

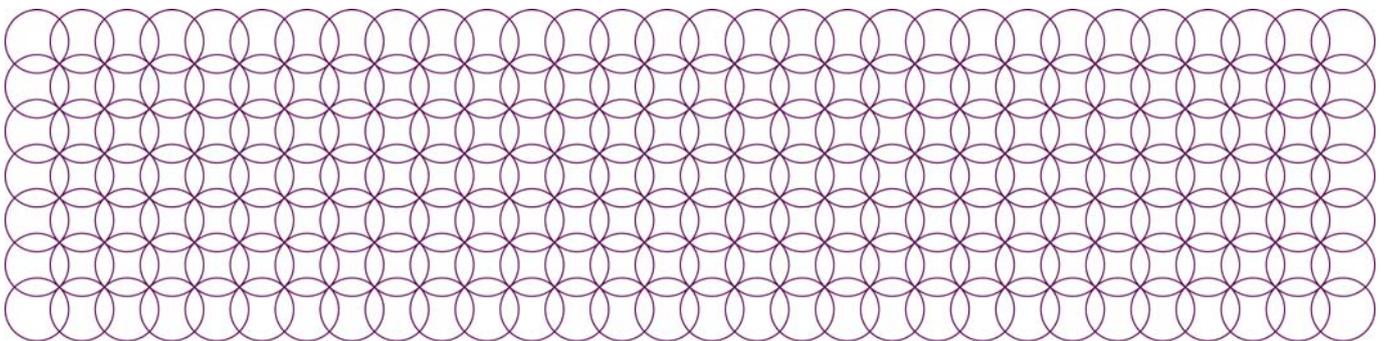


Ministry of  
**JUSTICE**

# **Justice Data Lab**

## Privacy Impact Assessment Report

March 2013







Ministry of  
**JUSTICE**

## **Justice Data Lab**

### Privacy Impact Assessment Report

**This information is also available on the Ministry of Justice website:  
[www.justice.gov.uk](http://www.justice.gov.uk)**



## Contents

Section 1 – Executive Summary	3
Section 2 – Introduction	4
Section 3 – Justice Data Lab details	6
Section 4 – Data Flow Analysis	32
Section 5 – Data Protection Analysis & Risk Management Plan	35
Section 6 – Communication/Publication Strategy	37
Section 7 – Approval of Report	38

---



## **Section 1 – Executive Summary**

### **Background**

This document is a full scale Privacy Impact Assessment for the Justice Data Lab

### **Findings**

This Privacy Impact Assessment shows that the Justice Data Lab initiative is capable of being compliant with the Data Protection Act and the European Convention of Human Rights at all stages of the initiative.

### **Review Process**

This Privacy Impact Assessment has been produced by the project lead for the Justice Data Lab. The initial draft was reviewed by internal Ministry of Justice colleagues with expertise in Information Assurance and was also subject to legal advice. The comments made by these colleagues have been reflected in the final version of this document.

## **Section 2 – Introduction**

### **Background**

A Privacy Impact Assessment (PIA) is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions. The primary purpose of a PIA is to visibly demonstrate that an organisation acts responsibly in relation to privacy. The deliverables and benefits of undertaking a PIA can be summarised as follows:

- The identification and management of risk;
- Avoidance of unnecessary costs;
- Prevention of inadequate solutions;
- Avoiding loss of trust and reputation;
- Informing citizens and partners of the organisation's communications strategy;
- Meeting and exceeding legal requirements.

### **Objective**

The objective of conducting this PIA is to identify any data protection issues with the proposed Justice Data Lab. It is important to remember that ultimately the focus of a PIA is compliance with the Data Protection Act (DPA). 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 PIA we ensure this principle is met.

### **HMG requirement**

The Data Handling Review, published in June 2008, states that all Departments will "introduce Privacy Impact Assessments, which ensure that privacy issues are factored into plans from the start, and those planning services are clear about their aims. Similarly, information risk management will be considered as part of the Government's "Gateway" reviews that monitor progress of the most important projects". The Data Handling Review has now been subsumed into HMG Information Assurance Standard No 6 – Protecting Personal Information and Managing Information Risk. Accordingly, PIAs are to be carried out on MoJ projects and policies that involve the processing of personal data.

## PIA Process

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

1. Initial assessment (i.e. the Screening Process) – Examines the project at an early stage, makes an initial assessment of privacy risk and decides which level of assessment<sup>1</sup> is necessary. This has been undertaken and the subsequent report is referenced in this report.
2. Where necessary, conduct, either:
  - Full-scale PIA – a more in-depth internal assessment of privacy risks and liabilities. It includes the need to identify stakeholders, analyse privacy risks, consults widely with stakeholders on privacy concerns and brings forward solutions to accept, mitigate or avoid them; or
  - Small-scale PIA – Similar to a full-scale PIA, but is less formalised. Requires less exhaustive information gathering and analysis. More likely to be used when focusing on specific aspects of a project.
  - Review – Sets out a timetable for reviewing actions taken as a result of a PIA and examines their effectiveness. Looks at new aspects of the project and assesses whether they should result in an updated PIA.

This report is a full scale PIA for the Justice Data Lab pilot.

---

<sup>1</sup> Full Scale PIA, Small Scale PIA or no PIA.

## **Section 3 – Justice Data Lab details**

### **Justice Data Lab Overview**

The Justice Data Lab was announced by the Secretary of State, the Right Honourable Chris Grayling MP in December 2012 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.

### **What is the Justice Data Lab initiative?**

The Justice Data Lab is being launched as a pilot for one year from April 2013. During this year, a small team from Analytical Services within the Ministry of Justice (the Justice Data Lab team) will support organisations that provide offender services by allowing them easy access to aggregate re-offending data, specific to the group of people they have worked with. This will support organisations in understanding their effectiveness at reducing re-offending.

Participating organisations will supply the Justice Data Lab with details of the offenders who they have worked with, and information about the services they have provided. The Justice Data Lab will supply aggregate one-year proven re-offending rates for that group, and that of a matched control group of similar offenders. The re-offending rates for the organisation's group and the matched control group will be compared using statistical testing to assess the impact of the organisation's work on reducing re-offending. The results will then be returned to the organisation in a clear and easy to understand format, with explanations of the key metrics, and any caveats and limitations necessary for interpretation of the results.

