FASTVIEW360
superfast video monitoring

DATA PROCESSING ADDENDUM
(UK GDPR COMPLIANT)

2026

200, London Road,
Stapeley, CW5 7JW

www.fastview360.co.uk

01270 360360

info@fastview360.co.uk

DATA PROCESSING ADDENDUM
(UK GDPR Compliant)

This Data Processing Addendum ("Addendum") forms part of the Master Services Agreement ("Agreement") between the Supplier and the Customer. In the event of any conflict between this Addendum and the Agreement, the terms of this Addendum shall prevail in respect of the processing of Personal Data. Except as modified below, the terms of the Agreement shall remain in full force and effect.

1. Definitions

In this Addendum the following terms shall have the meanings set out below:

- **"Appropriate Safeguards"** means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time, including (without limitation) standard data protection clauses adopted or approved by the Secretary of State or the ICO under UK GDPR Article 46, and any applicable adequacy regulations made under UK GDPR Article 45;
- **"Data Controller"** has the meaning given to that term (or to the term "controller") in Data Protection Laws;
- **"Data Processor"** has the meaning given to that term (or to the term "processor") in Data Protection Laws;
- **"Data Protection Laws"** means all applicable UK data protection and privacy legislation in force from time to time, including: (i) the UK General Data Protection Regulation (as defined in section 3(10) of the Data Protection Act 2018, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019) ("UK GDPR"); (ii) the Data Protection Act 2018 ("DPA 2018"); (iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended); and (iv) any guidance, codes of practice and binding decisions of the Information Commissioner's Office ("ICO") or any successor supervisory authority; each as amended, re-enacted or replaced from time to time;
- **"Data Protection Losses"** means any costs (including reasonable legal costs), liabilities, claims, demands, actions, settlements, interest, charges, expenses, losses, damages, administrative fines, penalties, sanctions, costs of compliance with an investigation by a Supervisory Authority and/or compensation ordered by a Supervisory Authority;
- **"Data Subject"** has the meaning given to that term in Data Protection Laws;
- **"Data Subject Request"** means a request made by or on behalf of a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;
- **"Effective Date"** means the date on which the Agreement comes into force, or if this Addendum is entered into after the Agreement, the date on which this Addendum is executed by both parties;
- **"ICO"** means the Information Commissioner's Office or any successor supervisory authority in the United Kingdom;
- **"Personal Data"** has the meaning given to that term in Data Protection Laws;
- **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to,

Protected Data transmitted, stored or otherwise processed by the Supplier or its Sub-Processors;

- **"Processing Instructions"** has the meaning given to that term in clause 4.1.1;
- **"Protected Data"** means Personal Data processed by the Supplier on behalf of the Customer pursuant to or in connection with the Agreement;
- **"Sub-Processor"** means any third-party Data Processor engaged by the Supplier (or by any Sub-Processor of the Supplier) to process Protected Data on behalf of the Customer in connection with the Agreement;
- **"Supervisory Authority"** means the ICO or any other competent supervisory authority with jurisdiction over the processing of Protected Data; and
- **"Term"** means the period from the Effective Date until termination or expiry of the Agreement.

2. Term

This Addendum shall take effect on the Effective Date and shall remain in force until termination or expiry of the Agreement and thereafter until all Protected Data has been deleted or returned in accordance with clause 11.

3. Scope and Roles

1. This Addendum applies where and to the extent that the Supplier processes Protected Data on behalf of the Customer in connection with the provision of the Services.
2. The parties acknowledge and agree that, in relation to the Protected Data, the Customer is the Data Controller and the Supplier is the Data Processor.
3. The Supplier shall process Protected Data only in accordance with this Addendum and the Processing Instructions, except to the extent required to comply with applicable law.
4. The Customer shall comply with all Data Protection Laws in connection with its use of the Services and the processing of Protected Data, including:
   a) maintaining all necessary registrations and notifications with the ICO;
   b) ensuring there is a lawful basis for the processing of Protected Data and that all necessary fair processing information has been provided to, and all necessary consents obtained from, relevant Data Subjects;
   c) ensuring that all Processing Instructions given to the Supplier are lawful; and performing its obligations as Data Controller under Data Protection Laws.
5. The Supplier shall promptly notify the Customer if, in the Supplier's reasonable opinion, any Processing Instruction would infringe Data Protection Laws.

4. Processing Instructions and details of processing

1. The Supplier shall, and shall ensure that all persons authorised to process Protected Data shall, process Protected Data only:
   a) on and in accordance with the Customer's documented instructions as set out in this Addendum and Schedule 1 (Data Processing Details), as updated by written agreement between the parties from time to time ("**Processing Instructions**"); or

b) to the extent required by applicable law, in which case the Supplier shall (to the extent permitted by law) notify the Customer before carrying out such processing.

