Information Sharing Agreement

Between

National Police Chiefs' Council
ACRO Criminal Records Office

And

Secretary of State for Justice acting on behalf of Her Majesty's Prison and Probation Service (HMPPS)

Summary Sheet

Freedom of Information Act Publication Scheme	
Security Classification (GSC)	OFFICIAL
Publication Scheme Y/N	Yes
Title	A purpose specific Information Sharing Agreement between ACRO Criminal Records Office (ACRO), acting on behalf of UK police forces that are subject to the ACRO collaboration agreement, and Her Majesty's Prison and Probation Service (HMPPS).
Version	1.5
Summary	*Services* This Information Sharing Agreement (hereafter referred to as the Agreement) formalises the arrangements for the ACRO Criminal Records Office (ACRO), acting on behalf of UK police forces that are subject to the ACRO collaboration agreement, to provide Her Majesty's Prison and Probation Service (HMPPS) - Shared Services Connected Ltd (SSCL) with access to relevant information held on the Police National Computer (PNC), specifically convictions, cautions, reprimands and final warnings for a policing purpose, as part of a holistic suite of pre-appointment checks conducted on personnel by the external processor SSCL, and to assist internal investigations carried out by HMPPS.
Author	S.40(2) [redacted] Information Governance officer
Renewal Date	31/08/2022
Date Issued	31/08/2021
ISA Ref	ACRO/031
Location of Agreement	ACRO ISA Library
ACRO DPIA Reference	DPIA 034

Contents

Version Record

Version No.	Date	Amendments Made	Authorisation
1.0	*02/07/2019*	*Annual review: numerous amendments due to GDPR and Data Protection Act 2018*	AMdB, ACRO
1.1	08/09/2020	*Template amendments*	KN, ACRO
1.2	20/01/2021	*Post transition updates*	KN, ACRO
1.3	25/05/2021	*DPO Review*	KP, ACRO
1.4	12/08/2021	*HMPPS updates*	KN, ACRO
1.5	27/08/2021	*Volume and SLA confirmations*	KN, ACRO

1. Partners to the Agreement

1.1. ACRO Criminal Records Office
PO Box 481
Fareham
PO14 9FS

1.2. Her Majesty's Prison and Probation Service (HMPPS)
Ministry of Justice
Commercial and Contract Management
10 South Colonnade
Canary Wharf
London
E14 4PU

ICO Registration Number Z5679958

2. Agreed Terms

2.1. Interpretation

The following definitions and rules of interpretation apply in this Agreement.

2.1.1. Definitions:

ACRO: ACRO Criminal Records Office.

Agreed Purpose: has the meaning given to it in clause 3.2 of this Agreement.

Business Day: a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.

Business Hours: 9:00 am to 5:00 pm Monday to Friday on a day, that is not a public holiday.

CEO: Chief Executive Officer.

Criminal Offence Data is personal data relating to criminal convictions and offences or related security measures and includes personal data relating to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing. (DPA 2018 S11 (2)).

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

CPS: The Crown Prosecution Service.

Data Protection Legislation: the General Data Protection Regulation as enacted into English law (**UK GDPR**) as revised and superseded from time to time; the Data Protection Act 2018 **(DPA)**; and any other laws and regulations relating to the processing of personal data and privacy which apply to a party and, if applicable, the guidance and codes of practice issued by the relevant data protection or supervisory authority.

DBS: The Disclosure and Barring Service (an executive non-departmental public body, sponsored by the Home Office) helps employers make safer recruitment decisions each year by processing and issuing DBS checks for England and Wales.

DPA: Data Protection Act 2018.

DVLA: Driver and Vehicle Licensing Agency.

EIR: Environmental Information Regulations 2004.

FOIA: Freedom of Information Act 2000. Freedom of Information (FOI).

GSCP: Government Security Classification Policy.

HMPPS: Her Majesty's Prison and Probation Service.

MoJ: Ministry of Justice.

NPA: Non Police Agency.

NPCC: National Police Chiefs' Council.

NPPA: Non Police Prosecuting Agency.

Offences: a breach of a law or rule; an illegal act.

Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (UK GDPR 2018 Article 4).

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.

