

# **DATA PROCESSING CONTRACT**

THIS CONTRACT is made on the     day of

BETWEEN

## **1.0 The Parties**

**CHIEF CONSTABLE OF BRITISH TRANSPORT POLICE** (herein after called the "Controller") whose main address is 25 Camden Road, London, NW1 9LN of the one part; and

**ACRO CRIMINAL RECORDS OFFICE ("ACRO")** (herein after called the "Processor"), whose address is ACRO Criminal Records Office, PO Box 481, Fareham PO14 9FS.

## **BACKGROUND**

- (a) In response to the Coronavirus pandemic, the Coronavirus Legislation (as hereinafter defined) (including the Coronavirus Act 2020) entered into force in a bid to control the outbreak of the virus. The Coronavirus Legislation inter alia created new enforceable offences. Certain offences are discharged by the payment of a FPN and, non-payment of an FPN can lead to prosecution;
- (b) The Chief Executive Officer of ACRO (hosted by the Chief Constable of Hampshire Constabulary) is designated by the Secretary of State for Health and Social Care and the First Minister for Wales respectively, as a "designated officer" (who may be specified in a Fixed Penalty Notice pursuant to the relevant Coronavirus Legislation as the authority to whom payment of the relevant fixed penalty may be made, and who may sign a certificate stating that payment of the fixed penalty was, or was not, received by the date specified in the relevant certificate) and to assist police forces in processing and proceedings in relation to FPNs issued by police forces to the public, for contravening offences under the Coronavirus Legislation as required (including without limitation collecting fines resulting from a FPN and make onward payment to the relevant Local Authority);
- (c) The Controller is a 'Competent Authority' under Paragraph 10 of Schedule 7 of the DPA 2018. The Processor is a 'Competent Authority' under Paragraph 17 of Schedule 7 of the DPA 2018. Pursuant to section 35 of the DPA 2018 processing by the Controller and ACRO under this Contract is necessary for the performance of a task carried out for that purpose by a Competent Authority, and the processing is necessary for the law enforcement purpose and the following conditions (inter alia (sections 35(3-5) and Schedule 8 (conditions for sensitive processing) of the DPA 2018) ) apply: a function conferred by under any rule of law necessary in the substantial public interest; administration of justice; safeguarding of children and of individuals at risk; public health processing is necessary for reasons of public interest in the area of public health; archiving for purposes of public interest, research and statistical purposes; and or vital interests) or as otherwise stipulated by the Parties from time to time.] Pursuant to section 31 of the DPA 2018 (as hereinafter defined) "the law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, including the safeguarding against threats to public safety;
- (d) Under the Coronavirus Legislation, there exists a number of organisations that may issue FPNs and act as enforcement officers. Therefore, it is necessary for such

organisations to share certain Law Enforcement Data (as hereinafter defined) in order that it, the Controller and or ACRO (as appropriate), are capturing those who have contravened the relevant Coronavirus Legislation on more than one occasion under the 'penalty laddering'. The conditions for processing referred to in Recital (e) shall apply as appropriate or as otherwise agreed between the Parties;

- (e) In order to reduce the burden on the Controller, ACRO undertook to process FPN's on the Controller's behalf. ACRO and BTP have agreed that ACRO shall process Law Enforcement Data (as hereinafter defined) on behalf of BTP in relation to the enforcement of FPNs relating to the Coronavirus Legislation in England and Wales in accordance with, and pursuant to, the terms and conditions of this Contract.

## **2.0 Purpose**

- 2.1 The purpose of the processing together with the subject matter, duration and nature of the processing and the types of Personal Data and categories of Data Subjects types in respect of which the Processor may process the Personal Data is described within Schedule A.
- 2.2 In consideration of the various rights and obligations of the Parties, this Contract sets out the terms and conditions under which Law Enforcement Data held by the Controller will be disclosed to and used by the Processor.
- 2.3 The Purpose is consistent with the original purpose of the relevant Personal Data creation and/or collection. The Processor shall not Process Law Enforcement Data in a way that is incompatible with the Purpose.

The Processing of Law Enforcement Data for the Purpose will assist the Controller to fulfil its obligations as described in Schedule A. Both Parties will comply with all applicable requirements of the Data Protection Legislation, and the provisions of this Contract are in addition to, and does not relieve, remove or replace, a Party's obligations or rights under the Data Protection Legislation.

