

A background image showing a person's hands typing on a laptop keyboard and using a mouse. Overlaid on this is a digital interface with various icons and text related to data protection. A prominent icon is a glowing blue padlock. Other elements include a search bar, a "DATA PROTECTION" label, and several icons representing different aspects of security and data management.

GDPR COMPLIANCE

Traxess Software Solutions as a Service

DATA PRIVACY MATTERS TO US ●

The Traxess Software's as a Service are developed, deployed, and operated in full compliance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and related data-protection legislation applicable in the European Union, Switzerland, and the United Kingdom.

GDPR compliance is an integral part of the **Traxess Solutions Governance Framework**. All personal data processed within the platforms including traveller information, employee profiles, and incident response data is handled according to the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.

This document defines the data-protection measures, governance roles, and operational mechanisms implemented by **Traxess Ltd.** to ensure ongoing conformity with **GDPR and ISO 27001** controls (Annex A 8-18).

1. Roles and Responsibilities

- **Data Controller**

The customer organisation (e.g., a corporate client, public agency, or white-label partner) acts as the **Data Controller**. It determines the purpose and legal basis for processing personal data within the software solution (e.g., Corporate Resilience Management, Duty of Care Services, Traveller Tracking, or Incident Alerting).

- **Data Processor**

Traxess Ltd. acts as the **Data Processor**, processing personal data on behalf of the Controller in accordance with the contractual **Data Processing Agreement (DPA)** and internal **Information Security Management System (ISMS)** policies.

- **Sub-Processors**

Traxess engages a limited number of **Sub-Processors** for infrastructure and communication (hosting within certified European data centres and email/SMS gateway providers).

All Sub-Processors are contractually bound to **GDPR-equivalent obligations** and are listed in the **Sub-Processor Registry**, available to clients upon request.

2. Legal Basis for Processing

The processing of personal data within the Software Solutions is grounded on one or more of the following legal bases:

- **Performance of a Contract** (Art. 6 (1)(b)): Delivery of information, risk alerts, travel tracking, and duty-of-care notifications under the Service Agreement.
- **Compliance with Legal Obligations** (Art. 6 (1)(c)); Record-keeping, audit, and regulatory disclosure.
- **Legitimate Interest** (Art. 6 (1)(f)): Supporting organisational resilience and traveller safety.
- **Consent** (Art. 6 (1)(a)): Used where the Controller elects optional modules (e.g., location sharing, insurance or passport information).

3. Data Minimisation and Purpose Limitation

The Traxess Software Solutions are designed under **Privacy by Design and by Default** (Art. 25 GDPR):

- Only essential data fields are collected for traveller management, alert dissemination, and system authentication.
- Each module (e.g., Traveller Tracker, Messenger, Profile Manager) processes data strictly within its defined purpose.
- Retention schedules are embedded in the data lifecycle logic ensuring automatic anonymisation or deletion after contractual or statutory retention periods.

4. Support for Data-Subject Rights

The Software Solutions provide built-in tools enabling Controllers to exercise and manage data-subject rights:

GDPR Right	Sentinel Capability
Access (Art. 15)	Export traveller or user data via secure JSON/CSV from the Admin Console
Rectification (Art. 16)	Direct editing or API-based correction of personal fields
Erasure (Art. 17)	Permanent deletion of user records and audit confirmation
Restriction/Objection (Arts. 18–21)	Configurable status flags controlling processing scope
Portability (Art. 20)	Structured export interface for cross-system transfers

All requests received by Traxess are logged in the **GDPR Request Register** and executed under Controller instruction within statutory timelines.