PNC: Police National Computer.

s22a Agreement: An agreement is made pursuant to section 22A Police Act 1996 (as amended) which enables police forces, local policing bodies as defined in that Act and other parties as defined in that Act to make an agreement about the discharge of functions by officers and staff, where it is in the interests of the efficiency or effectiveness of their own and other police force areas. By entering into this Agreement, the Parties have taken account of the statutory guidance for police collaboration published by the Home Office in October 2012 in exercise of the Home Secretary's power under s23F Police Act 1996, to provide guidance about collaboration agreements and related matters.

SIRO: Senior Information Risk Owner.

Shared Personal Data: the personal data to be shared between the parties under clause 5.1.2 and 5.2.2 of this Agreement.

Special Categories of Personal Data is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited (UK GDPR 2018 Article 9).

SPOC: Single Points of Contact.

SSCL: Shared Services Connected Limited, MoJ's outsourced business processing supplier and data processor.

Subject Information Rights: means the exercise by a data subject of his or her rights under Articles 13-22 of the UK GDPR.

Supervisory Authority: the Information Commissioner or country equivalent.

2.1.2. **Controller**, **Processor**, **Data Subject** and **Personal Data**, **Special Categories of Personal Data**, **Processing** and "appropriate technical and organisational measures" shall have the meanings given to them in the Data Protection Legislation.

2.1.3. Clause and paragraph headings shall not affect the interpretation of this Agreement.

2.1.4. Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.

2.1.5. A reference to a statue or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.

2.1.6. Any words following the terms **including**, **include**, **in particular** or **for example** or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.

2.1.7. A reference to **writing** or **written** includes email.

2.1.8. Unless the context otherwise requires the reference to one **gender** shall include a reference to the other genders.

3. Purpose and Background of the Agreement

3.1. Background

3.1.1. ACRO is a national police unit under the NPCC working for safer communities. ACRO is the national police unit responsible for exchanging criminal conviction information between the UK and other countries. ACRO provides access to information held on the PNC to support the criminal justice work of some non-police prosecuting agencies; and assist safeguarding processes conducted by relevant agencies.

3.1.2. HMPPS carry out sentences given by the courts, in custody and the community, and rehabilitate those in its care through education and employment. As such, HMPPS falls under the Exceptions Order and is exempt from the Rehabilitation of Offenders Act 1974 (as amended), and can therefore check all those applying to work for the organisation for all spent and unspent convictions, to consider and manage any risks which may come to light through this.

3.1.3. HMPPS will investigate all internal cases of suspected fraud initially, and criminal offences committed whilst in custody will be followed up by HMPPS with relevant police colleagues and the CPS under the existing crime in prison protocol between HMPPS, NPCC and CPS. HMPPS does not prosecute directly, but separately carries out sentences given by the courts, in custody and the community, and rehabilitates people in its care through education and employment.

3.2. Purpose

3.2.1. This Agreement sets out the framework for the sharing of Personal Data when one Controller discloses Personal Data to another Controller. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other.

3.2.2. The purpose of this Agreement is to formalise the arrangements for the ACRO Criminal Records Office (ACRO), acting on behalf of UK police forces that are subject to the ACRO collaboration agreement, to provide HMPPS with access to relevant information held on the PNC, specifically convictions, adult cautions, youth cautions, reprimands and final warnings for a policing purpose as part of a holistic suite of pre-appointment checks conducted on personnel, to address urgent deployment of operational personnel and to assist internal investigations carried out by HMPPS.

3.2.3. Due to operational demands, HMPPS use ACRO to supplement DBS checks where it would compromise operational safety and stability in prisons not to do so. The original service level agreement was drawn up with the help of the Secretary of State for the Home Department to enable HMPPS access to PNC data swiftly. This has contributed to reducing the risk to the organisation and all those we are responsible for, including staff, prisoners and visitors, it is considered business critical to the management of prisons and probation operations. Even with this provision we are still at business critical levels of appointment to some prisons and probation settings.

3.2.4. ACRO will provide the necessary prints from the PNC to HMPPS via their current appointed data processor SSCL to support relevant processes of the DBS. Other data processors may be appointed from time to time who must comply with the requirements set out in this agreement.

3.2.5. This Agreement will be used to assist in ensuring that:

a) Personal Data is shared in a secure, confidential manner with designated points of contact;

b) Personal Data is shared only on a 'need to know' basis;

c) Shared Personal Data will not be irrelevant or excessive with regards to the Agreed Purpose;

d) There are clear procedures to be followed with regard to Shared Personal Data;

e) Personal Data will only be used for the reason(s) it has been obtained;

f) Data quality is maintained and errors are rectified without undue delay;

g) Lawful and necessary reuse of Personal Data is done in accordance with Data Protection Legislation, and

h) Subject information rights are observed without undue prejudice to the lawful purpose of either party.