- 2.4 Controllership of the Law Enforcement Data shall at all times remain with the Controller.
- 2.5 The Processor will only process the Personal Data to the extent, and in such a manner, as is necessary for the Purpose in accordance with the Controller's written instructions. The Processor will not process the Personal Data for any other purpose or in a way that does not comply with this Contract or the Data Protection Legislation, unless the Processor is otherwise required by relevant Law to otherwise Process the Law Enforcement Data. Where the Processor is relying on such Law as the basis for processing the Personal Data, the Processor shall promptly notify the Controller of this prior to performing the Processing required by such Law unless such Law prohibits the Processor from so notifying the Controller.
- 2.6 The Processor must comply promptly with any Controller written instructions from time to time requiring the Processor to amend, transfer, delete or otherwise process the Law Enforcement Data, or to stop, mitigate or remedy any unauthorised processing.
- 2.7 The Processor will maintain the confidentiality of the Law Enforcement Data and will not disclose the Law Enforcement Data to third-parties unless the Controller or this Contract specifically authorises the disclosure, or as required by domestic law, court or regulator.

If a domestic law, court or regulator requires the Processor to process or disclose the Law Enforcement Data to a third-party, the Processor must first inform the Controller of such legal or regulatory requirement and give the Controller an opportunity to object or challenge the requirement, unless the domestic law prohibits the giving of such notice.

- 2.8 The Parties acknowledge and agree that ACRO shall, in accordance with the terms and conditions of this Contract, outsource the printing and posting of FPN to Hampshire Print Services, this being a shared service between Hampshire Constabulary, the host force and Hampshire County Council.
- 2.9 The Processor will reasonably assist the Controller, at no cost to the Controller, with meeting the Controller's compliance obligations under the Data Protection Legislation, taking into account the nature of the Processor's processing and the information available to the Processor, including in relation to Data Subject rights, Data Protection Impact Assessments and reporting to and consulting with the relevant regulator under the Data Protection Legislation.
- 2.10 The Processor must notify promptly the Controller of any changes to the Data Protection Legislation or other Law that may reasonably be interpreted as adversely affecting the Processor's performance of the this Contract.

### 3.0 Definitions

- 3.1 The following words and phrases used in this Contract shall have the following meanings except where the context otherwise requires:

**Confidential Information** means all Law Enforcement Data and any other information relating to the Controller's customers and prospective customers, current or projected financial or trading situations, business plans, business strategies, developments and all other information relating to the Controller's business affairs including any trade secrets, know-how and any information of a confidential nature imparted by the Controller to the Processor during the term of this Contract or coming into existence as a result of the Processor's obligations, whether existing in hard copy form or otherwise, and whether disclosed orally or in writing.

**Contract** means this Data Processing Contract together with its schedules and all other documents attached to or referred to as forming part of this contract.

**Coronavirus** shall have the same meaning as set out in Section 1(1) of the Coronavirus Act 2020 (as amended from time to time).

**Coronavirus Legislation** means the Coronavirus Legislation in relation to England and Wales set out (and as amended from time to time) at <https://www.legislation.gov.uk/coronavirus> Including without limitation the Coronavirus Act 2020 and the Public Health (Control of Disease) Act 1984.

**Data, Controller, Data Subject, Processor, Process, Processing, Personal Data, Personal Data Breach, Pseudonymisation, Pseudonymised, and Personal Data relating to Criminal Convictions and Offences or Related Security Measures**, have the same meaning as set out in the Data Protection Legislation.

**Data Loss Event** means any event that results, or may result, in unauthorised access to Personal Data held by, or on behalf of, the Processor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach.

**Data Protection Impact Assessment** means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

**Data Protection Legislation** means all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (**DPA 2018**); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended .

**Data Subject Access Request** means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their personal data.

**FPN (Fixed Penalty Notice)** means a notice pursuant to the Coronavirus Legislation offering the person to whom it is issued the opportunity of discharging any liability to conviction for the offence by payment of a fixed penalty to a Local Authority specified in the notice (or as otherwise agreed in writing between the Parties from time to time).

**Law** means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which a Party is bound to comply.

**Law Enforcement Data** means, for the purposes of this Contract, any data including Personal Data, Special Categories of Personal Data and or Personal Data relating to Criminal Convictions and Offences or Related Security Measures, to be provided to, or collected by, or on behalf of, the Processor and processed on behalf of the Controller pursuant to this Contract.

**Local Authority** shall have the same meaning as set out in Section 78(7) of the Coronavirus Act 2020 in relation local authorities within England and Section 78(8) of the Coronavirus Act 2020 in relation local authorities within Wales (as appropriate).

