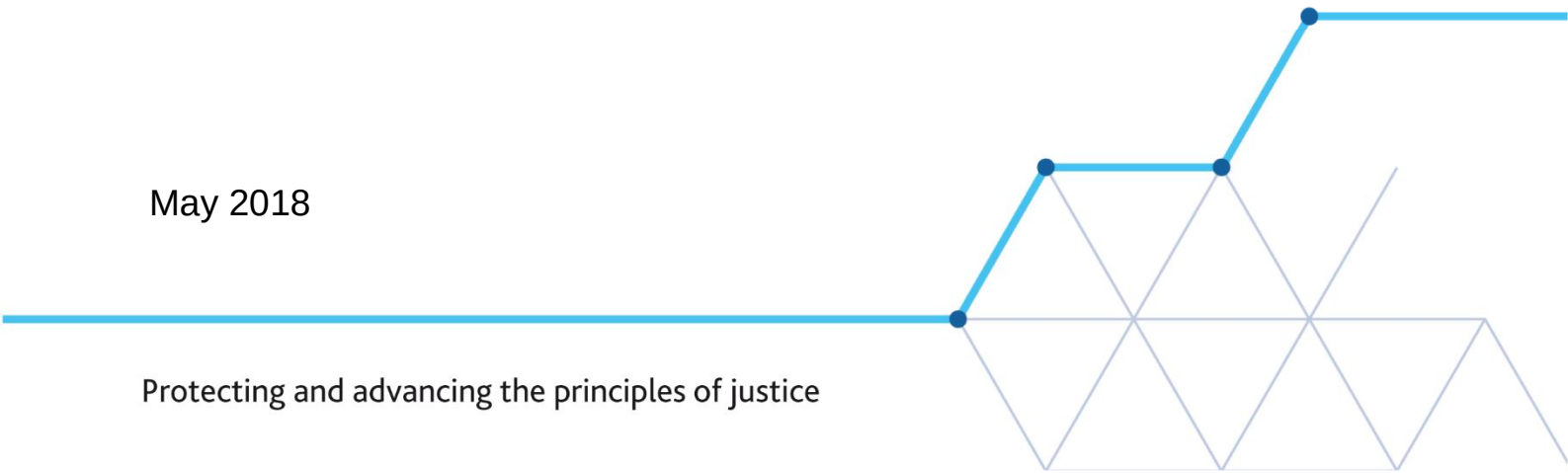
Ministry of Justice

Justice Data Lab

Data Protection Impact Assessment

May 2018



Protecting and advancing the principles of justice

Ministry of Justice

Justice Data Lab

Data Protection Impact Assessment

Contents

1. Executive Summary

This document is a Data Protection Impact Assessment (DPIA) for the Justice Data Lab (JDL) and demonstrates that the JDL initiative is compliant with the General Data Protection Regulation (GDPR) and the new Data Protection Act 2018 at all stages. It is an update of the original Privacy Impact Assessment (PIA) that demonstrated that the JDL was compliant with the Data Protection Act 1998, as required.

This DPIA has been produced by the project lead for the JDL. The initial draft was reviewed by internal Ministry of Justice colleagues with expertise in Data Compliance. The comments made by these colleagues have been reflected in the final version of this document.

2. Introduction

DPIA background

A Data Protection Impact Assessment (DPIA) is a process to systematically analyse your processing and help you identify and minimise data protection risks. It must achieve the following:

- describe the processing and your purposes;
- assess necessity and proportionality;
- identify and assess risks to individuals; and
- identify any measures to mitigate those risks and protect the data.

Objective

The objective of conducting this DPIA is to identify any data protection issues with the JDL. It is important to remember that ultimately the focus of a DPIA is compliance with the General Data Protection Regulation (GDPR) and the new Data Protection Act 2018 (referred to as 'data protection laws' in this report). However, compliance with any other relevant legislation should also be considered.

Underlying principle

Data sharing and testing must be undertaken within a clear legal framework with any intrusion upon an individuals' privacy to be kept to a minimum. By undertaking a DPIA we ensure this principle is met.

DPIA process

The process for conducting a DPIA is described by the ICO as follows:

1. Identify the need for a DPIA;
2. Describe the processing;
3. Consider consultation;
4. Assess necessity and proportionality;
5. Identify and assess risks;
6. Identify measures to mitigate risk;
7. Sign off and record outcomes;
8. Integrate outcomes into plan; and
9. Keep under review.

This report is a full scale DPIA for the JDL service.

3. Justice Data Lab details

Justice Data Lab Overview

The Justice Data Lab (JDL) was launched on 2nd April 2013 as part of the Transforming Rehabilitation Programme. The announcement of the Justice Data Lab followed a period of successful engagement with organisations that provide offender services, identifying the initiative as a key mechanism to improve research and evaluation capability for organisations delivering offender services by allowing access to high quality re-offending data. Following a two-year pilot, the JDL became a permanent service in April 2015.

What is the JDL?

The JDL is a small team from Analytical Services within the Ministry of Justice (the Justice Data Lab team) that support organisations that provide offender services by allowing them easy access to aggregate reoffending data, specific to the group of people they have worked with. This will support organisations in understanding their effectiveness at reducing reoffending.

Participating organisations supply the JDL with details of the offenders who they have worked with, and information about the services provided. The JDL will supply several aggregate one-year proven reoffending measures for that group, and that of a matched comparison group of similar offenders. The reoffending measures for the organisation's group and the matched comparison group will be compared using statistical testing to assess the impact of the organisation's work on reducing reoffending. The results will then be returned to the organisation in a clear and easy to understand report, with explanations of the key metrics, and any caveats and limitations necessary for interpretation of the results. This report is then published at https://www.gov.uk/government/collections/justice-data-lab-pilot-statistics.