4. Powers

4.1. HMPPS Legal Basis

4.1.1. For the purposes of this part, "the law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal penalties, including the safeguarding against the threat to public safety.

4.1.2. HMPPS falls under the Exceptions Order and is exempt from the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (as amended), Sch 1, Part II, s. 3, 7 & 9. It is a competent authority under schedule 7(42-43) of the DPA 2018 for the purposes of law enforcement processing to the extent of these powers.

4.1.3. HMPPS carries out an investigatory function but liaises with the police to bring about a prosecution using the following statutory powers:

- Prison Rules, Crime in prison, Prison Act 1952
- Crime and Disorder Act (Sec. 115)
- Common Law
- The Offender Management Act 2007
- Misuse of Drugs Act 1971
- Psychoactive Substances Act 2016
- Staff corruption/dishonesty acts

4.1.4. Processing of personal data for any of the law enforcement purposes is lawful in that the processing is necessary for the performance of a task.

4.1.5. HMPPS is permitted to process Special Category Personal Data for preventing or detecting unlawful acts when strictly necessary to meet the purpose and when the processing conditions of schedule 8 of the DPA 2018 are met. The condition(s) used for this agreement are:

- A function conferred by under any rule of law, necessary in the substantial public interest
- Safeguarding of children and of individuals at risk
- Anti-fraud organisations

4.2. ACRO Legal Basis

4.2.1. Section 22a of the Police Act 1996 enables police forces to discharge functions of officers and staff where it is in the interests of efficiency or effectiveness of their own and other police force areas. Schedule 7 paragraph 17 of the DPA 2018 establishes bodies created under section 22a of the Police Act 1996 as competent authorities.

4.2.2. ACRO is established through the National Police Collaboration Agreement relating to the ACRO Criminal Records Office (ACRO) under section 22a of the Police Act 1996. This agreement gives ACRO the authority to act on behalf of the chief constables to provide PNC enquiry, update and disclosure services to non-police agencies and non-police prosecuting agencies.

4.2.3. ACRO is a competent authority, by virtue of the s22a agreement, processing data for a law enforcement purpose.

4.2.4. Under the first data protection principle, processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law. Under section 35 (2) of the DPA 2018 the following applies;
The processing is necessary for the performance of a task.

4.2.5. Under section 35(3-5) and schedule 8 of the DPA, ACRO meets the conditions for sensitive processing as follows;
- Administration of Justice

4.3. Code of Practice for the Management of Police Information

4.3.1. This agreement outlines the need for the police and partners to work together to share information in line with the Policing Purpose as set out in the Management of Police Information Code of Practice. In line with section 39A of the Police Act 1996, Chief Officers are required to give "due regard" to this statutory code. The Policing Purposes summarise the statutory and common law duties of the police service for which personal data may be processed and are described as:
- Protecting life and property;
- Preserving order;
- Preventing the commission of offences;
- Bringing offenders to justice;
- Any duty or responsibility of the police arising from common or statute law.

4.4. Human Rights Act 1998

4.4.1. Under Article 8 of the Human Rights Act 1998, all data subjects have a right to a respect for their private and family life, home and correspondence.

4.4.2. Interference with this right may be justified where lawful and necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Lawful intrusion by the police service requires proportionate use of personal data for any of the policing purposes.

4.5. Common Law Duty of Confidentiality

This Agreement takes into account the common law duty of confidentiality which applies where information has a necessary quality of confidence or where information is imparted in circumstances giving rise to an obligation of confidence that is either explicit or implied. Where the duty applies, disclosure will be justified only by:
- consent
- a legal duty
- a public interest through consent, legal duty and the public interest or for the safeguarding of one or more people.

5. Process

5.1. Overview

5.1.1. ACRO, in response to requests made by HMPPS, or their appointed data processor SSCL, will conduct PNC searches and provide a PNC print to meet the identified information needs of HMPPS.

The PNC data will comprise of:

A Disclosure PNC print. The personal data disclosed under this print includes (if available): name, date of birth, birth place, sex, address, occupation, aliases (including DVLA name) and alias date of births. The home address that is printed in the ID part of the print is decided by the following rules:

- If there is more than one home address on the record, the most recent address is used,
- If there is no home address present, the most recent 'no fixed abode' address type will be used,
- If neither of the above address types are present, the most recent 'Other' address is printed.