During the course of the one year pilot the initiative will be evaluated, so there will be a clear decision on the direction of the Justice Data Lab at the end of the pilot year. This PIA will be reviewed and updated to reflect any new status of the Justice Data Lab.

To ensure compliance with the Data Protection Act, there will be 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 also in the accompanying guidance on accessing the Justice Data Lab.

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

## The aims of the Justice Data Lab

Currently many providers of offender services, particularly in the voluntary and charity sector (VCS), struggle to access re-offending data relevant to the offenders they work with. This means organisations have significant difficulties in measuring the effectiveness of their rehabilitation work, with respect to a reduction in re-offending. The lack of access to high quality re-offending information has 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 data lab will address this by providing organisations with aggregate re-offending data specific to the offenders they have been working with, and that of a matched control group – this will allow them to understand their specific impact in reducing re-offending. Supporting organisations by providing easy access to high quality re-offending information will allow them to focus only on what works, better demonstrate their effectiveness and ultimately reduce re-offending.

1.	<i>Project Name:</i> Justice Data Lab
2.	<i>What is the Project/Policy/Initiative?</i> To enable providers of offender interventions better access to re-offending data
3.	<i>What is the main function/purpose of the Project/Policy/Initiative?</i> To support research and evaluation by providers, primarily in the voluntary and charity sector where access to high quality data and analytical skills has typically been more challenging.
4.	<i>Has a Screening Process been completed, provide a summary of the findings. Include: date of report, whether full scale or small scale PIA recommended?</i> No, as the need for a full PIA was realised early 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.
5.	<i>Has a PIA that related to this proposal already been conducted?</i> No

6.	<p><i>Briefly, what are the main data that is to be processed as part of the Project/Policy/Initiative?</i></p> <p>This initiative is primarily analytical in nature, and as a result there are significant amounts of data which will be processed:</p> <p><b>From the provider</b></p> <p>Providers of offender interventions will supply the small team in Justice Statistics Analytical Services (JSAS) with personal details of those persons attending their offender intervention, and details of the intervention and how the supplied data was captured (for example, how many records are missing due to incomplete data).</p> <p>This project relies on successful sharing of individual level data from organisations that deliver services to offenders, to the Justice Data Lab at the Ministry of Justice. Projects which involve any sharing of personal and sensitive personal data within the meaning of the Data Protection Act 1998 need to be lawful, fair, justified and proportionate in order to comply with that Act and Article 8 of the European Convention on Human Rights.</p> <p>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.</p> <p>Obtaining consent from offenders who have received services from an organisation to the sharing and analysis of personal information can satisfy one of the conditions necessary to comply with the Data Protection Act. However this is not the only condition which may be relied on. If consent has not been sought, we think it is likely that organisations could satisfy the condition that disclosure of the data to the Ministry of Justice is necessary for the exercise of the Ministry of Justice's functions (condition 5(c) of Schedule 2 and condition 7(1)(c) of Schedule 3). This reflects the fact that the purpose of Justice Data Lab is to generate reliable data about the effectiveness of offender interventions. 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.</p> <p>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 if available information from Offender Assessments (OASys). These data are also available to JSAS for research and analytical purposes, for which this use of the data is compliant. The Information Asset Owners of the above data have been informed of this intended use and consent to this purpose.</p>
----	--

Individuals identified as part of the matched comparison group will also be matched to the PNC to create an aggregate re-offending rate.

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, including those under the Data Protection Act, and that satisfying one of the conditions of Schedule 2 and Schedule 3 is only part of their obligations under that Act. **Organisations should obtain their own legal advice about these issues if it is considered necessary.** However, for the reasons set out above we consider it likely that the sharing of data with the Ministry of Justice to request aggregate re-offending data through the Justice Data Lab will fulfil one of the relevant conditions in both Schedule 2 and Schedule 3.

**Within the Ministry of Justice**

The above information will be matched with data held by JSAS. 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 JSAS. 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 an aggregate re-offending rate to be calculated for the provider cohort.

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 if available information from Offender Assessments (OASys). These data are also available to JSAS for research and analytical purposes, for which this use of the data is compliant. The Information Asset Owners of the above data have been informed of this intended use and consent to this purpose.

Individuals identified as part of the matched comparison group will also be matched to the PNC to create an aggregate re-offending rate.

## System users

Who (role/function) will have access to the personal data being used in the project?

7.	<p><i>Which user group(s) will have access to the data?</i></p> <p>The provider organisation will be the data controllers for the data they hold on the individuals they work with. The provider organisation will satisfy themselves that sharing this information with the Ministry of Justice meets conditions of the Data Protection Act.</p> <p>Once shared with the Justice Data Lab, the Ministry of Justice will also become data controllers for the individual level data which has been shared.</p> <p>Once the data has transferred to the Ministry of Justice, the raw data from the provider organisation will be saved on a secure network. A secure folder will be set up where this raw data will be stored, and only individuals in the Justice Data Lab team will be able to access this information. Once this information has been matched to the PNC, an anonymous identifier will then be used on any subsequent analysis to refer to each of the individuals and reduce the risk of identification.</p> <p>The aggregate re-offending rates for the providers' cohort and the matched control group will be calculated and be checked for quality and statistical disclosure control. If this information is safe to be disseminated, it will be securely returned to the provider organisation in a Final Report.</p> <p>Further questions about the re-offending behaviour of specific individuals will not be permitted. The organisation will then be required to publish the information contained in the Final Report, at which point the organisation and the public will have access to this data.</p>
8.	<p><i>Will contractors/service providers to MoJ have access to the data?</i></p> <p>No</p>
9.	<p><i>Is any remote support/maintenance by a 3<sup>rd</sup> party proposed? How will this access by 3<sup>rd</sup> parties be limited/managed/logged and audited?</i></p> <p>The secure network is currently maintained by Steria, where any Steria staff accessing the network are Security Cleared. It is not possible to access the network remotely. Steria perform monthly maintenance on the network, with activities agreed and overseen by Ministry of Justice staff.</p>

**Business case**

Business justification of privacy intrusion and its implications.

