including: **Crime & Taxation.** DPA Schedule 2 Part 1 Paragraph 2 **Disclosure Required by Law.** DPA Schedule 2 Part 1 Paragraph 3 **Special Purposes.** DPA Schedule 2 Part 5 Paragraph 26	**Overtype here.**

UK GDPR 3rd Principle (Data Minimisation)

UK GDPR Article 5(c)

Requirement	Compliant?
G12. Personal data is adequate for the purpose(s) of processing	**Overtype here.**
G13. Personal data is relevant for the purpose(s) of processing	**Overtype here.**
G14. Personal data is limited to that required for the purpose(s) of processing	**Overtype here.**
G15. Consideration is given to the appropriate use DPA Schedule 2 exemptions where justified including: **Crime & Taxation.** DPA Schedule 2 Part 1 Paragraph 2 **Disclosure Required by Law.** DPA Schedule 2 Part 1 Paragraph 3 **Special Purposes.** DPA Schedule 2 Part 5 Paragraph 26.	**Overtype here.**

UK GDPR 4th Principle (Accuracy)

UK GDPR Article 5(d)

Requirement	Compliant?

G16. Personal data is accurate for the purpose(s) of the processing	**Overtype here.**
G17. Personal data is up-to-date where necessary for the purpose(s) of the processing	**Overtype here.**
G18. Personal data is erased or rectified without delay where required	**Overtype here.**
G19. Consideration is given to the appropriate use DPA Schedule 2 exemptions where justified including: **Special Purposes.** DPA Schedule 2 Part 5 Paragraph 26.	**Overtype here.**

UK GDPR 5th Principle (Storage Limitation)

UK GDPR Article 5(e)

Requirement	Compliant?
G20. Personal data enabling the identification of data subjects is retained no longer than is necessary for the purpose(s) of the processing,except where continued retention is solely for archiving in the public interest, scientific or historical research or statistical purposes in accordance with UK GDPR Article 89 & measures required by the UK GDPR are in place to safeguard the rights and freedoms of the data subjects.	**Overtype here.**

UK GDPR 6th Principle (Integrity & Confidentiality)

UK GDPR Article 5(f)

Requirement	Compliant?
G21. Appropriate measures are in place to prevent the personal data being accidentally or deliberately compromised	**Overtype here.**
G22. Those measures are commensurate to the nature of the personal data and the nature of harm that could result from a compromise or data breach	**Overtype here.**
G23. Those measures include physical, technical, and procedural types and have been developed in consideration of the reliability and training of staff involved in the processing	**Overtype here.**
G24. Appropriate measures are in place to swiftly and effectively identify, respond to and manage information security incidents and data breaches (including notification to the Commissioner and data subject) (UK GDPR Article 33 and 34) involving the personal data	**Overtype here.**
G25. UK GDPR Article 32 Security of processing requirements are met	**Overtype here.**

UK GDPR Accountability Requirement

UK GDPR Article 5

Requirement	Compliant?
G26. It is possible to demonstrate compliance with all the UK GDPR Principles	**Overtype here.**

Other UK GDPR Controller & Processor Obligations

Requirement	Compliant?
G27. Appropriate technical & organisational measures, including policy as required by UK GDPR Article 24 are implemented	**Overtype here.**
G28. Data Protection by Design & Default requirements set out in UK GDPR Article 25 are met	**Overtype here.**
G29. Where joint controllership exists that each parties' respective obligations under UK GDPR Article 26 to comply with the UK GDPR are documented	**Overtype here.**
G30. Where a processor is employed UK GDPR Articles 28 and 29 obligations are met including the requirement for a data processing contract to be place	**Overtype here.**
G31. Records of processing activities are maintained in accordance with UK GDPR Article 30	**Overtype here.**
G32. Data Protection Impact Assessments (DPIA's) are conducted in accordance with UK GDPR Articles 35 and 36j where required	**Overtype here.**

Where necessary, consider restricted transfers of personal data for general processing purposes to countries or territories beyond the European Union or to international organisations (**third countries)**

Requirement	Compliant?
G33. The restricted transfer is in compliance with UK GDPR Article 44 General principles for transfers of personal data, including where a third country is 'adequate' (UK GDPR Article 45) or where there are appropriate safeguards (UK GDPR Article 46, 47 or 48), or an GDPR Article 49 condition applies.	**Overtype here.**

Step 7: Sign-off and record of outcomes

Consultation Outcomes

Summary of consultation responses (if conducted):

Overtype here.

Summary completed by:

Overtype with rank, ID number, name and post.

Date completed:

Enter date here.

Business Lead's response to consultation responses (if conducted)

Overtype here.

Date completed:

Enter date here.

Data Protection Officer Comments

Data Protection Officer's comments, including whether the DPIA has been conducted appropriately and whether it must be sent to the ICO for review:

Overtype here.

Date completed:

Add Date Here.

Business Lead's Comments

Business Lead's confirmation of agreement with risk assessment, acceptance of identified responses to risks, consideration of Data Protection Officer's comments and acceptance of responsibility to update this DPIA as is necessary.

Overtype here.

Date completed:

Enter date here.