To ensure compliance with the new data protection laws, there are conditions on accessing the Justice Data Lab and the data that will be made available which must be compliant with Statistical Disclosure Control policy. These conditions are explained in this document, and in the accompanying guidance on accessing the JDL.

To ensure the JDL is successful, the processes and communications around access and use need to be transparent, legally compliant, and have data protection at the core.

Aims of the JDL

Previously, many providers of offender services, particularly in the voluntary and charity sector (VCS), struggled to access reoffending data relevant to the offenders they work with. This means organisations had significant difficulties in measuring the effectiveness of their rehabilitation work, with respect to a reduction in reoffending. The lack of access to high quality reoffending information had also prevented some organisations learning from and improving the services they deliver; and has made it difficult – if not impossible – for them to demonstrate their impact to commissioners.

The JDL addresses this by providing organisations with aggregate reoffending data specific to the offenders they have been working with, and that of a matched comparison group to allow them to understand their specific impact in reducing reoffending. Supporting organisations by providing easy access to high quality reoffending information allows them to focus only on what works, better demonstrate their effectiveness and ultimately reduce reoffending.

What kind of processing and data does this proposal involve?	
Who is the Lead/Manager/Senior Responsible Owner for the policy/ project/initiative?	*The Senior Responsible Owner is Lisa Barrett, with Steve Ellerd-Elliott as the Information Asset Owner. Project lead is Sarah French.*
What personal data will be processed as part of the project/ policy/initiative? **How many individuals' data will be involved?**	The Justice Data Lab (JDL) provides analysis to enable providers of offender interventions better access to reoffending data to assess their impact on reoffending behaviour. Providers of offender interventions will supply the JDL team in Justice Statistics with personal details of those persons attending their offender intervention, and details of the intervention and how the supplied data was captured. Key person-level identifiers required are first name, surname, DoB and gender, along with dates that refer to the participation in the intervention or the sentence that led to this participation. These individual records are then linked to internal MoJ administrative datasets (for example, the Police National Computer, reoffending databases, Offender Assessment information), and the characteristics of this cohort are reflected in the wider offender population to create a comparison group to match to and analyse aggregate reoffending information. Once the treatment cohort and comparison group are merged together, all person-level identifiers provided by the customer are removed. The JDL requires a minimum cohort of 60 individuals to be submitted for each analysis request. The largest cohort previously provided to the JDL has been around 58,000.
What is the source of the information? **Will it be collected directly from the individuals?** **Will it be collected by another organisation on behalf of MoJ?** **If so what is the relationship and authority/control the MoJ has over the organisation?** **Which organisation is the data controller, which is a data processor?**	The organisation that wishes to have their impact on reducing reoffending by JDL provides information on those offenders that they have worked with. In order to provide person-level records, the organisation must confirm that they are sharing this information in accordance with the GDPR, either via obtaining consent directly from offenders or (the most likely route) is that organisations could satisfy Article 5 1 (b), which states; Personal data shall be …. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); MoJ relies on Article 1(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. It is in the public interest to

	evaluate the effectiveness of interventions intended to reduce reoffending. As some of the data processed relates to criminal convictions and offences (Article 10) a condition in Part 1, 2 or 3 of Schedule 1 of the DPA (2018) must also be met. The processing meets the condition at paragraph 4 and also the requirements of section 19. This will clearly be of benefit to organisations providing offender services but the data is also necessary for Ministry of Justice to build an evidence base about various interventions, and to inform decisions about policy development and service delivery. The Ministry could not achieve these purposes through other means because it has no other way of accessing the data. It is of course for organisations, in their role as Data Controllers, to satisfy themselves that the sharing of the data with the Ministry of Justice complies with their legal obligations under the new data protection laws. Organisations should obtain their own legal advice about these issues if it is considered necessary. Organisations using the JDL would either collect the information directly from the individuals (for example, when an offender is registering for a rehabilitation-focused course) or via HMPPS. The customer organisation and the JDL are the data controllers, with the JDL team also acting as the data processor.
Does the project/policy/initiative involve the use of personal data MoJ currently processes of new purposes?	The information provided by customers are matched with data held by Justice Statistics. No new data needs to be sourced internally for the operation of the Justice Data Lab. The data on the offenders will first be matched to the copy of the Police National Computer (PNC) held by Justice Statistics. This copy of the PNC can be used for research and analytical purposes only, for which this purpose is compliant. Subsequently, the provider cohort will be matched to additional justice data to create a matched comparison group. This will include matching on characteristics such as gender, age, residential area, employment and benefit history, criminal history, reoffending information and, where available, information from Offender Assessments (OASys). These data are also available to Justice Statistics for research and analytical purposes, for which this use of the data is compliant. The Information Asset Owners of the above data are aware of this use and consent to this purpose.

Data Flow analysis – *set out in a diagram or table the data flows including where the data comes from, how it moves within MoJ, flows to and from other organisations. Include the collection, use storage and deletion of the data and the mechanisms (e.g. internet, courier, email) used to move the data.*

Organisation submits person-level data to JDL using Data Upload template	Must use a secure email account (e.g. CJSM, GSI) to justice.datalab@justice.gov.uk
JDL confirms receipt of data, and transfers data via Kingston device from inbox to MoJ secure network	The Kingston device is an approved secure encrypted removeable media device with access limited to several named individuals in Justice Statistics. Once transferred, original data is deleted from inbox and Kingston device
Treatment cohort provided is linked to several MoJ datasets held by Justice Statistics	This includes the Police National Computer, reoffending data, DWP/HMRC data, Offender Assessment information, linking characteristics and criminal history information as well as identifying suitable reoffending follow up period
Comparison group created and matched to treatment group. Aggregated reoffending metrics are calculated	Characteristics of the treatment cohort are reflected in the comparison group, extracted from the wider offender population. Propensity Score Matching is used to directly match the two groups, with the reoffending metrics analysed for statistical significance
A standard report and annex is shared with the customer via the original secure email account used to provide data	The customer has a review period of around 3-4 weeks prior to publication to make sure that they understand the report and that the JDL has reflected their intervention accurately. Reports are then published on .gov.uk in a quarterly publication cycle
Report is published and original data provided is deleted from secure network a month after publication	Data is retained for a month so that the JDL team can accurately respond to any queries from the analysis. Pseudo-anonymised data (i.e. with original personal identifiers, such as name, dob removed) is retained unless customers say otherwise.

