

Assessment details

ID 9386

Name HMPPS Person Record - STAGE 2: Full DPIA (only complete after Stage 1)

Organization HMPPS Digital

Description

Approver

Respondent

(External)

Template STAGE 2: Full DPIA (only complete after Stage 1)

Workflow Default assessment workflow

Creator

(External)

Date created 11/03/2024

Deadline

Completed date 25/06/2026

Date submitted 22/06/2026

Last updated 25/06/2026

Stage Completed

Approval stage

Status Active

Very high risks 0

High risks 0

Medium risks 0

Low risks 0

Total risks 0

Residual risk level None

Residual risk score 0.0

Result Approved

Result comments

Under Review - Approved) ; - Approved) ;

Primary record id

Primary record name

Template version 43

Open risk count 0

Open info request 0

Tags

Submission Progress (%) 98

Assessment questions

1 Processing Details

1.1 What activity are you assessing?

Please either select from the list of existing activities or create a new activity by typing the name of your activity following this naming convention below
HQ/AGENCY/ALB: DEPT: NAME OF INFORMATION FLOW
Example: HQ: Finance: Debt Collection

'Activities' relates to a 'processing activity' which is recorded in the data mapping section of OneTrust.

Response

hmpps person record | HMPPS Digital

Justification

None

1.2 Explain broadly what the project aims to achieve.

What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly? You may find it helpful to refer or link to other documents, such as a project proposal.

Response

hmpps person record | HMPPS Digital

Response

Currently, person data is spread throughout our digital state, with entire copies of someones identity in NDelius, Nomis, and services that hold court data. There are many other services that hold some of this data such as OASys, Digital Prison Services, Community Accommodation Services etc. These records are difficult to match to each other due to inaccuracies in recorded data from issues like manual keying errors, updating data in one place but not all, or data being purposely obfuscated.

The HMPPS Person Record service will replace a wide range of tactical solutions that exist within HMPPS that try to match one person to another by looking at a subset of a person's details.

At the moment we have plenty of opportunities within the justice journey for multiple records to be created for the same person, either by incorrectly recording information about a person, having new and differing data than what we know about the person already, or for someone to give false information.

The aim of HMPPS Person Record (Core Person Record) is to be a single service for person identity, for all services to use when they interact with a person in the care of HMPPS. Person identity in this context is data we consider to be in the "Person Domain" within the new Data Domain Model of HMPPS. For the person domain, this includes information related to a person in our care but not including operational information like offences, risks etc. Examples would be name, date of birth, gender, sex, and ethnicity.

We will search, match, and link people already in our digital estate to ensure we only have one record per person in our care. This is to reduce the number of duplicate records we hold on a person.

This project is a multi-year initiative that will go through multiple phases. The final aim is described above, but phases along the way will see us hold a link mapping for each representation of a person record we have, followed by syncing of the data between systems, before eventually reducing a person's record count down to one.

This new service will work by taking some key attributes we know about a person and perform a general, board search for any similar records we're aware of. We then pass those records in to a data science developed matching model, alongside even more things we know about the "candidate records" we've found, then make a determination of the record in question is a match to any of them, or no match. In the case of no match, we can with confidence create a new record for that person. When a match is found, we return to whatever service that called us, that we have identified an existing match for that record, and return the relevant identifiers for them.

The outcomes for this service are; to reduce the creation of duplicate records, and to reduce the number of duplicates we already have, to better manage the data we hold about a person for GDPR compliance, Subject Access Requests, and better operational use to deliver efficiencies. This will lead to better outcomes for people in our care, with better targeted rehabilitation, and management whilst in our care.

Justification

None

Comments

(External)

02/05/2024

I'm placing this comment here but it applies to the whole DPIA. We're working on this DPIA ahead of time so we can address any big questions that we may not have answered. We're not looking for an approval on this DPIA as we do not have a completed IT Health Check and won't for a few months.

1.3 Please describe in detail the process from start to finish.

Please include either a flow diagram or describe the process.

How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone outside your business area?