**Party** means a Party to this Contract.

**Police Manager** means [REDACTED] who has oversight and responsibility for ensuring the Processing on behalf of the Controller or other such person as shall be notified to the Processor from time to time is in compliance with the terms of this Contract. The Police Manager will assume responsibility for co-ordinating data protection compliance, notification, security, confidentiality, audit and co-ordination of subject rights and Freedom of Information requests as directed by the terms of this Contract.

**Project Manager** means [REDACTED] (Senior Manager for National Disclosure Unit) who has day-to-day management responsibility for the Processing and compliance with this Contract on behalf of the Processor or such other person as shall be notified to the Data Controller from time to time. The Project Manager will assume responsibility for data protection compliance, notification, security, confidentiality, audit and co-ordination of subject rights and Freedom of Information requests as directed by the terms of this Contract.

**Protective Measures** means appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful

loss, destruction, alteration, disclosure or damage of Personal Data which may include: Pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted.

**Purpose** means the purpose of the Processing as set out within Schedule A (or as otherwise agreed in writing between the Parties).

**Services** means the Data Processing activity and services to be undertaken by the Processor on behalf of the Controller pursuant to this Contract, as identified in Schedule A and as agreed in writing between the Parties from time to time.

**Special Categories of Personal Data** has the same meaning as in the Data Protection Legislation.

**UK GDPR** has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

**Working Day** means any day other than a Saturday, Sunday or public holiday in England and Wales.

#### **4.0 Miscellaneous**

Headings are inserted for convenience only and shall not affect the construction or interpretation of this Contract and, unless otherwise stated, references to clauses and schedules are references to the clauses of and schedules to this Contract;

Any reference to any enactment or statutory provision shall be deemed to include a reference to such enactment or statute as extended, re-enacted, consolidated, implemented or amended and to any subordinate legislation made under it; and

The word 'including' shall mean including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word, and the word 'include' and its derivatives shall be construed accordingly.

#### **5.0 Provision or collection of Law Enforcement Data**

5.1 The manner and frequency of transmission of Law Enforcement Data from the Controller to the Processor shall be as agreed by the Parties in writing from time to time. Unless otherwise agreed in writing between the Parties, the relevant enforcement officer acting for or on behalf of the Controller shall complete (and submit to the ACRO CV19 mailbox: [REDACTED] (or other email address as agreed in writing between the Parties from time to time) from a secure mailbox) a pro-forma form in respect of the specific Coronavirus Legislation that has been, or is alleged to have been, contravened (including without limitation the offenders personal details, whether or not the Police National Computer ("PNC") has been checked in relation to the offence or alleged offence, the PNC ID code, circumstances of the offence or alleged offence, date, time, body worn video reference number, details of the ID checked and identity of the Controller. With the exception of telephone requests in cases of emergency only, contact between the Processor and the Controller and other relevant organisations should only be made over a secure communication network which will be via PNN.police and .Gov. Care must be taken where personal information is shared or discussed by the Processor.

5.2 The Processor (and any agent or subcontractor) must not transfer or otherwise process the Law Enforcement Data outside the UK without obtaining the Controller's prior written consent.