Requirement		**Comments**
Data Protection Impact Assessment **GDPR Article.35** **or** **The Bill Section.62**	**Data Protection Impact Assessment (DPIA):** • Has a DPIA screening process for the proposal/project/system been completed? • If yes – please attach the DPIA screen form. • Has a DPIA/PIA that relates to the proposal/project/system been completed? • If yes – please attach the assessment.	A DPIA screening process has not been completed, as a full PIA was completed for the initiation of the JDL service, due to the need for a full PIA was realised due to the significant use of personal information, and the process proceeded to a full-scale PIA to ensure value for money for the tax payer. The original PIA was published in March 2013, available at https://www.gov.uk/government/publications/justice-data-lab
The Principles **GDPR Article.5** **or** **The Bill Section.32** • **Lawful** • **Specific** • **Limited** • **Accurate** • **Time-Bound** • **Secure**	**Lawful:** • What is the legal basis for processing the data? • Does this require the data to be processed, or simply allow it?	**What is it (e.g. Statutory / Common Law)?** The legal gateway which permits the sharing of offender data for this purpose is Section 14 of the Offender Management Act 2007. This section of the Act permits disclosure of information for the purposes of the management of offenders. GDPR Article 6 (e) processing is necessary for the performance of substantial task in the public interest. As data relating to criminal convictions and offences is being processed Article 10 of the GDPR and section 10 and schedule 1 paragraph 4 of the DPB 2018 apply.
	Specific: • What is the business use/purpose for processing the data?	The purpose for processing the data is to provide quantitative evidence for rehabilitation organisations to better demonstrate their impact on recidivism, and ultimately this informs the MoJ as to

	The use/purpose must be clear and specific.	which type of programmes work to reducing reoffending to inform future policy development
	Adequate: • What assessment has been made on the adequacy of the data being processed in relation to the purpose?	The data upload template that customers use to submit a request to the JDL specifies several key variables and contextual questions, without which a request cannot and would not be processed. If any organisation provides insufficient information then the request is returned, clarifying what is needed.
	Limited: • What assessment has been made on the relevance of the data being processed to the purpose? • Will the data be used for any other purpose?	The data provided by customers is extremely relevant, as there would be no other way to quantifiably assess the impact of rehabilitation organisations without providing sensitive individual level data to the customer, which comes with data security risks. The data provided by customers will not be used for any other purpose other than their JDL analysis. Pseudo-anonymised data (i.e. with original personal identifiers provided by the customer, such as name, dob removed) is retained unless customers say otherwise to feed into JDL development project to better assess as a whole what works to reduce reoffending.
	Accurate: • How will the accuracy of the data be checked? • How will inaccurate data be corrected? • How will it be kept up to date? • What processes will be in place to manage requests for rectification?	Provider organisations are required to complete a template which sets out the personal details required for the individuals they have worked with to be processed by the JDL. Clear guidance is provided to ensure that the meaning and reason behind collecting each of the fields is well explained. This helps ensure that accurate information is submitted to JDL. If there are any uncertainties around the data provided, the provider organisation will be contacted to achieve clarification. The communications included as part of the JDL makes clear that there is a standard required in submitting information to the Justice Data Lab to ensure the highest level of accuracy. The accuracy of the submitted information is crucial to producing high quality analysis and results in the Justice Data Lab which are accurate and meaningful to the provider organisations. There should be little processing required of the submitted data. For example, if the organisation could only submit surnames for each person, and it was evident that there were significant typing errors, then this request would be rejected to inaccurate data. The personal details received from providers are matched against the PNC to check for accuracy. Suspect matches (i.e. matches where we cannot be sure that the match on the PNC represents the individual concerned) are assessed and discarded where necessary. The providers are informed of the match rate between the information they supplied and the details on the PNC when a report on their cohort is completed.

		Matches are checked by comparing the following variables which are in order of the strength of the match: • Police National Computer Identifier or prison number (these are unique identifiers which would indicate confidence in the match produced) • Prison or probation start and end date (this would indicate the correct time period to start reoffending calculations had been identified) • Name (including forename and surname) • Date of Birth • Gender • Intervention start date If, for example, the individuals matched only on name and a combination of the remaining matching criteria we may not be confident that this would be an accurate match and we may discard the results. To ensure the highest level of accuracy, members of the Justice Data Lab team will have the necessary training to ensure the matches produced are of the highest possible quality and thorough quality assurance checks performed by a second JDL team member. Erroneous data collected by the organisation will be corrected according to local policies. Data submitted to the JDL should be correct at the time of sending. If the data is later identified as erroneous, then the organisation should contact a member of the JDL team. Depending on the nature and progression of the issue, the corrected data may be submitted, or the request halted. If the data is identified as erroneous after the final analysis has been shared, the request will not be corrected. Depending on the nature of the corrections needed, the final results may be identified as being incorrect and must be permanently deleted. Using erroneous data in the JDL could be extremely misleading – it will be the responsibility of the organisation to ensure that it is sharing correct and accurate data. If analysis from the JDL is identified as being erroneous after the results have been made available to the organisation, then the organisation will be contacted. The correct results will be made available, with an explanation of the errors which lead to the initial incorrect results being shared. Once the results of the request have been shared with the provider organisation, the organisation will have 3-4 weeks to raise any queries about the request (the review period). After the review period has elapsed, the individual level data shared with the JDL will be destroyed.