2. The subject matter, nature, purpose, types of Personal Data and categories of Data Subjects to be processed under this Addendum are set out in Schedule 1.
3. Where the Customer uses any Third Party Application not provided by the Supplier, the Supplier's obligations under this Addendum do not extend to Personal Data processed solely by that third party, and responsibility for such processing rests with the Customer and the relevant third-party provider.

5. Technical and organisational measures

1. The Supplier shall implement and maintain, at its own cost, appropriate technical and organisational measures to protect Protected Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access, having regard to:
   a) the state of the art and costs of implementation;
   b) the nature, scope, context and purposes of processing; and
   c) the risks to the rights and freedoms of Data Subjects, including the risk of varying likelihood and severity.
2. The measures referred to in clause 5.1 shall include, as appropriate, those described in Schedule 2 (Technical and Organisational Measures).
3. The Supplier shall, taking into account the nature of the processing, assist the Customer so far as reasonably practicable in fulfilling the Customer's obligations to respond to Data Subject Requests.

6. Sub-Processors

1. The Customer provides general written authorisation for the Supplier to engage Sub-Processors, subject to the conditions set out in this clause 6. The Supplier's current Sub-Processors are listed in Schedule 3 (Sub-Processors).
2. The Supplier shall:
   a) give the Customer at least 30 days' prior written notice before adding or replacing any Sub-Processor, giving the Customer sufficient details to enable it to assess whether the change raises any data protection concerns;
   b) prior to the relevant Sub-Processor carrying out any processing of Protected Data, ensure that each Sub-Processor is appointed under a written agreement containing obligations equivalent in substance to those imposed on the Supplier under this Addendum;
   c) remain liable to the Customer for the acts and omissions of its Sub-Processors to the same extent as if the Supplier had carried out the processing directly; and
   d) on request, provide the Customer with reasonable information about its Sub-Processors to enable the Customer to assess compliance with this clause.
3. The Customer may object to any new Sub-Processor on reasonable data protection grounds by notifying the Supplier in writing within 14 days of receiving notice under clause 6.2. The parties shall work together in good faith to resolve the objection. If the parties cannot agree within a further 14 days, either party may terminate the relevant Services on written notice without penalty.

4. The Supplier shall ensure that all persons authorised to process Protected Data (including employees and Sub-Processors) are subject to binding written obligations of confidentiality in respect of the Protected Data, or are under an appropriate statutory obligation of confidentiality.

7. Data Subject Rights and Customer Compliance

1. The Supplier shall promptly notify the Customer (and in any event within 5 Business Days) upon receiving a Data Subject Request relating to Protected Data, and shall not respond to such request directly except on the written instructions of the Customer or as required by law.
2. The Supplier shall provide such reasonable assistance as the Customer requires to enable the Customer to comply with its obligations under Data Protection Laws, including in respect of:
   a) responding to Data Subject Requests;
   b) security of processing;
   c) data protection impact assessments (as defined in UK GDPR Article 35);
   d) prior consultation with the ICO under UK GDPR Article 36; and
   e) notifications to the ICO and/or communications to Data Subjects in connection with a Personal Data Breach.
3. The Supplier's reasonable costs of providing assistance under clause 7.2 (other than assistance in connection with a Personal Data Breach caused by the Supplier's breach of this Addendum) may be charged to the Customer at the Supplier's standard rates in force at the time, provided that the Supplier notifies the Customer in advance of any such charges.

8. International Data Transfers

1. The Supplier shall not transfer Protected Data outside the United Kingdom without the prior written consent of the Customer, unless such transfer is made:
   a) to a country or territory covered by UK adequacy regulations in force at the time of the transfer;
   b) subject to Appropriate Safeguards; or
   c) in accordance with any other mechanism permitted by Data Protection Laws.
2. Where a Sub-Processor is located outside the United Kingdom, the Supplier shall ensure that Appropriate Safeguards are in place before any transfer of Protected Data to that Sub-Processor takes place, and shall make details of those safeguards available to the Customer on request.
3. For the avoidance of doubt, this clause 8 applies to all transfers outside the UK, including transfers to countries within the EEA where those countries are not covered by a UK adequacy decision.

9. Records, Information and Audit

1. The Supplier shall maintain written records of all categories of processing activities carried out on behalf of the Customer as required by UK GDPR Article 30.