10.	<p><i>What data is to be collected?</i></p> <p>This initiative is aimed at providing high quality re-offending data to organisations that provide offender interventions. Personal data on the individuals that have attended an offender intervention will be shared with the Ministry of Justice, providing the conditions of the Data Protection Act have been met.</p> <p><b>From the provider</b></p> <p>Providers of offender interventions will supply the small team in Justice Statistics Analytical Services (JSAS) with the following personal information of the offenders they have worked with:</p> <ul style="list-style-type: none"> <li>- Name</li> <li>- Date of Birth</li> <li>- Gender</li> <li>- Residential postcode of the offender</li> <li>- Intervention start date</li> <li>- Prison or probation start and end date</li> <li>- Police National Computer Identifier or prison number</li> </ul> <p>Name, date of birth, and intervention start date are required to ensure the correct individual is matched to their re-offending information. The remaining information will support a high match rate with the PNC, and ensure any subsequent analysis is as robust as possible. Any suspect matches will be discarded.</p> <p>The provider organisation will also need to supply information about the intervention, and general information the data supplied (for example, does this cohort exclude persons due to incomplete information)</p> <p><b>Within the Ministry of Justice</b></p> <p>The above information will be matched with data held by JSAS. No new data needs to be sourced for the Justice Data Lab.</p>
-----	---

<p>11.</p>	<p><i>Briefly, what are the Personal Data elements used by the system/project?</i></p> <ul style="list-style-type: none"> <li>- Name (forename and surname)</li> <li>- Date of Birth</li> <li>- Gender</li> <li>- Residential postcode of the offender</li> <li>- Intervention start date</li> <li>- Prison or probation start and end date</li> <li>- Police National Computer Identifier or prison number</li> </ul> <p>Name, date of birth, and intervention start date are required to ensure the correct individual is matched to their re-offending information. The remaining information will support a high match rate with the PNC, and ensure any subsequent analysis is as robust as possible. Any suspect matches will be discarded. Each of these variables is needed for the successful operation of the Justice Data Lab, none are excessive.</p>
<p>12.</p>	<p><i>Please detail the data subjects from whom the Data is being collected?</i></p> <p>Offenders who have attended an intervention run by a provider organisation (public, private or third sector) are the data subjects covered by the Justice Data Lab. The provider organisation must have worked with the offender between 2002 to 2010, for these years we are able to calculate re-offending behaviour of offenders (re-offending information from 2011 will be available from October 2013). The re-offending behaviour of these persons will be compared with administrative data held on all offenders.</p>

13.	<p><i>How will the data collected from individuals or derived from the system be checked for accuracy?</i></p> <p>Provider organisations will be required to complete a template which will set out the personal details required for the individuals they have worked to be processed in the Justice Data Lab. Clear guidance will be provided to ensure that the meaning and reason behind collecting each of the fields is well explained. This will help ensure that accurate information is submitted to the Justice Data Lab. If there are any uncertainties around the data provided, the provider organisation will be contacted to achieve clarification.</p> <p>The communications included as part of the Justice Data Lab will make clear that there will be 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.</p> <p>The personal details received from providers will be 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) will be discarded. The providers will be informed of the match rate between the information they supplied and the details on the PNC when a report on their cohort is completed.</p> <p>Matches will be checked by comparing the following variables which are in order of the strength of the match:</p> <ul style="list-style-type: none"><li>- Police National Computer Identifier or prison number These are unique identifiers which would indicate confidence in the match produced</li><li>- Prison or probation start and end date This would indicate the correct time period to start re-offending calculations had been identified</li><li>- Name (including forename and surname)</li><li>- Date of Birth</li><li>- Gender</li><li>- Intervention start date</li><li>- Residential postcode of the offender</li></ul> <p>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.</p>
-----	--

	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.
14.	<p><i>Why is the Data being collected?</i></p> <p>The provider organisations will collect information on the personal details of the offenders they work with for administrative purposes. The information will be shared with the Ministry of Justice as it is necessary to fulfil the policy objective of answering requests for aggregate re-offending data through the Justice Data Lab.</p> <p>For the providers, it is necessary to share this data with the Ministry of Justice to help them understand their impact on reducing re-offending.</p>
15.	<p><i>Will the project analyse the data to assist users in identifying previously unknown areas of note, concern, or pattern?</i></p> <p>The Justice Data Lab will provide organisations of offender interventions information on their effectiveness at reducing re-offending.</p> <p>The Justice Data Lab will also allow the Ministry of Justice a greater understanding of what works with offenders. This will support the Transforming Rehabilitation Programme, as there will be a more robust evidence base upon which potential bidders for Payment by Results contracts can innovate. This has the potential to significantly improve offender services, bring down crime, and reduce re-offending.</p>
16.	<p><i>How will the data collected from individuals or derived from the system be checked for accuracy?</i></p> <p>(question is a duplicate of 13 above)</p>
17.	<p><i>How is the Data collected?</i></p> <p>The data provided by the organisation may be collected in a number of ways but will reflect the cohort of individuals they have worked with. We will not prescribe a method for collecting this information, but we would recommend that it is collected in partnership with public sector organisations (for example probation trusts), but does not place an undue burden on them to provide data retrospectively.</p>

18.	<p><i>How is the data stored?</i></p> <p>We will not prescribe the method for data storage by the organisations who will access the Justice Data Lab, however its storage should be proportional to the business impact level of the data.</p> <p>The business impact level of the data being sent to the Ministry of Justice is likely to be IL3.</p> <p>Once the data has transferred to the Ministry of Justice, the raw data from the organisation will be transferred to a secure network. A secure folder will be set up where this raw data will be stored, and only individuals working as part of the Justice Data Lab team will be able to access this information. Once this information has been matched to the PNC, an anonymous identifier will then be used to refer to each of the individuals.</p> <p>Once the results of the request have been shared with the provider organisation, the organisation will have 20 working days to raise any queries about the request (the review period). After the review period has elapsed, the individual level data shared with the Ministry of Justice, and any individual level data which could be linked back to named individuals will be destroyed.</p> <p>Where the provider's data cannot be processed for any reason, it will be returned to the provider, and destroyed securely from the Ministry of Justice network within 5 working days of intention to process.</p>
-----	--

