SCHEDULE 7: GDPR Terms

These GDPR Terms (***Terms***) apply to the processing of Personal Information within the scope of the Privacy Laws by Auror and Customer in connection with the Platform where Customer is subject to (as relevant) the EU and/or UK GDPR. They do not limit or reduce any privacy or data protection commitments Auror makes to Customer in the Standard Terms and Conditions.

For the purposes of these Terms, Customer and Auror agree as follows:

1. Definitions

The terms and expressions in this Schedule 7 shall have the following meanings:

1.1 "**Controller**", "**personal data**", "**processor**", "**processing**", "**processed**" and "**processing**" shall have the meanings given to them in the applicable Privacy Laws;

1.2 "**Data Security Breach**" means a breach or breaches of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information;

1.3 "**Data Subject**" means an individual who is the subject of Personal Information;

1.4 "**Data Subject Request**" means an actual or purported request, notice or complaint made by, or on behalf of, a Data Subject in exercise of their rights under the applicable Privacy Laws relating to their Personal Information;

1.5 "**Privacy Contact**" means an individual appointed by a party in accordance with paragraph 5 below.

Any capitalized terms in Schedule 7 that are not defined in this paragraph 1 (or elsewhere in Schedule 7) shall have the meanings given to them in the Terms.

2. Joint Controller Terms

2.1 The Joint Controller Terms in this paragraph 2 apply to the extent that the parties are joint controllers of the Personal Information, as described in Annex 1 to this Schedule 7.

2.1.1 Each party shall ensure that it has lawful grounds under the Privacy Laws for the processing of the Personal Information.

2.1.2 Neither party shall engage a processor (or any replacement) to carry out any processing activities in respect of the Personal Information without entering into binding terms with that processor which satisfy the requirements of the Privacy Laws.

2.2 Customer shall ensure that Data Subjects are provided with transparency information regarding the processing of their Personal Information in accordance with the Privacy Laws, via a privacy policy (or similar document) and appropriate signage in the context of CCTV and/or automated number plate recognition cameras, which sets out (in each case as required by applicable Privacy Laws):

2.2.1 the roles and responsibilities of the parties, as joint controllers (where applicable);

2.2.2 how a Data Subject can exercise their rights;

2.2.3 (if applicable) the fact that the parties acting as joint controllers will share the Personal Information with other parties; and

2.2.4 a primary point of contact (whether for one party or each party acting as joint controllers).

2.3 Customer shall ensure that the affected Data Subjects are notified of any changes to the privacy policy described at paragraph 2.2 above, including (i) the roles and responsibilities of the parties; and/or (ii) the point(s) of contact.

Handling of Personal Information

2.4 Each party agrees as follows in respect of the Personal Information:

2.4.1 each party will implement appropriate technical and organisational measures to safeguard the Personal Information against any Data Security Breach. Such measures shall be proportionate to the harm which might result from any such Data Security Breach (and having regard to the nature of the Personal Information in question);

2.4.2 each party will use reasonable efforts to ensure the Personal Information that it processes is kept accurate and up to date;

2.4.3 each party will ensure that its staff are properly trained and are aware of their responsibilities for any Personal Information that they have access to;

2.4.4 each party will promptly notify the other party (within at least two (2) working days) if it receives a complaint or request relating to the other party's obligations under the Privacy Laws (other than a Data Subject Request, which is addressed in paragraphs 2.5 – 2.7 below);

2.4.5 on receipt of a notice under paragraph 2.4.4, each party will provide the other party with full co-operation and assistance in relation to any such complaint or request.

Data Subject Requests

2.5 Each party shall promptly notify the other party on receipt of a Data Subject Request.

2.6 Customer shall be the point of contact for, and shall take conduct of the handling of, any such Data Subject Requests, including those received by Auror.

2.7 Auror shall provide such information and co-operation and take such action as Customer reasonably requests in relation to any Data Subject Request within the timescales reasonably required by Customer, to enable Customer to respond to each Data Subject Request in accordance with the Privacy Laws.

International data transfers

2.8 Neither party shall transfer the Personal Information to any country outside the UK, unless that party ensures that (as required to comply with applicable Privacy Laws):

2.8.1 the transfer is to a country to which the UK Secretary of State or European Commission (as appropriate in light of the applicable Privacy Laws) has permitted the free flow of personal data;

2.8.2 there are appropriate safeguards in place as required by the Privacy Laws; or

2.8.3 it can rely on a derogation from the relevant obligations under the applicable Privacy Laws.