Response

The HMPPS Person Record service takes data from NDelius, Nomis, HMCTS Common Platform, and HMCTS Libra. These services all hold a 'complete' record of a person, each managing a different stage in a person's journey from court, to prison, and to probation. At the moment, there are basic matching processes taking place that do exact matches on a handful of key fields to try and establish links between the systems. These matches happen when information about a person is brought to the attention of HMPPS for example, when a court date is scheduled.

With HMPPS Person Record service, when any digital service within HMPPS wants to interact with a person on probation, a person in prison, or a defendant in court, they will come first to the HMPPS Person Record. The aim is to have a single identity for people in our care, of which all their other information can be associated to. All associated information about a person will be linked to the unique identifier for that person which HMPPS Person Record will master.

In order for the new digital service to achieve this, we shall have a database of identifiable attributes about a person that we can use to match them with other records. We shall store information about a person which is deemed as being within the "Person" domain within the data domain model.

An example of this goes as follows:

1. The details of each defendant attending a hearing are sent to HMPPS using a data feed from HMCTS.
2. The Person Record service goes through each person in the court data feed to look for a match in the Person Record database.
3. If no matches are found in any database, a new Person Record record is created, and the information we know about that person so far gets recorded.
4. If a match is found, then we respond to the referring service to tell give them the relevant HMPPS identifier for that person.

The data we hold about a person can be found in section 1.10. The fields we use for matching person are first name, middle names, last name, date of birth, aliases, postcodes, CRO, PNC, sentence dates.

The front line, front end driven services that use our service will show some or all the information we have for a person. This gives a user the opportunity to check the details are accurate for the person in their care. Some services that deal with record creations, will have functionality that will allow for a link to be created between records even if HMPPS Person Record has not automatically one so. This link will be honoured unless manually unlinked. Another journey exists where an "unlink" can be put in place, permanently separating records from one another so they cannot be linked again until a link request is made. In the event that duplicate records are identified, we are implementing an automatic service management request to have a live support agent look at the identified records. It will then follow their standard procedure for record merges should it be deemed needed.

SPLINK

SPLINK is a data science algorithm developed in house by Justice Digital. It's a probabilistic scoring algorithm that can take two pieces information about a person and score how likely they are to be the same person. We use SPLINK as part of our service to compare the details of a person, against all the records we have for every defendant, person on probation, and person in prison.

Court Data Feed:

This data is collected from HMCTS Libra and HMCTS Common Platform. For HMCTS Common Platform we receive a stream of real time digital 'events' (messages) using a message queue standard pattern. In this process, an 'event' is created by HMCTS for an action, and then published on a queue. We subscribe to that queue and listen for any events (messages) that are relevant to us. We read from the queue and process the events in a near realtime manner. For HMCTS Libra we receive a batch file every evening that contains hearings that are 15 days away. We receive another file every evening for hearings that are 8 days away. We receive another file every evening for hearings that are 3 days away. Each day between 07:00 and 10:00 we receive a batch file every 30 minutes. The defendant's details are in each of these files, along with a large amount of other court related data that the HMPPS Person Record does not use. All these data exchanges are done digitally.

Data Deletion

We listen to 'events' from both NDelius and nomis for when a record is deleted, and we delete our respective NDelius or Nomis record. If there are no more records left for a person, we then delete the HMPPS Person Record for that person. As an example, when a deletion is performed on a record within NDelius, an event is emitted which we listen to. Based on the record in the event, we will also delete the NDelius record we hold associated to the nominated person. If this person has other records with HMPPS, for example a Nomis record, we shall keep that record and our "HMPPS Record" for that person. If the Nomis record was then deleted, or if the person had no other records associated to them, we would then delete the HMPPS Person for them.

How does Machine Learning work within HMPPS Person Record?

Machine learning has been used to determine the weight of the frequency of the same results appearing, such as [REDACTED] and change the score weighting appropriately due to its commonality. The more common the data is, the lower the score rewarded. The more rare the data is, the more confidence we can put in it that if a match is made, it's a stronger match, therefore we increase its score. Machine Learning is a form of AI, therefore we have been working with colleagues to complete a n AI Ethics assessment of the service, however this is not a service using generative decision making or other traditional "AI" features.