5.1.2. In the event that no convictions are found on the PNC or the subject of the enquiry is 'No Trace', a response stating 'no relevant information held on PNC in relation to the subject of your enquiry' will be sent to HMPPS. This response will also indicate that in the absence of fingerprints the identity of the subject cannot be verified. Similar wording will apply to 'Trace' returns i.e. when a record is found and a PNC print provided.

5.1.3. HMPPS caseworker will review all referred information and may ask for additional information to aid decision making.

5.2. PNC Searches

5.2.1. Requests for a PNC search are to be made by HMPPS on a 'Names Enquiry' form which will be supplied by ACRO separately.

The following personal data is to be provided in support of each request:

- First name
- Any middle names
- Surname / family name
- Date of birth (dd/mm/yyyy)
- Any alias details (names, DoB)
- Place of birth (where known)
- Address
- HMPPS case reference

5.3. Additional Information Requirements

5.3.1. Other personal data which the SSCL caseworker may be aware of e.g. National Insurance Number, passport or driving licence number etc. can be provided to aid identification. This additional information will be used to confirm identity and is of particular value where the name or other personal details are identical on the PNC.

5.3.2. It is not necessary to obtain the additional information as a matter of course particularly if it is not currently recorded as part of the HMPPS normal administrative procedures.

5.3.3. If required, ACRO will seek additional information from SSCL to verify the identity of the subject of the request via the following secure HMPPS mailbox:
S.31(1)

5.3.4. No other mailbox is to be used unless this Agreement is updated to reflect a change of 'nominated' point of contact for HMPPS.

5.3.5. Where appropriate, SSCL will make contact with the subject of the enquiry to seek the additional information required by ACRO.

5.4 Contingency Backup

5.4.1 In an event where HMPPS require ACRO to provide a contingency service for PNC requirements, discussion must be had, prior to any checks, in order to establish volumes and expected turnaround times. This is necessary in order to ensure ACRO can provide the required service and cope with the demand.

6. Submission

6.1. Names Enquiry Forms

6.1.1. Completed 'Names Enquiry' forms are to be sent via secure email to the following email address:
S.31(1) [redacted]

6.1.2. As part of the submission process, in order that the information provided by ACRO is as accurate as possible, SSCL are advised to provide the role each subject will be undertaking and, where possible, the location (prison and/or county) the subject will be deployed in. This will not affect the result from PNC but may impact on the provision of any intelligence provided by the controlling force.

6.1.3. Erroneous/incomplete 'Names Enquiry' forms will not be processed. They will be returned to the HMPPS as invalid and a reason provided.

6.2. Telephone Requests

6.2.1. Requests may be made by telephone in cases of emergency and 'Names Enquiry' form submitted retrospectively. Such requests can only be made by a limited number of the SSCL staff.
SSCL STAFF (ON BEHALF OF HMPPS) - S.40(2) [redacted] *and* S.40(2) [redacted]

7. Provision of Information

7.1. Response to a PNC 'Names' Search

7.1.1. In response to a formal application, written or verbal, ACRO will provide a disclosure print to HMPPS with the following information derived from the PNC in response to applications made in accordance with this Agreement:

- All convictions, cautions, warnings and reprimands.
- Additional information as deemed relevant by ACRO where there is a pressing social need to do so (via a Force Disclosure Unit as appropriate).

7.1.2. It should be noted that the service provided under this Agreement only covers the provision of certain PNC prints depending on the request submitted by HMPPS. A disclosure print will be supplied by ACRO separately.

7.1.3. If HMPPS has a secondary query or wish to follow-up on the PNC information provided, a formal request is to be made through the nominated ACRO mailbox:
S.31(1) [redacted]

7.1.4. HMPPS will need to liaise directly with forces to explain specific information regarding the offending revealed in the prints provided under this Agreement or to gain access to statements, interviews under caution etc. relating to any previous offending. Forces may apply their own charges in respect of any information they disclose.

8. Information Security

8.1. Government Security Classification Policy

8.1.1. Parties to this Agreement are to ensure that personal data is handled, stored and processed at OFFICIAL level as defined by the Government Security Classification Policy (GSCP) and may carry the security marking OFFICAL – SENSITIVE, in which case specific handling conditions will be provided.