## **6.0 Access to the Law Enforcement Data**

- 6.1 Unless otherwise agreed in writing between the Parties, access to the Law Enforcement Data will be restricted to the Controller or those employees, agents or subcontractors of the Processor, directly involved in the processing of the Law Enforcement Data in pursuance of the Purpose.
- 6.2 Unless otherwise agreed between the Parties, the Processor will ensure that all of its employees, agents or subcontractors (a) are informed of the 'official' level as defined by the Government Security Classification Policy (GSCP) (including the confidential nature) of the Law Enforcement Data and are bound by written confidentiality obligations and use restrictions in respect of the Law Enforcement Data; (b) have undertaken training on the Data Protection Legislation and how it relates to their handling of the Law Enforcement Data and how it applies to their particular duties; and (c) are aware both of the Processor's duties and their personal duties and obligations under the Data Protection Legislation and this Contract.
- 6.3 Processing of certain Law Enforcement Data (as agreed in writing between the Parties from time to time) between ACRO and the Home Office is set out in a Memorandum of Understanding (MOU) between ACRO and the Home Office dated 8<sup>th</sup> June 2020 on the basis of paragraph 9(c) of Schedule 8 to the DPA 2018 and the purpose is to 'inform the NPCC, the Controllers and Ministers on the proportionality of such fixed penalties across a range of demographic characteristics, and for them to respond coherently to the public and parliamentary interest on this matter' and to facilitate statistical analysis to be undertaken by the Home Office to help police forces most effectively achieve their law enforcement purposes. Furthermore, Section 8 of the DPA 2018 provides that the 'public task basis' covers processing necessary for: the administration of justice; parliamentary functions; statutory functions; governmental functions; or activities that support or promote democratic engagement. Notwithstanding, ACRO shall ensure that any Law Enforcement Data transferred to the Home Office pursuant to the Contract shall be for statistical purposes only and is pseudonomised for that purpose.
- 6.4 Processing of certain Law Enforcement Data (as agreed in writing between the Parties from time to time) between ACRO and the Her Majesty Inspectorate of Constabulary and Fire & Rescue Service (HMICFRS) for the purposes of HMICFRS undertaking an inspection detailing the police response and effectiveness to Coronavirus (namely the FPN process ACRO have been asked to assist police forces with as ACRO have Processed certain Personal Data on behalf of certain police forces from time to time). The relevant data transferred by ACRO to the HMICFRS is a breakdown by week, force, regulation and social demographics, and ACRO shall ensure that Personal Data is not transferred to HMICFRS in relation to the Contract.
- 6.5 ACRO shall act as custodians for the penalty monies collected pursuant to the Contract, and will forward such payments to the relevant Local Authority in tranches (as agreed between the Parties in writing from time to time). Unless otherwise agreed in writing between the Parties, such Processing by ACRO will not contain any Personal Data, and shall be limited to details of the number of FPN's discharged and the Coronavirus Legislation to which they relate only. The offence location shall provided by ACRO in order that the relevant Local Authority can determine whether or not it is the correct Local Authority to receive such payment. The offence location may be a residential address however ACRO shall not transfer any Personal Data to enable the relevant

Local Authority to identify the individual, or whether or not it is the individual linked to the FPN or the address.

## **7.0 Data Protection and Human Rights**

- 7.1 The processing of any Personal Data shall be in accordance with the obligations imposed upon the Parties to this Contract by the Data Protection Legislation. All relevant codes of practice or data protection operating rules adopted by the Parties will also reflect the data protection practices of each of the parties to this Contract. The Processor must promptly notify the Controller of any changes to Data Protection Legislation that may adversely affect the Processor's performance of this Contract.
- 7.2 The Processor will only process the Law Enforcement Data to the extent, and in such a manner, as is necessary for the Purpose (and, where appropriate, any specific purposes agreed in writing between the Parties from time to time) in accordance with the Controller's written instructions from time to time (including without limitation sharing relevant Law Enforcement Data with approved subcontractors and or third parties (as appropriate)). The Processor will not process the Law Enforcement Data for any other purpose or in a way that does not comply with this Contract or the Data Protection Legislation. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
- 7.3 The only processing that the Processor is authorised to do is listed in Schedule A by the Controller and may not be determined by the Processor. Where deviation from Schedule A is required this will only occur where previously authorised in writing by the Police Manager to the Project Manager. The Processor shall not Process Law Enforcement Data in a way that is incompatible with the Purpose.
- 7.4 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:
- a) a systematic description of the envisaged processing operations and the purpose of the processing;
  - b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
  - c) an assessment of the risks to the rights and freedoms of Data Subjects; and
  - d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data
- 7.5 The Processor may not contact any Data Subject except where permitted by Schedule A.
- 7.6 The Processor shall notify the Controller immediately if it:
- a) receives a Data Subject Access Request (or purported Data Subject Access Request);
  - b) receives a request to rectify, block or erase any Personal Data;

- c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
  - d) receives any communication from the Information Commissioner's Office or any other regulatory authority in connection with Personal Data processed under this Contract;
  - e) receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
  - f) becomes aware of a Data Loss Event.
- 7.7 The Processor's obligation to notify under the preceding clause shall include the provision of further information to the Controller in phases, as details become available. The Processor must not disclose the Law Enforcement Data to any Data Subject or to a third party other than at the Controller's request or instruction, as provided for in this Contract or as required by law.
- 7.8 Taking into account the nature of the Processing, the Processor shall, at no additional cost, provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under preceding clauses (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:
- a) the Controller with full details and copies of the complaint, communication or request;
  - b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
  - c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
  - d) assistance as requested by the Controller following any Data Loss Event (including without limitation taking all reasonable steps to remedy such breach or loss or protect the Law Enforcement Data against any breach or threat and prevent an equivalent breach in the future (such steps shall include any action or changes reasonably required by the Controller and following such notification, as soon as reasonably practicable the Processor shall provide to the Controller full details of such breach as are available to the Processor and the steps being taken by the Processor (using such reporting mechanisms as may be reasonably specified by the Controller from time to time) of any actual, potential or threatened breach and the steps taken by the Processor in respect of such breach). For the avoidance of doubt, the Processor agrees that, subject to any relevant Law, the Controller has the sole right to determine whether to provide notice of any actual, threatened or potential breach of security or loss of Personal Data to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the Controller's discretion, including the contents and delivery method of the notice;
  - e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.



