Data Processing Agreement

Last updated: 2026-05-25

This Data Processing Agreement (the "DPA") is incorporated by reference into the Terms of Service at `/terms`. Continued use of the Service constitutes acceptance of this DPA. A counter-signed copy is available on written request to `legal@uasecure.com`. A downloadable PDF is linked at the bottom of this page.

Definitions

- **Personal Data** has the meaning given by Applicable Law. - **Data Subject** means an identified or identifiable natural person to whom Personal Data relates. - **Sub-processor** means any third party engaged by Processor to process Personal Data on behalf of the Controller. - **Standard Contractual Clauses** (or "SCCs") means the EU Commission Implementing Decision (EU) 2021/914 Module 2 (Controller to Processor). - **UK Addendum** means the UK Addendum to the SCCs issued by the UK Information Commissioner's Office. - **Applicable Law** means all data-protection and privacy laws and regulations applicable to the processing of Personal Data under this DPA, including the EU General Data Protection Regulation, the UK GDPR, and US state privacy laws as relevant. - **Controller** is the customer. - **Processor** is UASecure.

Subject matter, duration, nature, and purpose of the processing

The subject matter of the processing is the provision of mission-planning, fleet-management, and compliance-support services by Processor to Controller. The duration of the processing is the term of the Controller's subscription, plus the retention periods stated in `/privacy`. The nature of the processing covers storage, access control, and processing for the Service's documented purposes (including hosting, transactional email, error monitoring, payment processing, and other operational functions described at `/sub-processors`). The purpose of the processing is to operate the Service in accordance with the Controller's documented instructions.

Categories of Personal Data and Data Subjects

Personal Data processed under this DPA includes:

- Account information (email, name, organization, role). - Mission and operational data submitted by the Controller or its users. - Billing identifiers (such as customer IDs, last four digits of payment cards, billing address). - Technical telemetry collected per `/privacy` (such as IP addresses at request time, browser metadata, and error stack traces).

Data Subjects whose Personal Data is processed under this DPA include:

- Operators (Controller's users with administrative or operational access). - Crew members (pilots, visual observers, payload commanders, and others listed on mission records). - Third-party contacts entered into mission records by the Controller (such as property owners, points of contact, and emergency contacts).

Processor obligations

Processor will:

- Process Personal Data only on the Controller's documented instructions, including with respect to international transfers, unless required to do otherwise by Applicable Law (in which case Processor will inform the Controller of that legal requirement before processing, unless prohibited from doing so). - Ensure that personnel authorized to process Personal Data are bound by appropriate confidentiality obligations. - Implement appropriate technical and organizational measures to protect Personal Data, including TLS in transit, encryption at rest, role-scoped access controls, audit logging, and multi-factor authentication options. - Notify the Controller without undue delay, and in any

case within 72 hours of becoming aware, of any Personal Data breach affecting the Controller's Personal Data, with reasonable detail about the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed to address the breach. - Assist the Controller, taking into account the nature of the processing and the information available to Processor, with responding to Data Subject requests, with Data Protection Impact Assessments, and with prior consultations with supervisory authorities. - Grant the Controller, or an independent auditor instructed by it, the right to audit Processor's compliance with this DPA once per year on reasonable notice, subject to confidentiality obligations and at the Controller's expense.

Sub-processors

Controller authorizes Processor to engage the sub-processors listed at `/sub-processors`. UASecure will provide at least 30 days' advance notice of additions that materially expand the categories of Personal Data processed. Controller may object to a proposed sub-processor on reasonable grounds within the notice period. If the objection cannot be resolved through commercially reasonable efforts, the Controller may terminate the affected services with a prorated refund for any prepaid unused period.

International transfers

Where Personal Data is transferred from the European Economic Area, Switzerland, or the United Kingdom to a country that does not provide an adequate level of protection under Applicable Law, the SCCs (Module 2, Controller to Processor) are incorporated by reference into this DPA.

For the annexes the SCCs require:

- **Annex I (parties, processing details, competent supervisory authority)**: Data exporter is the Controller identified in the customer's UASecure organization record. Data importer is UASecure, a U.S. entity headquartered in Scottsdale, Arizona. The processing description and categories of Data Subjects are set out in the "Subject matter, duration, nature, and purpose" and "Categories of Personal Data and Data Subjects" sections above. The competent supervisory authority is, by default, the supervisory authority in the Member State where the data exporter is established; for transfers from the United Kingdom, the Information Commissioner's Office. - **Annex II (technical and organizational measures)**: the measures set out in the "Processor obligations" section above (TLS in transit, encryption at rest, role-scoped access, audit logging, multi-factor authentication availability, 72-hour breach notification). UASecure will furnish a current summary of additional measures on written request to `legal@uasecure.com`. - **Annex III (authorized sub-processors)**: the current list at `/sub-processors`, as updated from time to time per the Sub-processors section above.

The UK Addendum is incorporated by reference for transfers originating in the United Kingdom. Personal Data is processed in the United States. The SCCs and the UK Addendum govern those transfers.

Termination and data return

On written request to `legal@uasecure.com` within 30 days of termination of the Service, Processor will delete or return the Controller's Personal Data, at the Controller's election. Backups are deleted on the normal rotation schedule (at most 90 days after termination), at which point all copies are destroyed, except where retention is required by Applicable Law.

Liability

Each party's liability arising out of or related to this DPA is subject to the Limitation of Liability section of the Terms of Service.

Governing law and order of precedence

This DPA is governed by the same law as the Terms of Service. In the event of any conflict between this DPA and the Terms of Service regarding the processing of Personal Data, this DPA controls.

Acceptance

Continued use of the Service after the effective date constitutes acceptance of this DPA. A counter-signed copy is available on written request to `legal@uasecure.com`.

Contact

For DPA matters and breach notifications, contact `legal@uasecure.com`.