Known Linking Issues:

False positives are when we determine that two records are a match when in fact they are not. False negatives are when we determine two records are not a match when in fact they are. We do not have exact figures on the likelihood of these but our principles is to reduce false positives as much as possible, which will increase the number of false negatives we allow. We cannot eliminate either scenario from occurring as we're bound by the quality of the data available and the actions of people using the systems we're connected to. It is possible to place an override marker on a record to forcibly link or unlink two records if an error is observed. We also have in place an automated check that flags records that potentially have an issue, so they can be manually reviewed. In the event that a false positive or negative is spotted, it's standard procedure for staff to raise a request with the service desk to investigate the highlighted records. Within the Prepare a Case For Sentence service, it's possible for staff to link or unlink case information to records, which HMPPS Person Record will adhere to.

1.4 Describe the context of the processing

What is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way?

Response

Processing will take place within the HMPPS Person Record service in the form of comparing details we've received from another digital service, to the person records that we hold within our database.

This will be done using loose comparison of the person's details against our database to retrieve a number of "candidate matches". Then in turn, we shall take each "candidate match" record and compare them to the person's details we've been given, using the SPLINK comparison algorithm. The SPLINK algorithm will return a score for how likely that the two records match one another. If the score reaches a certain threshold, we identify the records as a match. If a match is made, we return the source system IDs for the person. If there is not a match to any records we hold, we then create a record for that person and store the details we know about them. Should a source system like NDelius or Nomis create a record for that person, we listen for a "record creation event/message" and then link the records together as "relating to the same person".

A service can also call HMPPS Person Record API to find out what records we have linked to a specific source system ID. If a service calls with an NDelius ID for a person we're aware of, we can return to them the other source system IDs we hold, which will include duplicate records within the same source system that was called for. This is to enable services to go and find more information out about a person from other systems with the relevant source system ID for that system.

The records we are storing are of 1) people in prisoners, 2) people on probation, and 3) defendants in court.

The HMPPS Person Record service is aimed at being a cross HMPPS digital service, to be used by all digital services that interact with one of the 3 types of people listed above. The people listed above will not have direct access to the records we have unless a service user facing service has requested them. The data we hold about these people can be accessed with a subject access request.

1.5 Is the project / initiative expected to last for 12 months or longer ?

Response

Yes

Justification

This service will require long term maintenance and improvement, as well as live support. When Nomis is decommissioned, every Digital Prison Service will be dependant on this service for person data. Over time, each legacy service (OASys, NDelius etc) will be moving to use HMPPS Person Record as the authoritative source of person information. There is no known date for the decommissioning of the HMPPS Person Record service.

1.6 Please list the Name and Role of your SIRO, IAO and IAL

Response

hmpps person record | HMPPS Digital

Response

Justification

None

1.7 What applications or systems does the data come from?

In other words, what do you use to obtain the data? In terms of data flow, this would be somewhere near the beginning.

An 'asset' is something that supports information-related activities. Assets could include software systems, applications, databases, or even file cabinets.

Please make sure when you are selecting/adding an asset you are not duplicating it from the dropdown list.

Response

Common Platform | HMCTS | Unknown NDELIUS | HMPPS | Unknown HMCTS: Libra | HMCTS | Unknown
HMPPS: Prisons: NOMIS/DPS | HMPPS | Unknown HMPPS: HMPPS Digital: Accommodation Service

Justification

None

Comments

(External)

Added the new Accommodation Service to this list.

22/06/2026

1.8 What applications or systems (assets) are used to store and process the data for this activity?

In other words, after the data is collected/obtained from the source, where will it spend most of its time? Will it stay put, or will it go somewhere else? In terms of flow, this would be somewhere in the middle.

An 'asset' is something that supports information-related activities. Assets could include software systems, applications, databases, or even file cabinets.

Please make sure when you are selecting/adding an asset you are not duplicating it from the dropdown list.

Response

HMPPS Person Record

Justification

None

1.9 What is the Nature of information?

If you are selecting criminal data, please also select basic personal data or special category data as necessary.