- 7.9 The Processor will promptly and without undue delay notify the Controller if any Law Enforcement Data is lost or destroyed or becomes damaged, corrupted, or unusable. The Processor will restore such Law Enforcement Data at its own expense. The Processor shall maintain detailed, complete, accurate and up to date records and information to demonstrate its compliance with this Contract, including but not limited to, the access, control and security of the Law Enforcement Data, approved subcontractors and affiliates, the Processing purposes, categories of Processing, any approved transfers of Personal Data to a third country and related safeguards, and a general description of the technical and organisational security measures (the "Records"). The Processor will ensure that the Records are sufficient to enable the Controller to verify the Processor's compliance with its obligations under this Contract and the Processor will provide the Contractor with copies of the Records upon request.
- 7.10 The Processor shall allow for audits of its Processing activity (including inspection of the Records) by the Controller or the Controller's designated auditor in accordance with the local and national arrangements and the Parties shall procure that the Processor shall make any documents available to public scrutiny where appropriate.
- 7.11 The Processor shall designate a data protection officer from time to time if required by the Data Protection Legislation. At the date of this Contract, the Processor's Data Protection Officer is [REDACTED]
- 7.12 Before allowing any subcontractor or any third party to Process any Law Enforcement Data related to this Contract, subject to the terms and conditions of this Contract, the Processor must:
- a) notify the Controller in writing of the intended subcontractor or relevant third party and Processing (including without limitation the relevant specific purposes in relation to such Processing);
  - b) obtain the prior written consent of the Controller;
  - c) maintain control over all Law Enforcement Data it entrusts to the subcontractor or relevant third party (as appropriate), including any specific purposes agreed between the Parties in writing, and enter into a written contract with the subcontractor or relevant third party (as appropriate) which give effect to the terms set out in this Contract such that they apply to the subcontractor or relevant third party (as appropriate), in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Controller's written request, provides the Controller with copies of such contracts (which, unless otherwise agreed between the Parties in writing, should terminate automatically on termination of this Contract for any reason); and
  - d) provide the Controller with such information regarding the subcontractor or relevant third party (as appropriate) as the Controller may reasonably require.
- 7.13 The Processor shall remain fully liable for all acts or omissions of any subcontractor or relevant third party (as appropriate). The Parties consider the Processor to control any Law Enforcement Data controlled by or in the possession of its subcontractors or relevant third party (as appropriate).
- 7.14 Those subcontractors and relevant third parties approved as at the commencement of this Contract (and the Services, if earlier) are as set out in Schedule A. For the avoidance of doubt, the Parties may amend the list of subcontractors and or relevant third parties

(including any specific purposes (if appropriate)) from time to time by agreement in writing.

- 7.15 On the Controller's written request, the Processor will audit a subcontractor's compliance with its obligations regarding the Law Enforcement Data and provide the Customer with the audit results.
- 7.16 The Controller may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).
- 7.17 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office and or relevant Data Protection Legislation.
- 7.18 The Parties agree and declare that the information accessed pursuant to this Contract will be used and processed with regard to the rights and freedoms enshrined within the European Convention on Human Rights. Further, the Parties agree and declare that the provision of information is proportional, having regard to the purposes of the Contract and the steps taken in respect of maintaining a high degree of security and confidentiality.
- 7.19 If any Party to this Contract receives a request for information under the provisions of the Freedom of Information Act 2000 identified as originating from the other Party, the receiving Party will contact the other Party promptly to determine whether the latter wishes to claim an exemption under the provisions of that Act.
- 7.20 Where the Processor receives a request for information under the provisions of the Freedom of Information Act 2000 in respect of information provided by or relating to the Controller, the Processor will contact the Police Manager to ascertain whether the Controller wishes to claim any exemption including the determination of whether or not the Controller wishes to issue a response neither to confirm nor deny that information is held.