5. Data Transfers and Hosting Locations

- All primary data processing and storage occur within European Economic Area (EEA) data centres operated by ISO 27001-certified providers:
 - **OVH Cloud Data Centre Roubaix, France** – ANSSI SecNum compliant
 - **Hetzner Data Centre Nuremberg, Germany**
- For international clients or global resilience operations, data transfers outside the EEA are protected by Standard Contractual Clauses (SCCs) and/or equivalent adequacy mechanisms.
- Data are not shared with any third party except is explicitly and contractually agreed between the parties and serves the purpose of the service contracted by the system owner.
- The data-residency map and transfer documentation are maintained in the Traxess Compliance Repository.

6. Technical and Organisational Security Measures (TOMs)

Traxess implements layered security controls covering people, process, and technology domains:

- **Encryption:** AES-256 at rest; TLS 1.3 in transit.
- **Access Control:** RBAC, least-privilege principle, MFA for administrative users.
- **Monitoring:** SIEM integration, real-time threat detection, and automated log analysis.
- **Resilience:** 24/7 infrastructure redundancy and geo-replicated backups.
- **Change Management:** secure DevOps pipelines with pre-deployment security testing.

- **Compliance Alignment:** ISO 27001/27017

7. Incident and Breach Management

Traxess maintains an **Incident Response Plan** and **Personal Data Breach Procedure** aligned with ISO 27035:

- Incidents are triaged, logged, and assessed for data-protection impact.
- In the event of a confirmed personal data breach, Traxess notifies the Controller without undue delay and within 72 hours of awareness, providing:
 - The nature and scope of the breach;
 - Categories and approximate number of affected data subjects;
 - Consequences and mitigation actions.
- Follow-up includes forensic analysis and lessons-learned review within the ISMS continual-improvement cycle.

8. Data Retention and Deletion

Data retention within the Traxess Software Solutions follows documented policies if not otherwise contractually agreed with the system business owner.:

Data Category	Retention Period	Action on Expiry
Traveller Profiles	Duration of Contract + 30 days Anonymisation after 6 months inactivity	Secure erasure
Booking Data	12 months	Secure erasure
GPS Tracking Logs	6 months	Secure erasure
Messenger Logs	6 months	Secure erasure
System Audit Logs	24 months	Archival to secure storage then deletion
Backup Images	≤ 90 days	Cryptographic wipe via secure overwrite

Deletion events are logged, and deletion certificates can be issued to Controllers upon request.

9. Documentation and Audit

To demonstrate compliance and accountability:

- **Record of Processing Activities (RoPA)** maintained under Art. 30 GDPR.
- **Data Protection Impact Assessments (DPIAs)** for all high-risk modules (Traveller Tracking, Location Services, Emergency Alert Broadcast).

- **Internal Audits** conducted quarterly under ISO 27001 schedule.
- **External Audits** provided annually.
- **Controllers retain audit rights as per the DPA**; read-only evidence access can be arranged via the Traxess Account Manager.

10. Awareness and Training

All Traxess personnel with access to client systems undergo:

- GDPR and Data-Protection Induction training upon hire;
- Annual refresher courses covering secure handling, classification, and incident escalation;
- Role-based security awareness sessions for developers, support engineers, and account managers.

Training completion is tracked and audited by the Information Security Manager.

11. Data Protection Officer (DPO) and Contact Details

The appointed **Data Protection Officer** oversees compliance with GDPR and national data-protection laws, performs DPIAs, and liaises with supervisory authorities.

Contact: Data Protection Officer (DPO)

Traxess Ltd.- Gartenstrasse 25 - CH-8002 Zurich - Switzerland

Email: info@traxess.ch

12. Continuous Improvement and Review

GDPR compliance within the client applications is reviewed semi-annually under the **ISMS Management Review Process**. Improvements are tracked through the **Corrective Action Log**, and any regulatory or technological developments are incorporated into the privacy roadmap.

13. Summary

The **Traxess Software Solutions** ensure GDPR compliance through a structured combination of legal adherence, technical safeguards, transparent governance, and ongoing review.

These measures protect personal data, enable accountability, and sustain client trust forming an integral part of the Traxess mission to deliver **secure, resilient, and compliant software services**.