Data Security Breaches

2.9 If a Data Security Breach occurs, the party which becomes aware of the Data Security Breach shall:

2.9.1 notify the other party of the Data Security Breach without undue delay (and in any event within 48 (forty-eight) hours of becoming aware of the Data Security Breach; and

2.9.2 provide the other party without undue delay with such details as that other party reasonably requires regarding:

(a) the nature of the Data Security Breach, including the categories and approximate numbers of affected Data Subjects and a description of the Personal Information affected;

(b) the likely consequences of the Data Security Breach; and

(c) any measures taken or proposed to be taken by the notifying party to address the Data Security Breach, including, where appropriate, measures to contain the Data Security Breach and mitigate its possible adverse effects.

2.10 The party affected by the Data Security Breach will provide regular updates to the other party on the progress of its investigation into the Data Security Breach.

2.11 The parties shall co-operate in good faith to ensure that such Data Security Breach is appropriately dealt with in accordance with the Privacy Laws, including (where applicable) through notification to the Information Commissioner's Office and/or other data protection authority within the timescales required by the Privacy Laws.

2.12 In respect of any Data Security Breach which Auror or Customer considers likely to cause high risk to a Data Subject, Auror and Customer shall cooperate to notify the affected Data Subjects without undue delay and Customer shall be the point of contact for such Data Subjects.

Retention and Deletion of Personal Information

2.13 Each party shall only retain the Personal Information for as long as reasonably necessary for the purpose set out in Annex 1 to this Schedule 7.

Claims by Data Subjects

2.14 If a Data Subject makes a claim for compensation under the Privacy Laws against one party (but not the other party) for damage suffered as a result of processing the Data Subject's Personal Information for the Purpose (a "**Claim**"):

2.14.1 the party in receipt of the Claim (the "**Affected Party**") will promptly notify the other party of the Claim;

2.14.2 the Affected Party will keep the other party fully informed of the progress of, and all material developments in relation to, the Claim;

2.14.3 the other party will provide the Affected Party with full co-operation and assistance in handling the Claim;

2.14.4 the Affected Party will have sole discretion over conduct of the Claim, but will use reasonable endeavours to consult with the other party prior to agreeing any compromise or settlement, or making any admission of liability.

2.15 If the Claim is successful and results in an award of compensation against the Affected Party, the parties agree that responsibility for the compensation awarded under the Claim shall be apportioned between the parties to such an extent as is just and equitable having regard to each party's share in the responsibility for the cause which gave rise to the Claim.

2.16 If the Affected Party agrees to a compromise or settles a Claim, the parties agree that responsibility for the compensation awarded shall be apportioned between the parties to such an extent as is just and equitable having regard to each party's share in the responsibility for the cause which gave rise to the Claim provided that the Affected Party consulted with the other party (or parties) prior to the agreement of any such compromise or settlement.

3. Controller and Processor Terms

3.1 This paragraph 3 applies to the extent that Auror processes the Personal Information as a processor on behalf of Customer as a controller (as described in Annex 2 to this Schedule 7).

3.2 **Customer control:** Customer will comply with all of its obligations under the applicable Privacy Laws as a controller of the Personal Information, including in respect of the processing instructions it gives to Auror as processor of the Personal Information, providing any required notices, and obtaining any required consents.

3.3 **Personal Information:** The subject matter, duration, nature and purpose of processing of the Personal Information, the type of Personal Information, the categories of Data Subjects and the obligations and rights of Customer in respect of Personal Information are set out in Annex 2 to this Schedule 7.

3.4 **General Processor obligations:** As a processor, Auror will:

3.4.1 only process the Personal Information to the extent, and in such a manner as is necessary for the Permitted Purpose and/or in accordance with Customer's other written instructions, except as required to comply with a legal obligation to which Auror is subject (in which case Auror will inform Customer of the relevant legal obligation unless prohibited from doing so on important grounds of public interest). Auror will not process the Personal Information for any other purpose or in a way that does not comply with this Agreement or the Privacy Laws;

3.4.2 maintain the confidentiality of all Personal Information and will not disclose Personal Information to any third party unless Customer specifically authorises the disclosure in accordance with this Agreement or where required by law;

3.4.3 promptly notify Customer if, in its reasonable opinion, Customer's instruction would not comply with the Privacy Laws (or would result in either Customer or Auror infringing the Privacy Laws); and

3.4.4 ensure its employees are bound by appropriate confidentiality obligations and use restrictions in respect of the Personal Information.