	Time-Bound: • How long will the data be kept? • Is the data covered by an existing retention and deletion schedule? If not will one be agreed with the Departmental Records Officer? • Will you be able to delete the data when you no longer need it? • If you can't delete it, can you anonymise it partly or wholly? • What processes will be in place to ensure the data is securely destroyed/deleted?	A retention and destruction schedule for individual level data shared as part of this initiative, and is outlined: Once the results of the request have been shared with the provider organisation, the organisation will have 3-4 weeks to raise any queries about the request (the review period). After the review period has elapsed (plus a month after publication to enable the JDL to answer any follow up queries), the individual level data shared with the Ministry of Justice will be destroyed. The aggregate reoffending data is IL0 and can be retained indefinitely. Any linked data (with person-level identifiers removed) will be retained unless the customer has stated they do not want this to happen. An internal register is kept of the different systems that the data could be held on (e.g. email inbox, MoJ secure network) and it is marked to register that the dataset has been deleted from each section, with a regular audit of this register conducted every quarter to ensure compliance by the JDL team leader.
	Secure: • How will the data secured and kept safe? • What technical / operational security features and/or policies protect it?	**What controls determine how data is accessed / read (passwords / encryption etc)?** Once the data is submitted to the JDL, it is transferred onto a secure network via a Kingston device, an approved secure encrypted removeable media device with access limited to several named individuals in Justice Statistics. Once transferred, the data is removed from the Kingston and the JDL inbox. The secure network houses the Police National Computer extract, and is accredited to IL5 level. It includes a number of physical and technical safeguards to protect the data on the network and policies to audit these processes. Further details on the safeguards in place can be given if necessary. Data is only housed where necessary and is deleted once analysis is published
Transparent **GDPR Article.12, 13 & 14** **or** **The Bill Section.42 and 43**	**Transparent / Duty to Inform:** • How will data subjects (e.g. customers, staff) be made aware of what is happening to their data? • Do individuals have an opportunity and/or right to decline to disclose or share their information? If so please provide a copy or link to any privacy notice.	Customers have access to a range of published guidance on the JDL process, available here: https://www.gov.uk/government/publications/justice-data-lab This includes the template that is used to submit requests, a user journey document that fully outlines what happens to their data and why, along with methodology documents so they can understand the statistical techniques behind a JDL analysis. During a request, the customer is kept up to date with the project by the lead analyst via emails/phone calls. Individuals share their data with the organisation who is seeking a JDL request – it is for the organisation to ensure that they are compliant with the new data protection laws to share this information and are responsible for issuing privacy notices accordingly.

Subject Access **GDPR Article.15** **or** **The Bill Section.43**	**Subject Access Requests:** • Will the personal data be extracted and provided to the data subject through usual business processes? • If not how will subject access requests be managed?	No personal information is made available via the JDL – once individual level data is submitted to the JDL, it is linked to various datasets before aggregated outputs are provided. No personal data would be provided from the JDL.
Data Transfers **GDPR Article.44 and 45** **or** **The Bill Section.70 to 74**	**Data Transfers:** • Will the data be held or transferred outside the UK? • If yes – where will it be held or transferred to? • Will the data be held or transferred outside the EEA? • If yes - where will it be held or transferred to? • If yes what processes will be place to ensure it is adequately protected?	No data provided to the JDL will be held or transferred outside the UK
Lawfulness **GDPR Article.6** **or** **The Bill Section.33, 34**	**Lawfulness:** Which of the following conditions will apply to how the data is used? • Consent (which is clear, informed and freely given)? • Contract (which stipulates the data processing is required)? • Legal obligation (Act of Parliament, SI)? • Vital (health) Interests (of data subject or another)? • Fundamental to the performance of a government function?	The legal gateway which permits the sharing of offender data for this purpose is Section 14 of the Offender Management Act 2007. This section of the Act permits disclosure of information for the purposes of the management of offenders. GDPR Article 6 (e) processing is necessary for the performance of substantial task in the public interest. As data relating to criminal convictions and offences is being processed Article 10 of the GDPR and section 10 and schedule 1 paragraph 4 of the DPB 2018 apply.
Consent **GDPR Article.7** **or** **The Bill Section.33 and 40**	**Consent:** • If you will be relying on consent will it be given by a confirmation or action by the individual? How will this be recorded? • Will plain language be used? • What processes will be in place to manage withdrawal of consent?	If an organisation is relying on consent to provide the JDL with their individual level data, it is their responsibility to abide by the new data protection laws to gain this consent.
Special Categories of Personal Data **GDPR Article.9** **or**	**Special Categories:** • Will any of the data that will be processed include information about individuals': race, ethnicity, health, religion, sex life/orientation, political views, TU membership, genetic or biometric data?	The mandatory data items to be provided by the organisation to the JDL are: - Name - Date of birth - Gender - Information relating to the sentence that led to involvement with the intervention being analysed

