ANNEX A
Response to Category 3

Extract from Contract Between Axon and the Scottish Ministers through the Scottish Government

13. DATA PROTECTION

13.1 The Service Provider acknowledges that Personal Data described in the scope of Schedule 10 (Data Protection) will be Processed in connection with the Services under this Contract.

13.2 For the purposes of any such Processing, the Parties agree that the Service Provider acts as the Processor and the Purchaser acts as the Controller in respect of the Purchaser Data, each Partner acts as the Controller in respect of its own Partner Data and each Stakeholder acts as the Controller in respect of its own Stakeholder Data. Although the Parties acknowledge that the Partners and the Stakeholders may act as independent controllers when using shared infrastructure pursuant to this Contract, the Parties further acknowledge that there may be circumstances where one or more Partners and/or one or more of the Stakeholders may be joint controllers in jointly determining the purposes and means of processing Personal Data.

13.3 Both Parties agree to negotiate in good faith any such amendments to this Contract that may be required to ensure that both Parties and each Partner and Stakeholder meet all their obligations under the Data Protection Laws. The provisions of this clause 13 are without prejudice to any obligations and duties imposed directly on the Service Provider under the Data Protection Laws and the Service Provider hereby agrees to comply with those obligations and duties.

13.4 The Service Provider will, in conjunction with the Purchaser and each other Controller and in its own right and in respect of the Services, make all necessary preparations to ensure it will be compliant with the Data Protection Laws.

13.5 The Service Provider will provide the Purchaser and each other Controller with the contact details of its data protection officer or other designated individual with responsibility for data protection and privacy to act as the point of contact for the purpose of observing its obligations under the Data Protection Laws.

13.6 The Service Provider must:
13.6.1 agree and comply with the terms of the data processing provisions set out in Schedule 10 (Data Protection);
13.6.2 process Personal Data only as necessary in accordance with obligations under this Contract and any written instructions given by the Purchaser and the Partners (which may be specific or of a general nature), including with regard to transfers of Personal Data outside the United Kingdom or the European Economic Area unless required to do so by United Kingdom, European Union or Member state law or regulatory body to which the Service Provider is subject; in which case the Service Provider must, unless prohibited by that law or regulatory body, inform the Purchaser of that legal requirement before processing the Personal Data only to the extent, and in such manner as is necessary for the performance of the Service Provider's obligations under this Contract or as is required by the Law;

13.6.3 subject to clause 13.6.2 only process or otherwise transfer any Personal Data in or to any country outside the United Kingdom or the European Economic Area with the Purchaser's prior written consent;
13.6.4 take all reasonable steps to ensure the reliability and integrity of any Service Provider Representatives who have access to the Personal Data and ensure that the Service Provider Representatives: (a) are aware of and comply with the Service Provider's duties under this clause; (b) are subject to appropriate confidentiality undertakings with the Service Provider or the relevant Subcontractor; (c) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Purchaser or as otherwise permitted by this Contract; and (d) have undergone adequate training in the use, care, protection and handling of Personal Data (and the Service Provider shall keep, for the Term and for any Termination Assistance Period, accurate records of such training and details of the content of all training courses, which shall be made available to the Purchaser immediately upon request).
13.6.5 implement appropriate technical and organisational measures including those set out in Schedule 10 (Data Protection) and in accordance with the Data Protection Laws to protect Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure, such measures being appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected.

13.7 The Service Provider shall not engage a Sub-contractor to carry out Processing in connection with the Services without prior specific or general written authorisation from the Purchaser. In the case of general written authorisation, the Service Provider must inform the Purchaser of any intended changes concerning the addition or replacement of any other Sub-contractor and give the Purchaser an opportunity to object to such changes.

13.8 If the Service Provider engages a Sub-contractor for carrying out Processing activities on behalf of the Purchaser and the other Controllers, the Service Provider must ensure that the same data protection obligations as set out in this Contract are imposed on the Sub-contractor by way of a written and legally binding contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures. The Service Provider shall remain fully liable to the Purchaser and the other Controllers for the performance of the sub-contractor's performance of the obligations.