19.	<p><i>Describe all the uses for the Personal Data (including for test purposes).</i></p> <p>During January and February 2013, data from a small number of organisations will be used to test the methodology and dissemination of results being developed for use in the Justice Data Lab. These organisations have given their consent that the data can be used for this purpose and the transfer of data will be confirmed as being compliant with the Data Protection Act.</p> <p>From April 2013, the Justice Data Lab will go live, and the personal data will be used only to provide results back to the organisations through the Justice Data Lab. The Ministry of Justice will ensure it complies with the Data Protection Act in the processing of these requests.</p> <p>There are no further uses of the personal data shared from an organisation to the Ministry of Justice for the Justice Data Lab initiative. The uses of the personal data are confined to research and analysis only – no decisions relating to individuals will be made on the basis of the data being shared.</p> <p>Once the results of the request have been shared with the provider organisation, the organisation will have 20 working days to raise any queries about the request (the review period). After the review period has elapsed, the individual level data shared with the Ministry of Justice will be destroyed.</p> <p>To create a matched comparison group Ministry of Justice administrative data will be used. These administrative data sources include information from Accredited Interventions, and employment and benefit data.</p> <p>The extract of the Police National Computer held by the MoJ has also been matched with administrative datasets from DWP and HMRC, to provide information about offenders' benefit and P45 employment history, as well as whether they have P45 employment spells in the year prior to conviction. The MoJ / DWP / HMRC data share contains benefit and P45 employment histories for the 3.6 million offenders who received at least one caution or conviction in England or Wales between 2000 and 2010, and who were successfully matched to DWP/HMRC data. This data was shared for the purposes of research and analysis, for which the intended use through the Justice Data Lab is compliant.</p> <p>Using this information to create matched comparison groups is important, because it will give more information about the characteristics of the populations, ensuring that the matched control group are as similar to the organisations' cohort as possible. This will enable the comparison of the organisations' cohort and the matched control group's aggregate re-offending rates to be as statistically robust and meaningful as possible.</p>
-----	--

<p>20.</p>	<p><i>How is the data going to be transferred?</i></p> <p><b>Transfer of data from the provider organisation to the Ministry of Justice</b></p> <p>Providers are permitted to use the methods described below, once they have satisfied themselves that they have the legal gateway to act with the data in the way they wish to.</p> <ul style="list-style-type: none"> <li>• It can be emailed from an offender management organisation, including; the police, probation trust or prison establishment, providing a Government Secure email address is used.</li> <li>• It can be sent from a Criminal Justice Secure email (CJSM) account.</li> </ul> <p>The data will be transferred using CJSM accounts, or through Government Secure email accounts, which are protected up to IL3 data transfers. The data will be encrypted, and the password sent separately. There will be no other permitted methods to transfer data to the Ministry of Justice.</p> <p><b>Data transfers from the Ministry of Justice to the Provider Organisation</b></p> <p>Once completed, a formal report containing the aggregate results will be sent to the organisation. This will be an email to the organisations CJSM account, or through the Government Secure email account. Note that the report will contain aggregate results only and therefore have been rated as ILO.</p>
<p>21.</p>	<p><i>What quantity of data will be collected and stored (aggregated?), will the project store or transmit more than 250 Personal Data records?</i></p> <p>The Justice Data Lab will set a minimum threshold for the number of individual records that can be received (no less than 60 records) – this is due to needing a minimum number of records to produce analysis of statistical integrity.</p> <p>There will not be a maximum number of records which would be permitted, but each request will be dealt with on a case by case basis to ensure its statistical integrity and compliance with the Data Protection Act.</p>

<p>22.</p>	<p><i>Will Sensitive Personal Data be processed, stored or transferred during this project? Sensitive Personal Data is Personal Data that consists of racial or ethnic origin, political opinions, religious beliefs, etc.</i></p> <p>The data supplied will include:</p> <ul style="list-style-type: none"> <li>- Intervention start date</li> <li>- Prison or probation start and end date</li> <li>- Police National Computer Identifier. or prison number</li> </ul> <p>This data is sensitive personal data according to s 2(g) and (h) of the DPA. The Justice Data Lab will also be processing information about offenders, which should be regarded as sensitive personal data.</p> <p>Sensitive personal data on offenders is held on the administrative datasets that will be used for the production of the analysis. This will include information about ethnicity, offending history, and high level criminogenic needs.</p>
<p>23.</p>	<p><i>What specific legal authorities/arrangements/ agreements define the collection of data?</i></p> <p>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.</p> <p>The data collected on individuals will have been collected for administrative purposes by the provider organisation.</p> <p>The Justice Data Lab aims to improve the evidence base for offender management, and plays a key role in the Transforming Rehabilitation Programme.</p>
<p>24.</p>	<p><i>Was notice provided to the individual prior to collection of the data? If yes, please provide a copy of the notice as an appendix to this document (A notice may include a posted privacy policy or a privacy notice on forms). If notice was not provided, why not?</i></p> <p>The data collected on individuals by a provider organisation will have been collected for their administrative purposes. The method of which is a local decision for provider organisations</p> <p>Before the data is transferred to the Ministry of Justice, the organisation must confirm that it considers that the conditions in schedule 2 and 3 of the Data Protection Act have been met with regards to onwards supply of personal details, and that they are able to share data under section 14 of the Offender Management Act 2007. This has been described above. The Ministry will not process any requests where this confirmation has not been given.</p>