The Bill Section.40	• Which of the following options will be applied to that processing? a) Explicit Consent? b) Necessary in compliance with legal obligation? c) Vital (health) Interests? d) By a legitimate, not-for profit body with a political, philosophical, religious or trade union aim? e) Data which has manifestly been made public by the data subject? f) Establishing / defending a legal claim or Courts acting in a judicial capacity? g) Substantial public interest? h) Preventative occupational medicine, or occupational health? i) Public interest in the public health (serious)? j) Archiving in the public interest or for historical/scientific research?	With the following items being desired to improve matching quality: - Police National Computer ID - Prison number Any other characteristic (e.g. ethnicity, nationality) will be determined from datasets held by Justice Statistics. Gender is a key matching variable to ensure robust and high quality analysis, and is provided by customers in accordance with compliance with the data protection laws
Criminal Convictions & Offences **GDPR Article.10** **or** **The Bill Part.3**	**Criminal Convictions:** • Will the information include personal data about offences/convictions? • Do you have a legal reason to have it and use it?	In order to identify the sentence that relates to when an individual was supported by a rehabilitation organisation (and in turn, identify the appropriate follow up period in which to measure whether they reoffended or not), we ask for one or more of the following: - Index date (date of release from prison/start of community sentence) - Conviction date - Start/end date of intervention programme The first two are preferred as it would enable to more direct match with datasets held by Justice Statistics and improve the quality of analysis. However, organisations can provide information solely on their time with the individual along with contextual information about their programme, which can be used to find appropriate reoffending periods.
Right to Erasure **GDPR Article.17** **or** **The Bill Section 45 and 46**	**Erasure:** • What processes will be in place to manage requests for erasure?	Should an organisation wish to withdraw their full cohort, they should email justice.datalab@justice.gov.uk . Providing that the request has not begun then we will delete the data from the secure network and confirm with the organisation.

		If an individual withdraws their consent from the organisation, the organisation should inform the JDL team, who will then seek to delete the individual record from the secure network and confirm once complete.
Right to Restriction **GDPR Article.18** **or** **The Bill Section 45 and 46**	**Restriction:** • What processes will be in place to manage requests to restrict processing?	This would be managed at a local level between the individual and the organisation that seeks to use the JDL service. Data is only then shared with the JDL in accordance with the data protection laws
Data Portability* **GDPR Article.20**	**Portability:** • Will the data be extractable in a machine-readable format? • What processes will be in place to manage requests to port the data? *NB: This will not apply to most government (legislation based) processing.	Data will not be permitted to be ported
Automated Decision Making **GDPR Article.22** **or** **The Bill Section 47 and 48**	**Automated Decision Making:** • Will the processing involve automated decision making affecting a person? • If yes please explain the circumstances. • What processes will be in place to manage objections to automated decision-making?	No decisions will be taken by an automated process – each point of data linking will account for the information provided by the organisation, both in terms of the data items provided and the contextual information about the intervention in order to adapt to fit the programme being analysed
Joint Controllers & Processors **GDPR Articles.26 to 30** **or** **The Bill Section 56 to 59**	**Data Sharing / Contracts:** • Will the data be shared with other business units/teams/parts of the Department? • If yes how will the data be shared/disclosed? • Will the personal data be shared with an external organisation? - OGD? - Supplier? - Third party? • What kind of arrangement will be in place to covers this? - Contract? - Data Sharing Agreement? - Memorandum of Understanding? - Other?	Data provided to the JDL for the purpose of receiving a JDL analysis and report will be not shared outside of the JDL team, neither internally within MoJ nor externally.

	• How will the data be shared/disclosed with the other organisations?	
Security **GDPR Article.32** **or** **The Bill Section.64**	**Security:** • Will the data encrypted? • Will the data pseudonymised? If so how? • How will the data be protected against risk of loss, confidentiality, availability and integrity? • Will back-ups be taken? • Will the security of the system/premises be tested regularly? • Will the security of the system be required to have any formal accreditation or independent certification (e.g. ISO27001)? • What processes will be in place to determine who will have access to the data/system? • What level of security clearance will be required to access the system/data? • What data protection/security training will users of the data/system be required to have? • How will access to the system be granted? • What information asset register and/or risk register will the data be recorded on?	The data is not encrypted itself and no back ups are taken. Once the data is submitted to the JDL, it is transferred onto a secure network via a Kingston device, an approved secure encrypted removeable media device with access limited to several named individuals in Justice Statistics. Once transferred, the data is removed from the Kingston and the JDL inbox. The secure network houses the Police National Computer extract, and is accredited to IL5 level. It includes a number of physical and technical safeguards to protect the data on the network and policies to audit these processes. Further details on the safeguards in place can be given if necessary. Pseudo-anonymised data (i.e. with original personal identifiers, such as name, dob removed) is retained unless customers say otherwise. This leaves only information already owned by Justice Statistics and does not include any information originally provided by the organisation.
Auditable Logging** **The Bill Section.60**	**Logging:** • Will the system / process have a logging function to track changes and access to the data so that a record (or log) is created each time a user does something with the data, such as- (a) adding / collecting it;	NA

	(b) altering or amending it; (c) viewing or reviewing it; (d) sharing, disclosing or transferring it (inc. to whom) (e) combining it with other data (e.g. to identify / prove something) (f) deleting or archiving it. **NB: This only applies to criminal law enforcement processing of personal data.	
Data Distinction** **The Bill Section.36(3)**	**Distinction (of data subjects):** • Will the system / process make a clear distinction between personal data relating to different types of data subject, and why it is being processed for criminal law enforcement purposes? This should include— (a) persons suspected of committing a criminal offence; (b) persons convicted of a criminal offence; (c) persons who are or may be victims of a criminal offence; (d) witnesses or other persons with information about offences The distinction should prevent the confusion of the above individual's data. **NB: This only applies to criminal law enforcement processing of personal data.	NA
Other privacy legislation and policies -		**Comments**
Privacy & Electronic Communications Regulations 2003	**Technology** Does the project/policy/initiative involve new or inherently privacy-invasive electronic communications technologies? For the avoidance of any doubt, 'communication' means any information exchanged or	No new technologies are being employed to support this initiative – the JDL will be operated from current Analytical Services / MoJ infrastructure.

