



Ministry
of Justice

Brandon Myers
[REDACTED]

Disclosure Team
Ministry of Justice
102 Petty France
London
SW1H 9AJ

data.access@justice.gov.uk

15 July 2026

Dear Mr Myers

Freedom of Information Act (FOIA) Request – 260616044

Thank you for your request dated 16 June 2026 in which you asked for the following information from the Ministry of Justice (MoJ):

I am writing to request recorded information under the Freedom of Information Act 2000. This request concerns the Ministry of Justice's use of the open-source probabilistic record-linkage library Splink, as described in the MoJ's published Algorithmic Transparency Recording Standard record "MoJ: Splink Master Record." That record states that Splink is used operationally — including a real-time Core Person Record (CPR), a Probation in Court function, and a pilot sharing Police National Computer numbers with police — to link individuals across HMCTS court, HMPPS prison, and probation case-management systems (DELIUS, NOMIS, Common Platform, LIBRA, FamilyMan, CaseMan).

I request the following recorded information:

- 1. Governance documents. The complete Data Protection Impact Assessment(s) and the internal Algorithmic Transparency Record(s) for (a) the Core Person Record service and (b) the Probation in Court system, in full or with only those redactions strictly necessary under the Act (please itemise any exemption applied, with the public-interest balancing where engaged).**
- 2. Model configuration. The Splink settings/configuration for these systems (JSON settings dictionaries and/or Python model scripts), specifically including: the blocking rules used to partition records; and the comparison definitions / comparison vectors, i.e. the comparison levels and string-similarity thresholds (e.g. Levenshtein, Jaro–Winkler, or Jaccard cut-offs) applied to forename, surname, date of birth, and address fields.**
- 3. Decision threshold. The match-weight (log2 Bayes factor) threshold, or equivalent posterior match-probability cut-off, at or above which two records are treated as a definitive link within operational court/probation workflows; and any separate "clerical review" band between auto-accept and auto-reject thresholds.**
- 4. Error performance. The target and observed false-positive and false-negative (false-match and missed-match) rates accepted for these operational**

systems; and the methodology for estimating the m and u probabilities for each matching parameter (including use of the Expectation–Maximization algorithm and any labelled/clerical ground-truth set used to validate accuracy).
5. Human review & redress. Recorded information on whether, and at what point, a human reviews a candidate match before it takes operational effect (including before each PNC share in the probation → police pilot); and the process by which an individual affected by an erroneous link can have it corrected.

Your request is being handled under the FOIA.

We can confirm that the MoJ holds the information that you have requested.

Our response to each part of your request is set out below.

1. Governance documents

There are no separate internal Algorithmic Transparency Records for the Core Person Record (CPR) service or the Probation in Court service. The relevant Algorithmic Transparency Record is the published MoJ: Splink Master Record, which is exempt from disclosure under section 21 of the FOIA, because it is reasonably accessible to you. The information can be accessed via publicly available sources, which can be accessed at:

<https://www.gov.uk/algorithmic-transparency-records/moj-splink-master-record>

Data Protection Impact Assessment (DPIA)

The MoJ holds a Data Protection Impact Assessment (DPIA) relating to the Core Person Record service. However, this information is exempt from disclosure under section 31 of the FOIA.

Section 31(1)(a) is engaged because the DPIA contains detailed information about the operation, structure and security controls of MoJ systems, including information relating to data matching processes, system architecture and risk management measures. Disclosure of this information would be likely to prejudice the prevention or detection of crime and the effective operation and security of MoJ systems. Section 31 is a qualified exemption and therefore subject to the public interest test.

Public interest considerations favouring disclosure

Disclosure would promote transparency and accountability regarding the MoJ's use of data matching technologies.

Disclosure would improve public understanding of how personal data is processed within the Core Person Record service.

Disclosure would contribute to public scrutiny of the governance and management of digital services used across the justice system.

Public interest considerations favouring withholding the information

Disclosure would reveal detailed information about the operation, design and security controls of MoJ systems.

Releasing this information would increase the risk of vulnerabilities being identified and exploited, thereby undermining the security of justice systems and the information they hold.

There is a strong public interest in protecting the integrity, security and effective operation of systems used to support justice services and the management of sensitive information.

Having considered these factors, we have concluded that the public interest in maintaining the exemption outweighs the public interest in disclosure. Therefore, the information is withheld under section 31 of the FOIA.