Response

hmpps person record | HMPPS Digital

Response

Basic personal data

Criminal data

Children's Data

Special category data

Justification

None

Comments

██████████ (External)

13/11/2024

I have included Criminal Data in this as we now store the Sentence Date of a person. This is used for matching a person record.

██████████ (External)

03/10/2025

Children data has been included in this because Nomis holds the records for children under the age of 18 who are being held within the prison estate. Therefore HMPPS Person Record has a copy of these records. Children data is available due to the data feeds we get from the Common Platform service operated by HMCTS, but we do not store the data of any records with the IsYouth flag enabled.

██████████ (External)

08/10/2025

A further note to this. We will hold the data of people defined as children but only due to the handover process between Youth Justice Services and the probation Service as a person approaches the age of 18. Their details are created and stored within NDelius during this transition and therefore we also store their details.

1.10 Please select the groups of data subjects you are processing data about for this activity, and for each group, select the categories of data and individual data elements processed.

Response

Offenders

Personal identification

Date of birth

Marital status

Medical or
Healthcare

Gender

Racial or ethnic origin

Weight

Religion / Religious
Beliefs

Unique personal
identifier

Last name

First name

Full name

Sexual orientation

Military or veteran status

Height

Disability or specific condition

Age

Citizenship status

Nationality

Government identifiers

Passport number

Social Security
Number

Drivers license number

National identification number

National Insurance
Number

National identity card
details

Family information

Next of Kin

Contact information

Previous residence address

Home address

Contact details

Phone numbers

Emergency contact details

Personal
email

People on probation

Personal identification

Medical or Healthcare
 Sexual orientation
 Citizenship status
 Signature
 Height
 Gender
 Disability or specific condition
 First name
 Weight
 Military or veteran status
 Last name
 Racial or ethnic origin
 Date of birth
 Marital status
 Age
 Nationality
 Religion / Religious Beliefs

Government identifiers

National Insurance Number
 Drivers license number
 Passport number

Family information

Next of Kin

Comments

██████████ (External)

14/11/2024

We also handle Defendant data. This is because we get a feed of data from HMCTS Common Platform and Libre which contains people considered to be a defendant, people who have been convicted but not yet sentenced, and people who have been sentenced to either custody or probation.

The defendant information is the same as the information we capture for people in custody and on probation.

We also process information of people considered as "youths". This is because we get a feed of data from HMCTS (Common Platform and Libre) and have a dependent service that needs that data. HMPPS Person Record as a service does not intend to use the data of subjects considered "youths" but other downstream services such as Electronic Monitoring does require this information.

1.11 What is the estimated number of records being processed for this activity?

Select the range considering duration of processing/activity. E.g. if your activity is going to run for a year, consider the number of records likely to be created for the entirety of that time. A record consists of all personal data you may hold for an individual.

Response

hmpps person record | HMPPS Digital

Response

H. 1,000,001+

Justification

None

2.1 Describe when and how you will seek individuals' views (Include findings) – or justify why it's not appropriate to do so.

Who have you consulted? (Stakeholders include, Data subjects, Data Processors, Legal Representatives, Commercial, Project Managers, Product Managers, cyber/information security experts etc.)

Response

We've been working with [REDACTED] Director of Digital, [REDACTED] Deputy Director of Probation Digital, and [REDACTED] Deputy Director of Prison to assess the risk being mitigated, [REDACTED] mitigate the risk, and [REDACTED] ing needed to carry out the plan. We've al [REDACTED] ing closely with our colleagues in Data Science, and Data Directory to use the latest methods and solutions available to us to future-proof our service.

2.2 Please provide justification to demonstrate that the use of personal data is necessary and there are no less intrusive ways to achieve the same outcome?

E.g by using less or no personal data.

Is there a clear defined use of each data type/elements for the purpose(s) of this activity?

Response

The HMPPS Person Record service shall become the only place in HMPPS to hold personally identifiable information about a person in court, in prison and on probation. This will be a significant step forward compared to where we are now as personally identifiable information about these people are spread and duplicated throughout our whole digital estate.