	conveyed between finite parties by means of a public electronic communications service, but does not include information conveyed as part of a programme service, except to the extent that such information can be related to the identifiable subscriber or user receiving the information.	
	Communication providers Does the project/policy/initiative involve new or existing communication providers? For the avoidance of doubt, 'communication providers' means a person or organisation that provides an electronic communications network or an electronic communications service.[1]	No new communication providers are being employed to support this initiative – the JDL will be operated from current Analytical Services / MoJ infrastructure.
	Communication subscribers / users Does the project/policy/initiative involve new or existing communication subscribers / users? For the avoidance of doubt, 'communication subscriber' means a person who is a party to a contract with a provider of public electronic communication services for the supply of such services. 'User' means an individual using a public electronic communications service.	No new communication subscribers/users are being employed to support the JDL.
Human Rights Act 1998	**Article 2: Right to Life** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to life, subject to any limitations as may be defined in Article 2(2)? For the avoidance of any doubt, the limited circumstances are that in peacetime, a public authority may not cause death unless the death results from force used as follows: • Self defence or defence of another person from unlawful violence;	No

[1] Source – Communications Act 2003

	• Arresting of someone or the prevention of escape from lawful detention; and A lawful act to quell a riot or insurrection	
	Article 3: Prohibition of Torture Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not subjected to torture or inhuman or degrading treatment? For the avoidance of doubt, this is an absolute right.	No
	Article 4: Prohibition of Slavery or Forced Labour Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not held in servitude or forced to perform compulsory labour? For the avoidance of doubt, this is an absolute right; the following are excluded from being defined as forced or compulsory labour: • Work done in ordinary course of a prison or community sentence; • Military service; Community service in a public emergency; and normal civic obligations.	No
	Article 5: Right to Liberty and Security Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not deprived of their liberty subject to certain limitations? For the avoidance of doubt, the following limitations apply when a person is: • Held in lawful detention after conviction by a competent court; • Lawfully arrested or detained for non-compliance with a lawful court order or the fulfilment of any lawful obligation; • Lawfully arrested or detained to effect the appearance of the person	No

	before a competent legal authority; • Lawfully detained to prevent the spreading of infectious diseases; • Lawfully detained for personal safety (applies to persons of unsound mind, drug addicts etc.); and Lawfully detained to prevent unlawful entry into the country or lawful deportation from the country.	
	Article 6: Right to a Fair Trial Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to have a public hearing within a reasonable time by an independent and impartial tribunal established by law? For the avoidance of doubt, the hearings included are both civil and criminal proceedings that are not specifically classified as hearings that must be heard 'in camera', i.e. closed to the public	No
	Article 7: Right to no Punishment without Law Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to not be prosecuted for a crime that was not, at the alleged time of commission, constitute a criminal offence under national or international law? For the avoidance of doubt, this is an absolute right	No
	Article 8: Right to Respect for Private and Family Life Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to respect for privacy in terms of their private and family life subject to certain qualifications? For the avoidance of doubt, the qualifications are: • Legal compliance; • National security; • Public safety;	No. The Justice Data Lab will produce only results which will describe an organisation's impact on reducing reoffending, no operational decisions will be taken about an individual, nor will any decisions be taken on policy based on an individual's reoffending behaviour. However, the aim of the Justice Data Lab is to better understand the effectiveness of offender management to ultimately reduce reoffending. This is unlikely to adversely impact on an individual's right to private and family life.

	• National economy; • Prevention of crime and disorder; • Protection of public health and morals; Protection of rights and freedom of others.	
	Article 9: Right to Freedom of Thought, Conscience & Religion Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to freedom of thought, conscience and religion subject to certain qualifications? For the avoidance of doubt, the qualifications are: • Unless prescribed by law; • In interest of public safety; • Protection of public order, rights or morals; Protection of rights and freedoms of others.	No
	Article 10: Right to Free Expression Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to hold opinions and express their views singly or in dialogue subject to certain qualifications? For the avoidance of doubt, the qualifications are as set out in Article 9 above.	No
	Article 11: Right to Freedom of Assembly & Association Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to freedom of peaceful assembly and association with others subject to certain qualifications/ For the avoidance of doubt, the qualifications are as set out in Article 9 above.	No
	Article 12: Right to Marry Does the project/policy/initiative involve new or existing data processing that adversely	No

	impacts an individual's right to marry and found a family subject to certain restrictions? For the avoidance of doubt, the restrictions are regulated by law so long as they do not effectively take away the right, e.g. age restrictions apply	
	Article 14: Right to Freedom from Discrimination Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be treated in a manner that does not discriminate the individual from others subject to certain restrictions? For the avoidance of doubt, this right is restricted to the conventions as set out in the European Convention of Human Rights 1950; the grounds for discrimination can be based on: • Sex • Race • Colour • Language • Religion • Political persuasion • Nationality or social origin • Birth • Other status.	No, and we also assume that provider organisations will not discriminate in the delivery of their services, now, or in future as a result of their request to the Justice Data Lab.
	Articles: 16 / 17 / 18 Not relevant for the purpose of this questionnaire	
Regulation of Investigatory Powers Act (RIPA) 2000	Does the project/policy/initiative involve new or inherently privacy invasive electronic technologies to intercept communications? (For the avoidance of doubt, 'communications' is defined in RIPA Part V, section 81(1)). Does the project/policy/initiative involve new or inherently privacy invasive electronic technologies pertaining to the acquisition and disclosure of data relating to communications? Does the project/policy/initiative involve new or inherently privacy invasive electronic	No

	technologies pertaining to the carrying out of surveillance? Does the project/policy/initiative involve new or inherently privacy invasive electronic technologies pertaining to the provision of the means by which electronic data protected by encryption or passwords may be decrypted or accessed? Does the project/policy/initiative undertake any of the functions of the Security Service, the Secret Intelligence Service or the Government Communications Headquarters?	