13.9 The Service Provider must provide to the Purchaser and the other Controllers reasonable assistance including by such technical and organisational measures as may be appropriate in complying with the Data Protection Laws. 13.10 The Service Provider must notify the Purchaser if it:
13.10.1 receives a Data Subject Access Request (or purported Data Subject Access Request);
13.10.2 receives a request to rectify, block or erase any Personal Data;
13.10.3 receives any other request, complaint or communication relating to the obligations of the Service Provider or the Purchaser or any other Controller under the Data Protection Laws;
13.10.4 receives any communication from the Supervisory Authority or any other regulatory authority in connection with Personal Data processed under this Contract; or
13.10.5 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; and such

notification must take place as soon as is possible but in any event within three (3) Working Days of receipt of the request or any other period as agreed in writing with the Purchaser from time to time.

13.11 Taking into account the nature of the Processing and the information available, the Service Provider must assist the Purchaser and each Controller in complying with the Purchaser's and each Controller's obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations in accordance with the Data Protection Laws. These obligations include:
13.11.1 ensuring an appropriate level of protection through technical and organisational measures that take into account the circumstances and purposes of the Processing as well as the projected probability and severity of a possible infringement of the Law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events;
13.11.2 notifying a Personal Data breach to the Purchaser and the relevant Controller without undue delay and in any event no later than twenty four (24) hours after becoming aware of a Personal Data breach;
13.11.3 assisting the Controller with communication of a personal data breach to a Data Subject;
13.11.4 supporting the Controller with preparation of a data protection impact assessment; and
13.11.5 supporting the Controller with regard to prior consultation of the Supervisory Authority.

13.12 At the end of the provision of Services relating to Processing the Service Provider must, on written instruction of the Purchaser, delete or return to the Purchaser (or to one or more Controllers specified by the Purchaser) all Personal Data and delete existing copies unless UK law requires storage of the Personal Data.

13.13 The Service Provider must maintain written records including in electronic form, of all Processing activities carried out in performance of the Services or otherwise on behalf of the Purchaser and each other Controller containing the information set out in the Data Protection Laws.

13.14 The Service Provider must:
13.14.1 provide such information as is necessary to enable the Purchaser and each other Controller to satisfy itself of the Service Provider's compliance with this clause 13;
13.14.2 allow the Purchaser and each other Controller, and its and their employees, auditors, authorised agents or advisers reasonable access to any relevant premises, during normal business hours, to inspect the procedures, measures and records referred to in this clause 13 and contribute as is reasonable to those audits and inspections; and
13.14.3 inform the Purchaser and any instructing Controller if in its opinion an instruction from the Purchaser or instructing Controller infringes any obligation under Data Protection Laws.

13.15 If requested, the Service Provider must make such records referred to in clause 13.11 available to the Supervisory Authority on request and co-operate with the Supervisory Authority in the performance of its tasks.

13.16 The Parties acknowledge that the inspecting party will use reasonable endeavours to carry out any audit or inspection under clause 13.12.2 with minimum disruption to the Service Provider's day to day business.

Schedule 2, Part 1, Statement of Requirements

SEC-24 Personal Information The data protection requirements are set out at Clause 13 and Schedule 10 of the Services Contract. Where Personal Data is involved, the Service Provider MUST contractually enforce all of these security conditions onto any thirdparty service providers, sub-contractors or partners who could potentially access the Purchaser Data, Partner Data or Stakeholder Data in the course of providing the service. The required security conditions should be either ISO/IEC 27001 (Information Security Management Systems Requirements) or equivalent or HMG Cyber Essentials Plus certification or equivalent. The Service Provider must indicate the arrangements under the Data Protection Act/GDPR and ISO27018 https://www.gov.uk/government/publications/cyberessentialsscheme-overview 129 Schedule 2, Part 1: Statement of Requirements
SEC-25 3rd Party Suppliers and Contractors The Service Provider MUST contractually enforce all of these security conditions onto any third-party Service Providers, sub-contractors or partners who may have access to the Purchaser Data and/or Partner Data in the course of providing the service. The required security conditions should be either ISO/IEC 27001 (Information Security Management Systems Requirements) or equivalent or HMG Cyber Essentials Plus certification or equivalent. https://www.gov.uk/government/publications/cyberessentials-scheme-overview

