DOCUMENT IDENTITY BANNER	
File	ISMS_I_Technical and Organizational Measures (TOMs)
Date of creation	10.06.2026
Last validation	10.06.2026
Version	V1.0

Introduction

This document describes the Technical and Organisational Measures (TOMs) implemented by Swibeco SA as a data processor, in accordance with Article 32 of the General Data Protection Regulation (GDPR - EU 2016/679), to ensure a level of security appropriate to the risk for the personal data processed.

These measures take into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, as well as the risks to the rights and freedoms of natural persons.
Swibeco SA is certified **ISO/IEC 27001**. All measures described below are implemented within the framework of a certified Information Security Management System (ISMS), audited and maintained in accordance with this international standard.

Category / Measure	Description	Implementation at Swibeco
1. Access Control		
Identity and Access Management (IAM)	Access rights granted on a least-privilege basis. Periodic access rights reviews are conducted.	In place
Multi-Factor Authentication (MFA)	MFA is mandatory for access to any systems and administration tools.	In place
Password Policy	Strong password requirements enforced (minimum length, complexity).	In place
Environment Separation	Strict separation between nonproduction and production environments.	In place
2. Data Encryption		
Encryption in Transit	All communications are encrypted using TLS 1.2 minimum (TLS 1.3 preferred). SSL/TLS certificates are actively managed and renewed.	In place
Encryption at Rest	Stored data is encrypted at rest using AES-256, including databases and backups.	In place
Cryptographic Key Management	Cryptographic keys are managed securely with periodic rotation and strict access controls.	In place
3. Infrastructure and Hosting		
Secure Hosting in Switzerland	The platform is hosted by Exoscale in a Swiss data center (CH-GVA-2). Data does not leave Switzerland.	In place
Physical Data Center Security	Exoscale data centers are equipped with physical access controls (badges, biometrics), CCTV, redundant power supply, and fire suppression systems.	In place
High Availability and Redundancy	Redundant architecture ensures service availability. Real-time data replication is in place.	In place

Category / Measure	Description	Implementation at Swibeco
Firewall and Network Segmentation	Web Application Firewall (WAF) and network firewalls are configured.	In place
4. Backup and Business Continuity		
Regular Backups	Automated daily backups of data and databases. Retention periods are configured to meet legal requirements.	In place
Restore Testing	Regular backup restoration tests are performed to validate data integrity and recoverability.	In place
Business Continuity Plan (BCP)	Documented business continuity plan covering major disaster scenarios.	In place
5. Monitoring, Logging and Incident Detection		
Access and Event Logging	Access, authentication, and security event logs are collected and stored securely.	In place
Monitoring and Alerting (SIEM)	Continuous system monitoring with automated alerts triggered on anomalies or security events.	In place
Security Incident Management	Documented procedure for detection, qualification, notification, and handling of security incidents, including personal data breaches.	In place
Penetration Testing	Regular penetration tests conducted by independent third parties to identify and remediate vulnerabilities.	In place
Vulnerability and Patch Management	Vulnerability monitoring process (CVE tracking) with security patches applied within defined timeframes based on criticality.	In place
6. Secure Development (Secure by Design)		
Secure Software Development Lifecycle (SDLC)	Security integrated throughout the development lifecycle: code reviews, static analysis (SAST), automated security controls in CI/CD pipelines.	In place
Third-Party Dependency Management	Inventory and analysis of third-party software components (SCA). Regular updates to reduce exposure to known vulnerabilities.	In place
Application Security Testing (DAST/SAST)	Automated static and dynamic application security testing integrated into the delivery pipeline.	In place
7. Governance and Organisational Measures		
ISO/IEC 27001 Certification	Swibeco SA is certified ISO/IEC 27001 by an accredited certification body. The scope covers the entire platform and services. Certificate available upon request.	**Certified**
Security Governance Structure	A formal security governance structure is in place, comprising a designated ISMS Manager, a Data Protection Officer (DPO), and a Security Committee that meets regularly to review security posture, risks, and compliance.	In place
Internal and External Audits	Annual internal ISMS audits are conducted. External surveillance and recertification audits are performed by the accredited certification body. Results are reviewed by Management through a formal Management Review.	In place

Category / Measure	Description	Implementation at Swibeco
Security KPIs and Dashboards	Key security performance indicators are tracked and reviewed regularly by the Security Committee to monitor the effectiveness of controls and drive continuous improvement.	In place
Information Security Policy (ISMS Policy)	A formal, board-approved Information Security Policy is in place, reviewed annually and communicated to all staff.	In place
Secure Development Policy	A dedicated Secure Development Policy defines mandatory security requirements throughout the software development lifecycle.	In place
IT Charter	An IT Charter governs acceptable use of company systems and tools, including specific provisions for the use of AI tools, binding on all employees and contractors.	In place
Access Management Policy	Formal policy governing the provisioning, modification, and revocation of access rights across all systems and environments.	In place
Incident Response Procedure	Documented incident response policy and procedure covering detection, escalation, containment, notification, and post-incident review.	In place
Risk Register and Periodic Risk Reviews	A formal risk register is maintained and reviewed on a regular basis. Risk assessments are systematically performed before launching new projects or products, integrating security and privacy by design from the outset.	In place
Data Protection Impact Assessments (DPIA)	DPIAs are conducted for all processing activities that are likely to result in a high risk to data subjects.	In place
Supplier Security Due Diligence	Security due diligence is conducted before onboarding any third-party vendor or sub-processor.	In place
Sub-processor Management	A Data Processing Agreement (DPA) is signed with every critical sub-processor prior to engagement. An up-to-date sub-processor inventory is maintained and subject to periodic review.	In place
Employee Onboarding and Offboarding	Formal onboarding procedure includes security and security training, NDA/confidentiality agreement, and background checks for sensitive roles. Offboarding procedure ensures timely revocation of all access rights and recovery of equipment upon departure.	In place
Access Review on Role Change	Access rights are systematically reviewed and updated when an employee changes role or department, ensuring alignment with the least-privilege principle.	In place
Confidentiality Agreements (NDA)	All employees and contractors with access to personal or confidential data sign a confidentiality agreement prior to being granted system access.	In place
Security Awareness Training	All employees complete mandatory security and awareness training at onboarding and on an annual basis. Regular refresher sessions are scheduled throughout the year. Phishing simulation campaigns are conducted periodically to test and reinforce awareness.	In place
8. Data Subject Rights		

Category / Measure	Description	Implementation at Swibeco
Rights Request Procedure	Documented process for handling requests for access, rectification, erasure, portability, restriction, and objection within legal deadlines.	In place
Pseudonymisation and Data Minimisation	Data minimisation principle applied (only strictly necessary data collected). Pseudonymisation applied where appropriate.	In place
Retention Periods	Retention periods defined per data category. Automated deletion applied at the end of the applicable retention period.	In place