Risk(s) identified in the assessment (for example risks to individuals, corporate risks, compliance risks)	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project/policy/initiative?
Risk in transferring data securely	Mandatory use of either GSI or CJSM secure account, made explicit in the Data Upload Template used to submit a request to the JDL. Any data provided without a secure account is deleted upon receipt	Reduced risk	Yes
Risk in housing personal data	Data retained on secure network once submitted to the JDL, deleted from JDL inbox once transfer complete. Only aggregated information is provided back to customer/published. Data provided is then deleted and only pseudo-anonymised data is retained.	Reduced risk	Yes

Stakeholders/Participants. **What organisations and individuals contributed to this assessment (include their role/function)?**

Name	Role	Organisation	Nature of Input
Sarah French	JDL team leader	Ministry of Justice	Drafted this report, aided by internal guidance on the GDPR alongside the previously published PIA that assessed compliance against the Data Protection Act

Approved by:	Date:

Alternative solution

The original PIA explored a potential alternative, with an external organisation carrying out the functions of the JDL. Whilst it may have been a better value for money approach, this was rejected due to the considerable risks associated with an external body having access to the Police National Computer and other linked Criminal Justice Data that would have outweighed the potential value for money aspects. As such, the JDL approach was adopted to ensure the best protection of provider data, and existing Criminal Justice data which is needed to provide robust comparison groups.

Data protection/risk reducing designs

The following solutions are in place to reduce risk:

- Government Secure Email address are used to send data from provider organisations to the Ministry of Justice where available. These are secure accounts which means that the risk of data intrusion during transfer to the Ministry of Justice is reduced

- CJSM accounts are used to send data from provider organisations to the Ministry of Justice when other secure email accounts are not available to the organisation. These accounts accredit data transfers to IL3 and means that the risk of data intrusion during transfer to the Ministry of Justice is reduced. In requesting a CJSM account, the authenticity of provider organisations will be checked, ensuring that only genuine organisations will be requesting JDL services.

- Once the data is received by the Ministry of Justice, it is retained on a secure network. Only members of the JDL team will be able to access this data. This will promote the integrity, privacy and protection of the data, and the copy of the Police National Computer information that the Ministry of Justice hold for research and analysis purposes only. All staff accessing the Police National Computer undergo training and vetting and abide by the Security Operating Agreement for this network.

- The anonymised datasets (produced from the merging of the provider organisations individual level data, and the administrative data) from which the aggregated results are produced, and the analytical code used to produce the aggregated results are retained for a

month after publication (should any queries arise). Following this, the linked dataset is stripped of any person-level identifier provided by the organisation and a pseudo-anonymised version is retained (unless the customer has opted out of this). This is to have useful information to feed into wider JDL projects whilst retaining anonymisation of individuals analysed. These datasets and analytical code will be stored only on the secure network, with access to them permitted only by named individuals from the JDL team.

4. Data flow analysis

JDL data flow diagram and description

This section outlines the flow of data through the JDL:

From the provider

Providers of offender interventions will supply the JDL team in Justice Statistics with personal details of those persons attending their offender intervention. The data will be send through a CJSM account, or through Government Secure email accounts.

To ensure compliance with the data protection laws, the provider will have to confirm that the information being shared complies with these laws.

Within the Ministry of Justice

Once the data has been received by the MoJ, it will be stored on a secure server, with access only by members of the JDL team. The above information will be matched with data held by Justice Statistics. No new data needs to be sourced internally for the operation of the JDL.

The data on the offenders will first be matched to the copy of the Police National Computer (PNC) held by Justice Statistics. This copy of the PNC can be used for research and analytical purposes only, for which this purpose is compliant. Matching to the PNC will allow a link to appropriate variables needed to link to other datasets.