Person data the HMPPS Person Record service holds will then be used with other data such as risk, offence etc so that other digital services can conduct their normal operations.

There will be other locations where this data exists such as reporting platforms in a read only format, and in legacy systems to be decommissioned.

Comments



22/05/2024

Other systems will likely hold read-only copies of some personal data for performance optimisations, particularly person names. Data and reporting platforms will also hold read-only copies of personal data

2.3 How will you ensure data quality/accuracy ?

How will you ensure the personal data you hold is correct and kept up to date? E.g. collected directly from individuals and individuals have direct access to their profile to maintain the accuracy of their data.

Are individuals given direction on how they can update/main their records? Do we routinely request a review of records or check records for accuracy? If so, how?

Response

The HMPPS Person Record service will continually look to link records it's aware of to find opportunities to link the records of a person together. It will also reduce the number of new records being created by making it easier to find someone who already has a record. This means less duplicated data coming into the HMPPS digital estate and will make keeping existing data up to date easier.

Our service of matching records and holding data on a person can only be as accurate as the data we are sent from the source services. We are working with teams to improve the quality of the data, with feedback loops for when corrections are made etc, but we are limited to the quality of the data we are supplied with.

There is no definitive source of truth to compare our collection of records for a person, but for people who are under supervision either in prison or probation, their records will be interacted with on a regular basis. If an irregularity is observed, then an incident can be raised using the service desk portal to have the irregularity investigated. An administration tool is currently being developed which will allow support staff to change the record links within a collection/cluster, by the use of override markers. This means that links that have been manually created will always remain, and exclusions between records will always remain.

2.4 Please provide a link to the retention schedule, attach it to this question or specify the schedule within the narrative.

E.g. data retained for 2 years from the point of collection as per the attached retention schedule. The Ministry of Justice uses Record Retention and Disposition Schedules (RRDS) to manage its compliance with the Public Records Acts. This can be found [here](#)

Response

hmpps person record | HMPPS Digital

Response

CPR will be the service that holds personal information relating to persons in our care (people on probation and people in prison). Therefore we have a legal obligation to hold this data in accordance with any sentencing requirements. Related to this is our obligation to carry out our duty in an official capacity and with authority.

We plan to adhere to the GDPR guidelines set out by the data protection team, with the ability to delete a person's records when a request is triggered. Agreement on when that trigger can be used is currently with various HMPPS boards that have yet to make a decision on what data can be deleted. There has been no update on this therefore we are instructed to continue retaining the data until told otherwise.

Justification

None

- 2.5 How will the Records Retention and Deletion Schedule be implemented ? Please also provide details on how you will monitor this within the justification section.
Please also provide details on how you will monitor the management of the retention and deletion schedule.

Response

Manual process for deleting records managed by team.
Please provide further details on who is responsible for manually deleting records in the box below.

Justification

It is expected that HMPPS Person Record will be in a position to delete data once all systems dependent on the Person have duly deleted their data set and no longer require a person record. Therefore, data deletion messages from other systems will be received, processed and once no remaining links exist, HMPPS Person Record will be able to set the person record for deletion

- 2.6 Does a moratorium exist on the destruction of the personal data being processed?

If Yes, please specify the type of moratorium that relates to the destruction of the personal data. A moratorium would exist if, for example, there was an ongoing inquiry which required that the personal data be kept longer than usual.

Response

Yes

Justification

nDelius and Nomis do not currently delete any data about a person. There is a moratorium in place on the destruction of data thats related to Child Sex Abuse and this has extended the storage of records by 20 years.

- 2.7 How will data subjects be informed about the purposes of the processing?

Please attach the type of communication/privacy notice.

Response

Privacy notice provided at the point of collection

Justification

None

- 2.8 What process is in place to manage the applicable individual rights?

Please describe the process for fulfilling the below individual rights. Please also note any rights which you are unable to fulfil as part of this activity and list any exemptions that apply. [ICO Guidance on exemptions](#)

[The right of access](#)

[The right to rectification](#)

[The right to erasure](#)

[The right to restrict processing](#)

[The right to data portability](#)

[The right to object](#)

[Rights in relation to automated decision making and profiling.](#)

Response

The Subject Access Request team will be a user of our service to retrieve any information about a person they search for. They shall also be a user of our service to find other digital representations of a person they're looking for, should someone have multiple records with us.