THIS SCHEDULE COMPRISES SCHEDULE 10 TO THE FOREGOING SERVICES CONTRACT BETWEEN THE SCOTTISH MINISTERS ACTING THROUGH THE SCOTTISH GOVERNMENT AND AXON PUBLIC SAFETY UK LTD SCHEDULE 10 DATA PROTECTION

Part 1: Data Processing provision as required by the Data Protection Laws. This Part includes certain details of the Processing of Personal Data in connection with the Services: 1. Subject matter and duration of the Processing of Personal Data The subject matter and duration of the Processing of Personal Data are set out in this Contract. Under this Contract, the Service Provider will only undertake Processing of Personal Data on behalf of the Purchaser and the Partners in accordance with this Schedule, the Data Protection Laws as it applies to the Service Provider and when specifically directed by the Purchaser and the Partners in writing.
Part 2: The nature and purpose of the Processing of Personal Data The Solution will support the collection, management and sharing of digital evidence across the justice sector in Scotland. The Solution will receive, store, process and present data collected from interactions with criminal justice partners, public sector bodies, local authorities, businesses and members of the public, which are to be used for purpose of the investigation and prosecution of crimes in Scotland. During the Term the Purchaser and the Partners may request the Service Provider to support the Processing of Personal Data relevant to the Services. The Service Provider shall comply with any further written instructions with respect to processing by the Purchaser and the Partners. Any such further instructions shall be incorporated into this Schedule.
Part 3: The types of Personal Data to be Processed The following data will be processed in relation to the investigation and prosecution of crimes. The types of data will include but may not be limited to: Documents and multimedia (including video, audio and images) containing imagery and audio of persons, names, address, correspondence address, date of birth, date of death, Hospital Record Number (or other NHS identifiers), telephone number, email address, accessibility requirements/preferences, nationality, residency details and related information, immigration status, details of medical conditions and medical history, details of functional abilities and impairments, details of existing or previous care and living arrangements, school details (child only), medical records, and equalities data (sex/gender/race etc.). The following types of data will be processed in relation to: Third parties who may be asked to provide

supporting information (e.g. Professional and Expert Witnesses), subject to the solution design, including: · Name, address, profession, phone number, email address Staff working in criminal justice organisations (including, but not limited to: Police Officers; Prosecutors; Criminal Defence Solicitors; and the Judiciary): · Name, location, staff number, job role, phone number, email address 516 Schedule 10

Part 4: The categories of Data Subject to whom Personal Data relates The personal data will relate to the following Data Subject Categories: · Members of the public, local authority or business operators in the submission and collection of data to be used in criminal investigations and prosecutions; · Third parties who provide supporting information or services, including expert witnesses, forensic specialists, doctors, social workers, and other health and social care professionals; · Staff working in criminal justice organisations.

Part 5: The obligations and rights of the Purchaser and the Partners The obligations and rights of the

Purchaser and the Partners as Controllers are set out in clause 13 (Data Protection) of this Contract.

Part 6: Minimum technical and organisational measures The Service Provider shall comply with any specific security provisions imposed by the Data Protection Laws. The Service Provider shall, as a minimum requirement, give due consideration to the following types of security measures: · Information Security Management Systems; · Physical Security; · Access Control; · Security and Privacy Enhancing Technologies; · Awareness, training and security checks in relation to personnel; · Incident/Response Management/Business Continuity; and · Audit Controls/Due Diligence. The Purchaser, the Partners and the Service Provider acknowledge that the Personal Data shall be transferred from the Controller to the Service Provider and that the Service Provider shall agree the secure mechanism for the direct transfer as proposed by the Controller and/or the Purchaser from time to time.