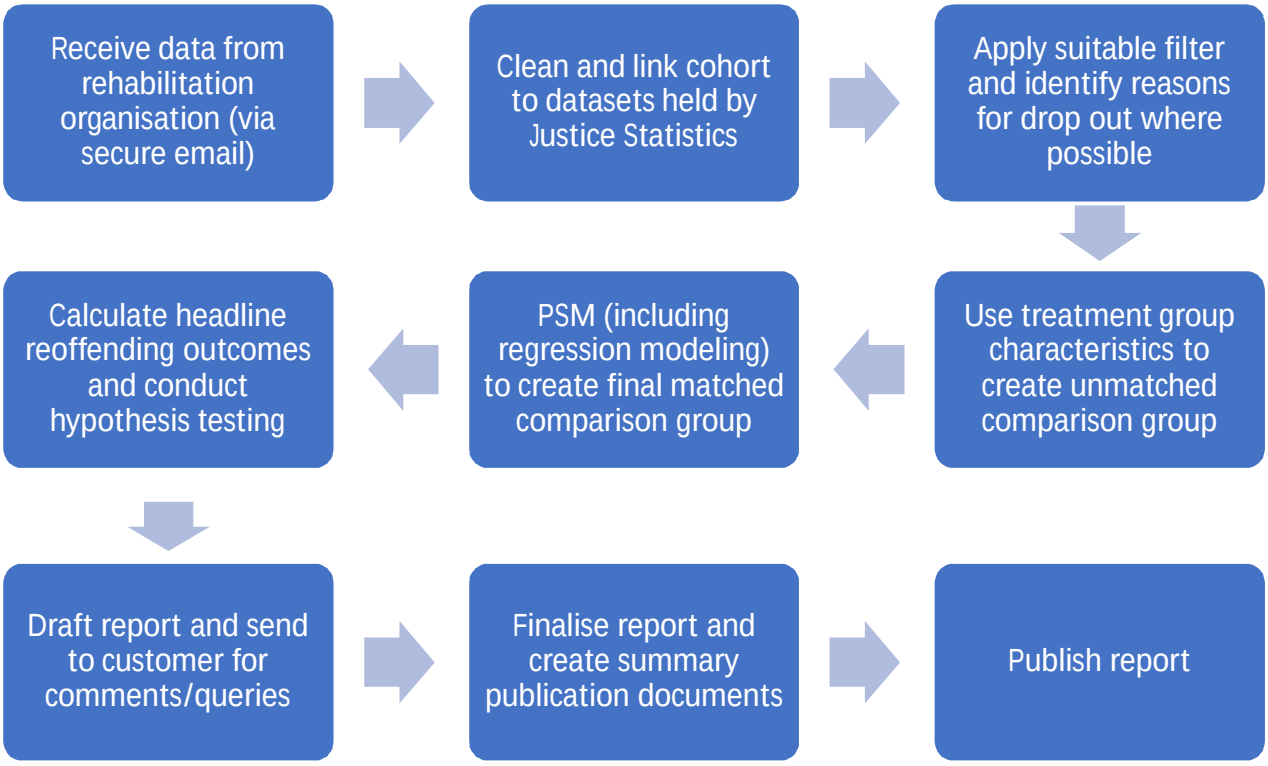
Subsequently, the provider cohort will be matched to additional justice data to create a matched comparison group. This will include matching on characteristics such as gender, age, residential area, employment and benefit history, criminal history and reoffending information. These data, including the data shared from DWP and HMRC are available to Justice Statistics for research and analytical purposes, for which this use of the data is compliant. Individuals identified as part of the matched comparison group will also be matched to the PNC to create an aggregate reoffending rate.

From the Ministry of Justice to the Provider

Once an aggregate reoffending rate has been produced for the provider cohort, and that of a matched comparison group, these statistics will be prepared in a standard report template. This standard report template will be returned to the provider organisation through the CJSM account, or through Government Secure email account.

Data flow diagram

A simple diagram outlining the data flow and the organisations/business units transmitting and receiving data:



5. Data protection analysis and risk management plan

Stakeholders/participants

In addition to stakeholders within the Ministry of Justice, the following external stakeholders have been identified as having an interest in this initiative:

- Individuals (ex-offenders) who have received services from provider organisations
- Provider organisations wishing to access services through the Justice Data Lab
- Potential bidders under the Transforming Rehabilitation Program who may use the aggregate analysis produced under the Justice Data Lab to commission services
- Her Majesty's Prison and Probation Service (HMPPS)
- The Home Office, who are data controllers for the Police National Computer who have shared information on employment and benefits for research and analytical purposes only, under which this initiative is compliant.
- Department for Work and Pensions, and Her Majesty's Revenue and Customs who have shared information on employment and benefits for research and analytical purposes only, under which this initiative is compliant.
- Cabinet Office, who have policy oversight of engaging the Voluntary and Charity sector.
- Information Commissioners Office

No stakeholders have been contacted regarding this DPIA, due to time constraints – however there is a robust communications and engagement process in place so that organisations or persons with an interest have been able to feed into the JDL's initial creation and continued development.

Analysis process

This screening process has identified robust practices in place that wholly support the JDL. There have been careful consideration of the protection of data through all stages of the process, and data protection is at the core of this initiative.

- The data collected as part of this service is necessary and justified.
- The technology in place supports the protection of data throughout the process, and ensures that it is handled correctly at all times
- The organisations involved are relevant to the process, with no excessive transfer or use of the data

Analysis summary

The JDL is compliant with the GDPR, DPA 2018 and the ECHR at all stages of the service and clear guidance about the steps of the process and procedures in place is provided (for example the use of CJSM accounts, or Government Secure email accounts) so that this compliance continues to be met throughout the operation of the JDL. Appropriate training of all Ministry of Justice staff is in place to ensure they understand thoroughly these procedures.

Risk management

The following risks have been identified:

- That provider organisations send data without assuring compliance with the data protection laws; and/or

- That provider organisations do not send the data through a Government Secure Email account, or a CJSM accounts, thereby increasing the risk of data intrusion or loss. In the User Journey document and Data Upload template, these permitted methods are explained clearly. Any data not sent through the permitted methods will be deleted and purged, explaining as such to the customer.

Risk mitigation

The above risks can be mitigated by clear procedural guidance, and thorough training of JDL staff.

The risk around assuring compliance with the data protection laws is mitigated through asking for assurance from each provider organisation upon request of service, and not proceeding without assurance. JDL staff are trained to ask for this assurance each time.

Summary

The JDL is capable of being compliant with the GDPR, DPA 2018 and the ECHR at all stages of the service.

6. Communication/publication strategy

Communications

This DPIA will be published alongside full guidance on the JDL.

Publication strategy

A communications strategy to ensure that this service is explained clearly and appropriately to the public has been in place since the pilot launch in 2012. The JDL aims ultimately to reduce reoffending by generating clear analysis of what is promising, and what works at reducing reoffending and has been well received by the public. This DPIA, as an update of the original PIA, is likely to be fully accepted by the public, and the Stakeholders identified for the project.

Justice Data Lab summary publication

All sections of this report can be published

7. Approval of report

Approval of: Justice Data Lab service	**Name: Sarah French**
Project Manager	Sarah French
Information Asset Owner	Steve Ellerd-Elliott, Chief Statistician for Ministry of Justice
Date of approval	25th May 2018

Alternative format versions of this report are available on request from justice.datalab@justice.gov.uk.