## **8.0 Confidentiality**

- 8.1 The Processor shall not use or divulge or communicate to any person (other than those whose province it is to know the same for the Purpose, or without the prior written authority of the Controller) any Confidential Information obtained from or created on behalf of the Controller, which it shall treat as private and confidential and safeguard accordingly unless the Controller or this Contract specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires the Processor to Process or disclose Confidential Information, the Processor must first inform the Controller of the legal or regulatory requirement and give the Controller an opportunity to object or challenge the requirement, unless the law prohibits such notice.
- 8.2 The Processor shall ensure that any individuals who process Confidential Information (including without limitation any Law Enforcement Data) under this Contract are aware of their responsibilities in connection with the use of that Law Enforcement Data as a pre-requisite for that individual to process Law Enforcement Data.

- 8.3 For the avoidance of doubt, the obligations or the confidentiality imposed on the Parties by this Contract shall continue in full force and effect after the expiry or termination of this Contract.
- 8.4 Respect for the privacy and rights of Data Subjects will be afforded at all stages of the Purpose.
- 8.5 The restrictions contained within this section shall cease to apply to any Confidential Information which may come into the public domain otherwise than through unauthorised disclosure by the Parties to the Contract.

#### **9.0 Retention, Review and Deletion**

- 9.1 The Processor must promptly comply with any Controller request or instruction requiring the Processor to amend, transfer, delete, return and not retain, all or any Law Enforcement Data or otherwise Process the Law Enforcement Data, or to stop, mitigate or remedy any unauthorised Processing. If appropriate, the Processor will certify in writing that it has destroyed the Law Enforcement Data within 14 days after it completes the destruction.
- 9.2 The Law Enforcement Data will be retained by the Processor and then securely disposed by the Processor in accordance with Schedule A. If any law, regulation, or government or regulatory body requires the Processor to retain any documents or materials that the Processor would otherwise be required to return or destroy, it will notify the Controller in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

#### **10.0 Security**

- 10.1 The Processor recognises that the Controller has obligations relating to the security of Law Enforcement Data in his control under the Data Protection Legislation, ISO7799 and the National Policing Community Security Policy or as otherwise stipulated by the Controller from time to time. The Processor will continue to apply those relevant obligations as detailed below on behalf of the Controller during the term of this Contract.
- 10.2 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Contract:
- a) process that Personal Data only in accordance with Schedule A, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Customer before processing the Personal Data unless prohibited by Law;
  - b) ensure that it has in place, and implement at all times, Protective Measures (and document those measures in writing and periodically review them to ensure they remain current and complete, at least annually) which have been reviewed and approved by the Controller] as appropriate to protect against a Data Loss Event having taken account of the:
    - a. nature of the data to be protected;
    - b. harm that might result from a Data Loss Event;

- c. state of technological development; and
- d. cost of implementing any measures;
- e. ensure that:
  - i. employees of the Processor do not Process Law Enforcement Data except in accordance with this Contract (and in particular Schedule A);
  - ii. it takes all reasonable steps to ensure the reliability, integrity and trustworthiness of any employees who have access to the Law Enforcement Data (including without limitation conducting background checks consistent with applicable law on all of the Processor's employees with access to the Law Enforcement Data) and ensure that they:
    - 1. are aware of and comply with the Processor's, and their own personal, duties and obligations under this Contract (as appropriate);
    - 2. are subject to appropriate confidentiality undertakings with the Processor or any subcontractor;
    - 3. are informed of the confidential nature of the Law Enforcement Data and do not publish, disclose or divulge any of the Law Enforcement Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Contract; and
    - 4. have undergone adequate training in the use, care, protection and handling of Personal Data and how it applies to their particular duties; and
    - 5. not transfer Law Enforcement Data outside of the United Kingdom] unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
      - a. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (in accordance with relevant Data Protection Legislation) as determined by the Customer;
      - b. the Data Subject has enforceable rights and effective legal remedies;
      - c. the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
      - d. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Law Enforcement Data;
      - e. at the written direction of the Controller, delete or return Law Enforcement Data (and any copies of it) to the Processor on

termination of the Contract unless the Processor is required by Law to retain the Personal Data.

### **11.0 Indemnity**

In consideration of the provision of the Law Enforcement Data for the Purpose the Processor undertakes to indemnify and keep indemnified the Data Controller against any liability, which may be incurred by the Controller as a result of the Processor's breach of this Contract and or Data Protection Legislation.

### **12.0 Disputes**

12.1 In the event of any dispute or difference arising between the Parties out of this Contract, the Police Manager and the Project Manager or the persons appointed pursuant to this Contract shall meet in an effort to resolve the dispute or difference in good faith.

