

**Source:** <https://langfuse-docs-git-migrate-chatbot-ai-sdk-v7-langfuse.vercel.app/md-src/security/toms.md>

# Langfuse Technical and Organisational Measures (TOMs)

---

Langfuse implements the following technical and organisational measures (TOMs) to protect the confidentiality, integrity, and availability of data.

**Latest revision:** October 17th, 2025 | [download as PDF](#)

## 1. Confidentiality

---

### 1.1 Physical Access Control

Preventing unauthorised persons from gaining access to data processing systems.

#### *Technical Measures*

- Locking systems
- Lockable storage containers

#### *Organisational Measures*

- Physical Security Policy
- Visitors accompanied by employees
- Information Security Policy

### 1.2 Logical Access Control

Preventing data processing systems from being used by unauthorised persons.

#### *Technical Measures*

- Login with username and strong password or SSO where available
- Encryption of devices
- Enforced MFA where applicable
- Automatic desktop lock

#### *Organisational Measures*

- User permission management
- Creating user profiles
- Information Security Policy

### **1.3 Authorisation Control**

Ensuring employees can only access data subject to their authorisation and cannot read, copy, modify or remove Personal Data without permission.

#### *Technical Measures*

- Logging of access to applications or databases (entering, changing, deleting data)
- SSH encrypted access
- TLS encryption in transit

#### *Organisational Measures*

- Minimum number of administrators
- Management of user rights by administrators
- No shared accounts where technically feasible
- Information Security Policy

### **1.4 Separation Control**

Ensuring data collected for different purposes is processed separately.

#### *Technical Measures*

- Separation of production and test environments
- Multi tenancy of relevant applications

#### *Organisational Measures*

- Control via authorisation concept
- Determination of database rights
- Information Security & Data Protection Policies

## **2. Integrity**

---

### **2.1 Transfer Control**

Ensuring Personal Data cannot be read, copied, altered or removed by unauthorised persons during electronic transmission or transport/storage on media.

### *Technical Measures*

- Provision via encrypted connections (SFTP, HTTPS, secure cloud stores)

### *Organisational Measures*

- Information Security & Data Protection Policies

## **2.2 Input Control**

Ability to verify whether and by which user Personal Data has been entered, modified or removed.

### *Technical Measures*

- Manual or automated logging of database access
- Traceability through individual user names (not groups)

### *Organisational Measures*

- Assignment of rights based on an authorisation concept
- Information Security Policy

## **3. Availability and Resilience**

---

### **3.1 Availability Control**

Protecting Personal Data against accidental destruction or loss.

### *Technical Measures*

- Hosting in certified data centres by reputable cloud providers (e.g. AWS)
- Using multiple availability zones within a cloud region
- Backup concept
- Use of as many fully managed services as feasible to reduce downtimes
- Monitoring and alerting for capacity and functioning of core processes
- Using highly available and horizontally scalable architectures where possible

### *Organisational Measures*

- Business continuity and disaster recovery plan
- Information Security Policy

### **3.2 Recoverability Control**

Rapid restoration of availability and access after an incident.

#### *Technical Measures*

- Backup monitoring and reporting
- Automated restoration tools
- Regular recovery tests with logged results

#### *Organisational Measures*

- Recovery concept aligned to data criticality and Client specs
- Information Security Policy

## **4. Regular Review, Assessment and Evaluation**

---

### **4.1 Data Protection Management**

- Central documentation of data protection regulations accessible to employees
- Privacy Officer appointed
- Annual review of TOMs and updates
- Staff trained and bound to confidentiality
- Regular awareness trainings
- Processes for information obligations (Art 13/14 GDPR)
- Formal DSAR process
- Data protection in corporate risk management

### **4.2 Incident Response Management**

- Email security gateway, anti malware, and filtering controls with regular updates
- Documented incident response process covering authority notifications
- Formalised procedure for handling incidents
- Involvement of Privacy Officer and CTO
- Ticket based documentation and follow up of incidents

### **4.3 Data Protection by Design and Default**

- No more Personal Data collected than necessary
- Privacy friendly default settings in software

### **4.4 Order Control (Sub Processors)**

- Vendor due diligence and DPAs/SCCs in place

- Monitoring of subcontractors
- Audit rights over contractors
- Secure deletion of data after contract end

## **5. Organisation and Staff**

---

- Information security as a core corporate objective
- Employees bound to confidentiality and data secrecy
- External parties subject to NDA before work commences