Documents marked using GSCP will describe specific handling conditions to mitigate the risks necessitating such marking. These may include:

- Any specific limitations on dissemination, circulation or intended audience
- Any exception to consult should reuse be anticipated
- Additional secure handling and disposal requirements

8.2. Security Standards

8.2.1. It is expected that partners of this agreement will have in place baseline security measures compliant with or be equivalent to ISO/IEC 27001:2013 and HMG standards in relation to information security. Partners are at liberty to request copies of each other's:

- Information Security Policy
- Records Management Policy
- Data Protection Policy

8.2.2. Each partner will implement and maintain appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss or destruction of, or damage.

8.2.3. Each partner will ensure that employees or agents who have access to personal data have undergone appropriate Data Protection training to be competent to comply with the terms of this agreement.

8.3. Volumes

8.3.1. Is it estimated that for the year 2021/22, HMPPS will request c35,000 PNC checks.

8.3.2. HMPPS will advise ACRO if the number of PNC checks is likely to be exceeded.

8.3.3. ACRO will audit requests against the lawful basis and these volumes to ensure that personal data is not being disclosed contrary to the lawful basis and that the agreement is fit to meet any increase in lawful demand.

8.4. Transmission

8.4.1. With the exception of telephone requests in cases of emergency, contact between ACRO and HMPPS via their approved data processor SSCL should only be made over a secure communication network and care must be taken where personal information is shared or discussed.

8.4.2. Emails must not be password protected, contain personal data or contain the descriptor 'Private and Confidential' in subject field, or be over 6MB in file size.

8.4.3. HMPPS reference number must be included in the subject field of every email sent to ACRO.

8.4.4. Where email transmission is unavailable, records may be transferred by post via encrypted disk, where encryption meets current industry standards.

8.5. Retention and disposal

8.5.1. Information shared under this Agreement will be securely stored and disposed by secure means when no longer required for the purpose for which it is provided as per each parties Information Security Policy, unless otherwise agreed in a specific case, and legally permitted. Each party will determine and maintain their own retention schedule.

9. Information Management

9.1. Accuracy of Personal Data

9.1.1. The parties will take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is erased or rectified without delay and will notify the partners to this agreement of the erasure or rectification.

9.1.2. Where a partner rectifies personal data, it must notify any competent authority from which the inaccurate personal data originated, and should notify any other data of the correction, unless a compelling reason for not doing so exists.

9.1.3. It is the responsibility of all parties to ensure that the information is of sufficient quality for its intended purpose, bearing in mind accuracy, validity, reliability, timeliness, relevance and completeness.

9.2. Accuracy Disputes

9.2.1. Should the validity of the information disclosed be disputed by HMPPS or a third party, HMPPS will contact ACRO to determine a suitable method to resolve the dispute.

9.3. Turnaround

9.3.1. This Agreement requires a 4 business day turnaround on all cases submitted to ACRO, except where ACRO requires further information from HMPPS to make a positive match. In these circumstances, ACRO will process the enquiry when the required information has been supplied by HMPPS via SSCL as the data processor.

9.3.2. Turnaround times do not include the day a request is received or the day a response is returned to HMPPS.

9.3.3. Responses to requests for additional information must be made by HMPPS within 10 working days. If ACRO do not receive the information, the request will be closed.

9.3.4. Information will be exchanged without undue delay. In the event of a delay outside of either parties' control, this will be informed to the other party as soon as practical.

9.3.5. An exception to the 4 business day turnaround are those occasions where the conviction data is held on microfiche in the national police microfiche library at Hendon. In these cases, ACRO will provide a response when the required information has been supplied by the custodians of the microfiche.

9.3.6. In some circumstances HMPPS may require information urgently, for example, due to ongoing court proceedings. In these circumstances ACRO will endeavour to complete the check more quickly as agreed with HMPPS. Such requests will be treated as an exception, and will considered on a case by case basis.

9.3.7. In this Agreement, "4 day turnaround" means 4 business days and in this regard it should be noted that normal business for ACRO hours are 9:00am to 5:00pm Monday to Friday on

a day, that is not a public holiday. An 'Out of hours' service is not covered by this agreement.