12.2 The Parties will, with the help of the Centre for Dispute Resolution, seek to resolve disputes between them by alternative dispute resolution. If the Parties fail to agree within 56 days of the initiation of the alternative dispute resolution procedure, then the Parties shall be at liberty to commence litigation.

### **13.0 Term, Termination and Variation**

13.1 The Parties hereby acknowledge and agree that the terms and conditions of this Contract are deemed to have been in effect from 1 April 2020. This Contract shall continue, unless terminated earlier in accordance with provisions of this Contract, or the Home Secretary or Secretary of State for Health and Social Care and the First Minister for Wales, suspends operation of all provisions under the relevant Coronavirus Legislation (whichever is the earlier) when it shall terminate automatically without notice.

13.2 Without prejudice to any other right or remedy, the Controller may at any time by notice in writing terminate this Contract forthwith if the Processor is in material breach of any obligation under this Contract.

13.3 At the discretion of the Controller this Contract shall terminate after the replacement of the Project Manager.

13.4 Without prejudice to any other right or remedy, either Party may terminate this Contract by giving 30 days' notice in writing to the other Party.

13.5 This Contract will remain in full force and effect so long as the Processor retains any Law Enforcement Data related to this Contract in its possession or control.

13.6 Any provision of this Contract that expressly or by implication should come into or continue in force on or after termination of this Contract in order to protect Law Enforcement Data will remain in full force and effect.

13.7 The Controller will have the final decision on any proposed variation to this Contract. Unless otherwise set out in the Contract, no variation of the Contract shall be effective

unless it is contained in a written instrument signed by both Parties and annexed to this Contract

#### **14.0 Miscellaneous**

- 14.1 This Contract acts in fulfilment of part of the responsibilities of the Controller as required by relevant Data Protection Legislation (including but not limited to section 34 of the DPA 2018).
- 14.2 Neither party shall be in breach of this Contract nor liable for delay in performing, or failure to perform, any of its obligations under this Contract if such delay or failure result from events, circumstances or causes beyond its reasonable control. In such circumstances the affected party shall be entitled to a reasonable extension of the time for performing such obligations. If the period of delay or non-performance continues for 30 days, the party not affected may terminate this Contract by giving 7 days' written notice to the affected party.
- 14.3 Nothing in this Contract 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.
- 14.4 Save for the British Transport Police Authority, a person who is not a party to this Contract shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Contract. This does not affect any right or remedy of a third party which exists, or is available, apart from that Act. The rights of the parties to terminate, rescind or agree any variation, waiver or settlement under this Contract are not subject to the consent of any other person.
- 14.5 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
- 14.6 Any notice or other communication given to a party under or in connection with this Contract must be in writing and delivered to:
- For Controller: [REDACTED] at British Transport Police, Information Management, 2nd Floor, 3 Callaghan Square, Cardiff, CF10 5BT / Heddlu Trafnidiaeth Prydeinig, 3 Sgŵar Callaghan, Caerdydd CF10 5BT.
- For the Processor: [REDACTED] at ACRO Criminal Records Office, PO Box 481, Fareham PO14 9FS
- 14.7 The above notice provision 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. A notice given under this Contract is not valid if sent by email.
- 14.8 This Contract constitutes the entire agreement between the Parties as regards the subject matter hereof and supercedes all prior oral or written Contract regarding such subject matter.

14.9 If any provision of this Contract is held by a Court of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability shall not affect the remaining provisions of this Contract, which shall remain in full force and effect.

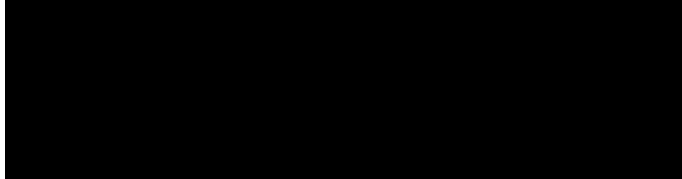
14.10 Without prejudice to the foregoing, if during the term of this Contract the Data Protection Legislation changes in a way that the Contract is no longer adequate for the purpose of governing lawful data sharing exercises, the Parties agree that they will negotiate in good faith to review the Contract in the light of the new legislation.

14.11 The validity, construction and interpretation of the Contract and any determination of the performance which it requires shall be governed by the Laws of England and Wales and the Parties hereby submit to the exclusive jurisdiction of the Courts of England and Wales.

Signed on behalf of the Chief Constable of British Transport Police



Signed on behalf of  CEO ACRO Criminal Records Office



**Schedule A:** Details of Law Enforcement Data to be provided to, or collected by, the Processor and processed on behalf of the Controller.