In addition, some information within the DPIA constitutes the personal data of third parties and is exempt from disclosure under section 40(2) of the FOIA.

Section 40(2) and section 40(3A)a of the FOIA taken together mean that personal data can only be released if to do so would not contravene any of the principles set out in Article 5(1) of the UK General Data Protection Regulation (UK GDPR) and section 34(1) of the Data Protection Act 2018.

Article 5(1)(a) of the UK GDPR states that: “*Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*”. In the case of an FOIA request, the personal data is processed when it is disclosed in response to the request. This means that the information can only be disclosed if to do so would be lawful, fair and transparent. Disclosure of information under the FOIA is deemed to be to the wider world.

In order to be lawful, one of the lawful bases listed in Article 6(1) of the UK GDPR must apply to the processing. It must also be generally lawful. It is our view that the lawful basis most applicable is basis 6(1)(f) which states: “*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*”.

In considering the application of Article 6(1)(f) of the UK GDPR in the context of a request for information under the FOIA, it is necessary to consider the following three-part test:-

i. Legitimate Interest Test:

We recognise that there is a legitimate public interest in understanding how the MoJ processes personal data and manages privacy risks associated with the Core Person Record service. Disclosure may contribute to transparency and accountability in relation to the use of data matching technologies.

ii. Necessity Test:

We do not consider that disclosure via the FOIA is necessary to meet this legitimate interest. Information concerning the Core Person Record service, including governance arrangements and operational information, is already publicly available through the published Algorithmic Transparency Record and other publicly

accessible sources. Disclosure of the personal data itself would not materially further public understanding of the service.

There is no need to consider the balancing part of the three part test as it fails at the necessity stage.

We have concluded that releasing the requested information into the public domain would be unlawful in this instance; the personal information is therefore exempt from disclosure under section 40(2). Individuals have a clear and strong expectation that their personal data will be held in confidence and not disclosed to the public under the FOIA.

This is an absolute exemption and does not require a public interest test under the FOIA.

2. Model configuration

The model configuration for the Core Person Record service has been published as open source. This is exempt from disclosure under section 21 of the FOIA, because it is reasonably accessible to you. The information can be accessed via the following link

https://github.com/ministryofjustice/hmpps-person-match/tree/main/hmpps_cpr_splink/cpr_splink/model/model_files

3. Decision threshold

The operational matching thresholds are defined within the published source code. This is exempt from disclosure under section 21 of the FOIA, because it is reasonably accessible to you. The information can be accessed via the following link

https://github.com/ministryofjustice/hmpps-person-match/blob/main/hmpps_cpr_splink/cpr_splink/model/model.py

For context, we can also confirm that there is no separate clerical review threshold when records are initially matched. Records enter a clerical review queue only where they have previously been linked and subsequent updates to the source data reduce the match score below the matching threshold. This occurs when the revised score falls below the fracture threshold of 18, as defined in the published source code.

4. Error performance

The model configuration used during training is published. This is also exempt from disclosure under section 21 of the FOIA, because it is reasonably accessible to you. The information can be accessed via the following link

https://github.com/ministryofjustice/hmpps-person-match/tree/main/hmpps_cpr_splink/cpr_splink/model/model_files

5. Human review and redress

Information regarding human review and appeals is published within the Algorithmic Transparency Record. This is also exempt from disclosure under section 21 of the

FOIA, because it is reasonably accessible to you. The information can be accessed via the following link

<https://www.gov.uk/algorithmic-transparency-records/moj-splink-master-record#human-review>

In addition, we can confirm that:
there are no complaint procedures specific to Splink itself, as Splink does not directly make decisions about individuals.
where linkage errors are identified, manual overrides can be recorded within the system to prevent the same erroneous linkage from recurring;
services using links generated by the Core Person Record service are able to overwrite those decisions, which updates the match held within CPR; and
support staff are able to review existing links and amend them where appropriate.

Appeal Rights

If you are not satisfied with this response, you have the right to request an internal review by responding in writing to one of the addresses below within 40 working days of the date of this response.

data.access@justice.gov.uk

Disclosure Team, Ministry of Justice, 102 Petty France, London, SW1H 9AJ

You do have the right to ask the Information Commissioner's Office (ICO) to investigate any aspect of your complaint. However, please note that the ICO is likely to expect internal complaints procedures to have been exhausted before beginning their investigation.

Yours sincerely,

Justice Digital