9.4. Quality Assurance and Control

9.4.1. ACRO employ strict quality control procedures and staff undertaking this work are all appropriately trained.

9.4.2. On a monthly basis ACRO will provide regular management information to HMPPS to include the:

- Number of PNC 'Names Enquiry' forms received
- Number of PNC Disclosure Prints provided
- Details of any cases that fall outside agreed 'Service Levels'
- Number of issues and/or disputes

10. Complaints and Breaches

10.1. Complaints

10.1.1. Complaints from data subjects, or their representatives, regarding information held by any of the parties to this agreement will be investigated first by the organisation receiving the complaint. Each data controller will consult with other parties where appropriate.

10.2. Breaches

10.2.1. Each party shall comply with its obligation to report a Personal Data Breach to the appropriate Supervisory Authority and (where applicable) data subjects under Articles 33 and 34 of the UK GDPR and shall inform the other party of any Personal Data Breach irrespective of whether there is any requirement to notify any Supervisory Authority or data subject(s).

10.2.2. The parties agree to provide reasonable assistance as is necessary to each other to facilitate handling of any Personal Data Breach in any expeditious and compliant manner.

10.2.3. In the event of a dispute or claim brought by a data subject or the Supervisory Authority concerning the processing of Shared Personal Data against either or both parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

10.2.4. The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the Supervisory Authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

10.2.5. All security incidents and breaches involving police data shared under this agreement must be reported immediately to the SPOCs designated in this agreement.

11. Information Rights

11.1. Freedom of Information Act 2000

11.1.1. Where a party to this agreement is subject to the requirements of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) all parties shall assist and co-operate with the other to enable the other party to comply with its obligations under FOIA and the EIR. This is in line with the requirements laid out in the Lord Chancellor's Code of Practice issued under section 45 of FOIA.

11.1.2. Where a party receives a request for information in relation to the information which it received from another party, it shall (and shall procure that its sub-contractors shall):

- Contact the other party within two working days after receipt and in any event within two working days receiving a Request for Information;
- The originating authority will provide all necessary assistance as reasonably requested by the party to enable the other party to respond to a request for Information within the time for compliance set out in Section 10 of the FOIA or Regulation 5 of the EIR.

11.1.3. On receipt of a request made under the provisions of the Freedom of Information Act 2000 in respect of information provided by or relating to the information provided by ACRO, the HMPPS representatives is to ascertain whether the NPCC wishes to propose the engagement of any exemptions via the NPCC FOI mailbox: npcc.foi.request@cru.pnn.police.uk

11.1.4. The decision as to whether to disclose the information remains with HMPPS, but will be made with reference to any proposals made by the NPCC.

11.2. Data Subject Information Rights

11.2.1. For the purpose of either party handling information rights under Chapter III of both the DPA 2018 and UK GDPR, it is necessary to ensure neither party causes prejudice to the unlawful activity of the other by releasing personal data disclosed by one party to the other, or indication by the method or content of their response that such data exists. The parties agree that consultation between the parties is necessary to identify relevant prejudice and ensure it is both substantial and proportionate to the exemption which is to be applied.

11.2.2. A relevant request requiring consultation includes those requests exercised under the rights to access, erasure, rectification, restriction or objection which requires consideration of data provide to one party by the other.

11.2.3. Consultation will occur without undue delay and no later than 72 hours after identification of the relevant request.

11.2.4. Where HMPPS receives a relevant request, the HMPPS via their designated data processor SSCL representative is to contact the ACRO Data Protection Officer at: dataprotectionofficer@acro.pnn.police.uk to ascertain whether ACRO wishes to propose to HMPPS that they apply any relevant exemptions when responding to the applicant.

11.2.5. Where ACRO receives a relevant request, the NPCC Data Protection Officer is to contact SSCL who will notify HMPPS representatives to ascertain whether HMPPS wishes to propose to ACRO that they apply any relevant exemptions prior to responding to the applicant.

11.2.6. Both parties will otherwise handle such requests in accordance with the DPA 2018 and UK GDPR.

11.3. Fair processing and privacy notices

11.3.1. Each partner will take all reasonable steps to comply with the obligation to notify the data subject of the processing activity, unless an exemption applies.

11.3.2. ACRO will maintain a general notice, describing the mandatory privacy information at Articles 13 and 14 of UK GDPR and s44(1) and (2) DPA 2018. ACRO will not contact the data subjects directly with this privacy information on the basis that HMPPS has already taken steps to inform the individual, or has exercised an appropriate exemption to article 13 or 14, or exercised an exemption at s44(4) DPA 2018.