2. The Supplier shall make available to the Customer, on reasonable written request, all information necessary to demonstrate compliance with its obligations under this Addendum, and shall allow for and contribute to audits and inspections by the Customer (or a third-party auditor mandated by the Customer), subject to the conditions in clause 9.3.
3. Audits under clause 9.2 are subject to:
   a) the Customer giving the Supplier not less than 30 days' prior written notice (except in cases of a reasonably suspected Personal Data Breach, where shorter notice may be given);
   b) audits being conducted during normal business hours with minimum disruption to the Supplier's operations;
   c) the Customer and any third-party auditor entering into a confidentiality agreement reasonably acceptable to the Supplier before commencing any audit;
   d) the Customer bearing its own costs and paying the Supplier's reasonable costs of assisting with the audit; and
   e) audits being limited to matters relevant to the Supplier's obligations under this Addendum and not extending to data belonging to other customers.
4. The Supplier may object in writing to any third-party auditor proposed by the Customer on reasonable grounds (including that the auditor is a competitor of the Supplier), in which case the parties shall agree on an alternative auditor in good faith.
5. As an alternative or supplement to an on-site audit, the Supplier may satisfy the Customer's audit rights under clause 9.2 by providing up-to-date copies of relevant third-party certifications, audit reports or security assessments (such as ISO 27001 certification or SOC 2 Type II reports) where these address the matters under review.

10. Personal Data Breach Information

1. The Supplier shall notify the Customer without undue delay, and in any event within 48 hours of becoming aware, of any Personal Data Breach involving Protected Data, providing the Customer with sufficient information to enable it to comply with its obligations under Data Protection Laws.
2. The Supplier's notification under clause 10.1 shall include, to the extent then known:
   a) the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records affected;
   b) the name and contact details of the Supplier's data protection officer or other relevant contact;
   c) the likely consequences of the Personal Data Breach; and
   d) the measures taken or proposed to address the Personal Data Breach, including measures to mitigate its possible adverse effects.
3. The Supplier shall cooperate with the Customer and take such steps as are reasonably requested to assist in the investigation, mitigation and remediation of each Personal Data Breach.
4. As Data Controller, the Customer is responsible for determining whether notification of the Personal Data Breach to the ICO and/or Data Subjects is required under Data Protection Laws and, if so, for providing such notifications. The Supplier shall provide reasonable assistance to the Customer in this regard.

5. The Customer shall notify the Supplier without undue delay if it becomes aware of a Personal Data Breach that may affect the Supplier's systems or processing activities.

11. Return and Deletion of Protected Data

1. On termination or expiry of the Agreement or earlier written request by the Customer, the Supplier shall, at the Customer's election, either:
   a) securely delete or destroy all Protected Data (including all copies) in its possession or under its control; or
   b) return all Protected Data to the Customer in a commonly used electronic format,
   c) in each case within 30 days of such termination, expiry or request, and confirm in writing to the Customer that it has done so.
2. Secure deletion under clause 11.1 shall be carried out in a manner consistent with good industry practice (including, where appropriate, the standards set out in NIST SP 800-88 or equivalent), and shall extend to Protected Data held by Sub-Processors.
3. The Supplier may retain Protected Data beyond the period in clause 11.1 only to the extent and for the period required by applicable law, in which case the Supplier shall inform the Customer of that requirement and shall continue to be bound by the obligations of this Addendum in respect of such retained data.
4. If no written instruction is received within 60 days of termination or expiry of the Agreement, the Supplier shall securely delete all Protected Data in accordance with clause 11.2 and notify the Customer accordingly.

12. Liability

1. Each party's liability to the other under or in connection with this Addendum shall be subject to the exclusions and limitations of liability set out in the Agreement, except that nothing in this Addendum or the Agreement shall limit either party's liability:
   a) for death or personal injury caused by negligence;
   b) for fraud or fraudulent misrepresentation; or
   c) to the extent that such limitation is not permitted by applicable law, including Data Protection Laws.
2. The Customer shall indemnify and keep the Supplier indemnified against all Data Protection Losses suffered by the Supplier arising directly from:
   a) any breach by the Customer of its obligations under Data Protection Laws or this Addendum; or
   b) any Processing Instruction given by the Customer that causes the Supplier to infringe Data Protection Laws,
   c) except to the extent that such Data Protection Losses arise from the Supplier's own breach of this Addendum or negligence.
3. The Supplier shall indemnify and keep the Customer indemnified against all Data Protection Losses suffered by the Customer arising directly from any breach by the Supplier of its obligations under this Addendum, except to the extent that such Data Protection Losses arise from the Customer's breach of Data Protection Laws or this Addendum.