3.1 Is MoJ the Data Controller or Joint Controller?

Please Justify your answer (Name the data controller/joint controllers)

Controller: the natural or legal person, public authority, agency or other body which determines the purposes and means of the processing of personal data.

Joint Controller: Two or more controllers or data owners that jointly determine why and how to process personal data

If you are unsure whether MoJ is a Data Controller or Joint Data Controller please select 'Data Controller'

Further details and examples available at [Controllers and processors / ICO](#)

Response

hmpps person record | HMPPS Digital

Response

Data Controller

Justification

HMPPS

3.2 Will a data processor be used?

If Yes please justify your answer below by stating the name of the data processor(s).

A processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller Processors act on behalf of the relevant controller and under their authority.

Further details and examples available at [Controllers and processors / ICO](#)

Response

hmpps person record | HMPPS Digital

Response

No

Justification

None

3.3 Will a data sub-processor(s) be used?

If Yes please justify your answer below by stating the name of the data sub-processor(s).

Where a processor engages another processor, this is known as a sub processors for the data controller.

Response

No

Justification

None

3.4 What applications or systems may have the data sent/transferred to them as a part of this activity?

In other words, does the data go anywhere after being in the storage assets? In terms of data flow, this would be somewhere near the end.

An 'asset' is something that supports information-related activities. Assets could include software systems, applications, databases, or even file cabinets.

Please make sure when you are selecting/adding an asset you are not duplicating it from the dropdown list.

Response

Prepare a Case for Sentence Probation Integration NOMIS | Justice Digital | Unknown
Analytical Platform | Data and Analysis | Unknown Delius | HMPPS | Unknown

Justification

None

3.5 What Public or not for profit entities is the personal data transferred to?

Examples of public or not for profit external entities include charities, educational providers, NHS, local authorities, councils, HMRC, etc. If your external entity is not in the list, please add it as an option under other.

Response

Not applicable

Justification

None

3.6 Is a data sharing agreement, memorandum of understanding OR contract in place with any third party involved in the processing?

If yes, please attach any agreements in place e.g. the Contract, DSA, ISA or MOU.

Response

hmpps person record | HMPPS Digital

Response

Not Applicable

Justification

None

3.7 Is the data shared, hosted or accessed by any third party outside the UK? If yes, please state the location of the third party.

E.G. Processing involves support services accessing data from countries outside of the UK or data may be hosted on cloud services outside of the UK.

Please provide further details within the justification box.E.g. hosted in UK, but support provided from USA.

Response

hmpps person record | HMPPS Digital

Response

United Kingdom

Justification

Not outside the UK.

4 Project Regime

4.1 What regime applies to this project?

Response

hmpps person record | HMPPS Digital

Response

Part 3 of the Data Protection Act 2018

GDPR

Justification

None

4.2 UK/EU GDPR - Personal data: On which of the following lawful bases does processing of personal data take place (please select one or more options)?

Please provide a justification for the lawful basis for processing of personal data in the justification box below.

Please see below for an explanation of the different lawful bases for processing personal data:

Consent - the individual has given clear consent for you to process their personal data for a specific purpose (e.g. processing a service user's data for the purpose of user research, where that user is given the choice to take part and has control over how their data is used). Consent is not usually an appropriate lawful basis for MoJ business purposes.

Contract - the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract (e.g. processing HR data for an employee for the purposes of their employment contract)

Legal obligation - the processing is necessary for you to comply with the law (not including contractual obligations) (e.g. processing employee data for the purposes of a legal requirement)

Vital interests - the processing is necessary to protect someone's life (e.g. sharing offender health data during a medical emergency)

Public task - the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law (e.g. processing a court user's data to enable HMCTS to fulfil their official duties to manage court proceedings).