11.3.3. HMPPS will take all reasonable steps to inform the data subject that checks will be conducted through ACRO, except where doing so would prejudice the purpose of the check in a way which would allow use of an exemption to this obligation. Where HMPPS does not provide this information to the data subject, ACRO agrees to rely upon the correct use of an exemption by HMPPS and will not contact the data subject to avoid the same prejudice.

12. Reuse of Personal Data Disclosed under this Agreement

12.1. Personal data shall be collected for the specified, explicit and legitimate purposes stated in this document and cannot be further processed in a manner that is incompatible with those purposes without the written consent of the party that provided the information in the first instance, unless required to by law.

13. Roles and Responsibilities

13.1. Disputes

ACRO and HMPPS will designate Single Points of Contact (SPOC) who will work together to jointly solve problems relating to the sharing of information under this Agreement and act as point of contact in the event of a suspected breach by either party.

- ACRO (UK PNC enquiries and updates):
  ACRO Head of Section: S.40(2) and S.40(2)
  S.31(1)

- HMPPS:
  HMPPS Security Vetting Policy Lead: S.40(2)
  S.31(1)

13.1.1. Initial contact should be made by email with the subject heading:
FAO ACRO/HMPPS ISA SPOC Ref no: XXXX

13.1.2. The above designated SPOCs will have joint responsibility of resolving all day to day operating issues and initiating the escalation process set out if/when necessary.

13.2. Escalation

In the event that the nominated SPOC cannot agree on a course of action or either party appears not to have met the terms and conditions of this Agreement, the matter should initially be referred jointly to the following:

- ACRO (UK PNC enquiries and updates):
  ACRO National Services Deputy Manager: S.40(2)
  S.31(1)
  S.31(1)
- ACRO (Information Sharing Agreement):
  ACRO Information Management
  S.31(1)
  S.31(1)

- HMPPS:
  HMPPS Head of Personnel Security Countermeasures: S.40(2)
  S.31(1)

13.2.1. Both ACRO, HMPPS and SSCL SPOCs have a responsibility to create a file in which relevant information and decisions can be recorded. The file should include details of the data accessed and notes of any correspondence, meeting attended, or phone calls made or received relating to this Agreement.

14. Charges

14.1. Price and Rates

14.1.1. The HMPPS shall pay ACRO for the provision of services set out in this Agreement and in line with the "Letter of Charges" provided to HMPPS separately and are reviewed annually.

14.1. Invoices

Invoices shall contain the following information:

- Purchase Order Number
- The Agreement Reference Number
- The period the service charge refers to
- All applicable service charges
- The name and address of both Parties (ACRO and HMPPS)

14.1.1. The Purchase Order Number is to be provided by HMPPS for the appropriate financial year to ensure payment of invoices can be made. If a Purchase Order Number is not in hand prior to receiving enquiries ACRO reserves the right to suspend the processing of services covered under this Agreement until one has been provided.

14.1.2. HMPPS shall pay all monies owed to ACRO within a period of 30 days from receipt of the original invoice unless the amount shown on the invoice is disputed by HMPPS.

14.1.3. If HMPPS is in default of this condition, ACRO reserves the right to withdraw the service by advising in writing.

15. Review

15.1. Frequency

15.1.1. This ISA will be reviewed annually.

15.1.2. This Agreement makes up to 2021/22 annual renewal.

16. Warranties and Limitations

16.1. Warranties

16.1.1 Each party warrants and undertakes that it will:

- Process the Shared Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments that apply to its personal data processing operations;
- In particular, use all reasonable efforts to ensure the accuracy of any Personal Data shared;
- Publish or otherwise make available on request a copy of this, unless the Clause contains confidentiality information;
- Respond within a reasonable time and as far as reasonably possible to enquiries from the relevant Supervisory Authority in relation to the Shared Personal Data;
- Respond to Subject Access Requests in accordance with the Data Protection Legislation;
- Where applicable, pay their own appropriate fees with all relevant Supervisory Authorities to process all Shared Personal Data for the Agreed Purpose; and
- Take all appropriate steps to ensure compliance with the security measures set out in Clause 8.2.2 above.

16.2. Limitation of liability

16.2.1 Neither party excludes or limits liability to the other party for:

- Fraud or fraudulent misrepresentation;
- Death or personal injury caused by negligence;
- A breach of any obligations implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982; or
- Any matter for which it would be unlawful for the parties to exclude liability.