3.5 **Controller obligations**: Customer is responsible for ensuring that it has complied with its obligations of lawfulness under the Privacy Laws, including by ensuring that it has established an appropriate lawful basis and/or that any necessary Data Subject consents to the processing of Personal Information under this Agreement are appropriately obtained and a record of such consents is maintained. Customer also warrants and represents that it:

a) is, and will at all relevant times remain, duly and effectively authorised to give any instructions provided under paragraph 3.4.1(a); and

b) has all necessary rights to provide the Personal Information to the Processor for Processing under this Agreement.

3.6 **Security**: Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, Auror will implement appropriate technical and organisational measures to protect the Personal Information against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Information and/or against a Data Security Breach to ensure a level of security appropriate to the risk involved, including by implementing the security measures set out below, as appropriate:

(a) the pseudonymisation and encryption of Personal Information;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of security measures.

3.7 **Data Breach:** In the event of any Data Security Breach suffered by Auror in relation to the Personal Information described in this paragraph 3, Auror will:

a) notify Customer promptly and without undue delay (and in any event within 48 (forty-eight) hours) upon becoming aware of any such Data Breach; and

b) provide Customer with sufficient information to allow it to meet its obligations under the Privacy Laws, including the information set out at paragraph 3.8 below.

3.8 Auror will provide Customer with such details as Customer reasonably requires regarding:

(a) the nature of the Data Security Breach, including the categories and approximate numbers of affected Data Subjects and a description of the Personal Information affected;

(b) the likely consequences of the Data Security Breach; and

(c) any measures taken or proposed to be taken by Auror to address the Data Security Breach, including, where appropriate, measures to contain the Data Security Breach and mitigate its possible adverse effects.

3.9 Auror will co-operate with Customer and take reasonable steps as directed by Customer to assist in the investigation, mitigation and remediation of any Data Security Breach.

3.10 **Appointment of sub-processor(s):** Auror may authorise a third party (***sub-processor***) to process Personal Information on its behalf provided it first obtains Customer's prior written authorisation to the appointment of such a sub-processor in relation to Personal Information and enters into a written contract with the sub-processor that contains substantially the same terms as those set out in this Agreement (***sub-processor agreement***).

3.11 If a sub-processor fails to fulfil its obligations under a sub-processor agreement, Auror will remain liable to Customer for the performance of the sub-processor's obligations.

3.12 The parties acknowledge that Auror uses the Microsoft Azure platform to store and process Personal Information on its behalf and agree that Microsoft is a pre-approved sub-processor as at the Commencement Date of this Agreement.

3.13 **Data Subject rights:** Auror, taking into account the nature of the processing, will take such technical and organisational measures as are reasonably appropriate to enable Customer to comply with and respond to any Data Subject Request.

3.14 **Data return and destruction:** Upon request by Customer, within 90 days of the termination or expiry of this Agreement and these Terms, Auror will securely delete or destroy or, if directed in writing by the Controller, return and not retain, all or any Personal Information in its possession or control unless otherwise required by any applicable law, regulation, or government or regulatory body requirement.

3.15 **Record keeping:** Auror will maintain a written record (including in electronic form) of all categories of processing activities carried out for Customer, including the categories of processing carried out on behalf of Customer and any transfers of personal data to a third country and related safeguards (***Records***).

3.16 **Audit:** If Customer has reasonable grounds to believe that Auror has breached these Terms, then: (i) Customer must first issue a written notice to Auror requiring that Auror provide to Customer, without undue delay, any Records and other written information reasonably necessary to allow Customer to verify compliance with the Terms; and (ii) if the Customer is unable to verify (in Customer's reasonable opinion) Auror's compliance with the Terms based on the information provided by Auror under sub-clause (i) above or if Auror fails to respond within a reasonable time period following the receipt of the written notice provided under sub-clause (i), the Customer may provide further written notice to Auror requiring Auror to provide Customer and any properly appointed third-party representatives subject to appropriate confidentiality obligations in the circumstances (***Representatives***) to audit Auror's compliance with these Terms on at least 30 days' prior written notice. Auror will give Customer and its Representatives all reasonably necessary assistance to conduct such audits, including remote electronic access to the Records and Personnel. Customer will use (and will ensure its Representatives use) best endeavours to avoid causing any damage, injury, loss, delay or disruption to Auror's business activities, including the operation or availability of the Platform and the provision of any services by Auror. Customer shall be responsible for the cost and expenses of any such audit.