**Not Protectively Marked**

25.	<p><i>Do individuals have an opportunity and/or right to decline to provide data?</i></p> <p>The collection of data by provider organisations ought to have been carried out in compliance with the Data Protection Act – the method of which is a local decision for provider organisations. Organisations have many responsibilities under the Data Protection Act. Ensuring that individuals have the right and opportunity to request that their data is not used in a request to the Justice Data Lab is one of the responsibilities that a provider organisation will have.</p>
26.	<p><i>Are we processing the data for the original purpose for which it was collected? Do individuals have the right to consent to particular uses of the data, and if so, how does the individual exercise that right?</i></p> <p>For many provider organisations, research and analysis (including by another organisation) will have been anticipated as part of the end use of the individual data collected, and have informed the individuals concerned of this purpose. This would permit the use of their data through the Justice Data Lab.</p> <p>It is likely that among the organisations who may access the Justice Data Lab there will be variations in the purpose that consent has been obtained for. It will be the responsibility of the organisation to confirm consent would cover the use of the individual level data in the Justice Data Lab, and other alternative conditions in schedule 2 and 3 of the Data Protection Act. .</p> <p>Before the data is transferred to the Ministry of Justice, the organisation must confirm that it considers that the conditions in schedule 2 and 3 of the Data Protection Act have been met with regards to onwards supply of personal details, and that they are able to share data under section 14 of the Offender Management Act 2007. This has been described above. The Ministry will not process any requests where this confirmation has not been given.</p>
27.	<p><i>What are the procedures which allow individuals the right to gain access to their own data?</i></p> <p>This will be defined at the local level between the individual and the organisation.</p>

<p>28.</p>	<p><i>What are the procedures for correcting erroneous data?</i></p> <p>Erroneous data collected by the organisation will be corrected according to local policies.</p> <p>Data submitted through the Justice Data Lab 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 Justice Data Lab team in the Ministry of Justice. 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 Justice Data Lab could be extremely misleading – it will be the responsibility of the organisation to ensure that it is sharing correct and accurate data.</p> <p>If analysis from the Justice Data Lab 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.</p> <p>Once the results of the request have been shared with the provider organisation, the organisation will have 20 working days to raise any queries about the request (the review period). After the review period has elapsed, the individual level data shared with the Ministry of Justice, and any individual level data which could be linked back to named individuals will be destroyed.</p>
<p>29.</p>	<p><i>How are individuals notified of the procedures for correcting their data?</i></p> <p>For data held by the organisation, this will be a local arrangement between the organisation and the individual.</p> <p>Once the data has been submitted to the Justice Data Lab it would be the responsibility of the organisation to correct the data shared with the Ministry of Justice as described above.</p>
<p>30.</p>	<p><i>If no redress is provided, are alternatives available?</i></p> <p>This is a local decision between the organisation and the individual</p>

## Organisational relationships

[Relationships with participating organisations.]

31.	<p><i>Is the data shared with internal organisations/departments? If yes, please list.</i></p> <p>During the Pilot of Justice Data Lab, the data sent from the provider organisation to the Justice Data Lab will not be shared with any other internal organisations or Departments.</p>
32.	<p>For each organisation/department, what data is shared and for what purpose?</p> <p><b>N/A</b></p>
33.	<p>How is the data transmitted or disclosed?</p> <p><b>N/A</b></p>
34.	<p><i>[Is data shared with external organisations/departments/non-Government organisations? If yes, which organisations/departments?]</i></p> <p>Data will be shared from provider organisations which provide offender interventions, who will be sharing data in compliance with the Data Protection Act</p>
35.	<p><i>[Specify which, if any, of these organisations are outside of the European Economic Area, and specify how the DPA is being complied with?]</i></p> <p>There are no organisations outside the EEA, all organisations will be providing offender services within England and Wales.</p>
36.	<p><i>[For each external organisation, what data is shared and for what purpose?]</i></p> <p><b>N/A</b></p>
37.	<p><i>[How is the data transmitted or disclosed to all external organisations?]</i></p> <p>The method of data transfer for each stage will be:</p> <p>1 – organisations will submit data securely through CJSM accounts, or through Government Secure email accounts</p> <p>2 – aggregate re-offending data will be submitted to the provider organisation through email in a standard reporting template</p>

38.	<p><i>[How is the shared data secured by the recipient? How long will the data be retained for? How is the data going to be securely destroyed?]</i></p> <p>The aggregate re-offending data is IL0, and can be retained by the recipient indefinitely.</p> <p>Once the results of the request have been shared with the provider organisation, the organisation will have 20 working days to raise any queries about the request (the review period). After the review period has elapsed, the individual level data shared with the Ministry of Justice, and any individual level data that could be linked back to named individuals will be destroyed.</p>
39.	<p><i>[Is there a Memorandum of Understanding (MoU), contract, or any data sharing agreement in place with any external organisations with whom data is shared through the system, and does the agreement reflect the scope of the data to be shared?]</i></p> <p>This Privacy Impact Assessment will be published alongside a document outlining the conditions of service for the Justice Data Lab. This in effect will form a service level agreement between the provider organisation and the MoJ – i.e. the responsibilities on both parties.</p>
40.	<p><i>[What training is required for users from agencies outside MoJ prior to receiving access to the data and how is the training audited for compliance to current MoJ policy?]</i></p> <p>Training is not required for organisations receiving aggregate re-offending data</p>

### Technology employed

[Provides details of technologies used to mitigate any risks, or those that may increase a risk. This section may be protectively marked PROTECT or RESTRICTED, dependent on content. You may wish to consult your IT business partner when completing this section.]

41.	<p><i>[Was the system built from the ground up (“bespoke”); or, was a COTS product purchased and installed?]</i></p> <p>No new technologies are being employed to support this initiative – the Justice Data Lab will be operated from current Analytical Services / MoJ infrastructure</p>
-----	---

**Not Protectively Marked**

42.	<p><i>[Describe how data integrity, privacy and security were analysed as part of the decisions made for your system (Security Working Group, User Requirements Document, Security Requirements Document)?]</i></p> <p>The Ministry of Justice regularly receives requests for data, similar to those that will be answered through the Justice Data Lab. There are robust processes in place that securely support these requests. The security in place for these requests was considered in understanding the baseline measures which should be in place to protect the data shared as part of the Justice Data Lab. The final solution should be one which retains the integrity, privacy and promotes the security of the shared data.</p> <p>The standalone secure network will be used to host the individual level data from provider organisations. This decision was taken as it is the system where the aggregate re-offending data is calculated from the Police National Computer (PNC) data held by the MoJ. This network has active access permissions and presents a secure mechanism by which provider organisation's data can only be accessed by members of the Justice Data Lab team.</p>
43.	<p><i>[What design choices were made to enhance privacy?]</i></p> <p>This system is already part of business as usual for Analytical Services. No design choices are relevant.</p>
44.	<p><i>[Does the system use "roles" to assign privileges to users of the system?]</i></p> <p>Yes, the system uses roles to assign privileges, consistent with a secure network</p>
45.	<p><i>[What procedures are in place to determine which users may access the system and where are they documented?]</i></p> <p>There is a JSAS network policy which is used to understand whether MoJ staff need to be granted access to this secure network based on the business need and if there are any alternative arrangements in place on the MoJ main network. This is documented in the PNC system operations (SyOps) document.</p>
46.	<p><i>[How are the actual assignments of roles and rules verified according to established security and auditing procedures?]</i></p> <p>The head of the Data Integration Analysis and Linking unit will sign off any requests for access to this secure network and ensure all access is compliant with the System Operating Procedures (SyOps) which is in place as part of the secure network</p>
47.	<p><i>[What auditing measures and technical safeguards are in place to prevent misuse of data?]</i></p> <p>This is a secure network. 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.</p>