16.2.2 Subject to clause 16.2.1,neither party shall in any circumstances be liable whether in contract, tort (including for negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, for:

a) Any loss (whether direct or indirect) of profits, business, business opportunities, revenue, turnover, reputation or goodwill;

b) Loss (whether direct or indirect) of anticipated savings or wasted expenditure (including management time); or

c) Any loss or liability (whether direct or indirect) under or in relation to any contract.

16.2.3 Clause 16.2.2 shall not prevent claims, for:

- Direct financial loss that are not excluded under any of the categories set out in clause 16.2.2(a);or
- Tangible property or physical damage.

17. Variation

17.1. No variation of this Agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

18. Waiver

18.1. No failure or delay by a party to exercise any right or remedy provided under this Agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

19. Severance

19.1. If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this Agreement.

19.2. If any provision or part-provision of this Agreement is deemed deleted under clause 16.1, the parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

20. Changes to the applicable law

20.1. If during the Term the Data Protection Legislation change in a way that the Agreement is no longer adequate for the purpose of governing lawful data sharing exercises, the Parties agree that the SPOCs will negotiate in good faith to review the Agreement in the light of the new legislation.

21. No partnership or agency

21.1. Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party. Each party confirms it is acting on its own behalf and not for the benefit of any other person.

22. Rights and remedies

22.1. The rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

23. Notice

23.1 Any notice given to a party under or in connection with this Agreement shall be in writing, addressed to the SPOC and shall be:

- Delivered by hand or by pre-paid first-class post or other next working day delivery service at its principal place of business; or
- Sent by email to the SPOC.

23.2 Any notice shall be deemed to have been received:

- If delivered by hand, on signature of a delivery receipt; and
- If sent by pre-paid first-class post or other next working day delivery service, at 9.00 am on the second business day after posting or at the time recorded by the delivery service; and
- If sent by fax or email, at the time of transmission, or if this time falls outside business hours in the place of receipt, when business hours resume.

23.2.1 In this clause, 24 business hours means 9:00 am to 5:00 pm Monday to Friday on a day that is not a public holiday in the place of receipt, and 'business day' shall be construed accordingly.

23.3 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

24 Governing law and Jurisdiction

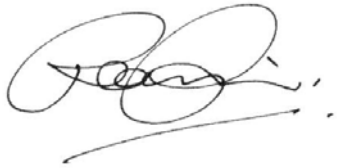
24.2 This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales, and subject to the jurisdiction of the courts of England and Wales.

25 Signature

25.2 Undertaking

25.2.1 By signing this Agreement, all signatories accept responsibility for its execution and agree to ensure that staff for whom they are responsible are trained so that requests for information and the process of sharing is sufficient to meet the purpose of this Agreement.

25.2.2 Signatories must ensure compliance will all relevant legislation.

Signed on behalf of ACRO	Signed on behalf of Secretary of State for Justice
Signature: 	Signature: Luis Moedinger Luis Moedinger (Sep 23, 2021 10:02 GMT+1)
Full Name: Rob Price	Full Name: Luis Moedinger
Position Held: CEO ACRO	Position Held: Commercial Deputy Director
Date: 16th September 2021	Date: Sep 23, 2021

ACRO-HMPPS SSCL ISA 2021-22 (17.9) (1) (004)

Final Audit Report 2021-09-23

Created:	2021-09-21
By:	S.40(2) [redacted]
Status:	Signed
Transaction ID:	CBJCHBCAABAAbg8NI3aUWk00xr4Yx3FXcPPgms8-Tzui

"ACRO-HMPPS SSCL ISA 2021-22 (17.9) (1) (004)" History

Document created by S.40(2) [redacted]
2021-09-21 - 10:44:54 AM GMT-S.31(1) [redacted]

Document emailed to Luis Moedinger S.31(1) [redacted] for signature
2021-09-21 - 10:45:36 AM GMT

Email viewed by Luis Moedinger S.31(1) [redacted]
2021-09-23 - 9:01:53 AM GMT-S.31(1) [redacted]

Document e-signed by Luis Moedinger S.31(1) [redacted]
Signature Date: 2021-09-23 - 9:02:56 AM GMT - S.31(1) [redacted]

Agreement completed.
2021-09-23 - 9:02:56 AM GMT