Legitimate interests - the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if processing is carried out by public authorities in the performance of their tasks or you are processing data to perform your official tasks) (e.g. processing a service user's personal data to improve the service MoJ provide where it benefits that service user and/or the MoJ and the service is not related to our official function as a department)

Response

hmpps person record | HMPPS Digital

Response

Necessary for the performance of task in public interest or exercise of official authority

Justification

CPR will be the service that holds personal information relating to persons in our care (people on probation and people in prison). Related to this is our obligation to carry out our duty in an official capacity and with authority.

Comments

(External)

17/03/2025

I have attached an email between CPR and Access, Retention and Library which states that we're authorised to retain data we receive from HMCTS for a period of 3 years before being required to delete it. This is specifically for data we receive about a person who subsequently becomes of no interest to HMPPS, for example, by being found not guilty.

4.4 UK/EU GDPR - Special categories of personal data: On which of the following lawful bases does processing of special categories of personal data take place (please select one or more options)?

Special category data can only be processed if at least one of the specific conditions below is met. You need to consider the purposes of your processing and identify which of these conditions are relevant.

Explicit consent - the individual has given clear consent for you to process their special category personal data for a specific purpose (e.g. processing a service user's data for the purpose of user research, where that user is given the choice to take part and has control over how their data is used). Explicit consent must be obtained in a clear statement and collected separately to other consents. The data subject should be informed about the nature of the special category data at the point of gaining explicit consent. Explicit consent is usually not an appropriate condition for MoJ business purposes.

Employment, social security and social protection (if authorised by law) – this condition is relevant to employers and public authorities providing social services and benefits where the purpose is to comply with employment law or social security and social protection law.

Vital interests – the processing is necessary to protect someone's life where the individual is physically or legally incapable of giving consent.

Not-for-profit bodies – this condition is relevant to not-for-profit bodies, for example charities, clubs, political parties, churches, trade unions and other associations if they have a political, philosophical, or religious aim. The processing of special category data must relate to the legitimate activities of the not-for-profit body.

Made public by the data subject – the special category data must have been made public by the individual themselves and must be realistically accessible to members of the public.

Legal claims or judicial acts – this condition is relevant when the purpose of processing special category data is to establish, exercise or defend legal claims. This includes actual or prospective court proceedings, obtaining legal advice or establishing, exercising or defending legal rights in any other way. This condition also applies whenever a court (or tribunal) is acting in its judicial capacity.

Reasons of substantial public interest (with a basis in law) – This condition requires one of the substantial public interest conditions to be met, these can be found in the next question.

Health or social care (with a basis in law) – this condition covers the following purposes:

- preventive or occupational medicine;
- the assessment of an employee's working capacity;
- medical diagnosis;
- the provision of health care or treatment;
- the provision of social care (this is likely to include social work, personal care and social support services); or
- the management of health care systems or services or social care systems or services.

Public health (with a basis in law) – this condition can only be relied upon when the special category processing is carried out either:

- by, or under the responsibility of, a health professional; or
- by someone else who in the circumstances owes a legal duty of confidentiality.

Archiving, research and statistics (with a basis in law) – this condition can only be relied upon when the processing of special category data for archiving, research and statistical reasons is in the public interest (a benefit to the wider public or society as a whole). For research, this must be either scientific or historical in nature.

Response

hmpps person record | HMPPS Digital

Response Substantial public interest Justification None

4.5 What substantial public interest condition(s) is applicable?

Response

hmpps person record | HMPPS Digital

Response Informing elected representatives about prisoners Statutory and Government purposes Preventing fraud Publication of legal judgements Protecting the public Administration of justice and parliamentary purposes Justification None
--

4.6 How is the criminal offence data processing carried out (please select one or more of the options below)?

Response

hmpps person record | HMPPS Digital

Response

Carried out in official capacity

Justification

None

4.7 Please identify the basis in law that applies to the criminal offence data processing

Response

hmpps person record | HMPPS Digital

Response

Legal obligation - including Offender Management Act 2007, Criminal Justice Act 1991, Criminal Justice Act 2003, Prison Act 1952 and Prison Rules 1999.
Performance of a public task - administration of justice and exercise of a function of the Secretary of State.