48.	<p><i>[Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system.]</i></p> <p>All members of the Justice Data Lab team will be trained in how to access the JSAS network securely and to ensure data protection in adherence with the SyOps agreement. In addition, all team member will receive training in statistical disclosure control, and general training on how to use the software on the secure network.</p>
-----	---

### Legislation and policies

[Identification of legislation applicable to this project.]

49.	<p>[Privacy &amp; Electronic Communications Regulations 2003]</p> <p><b>Technology</b></p> <p><i>Does the project involve new or inherently privacy-invasive electronic communications technologies?</i></p> <p><i>For the avoidance of any doubt, ‘communication’ means any information exchanged or conveyed between finite parties by means of a public electronic communications service, but does not include information conveyed as part of a programme service, except to the extent that such information can be related to the identifiable subscriber or user receiving the information.’]</i></p> <p>no</p>
50.	<p>[Privacy &amp; Electronic Communications Regulations 2003]</p> <p><b>Communication providers</b></p> <p><i>Does the project involve new or existing communication providers?</i></p> <p><i>For the avoidance of doubt, ‘communication providers’ means a person or organisation that provides an electronic communications network or an electronic communications service.<sup>2</sup>]</i></p> <p>no</p>

---

<sup>2</sup> Source – Communications Act 2003

<p>51.</p>	<p><i>[Privacy &amp; Electronic Communications Regulations 2003</i></p> <p><b>Communication subscribers / users</b></p> <p><i>Does the project involve new or existing communication subscribers / users?</i></p> <p><i>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.]</i></p> <p>no</p>
<p>52.</p>	<p><i>[Human Rights Act 1998</i></p> <p><b>Article 2: Right to Life</b></p> <p><i>Does the project 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)?</i></p> <p><i>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:</i></p> <ul style="list-style-type: none"> <li>• <i>Self defence or defence of another person from unlawful violence;</i></li> <li>• <i>Arresting of someone or the prevention of escape from lawful detention; and</i></li> <li>• <i>A lawful act to quell a riot or insurrection.]</i></li> </ul> <p>no</p>
<p>53.</p>	<p><i>[Human Rights Act 1998</i></p> <p><b>Article 3: Prohibition of Torture</b></p> <p><i>Does the project involve new or existing data processing that adversely impacts an individual’s right to be not subjected to torture or inhuman or degrading treatment?</i></p> <p><i>For the avoidance of doubt, this is an absolute right.]</i></p> <p>no</p>

<p>54.</p>	<p><i>[Human Rights Act 1998</i></p> <p><b>Article 4: Prohibition of Slavery or Forced Labour</b></p> <p><i>Does the project 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?</i></p> <p><i>For the avoidance of doubt, this is an absolute right; the following are excluded from being defined as forced or compulsory labour:</i></p> <ul style="list-style-type: none"> <li>• <i>Work done in ordinary course of a prison or community sentence;</i></li> <li>• <i>Military service;</i></li> <li>• <i>Community service in a public emergency; and Normal civic obligations.]</i></li> </ul> <p>no</p>
<p>55.</p>	<p><i>[Human Rights Act 1998</i></p> <p><b>Article 5: Right to Liberty and Security</b></p> <p><i>Does the project involve new or existing data processing that adversely impacts an individual’s right to be not deprived of their liberty subject to certain limitations?</i></p> <p><i>For the avoidance of doubt, the following limitations apply when a person is:</i></p> <ul style="list-style-type: none"> <li>• <i>Held in lawful detention after conviction by a competent court;</i></li> <li>• <i>Lawfully arrested or detained for non-compliance with a lawful court order or the fulfilment of any lawful obligation;</i></li> <li>• <i>Lawfully arrested or detained to effect the appearance of the person before a competent legal authority;</i></li> <li>• <i>Lawfully detained to prevent the spreading of infectious diseases;</i></li> <li>• <i>Lawfully detained for personal safety (applies to persons of unsound mind, drug addicts etc.); and</i></li> <li>• <i>Lawfully detained to prevent unlawful entry into the country or lawful deportation from the country.]</i></li> </ul> <p>no</p>

<p>56.</p>	<p><i>[Human Rights Act 1998</i></p> <p><b>Article 6: Right to a Fair Trial</b></p> <p><i>Does the project 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?</i></p> <p><i>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.]</i></p> <p>no</p>
<p>57.</p>	<p><i>[Human Rights Act 1998</i></p> <p><b>Article 7: Right to no Punishment without Law</b></p> <p><i>Does the project 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?</i></p> <p><i>For the avoidance of doubt, this is an absolute right.]</i></p> <p>no</p>
<p>58.</p>	<p><i>[Human Rights Act 1998</i></p> <p><b>Article 8: Right to Respect for Private and Family Life</b></p> <p><i>Does the project 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?</i></p> <p><i>For the avoidance of doubt, the qualifications are:</i></p> <ul style="list-style-type: none"> <li>• <i>Legal compliance;</i></li> <li>• <i>National security;</i></li> <li>• <i>Public safety;</i></li> <li>• <i>National economy;</i></li> <li>• <i>Prevention of crime and disorder;</i></li> <li>• <i>Protection of public health and morals;</i></li> <li>• <i>Protection of rights and freedom of others.]</i></li> </ul> <p>The Justice Data Lab will produce only results which will describe an organisation’s impact on reducing re-offending, no operational decisions will be taken about an individual, nor will any decisions be taken on policy based on an individual’s re-offending behaviour. However, the aim of the Justice Data Lab is to better understand the effectiveness of offender management to ultimately reduce re-offending. This is unlikely to adversely impact on an individual’s right to private and family life.</p>