The Processor shall comply with any further written instructions with respect to processing from the Controller.

Any such further instructions shall be incorporated into this schedule.

Subject matter of the Processing	The provision of the Services by the Processor for the purposes of the enforcement of the Coronavirus Legislation and or as otherwise agreed in writing between the Parties.
Duration of the Processing	Unless otherwise agreed in writing between the Parties, a period of six years from date of the 'Case Finalisation' (being the date upon which the final outcome is administered in relation to a relevant case (including when a FPN is paid, or alternatively if it is contested, when the final outcome is administered by a Court) of the final FPN issued.

	<p>If further FPNs are issued, the retention period for all FPN records issued to the individual are to be retained for 6 years from the relevant Case Finalisation of the last FPN issued.</p>
<p>Purposes of the Processing</p>	<p>The provision of the Services by the Processor for the purposes of the enforcement of the relevant the Coronavirus Legislation (or as otherwise agreed in writing between the Parties from time to time) pursuant to this Contract.</p> <p>At the date of this Contract, offences have been created for the categories including but not limited to;</p> <ul style="list-style-type: none"> <li>• National travel restrictions</li> <li>• Local travel restrictions</li> <li>• International travel</li> <li>• Face coverings</li> <li>• Gathering in excessive numbers</li> <li>• Quarantine</li> <li>• Self-isolation</li> </ul>
<p>Nature of the Processing</p>	<p>As set out in this Contract (or as otherwise agreed in writing between the Parties from time to time), including but not limited to at the date of this Contract:</p> <p>In relation to, and for the purposes of, the Coronavirus Legislation, to permit ACRO to provide the Services, namely:</p> <ul style="list-style-type: none"> <li>(i) issuing valid fixed penalty notices on behalf of an authorised person made pursuant to the relevant Coronavirus Legislation ;</li> <li>(ii) the confirmation of the correct fixed penalty amount;</li> <li>(iii) the receipt of payments in respect of a FPN;</li> <li>(iv) the remittance of proceeds received from a FPN on behalf of the relevant Local Authority;</li> <li>(v) to issue a certificate confirming the payment status of a FPN in the event that a FPN is not paid;</li> <li>(vi) the remittance of proceeds received from the FPN to the relevant Local Authority in accordance with the terms of a the applicable agency agreement with such Local Authority for the management of such proceeds (a relevant Agency Agreement);</li> <li>(vii) the coordination with a relevant Local Authority's Chief Finance Officer to issue a certificate confirming the payment status of a FPN;</li> <li>(viii) providing confirmation to the Controller of the payment status of FPN and working with the Controller in order that further proceedings may be considered by the Crown Prosecution Service in the event of non-payment;</li> </ul>



	<ul style="list-style-type: none"> <li>(ix) issue valid Single Justice Procedure Notices for all relevant Controller offences on behalf of an authorised person;</li> <li>(x) make the relevant arrangements with Her Majesty's Courts and Tribunals Service for the listing of the SJP hearing, to include serving all relevant papers to court; and</li> <li>(xi) carrying out all associated administrative tasks .</li> </ul>
Type of Personal Data	Name, address, date of birth, contact details, ethnicity, offence committed, PNC ID, ID document number, Gender together with any other relevant categories of Personal Data, Special Categories of Personal Data and or Personal Data relating to Criminal Convictions and Offences or Related Security Measures as agreed between the Parties in writing from time to time
Categories of Data Subject	Police Officers, members of the public (including but not limited to witnesses), offenders, alleged offenders.
Arrangements for return or destruction of the data once processing is complete	].Any Confidential Information (including but not limited to any]Law Enforcement Data ) shared under this Contract will be securely stored and disposed by secure means when no longer required for the relevant Purpose for which it is provided as per each Parties' Information Security Policy, unless otherwise agreed in a specific case, and legally permitted. Subject to the terms and conditions of this Contract, each Party will determine and maintain its own retention schedule.
Approved Subcontractors and third parties	<p>Hampshire Print Services (Part of Hampshire County Council so a competent authority under s30 (1)(b) the DPA 2018 for printing and mailing out the relevant FPN letters)</p> <p>The Home Office</p> <p>Her Majesty Inspectorate of Constabulary and Fire &amp; Rescue Service (HMICFRS)</p> <p>Relevant Local Authorities</p> <p>Transport For London</p>

--	--

**OFFICIAL**

**OFFICIAL**

**OFFICIAL**

**OFFICIAL**