Justification

None

4.9 Part 3 of the Data Protection Act 2018 - Personal data: On which of the following lawful bases does processing of personal data take place (please select one option only)?

Response

hmpps person record | HMPPS Digital

Response

Processing is strictly for law enforcement purposes

Justification

None

4.10 Part 3 of the Data Protection Act 2018 - Sensitive data: Which of the following Schedule 8 conditions relating to the processing of sensitive data are being met (please select at least one option)?

Response

hmpps person record | HMPPS Digital

Response

Judicial and statutory purposes Administration of justice

Justification

None

4.11 Part 3 of the Data Protection Act 2018: Will the segregation of the data subjects be possible?

This involves the segregation of data for Victims, Witnesses, Offenders and Suspects.

Response

Yes

Justification

None

Comments

(External)

We will not store any data related to victims, witnesses, or suspects. We will store data of defendants and offenders.

01/05/2024

5 Identify security & risks

5.1 Have any privacy risks been identified which have not yet been mitigated?

If the answer to this question is Yes, please list any risks and mitigation's within the justification box below.

Response

☒ No

Justification

At this point privacy risks identified have been considered, and controls have been documented in this DPIA. Should new risks arise, the DPIA would be re-opened and updated.

5.2 Does this project adhere to relevant MoJ IT Security policies?

If the answer to this question is **No**, please detail the deviations from the IT Security policies and confirm that the SIRO has agreed to these deviations in the justification box below.

Response

☒ Yes

Justification

An ITHC was performed on this service but we are talking to the application security team to put in for another test as the service has grown.

5.3 Please select from the list below which technical measures are currently implemented to reduce, mitigate or eliminate the security risks identified.

Please include further details of the technical measures you selected. For example, if 'Backup' is selected, explain how frequent the backups will operate. Add any additional measures, or make suggestions, in the text box below.

Response

hmpps person record | HMPPS Digital

Response

Encryption at rest

Data backup

Role based access

System audit logs to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorised system activity

Business continuity plans

Multi-factor authentication

Background checks

Secure data transfer mechanisms (where applicable). e.g. Application Programme Interface (API) or Secure File Transfer Protocol

Penetration tests

Encryption in transfer

Limited system access to authorised users only

Justification

Both our S3 bucket and database are encrypted at rest.

5.4 Have any further security risks been identified so far?

If the answer to this question is **Yes** please provide details of where the relevant risk register can be viewed / accessed.

Response

☒ No

Justification

Risks for the HMPPS Person Record at a team level are tracked on the Core Person Record jira project, and at a service level via Probation Digital Delivery Ops. The HMPPS Person Record service will not handle who can and cannot see Limited Access Offenders within nDelius but we do plan to hold the flag that a person record has a restriction or exclusion.

5.6 Is a third-party supplier or partner involved in this project?

If the answer is 'Yes', please provide details of the third party supplier or partner in the justification box below. In the case of a third party website, please provide the URL.

Response

☒ No

Justification

All our digital infrastructure is provided by the Platforms and Architecture function within Justice Digital.

5.9 Has your service been through or is currently going through the GovAssure process?

GovAssure is the new mandatory cross-Government cyber assurance regime developed by the Government Security Group (GSG) in the Cabinet Office. It adopts the Cyber Assessment Framework (CAF) developed by the National Cyber Security Centre (NCSC) as the mechanism to assess the Department's services, aiding with the identification of vulnerabilities and risks to the services. GovAssure includes a self-assessment of services on a continuous basis as well as an external assessment with annual reporting to the Cabinet Office.

If you have any queries about GovAssure please contact GovAssure@justice.gov.uk

Response

No

Justification

None

Comments

[REDACTED] (External)

01/05/2024

Out product is not on the list of services that are subject to this new framework.

6 DPIA Completion

6.1 DPIA Completion

You are now ready to submit your DPIA for approval. Please ensure that you have completed all the previous questions comprehensively prior to submitting the DPIA.

Please use the next question to capture any additional information required for the DPIA.

6.2 Are there any additional issues that need to be considered for the project / initiative?

Response

Not answered

Assessment notes