59.	<p><i>[Human Rights Act 1998</i></p> <p><b>Article 9: Right to Freedom of Thought, Conscience &amp; Religion</b></p> <p><i>Does the project involve new or existing data processing that adversely impacts an individual’s right to freedom of thought, conscience and religion subject to certain qualifications?</i></p> <p><i>For the avoidance of doubt, the qualifications are:</i></p> <ul style="list-style-type: none"> <li>• <i>Unless prescribed by law;</i></li> <li>• <i>In interest of public safety;</i></li> <li>• <i>Protection of public order, rights or morals;</i></li> <li>• <i>Protection of rights and freedoms of others.]</i></li> </ul> <p>no</p>
60.	<p><i>[Human Rights Act 1998</i></p> <p><b>Article 10: Right to Free Expression</b></p> <p><i>Does the project 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?</i></p> <p><i>For the avoidance of doubt, the qualifications are as set out in Article 9 above.]</i></p> <p>no</p>
61.	<p><i>[Human Rights Act 1998</i></p> <p><b>Article 11: Right to Freedom of Assembly &amp; Association</b></p> <p><i>Does the project 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/</i></p> <p><i>For the avoidance of doubt, the qualifications are as set out in Article 9 above.]</i></p> <p>no</p>
62.	<p><i>[Human Rights Act 1998</i></p> <p><b>Article 12: Right to Marry</b></p> <p><i>Does the project involve new or existing data processing that adversely impacts an individual’s right to marry and found a family subject to certain restrictions?</i></p> <p><i>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.]</i></p> <p>no</p>

63.	<p><i>[Human Rights Act 1998</i></p> <p><b>Article 14: Right to Freedom from Discrimination</b></p> <p><i>Does the project 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?</i></p> <p><i>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:</i></p> <ul style="list-style-type: none"> <li>• Sex</li> <li>• Race</li> <li>• Colour</li> <li>• Language</li> <li>• Religion</li> <li>• Political persuasion</li> <li>• Nationality or social origin</li> <li>• Birth</li> <li>• Other status.]</li> </ul> <p>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.</p>
64.	<p><i>[Human Rights Act 1998</i></p> <p><b>Articles: 16 / 17 / 18</b></p> <p><i>Not relevant for the purpose of this questionnaire.]</i></p>
65.	<p><i>[Regulation of Investigatory Powers Act (RIPA) 2000</i></p> <p><i>Does the project involve new or inherently privacy invasive electronic technologies to intercept communications?</i></p> <p><i>For the avoidance of doubt, ‘communications’ is defined in RIPA Part V, section 81(1).]</i></p> <p>no</p>
66.	<p><i>[Regulation of Investigatory Powers Act (RIPA) 2000</i></p> <p><i>Does the project involve new or inherently privacy invasive electronic technologies pertaining to the acquisition and disclosure of data relating to communications?]</i></p> <p>no</p>

67.	<p><i>[Regulation of Investigatory Powers Act (RIPA) 2000</i></p> <p><i>Does the project involve new or inherently privacy invasive electronic technologies pertaining to the carrying out of surveillance?]</i></p> <p>no</p>
68.	<p><i>[Regulation of Investigatory Powers Act (RIPA) 2000</i></p> <p><i>Does the project 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?]</i></p> <p>no</p>
69.	<p><i>[Regulation of Investigatory Powers Act (RIPA) 2000</i></p> <p><i>Does the project undertake any of the functions of the Security Service, the Secret Intelligence Service or the Government Communications Headquarters?]</i></p> <p>no</p>

## Alternative solutions

### Alternative solutions

The following solutions were also considered:

- That an external organisation could carry out the functions of the Justice Data Lab team. This approach may present a better value for money option, however there are considerable risks associated with an external body having access to the Police National Computer and other linked Criminal Justice Data that were deemed to outweigh the potential value for money aspects. It is unlikely that without sufficient legal and security arrangements in place that the Home Office (owners of the Police National Computer) would support an external organisation to carry out this function. In addition, through launching the pilot from the MoJ, the timescales for implementation would be significantly earlier, bringing significant benefits for the prospective provider organisations.

## Solution adopted

### Solution adopted

The solution described in this Privacy Impact Assessment has been adopted to ensure the best protection of provider data, and existing Criminal Justice data which is needed to provide robust comparison groups. Keeping the solution within the Ministry of Justice also means that the Justice Data Lab can be implemented more quickly, making use of existing skills in analysis this data and working with provider organisations.

## **Data protection/risk reducing designs**

The following solutions are in place to reduce risk:

- Government Secure Email address can be used to send data from provider organisations to the Ministry of Justice. These are secure accounts which means that the risk of data intrusion during transfer to the Ministry of Justice is reduced
- CJSM accounts will be used to send data from provider organisations to the Ministry of Justice. These accounts accredit data transfers to IL3. This 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 Justice Data Lab services.
- Once the data has been received by the Ministry of Justice, it will be retained on a secure network. Only members of the Justice Data Lab 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 will be retained for the duration of the Justice Data Lab pilot and its evaluation period. This is necessary to evaluate the statistical methodology used in the Justice Data Lab, ensuring that the products that are produced are of a consistently high standard. These datasets and analytical code will be stored only on the secure network, with access to them permitted only by named individuals from the Justice Data Lab team.
- A retention and destruction schedule for individual level data shared as part of this initiative, and is outlined above: data will be destroyed after the 20 day review period. Data that cannot be processed will be destroyed after 10 working days after confirmation with the provider organisation. This will ensure that the individual level data is used only for the purposes of answering requests to the Justice Data Lab.

## **Section 4 – Data flow analysis**

### **Business data flow diagram and description**

This section outlines the flow of data through the Justice Data Lab

#### **From the provider**

Providers of offender interventions will supply the small team in Justice Statistics Analytical Services (JSAS) with personal details of those persons attending their offender intervention. The data will be sent through a CJSM account, or through Government Secure email accounts.