3.17 **Assistance with Customer's Compliance:** Auror will assist Customer in ensuring compliance with Customer's obligations under the Privacy Laws, including in relation to, as applicable, Customer's technical and organisational measures to protect the Personal Information, preparation of data protection impact assessments, and notification of a Data Security Breach to and/or other consultation with the UK Information Commissioner's Office (ICO).

3.18 **Annual penetration testing:** At least once per year, Auror will obtain a network-level vulnerability assessment performed by a recognised third-party audit firm based on recognised industry best practices.

3.19 **Cross-border transfers:** Auror (or any sub-processor) will not transfer or otherwise process Personal Information outside the UK without Customer's prior written consent.

4. Changes to the Privacy Laws

4.1 If during the term of this agreement, any of the Privacy Laws change in a way that this Schedule 7 is no longer adequate or appropriate for compliance with the Privacy Laws, the parties agree that they shall negotiate in good faith to review this agreement in light of the current Privacy Laws and amend, terminate and/or replace this agreement as appropriate.

Annex 1

Data Particulars (Joint Controllers)

Purposes for which the parties are joint controllers	• The parties will be joint controllers of the Personal Information to the extent that the Personal Information is processed: o to generate Platform Insights: high-level, aggregated insights which match data points across incidents to provide Customer with an overall picture of offending behaviour (e.g. total number of incidents attributed to an individual and the total value (i.e. loss) of those incidents) and, in turn, enable Customer to better understand trends and take actions to prevent further criminal activity; o as part of Customer's use of Connect the Dots (if selected by Customer in accordance with Schedule 2); o as part of Customer's use of ANPR (if selected by Customer in accordance with Schedule 2).
Types of data	• In relation to Platform Insights: Profile ID, name and known aliases, total event count, total value impacted by events, behaviour tags (e.g. whether the individual is known to be aggressive or use weapons); • In relation to Connect the Dots: images, name, age, build, event time and location, Event value and associated vehicles; • In relation to ANPR: images of vehicles, details of registration plates, colour, make and model of vehicles
Special Categories of personal data and/or criminal convictions data (if applicable)	• Criminal convictions data relating to potential perpetrators of criminal incidents • The parties may process special category data (including data relating to health, race and/or religion) to the extent that this forms part of distinguishing features etc.
Lawful Bases (and/or conditions for processing special category and criminal convictions data)	• Legitimate Interests • In relation to any special category or criminal convictions data, the parties also rely on the condition that processing is necessary for the purposes of preventing or detecting crime.
Categories of data subjects whose personal data will be processed	• Potential perpetrators of, and witnesses to, criminal offences and incidents/events recorded as part of the Platform.

Annex 2
Data Particulars (Controller to Processor)

Purposes for which Auror is a processor on behalf of Customer	• Auror will act as a processor on behalf of Customer to the extent that Customer uploads Customer Data to the Platform in order to log and report incidents/events as part of the Platform, including through the use of Modules set out at Schedule 2 above (save for Connect the Dots and ANPR, which are addressed in Annex 1 above).
Subject matter of the processing	• The use of the Platform by Customer, including the recording and/or sharing of personal data as part of the Platform
Duration of the processing	• The term of this Agreement

Nature and purpose of the processing	• Auror will process the Personal Information uploaded by Customer to the extent necessary for the Permitted Purpose.
Type of personal data	• Name; image, date of birth, age, address, mobile phone number, ID details, gender, height, build, distinguishing features and behaviour • Details relating to vehicles (including registration place, colour, make and model); • Further details about incidents, including details of witnesses, reference numbers assigned by law enforcement and officer details
Categories of data subjects	• Customer staff • Witnesses to and perpetrators of incidents logged by Customer on the Platform.