4. Nothing in this clause 12 shall affect the rights of Data Subjects under Data Protection Laws.

13. Amendments

1. This Addendum may only be amended by a written instrument signed by authorised representatives of both parties.
2. Notwithstanding clause 13.1, the Supplier may propose amendments to this Addendum where required to ensure compliance with Data Protection Laws, by giving the Customer not less than 30 days' written notice. If the Customer reasonably objects to the proposed amendment on data protection grounds, the parties shall negotiate in good faith to agree revised terms. If the parties are unable to agree within 20 days of the Customer's objection, either party may terminate the relevant Services on 30 days' written notice without penalty.

14. Governing Law and Jurisdiction

1. This Addendum and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of England and Wales.
2. The courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Addendum.

Schedule 1 - Data Processing Details

The following details describe the processing of Protected Data to be carried out by the Supplier under this Addendum:

Subject matter of processing: Provision of fleet camera management services

Nature and purpose of processing: The platform ingests and stores video footage (and, where enabled, audio) recorded by vehicle-mounted cameras and presents it to authorised users of the customer through a secure web portal. An automated detection capability flags defined driving-safety events for human review.

Duration of processing: For the Term and as otherwise set out in clause 11.

Types of Personal Data: External video; in-cab video; optional in-cab audio; behavioural / event data (e.g. smoking, phone, seatbelt); date, time and vehicle identifiers; location data associated with footage.

Categories of Data Subjects: No facial recognition or biometric identification is used. However, the optional drowsiness/fatigue detection infers a driver's physiological state and should be treated as health-related (special category) data under Article 9 — intentional processing, not incidental (see Section 5.1 and risk R9). Separately, footage may incidentally capture imagery revealing other special-category characteristics (e.g. health, religion, ethnicity); this is residual and is not used to infer or act on those characteristics.

Processing Instructions: The Supplier is authorised to process Protected Data only to the extent necessary to provide the Services as described in the Agreement.

Schedule 2 — Technical And Organisational Measures

The Supplier shall implement and maintain, as a minimum, the following technical and organisational measures:

- Encryption of Protected Data in transit using TLS 1.2 or higher and at rest using AES-256 or equivalent;
- Access controls ensuring that access to Protected Data is limited to authorised personnel on a need-to-know basis;
- Where available, multi-factor authentication for systems holding or providing access to Protected Data;
- Regular security testing, vulnerability scanning and penetration testing of relevant systems;
- Documented procedures for detecting, reporting and investigating Personal Data Breaches;
- Business continuity and disaster recovery procedures tested at least annually;
- Staff training on data protection obligations on induction and at regular intervals thereafter;
- Physical security measures appropriate to the facilities used to process Protected Data;

SCHEDULE 3 - APPROVED SUB-PROCESSORS

The following Sub-Processors are authorised to process Protected Data as at the Effective Date:

Sub-Processor Name	Location	Processing Activity	Transfer Mechanism
Freshworks	United States (corporate entity); Protected Data hosted in the EU data centre region Frankfurt	IT service management and service desk (Freshservice) — ticket handling, support correspondence and contact records relating to Customer personnel.	EU Standard Contractual Clauses as amended by the UK International Data Transfer Addendum, per the Freshworks DPA.
Pipedrive OÜ	Estonia (EEA); Protected Data hosted in the EU region	Customer relationship management — storage of business contact details and communications history relating to Customer personnel.	EEA is covered by UK adequacy regulations; no additional safeguard required. Pipedrive's own DPA applies SCCs/UK Addendum to its onward sub-processors in third countries.
BigChange Ltd	United Kingdom (platform and contracting entity). Data may be transferred to other BigChange group entities and third-party sub-processors located outside the UK/EEA.	Field service management — job scheduling, work order records and site contact details relating to Customer personnel.	Where transfers are made to countries without adequacy, BigChange undertakes under clause 5.2 of its DPA to put appropriate safeguards in place (EU SCCs and, where applicable, the UK Addendum).
Microsoft Ireland Operations Limited	EU/EEA; support may be provided from other locations	Cloud hosting, storage and collaboration services (M365 — OneDrive, SharePoint, Exchange Online, Teams, Entra ID)	Microsoft DPA incorporating EU SCCs / UK Addendum; DPF certification where applicable

The Supplier shall notify the Customer of any proposed changes to this Schedule in accordance with clause 6.2.

SIGNED BY THE PARTIES

Signed:

Wayne Moss – Managing Director

Date: 19/01/2026

Signed:

Toby Fournier - Head of Legal

Date: 19/01/2026