To ensure compliance with the Data Protection Act, the provider will have to demonstrate that the information being shared complies with the Data Protection Act.

#### **Within the Ministry of Justice**

Once the data has been received by the Ministry of Justice, it will be stored on a secure server, with access only by members of the Justice Data Lab team. The above information will be matched with data held by JSAS. 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 JSAS. 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 an aggregate re-offending rate to be calculated for the provider cohort.

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. These data, including the data shared from DWP and HMRC are available to JSAS 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 re-offending rate.

#### **From the Ministry of Justice to the Provider**

Once an aggregate re-offending rate has been produced for the provider cohort, and that of a matched control 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 table**

A simple table listing the data flow and the organisations/business units transmitting and receiving data, include the network/transmission medium used e.g. GSi or Internet. Include any relevant comments around removal/manipulation of original data by the transmitting or receiving organisation.

	Item	Detail
1	Transfer of data from provider organisation	<p>Providers of offender interventions will supply the small team in Justice Statistics Analytical Services (JSAS) with personal details of those persons attending their offender intervention. The data will be sent through a Government Secure Email account, or a CJSM account.</p> <p>This transmission will be in line with CJSM protocols and Information Assurance guidance. For more information see the following link:</p> <p><a href="http://intranet.justice.gsi.gov.uk/guidance-support/security/information-security/sending-information.htm">http://intranet.justice.gsi.gov.uk/guidance-support/security/information-security/sending-information.htm</a></p> <p>The relevant mailbox in the Ministry of Justice is <a href="mailto:justice.datalab@justice.cjsm.gsi.gov.uk">justice.datalab@justice.cjsm.gsi.gov.uk</a></p> <p>Before the data is sent, the provider organisation must satisfy itself that it is compliant with the Data Protection Act. The Ministry of Justice has procedures in place to comply with the Data Protection Act, when becoming the new data controllers for the shared data.</p>
2	Receipt of data from provider organisation	<p>The Ministry of Justice will confirm that the data has been received by a member of the Justice Data Lab team via a return email, or a phone call. Any clarifications needed regarding the data will be sought.</p>
3	Transfer of data from Justice Data Lab mailbox	<p>The data will then be transferred to the secure network, via a secure encrypted removable media device. Once the transfer of this data is confirmed, the original email holding the provider data will be deleted and purged. The data will also be deleted and purged from the secure encrypted removable media device.</p>
4	Matching of data to the Police National Computer (PNC)	<p>The provider data will be matched against the Police National Computer to find the aggregate re-offending rate for the cohort. Once the individuals have been identified, an anonymous identifier will be used for subsequent analysis.</p>
5	Finding a matched control group	<p>Stage 4 will allow overall characteristics about the provider cohort to be gathered which are related to offending behaviour (i.e. age, gender, ethnicity, previous offending history). These characteristics will be logged, and a group of offenders with similar characteristics will be identified.</p> <p>Once the matched control group has been found, an</p>

		<p>aggregate re-offending rate for that group will be calculated. A standard report will be prepared from the results of the analysis</p>
6	<p>Return of standard report to the provider organisation</p>	<p>The standard report will be returned to the provider, which will detail the aggregate re-offending rate for the provider cohort, and that of a matched control group. Key metrics regarding the strength of the association will be given.</p> <p>The report will be returned to the CJSM account, or Government Secure email accounts that was originally used to send the provider data.</p>
7	<p>Review period</p>	<p>Once the standard report has been returned to the provider organisation, there will be a period of 20 working days where questions regarding the report can be raised. After this point, the provider data will be destroyed from the secure network. If the data cannot be processed so that a report can be raised, the individual data will be destroyed after 10 working days after discussion with the provider organisation about the failure of the request.</p>

## Section 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
- National Offender Management Service (NOMS)
- 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 Privacy Impact Assessment, 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 development of the initiative.

### Analysis process

This screening process has identified robust practices in place that wholly support the Justice Data Lab initiative. There has 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 initiative 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**

This initiative is capable of being compliant with the Data Protection Act and the ECHR at all stages of the initiative.

However, there must be clear guidance about the steps of the process and procedures in place (for example the use of CJSM accounts, or Government Secure email accounts) so that this compliance continues to be met throughout the operation of this pilot. Appropriate training of all Ministry of Justice staff must be 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 Act
- 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, these permitted methods are explained clearly. Any data not sent through the permitted methods will be rejected and returned, and the data will be deleted and purged.

### **Risk mitigation**

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

The risk around assuring compliance with the Data Protection Act could be mitigated through asking for assurance from each provider organisation upon request of service, and not proceeding without assurance. Justice Data Lab staff will need to be trained to ask for this assurance each time.

### **Summary**

This initiative is capable of being compliant with the Data Protection Act and the ECHR at all stages of the initiative.

## **Section 6 – Communication/publication strategy**

### **Communications**

This Privacy Impact Assessment will be published alongside full guidance on the Justice Data Lab.

### **Publication strategy**

A communications strategy to ensure that this initiative is explained clearly and appropriately to the public has been developed. This initiative aims ultimately to reduce re-offending by generating clear analysis of what is promising, and what works at reducing re-offending – this is likely to be well received by the public. This Privacy Impact Assessment 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

## Section 7 – Approval of report

<b>Approval of:</b> Justice Data Lab initiative Project Manager Information Asset Owner	<b>Name: Nicola Abrams</b> Nicola Abrams Mike Elkins, Chief Statistician for Ministry of Justice
<b>Date of approval</b>	25 <sup>th</sup> March 2013

### ICT projects

The PIA document would form part of the project documentation and will subject to normal project reviews which will include ICT Information Assurance and Security (IA&S). The ICT IA accreditor will require the PIA as part of the accreditation process and the ICT project may not achieve accreditation if a PIA is not present.

### Completion of report

Following completion of the report you should send to Data Access & Compliance Unit: [data.compliance@justice.gsi.gov.uk](mailto:data.compliance@justice.gsi.gov.uk) who will ensure the report is saved in the PIA library.



© Crown copyright  
Produced by the Ministry of Justice

Alternative format versions of this report are  
available on request from  
[justice.datalab@justice.gsi.gov.uk](mailto:justice.datalab@justice.gsi.gov.uk)