Technical & Organizational Measures

1. INTRODUCTION

The present document supplements the Data Processing Agreement (DPA) between Client and Contractor pursuant to Art 28 GDPR (EU General Data Protection Regulation).

The technical and organizational measures are implemented by Welocalize in accordance with Art 32. They are continuously improved by Welocalize according to feasibility and state of the art and brought to a higher level of security and protection.

2. SCOPE

Confidentiality, integrity, availability and resilience, procedures for regular review, assessment and evaluation, organization and data protection at Welocalize.

3. DESCRIPTION

3.1. Confidentiality

3.1.1. Physical Access Control

Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

Technical Measures	Organizational Measures
Alarm system	Key regulation / List
Automatic access control system	Reception / Receptionist / Gatekeeper
Biometric access barriers	Visitors' book / Visitors' protocol
Smart cards / transponder systems	Employee / visitor badges
Manual locking system	Visitors accompanied by employees
Doors with knob outside	Care in selection of security guard personnel
Doorbell system with camera	Care in selection of cleaning services
Video surveillance of entrances	Information Security Policy
Biometric access control data center	Work instructions for operational safety
	Work instruction access control

3.1.2. Logical Access Control

Measures suitable for preventing data processing systems from being used by unauthorized persons.

Technical Measures	Organizational Measures
Login with username + strong password	User access control
Anti-Virus Software Servers	Creating user profiles
Anti-Virus Software Clients	Central password assignment
Anti-virus software mobile devices	Information Security Policy
Firewall	Mobile Device Policy
Intrusion Detection Systems	
Use of VPN for remote access	
Encryption of company smartphones	

Automatic desktop lock	
Encryption of notebooks / tablet	
Multi-factor authentication	

3.1.3. Authorization Control

Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

Technical Measures	Organizational Measures
Physical deletion of data carriers	Use of authorization concepts
Logging of accesses to applications, specifically when entering, changing, and deleting data	Minimum number of administrators
SSH encrypted access	Management of user rights by administrators
Certified SSL encryption	Information Security Policy
	Communication security policy

3.1.4. Separation Control

Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.

Technical Measures	Organizational Measures
Separation of productive and test environment	Control via authorization concept
Multi-tenancy of relevant applications	Determination of database rights
VLAN segmentation	Information Security Policy
Client systems logically separated	Data Protection Policy
Staging of development, test and production environment	Work instruction operational security
	Work instruction security in software development

3.1.5. Pseudonymization

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.

Technical Measures	Organizational Measures
log files are pseudonymized at the request of the client	Internal instruction to anonymize/pseudonymize personal data as far as possible in the event of disclosure or even after the statutory deletion period has expired
	Information Security Policy

	Data Protection Policy
	Specific internal regulations on cryptography

3.2. Integrity

3.2.1. Transfer Control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.

Technical Measures	Organizational Measures
Use of VPN where applicable	Survey of regular retrieval and transmission processes
Logging of accesses and retrievals	Transmission in anonymized or pseudonymized form
Provision via encrypted connections such as SFTP, HTTPS and secure cloud stores	Careful selection of transport personnel and vehicles
Use of signature procedures (case-dependent)	Personal handover with protocol
Encryption at rest using AES 256-bit encryption in addition to unique per-file keys	Information Security Policy
Encryption in transit utilizing HTTPS (TLS 1.2+) for web services, and TLS encryption for email transport	Data Protection Policy

3.2.2. Input Control

Measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems. Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).

Technical Measures	Organizational Measures
Technical logging of the entry, modification and deletion of data	Survey of which programs can be used to enter, change or delete which data
Manual or automated control of the logs (according to strict internal specifications)	Traceability of data entry, modification and deletion through individual usernames (not user groups)
	Assignment of rights to enter, change and delete data on the basis of an authorization concept
	Clear responsibilities for deletions
	Information Security Policy
	Work instruction IT user regulations

3.3. Availability and Resilience

3.3.1. Availability Control

Technical & Organizational Measures

Measures to ensure that personal data is protected against accidental destruction or loss (UPS, air conditioning, fire protection, data backups, secure storage of data media, virus protection, raid systems, disk mirroring, etc.).

Technical Measures	Organizational Measures
Fire and smoke detection systems	Backup concept
Fire extinguisher server room	No sanitary connections in the server room
Server room monitoring temperature and humidity	Existence of an emergency plan
Server room air-conditioning	Storage of backup media in a secure location outside the server room
UPS system and emergency diesel generators	Separate partitions for operating systems and data where necessary
Protective socket strips server room	Information Security Policy
RAID system / hard disk mirroring	Work instruction operational security
Video surveillance server room	
Alarm message in case of unauthorized access to server room	

3.3.2. Recoverability Control

Measures capable of rapidly restoring the availability of and access to personal data in the event of a physical or technical incident.

Technical Measures	Organizational Measures
Backup monitoring and reporting	Recovery concept
Restorability from automation tools	Control of the backup process
Backup concept according to criticality and customer specifications	Regular testing of data recovery and logging of results
	Existence of an emergency plan
	Information Security Policy
	Work instruction operational security

3.4. Procedures for regular Review, Assessment and Evaluation

3.4.1. Data Protection Management

Technical Measures	Organizational Measures
Central documentation of all data protection regulations with access for employees	Internal data protection officer appointed: Group Data Protection Officer, DPO
Security certification according to ISO 27001	Staff trained and obliged to confidentiality/data secrecy
A review of the effectiveness of the TOMs is carried out at least annually and TOMs are updated	Regular awareness trainings at least annually
Data protection checkpoints consistently implemented in tool-supported risk assessment	Internal Information Security Officer appointed: Group Information Security Officer, ISO

	Data Protection Impact Assessment (DPIA) is carried out as required
	Processes regarding information obligations according to Art 13 and 14 GDPR established
	Formalized process for requests for information from data subjects is in place
	Data protection aspects established as part of corporate risk management
	ISO 27001 certification of key parts of the company including data center operations and annual monitoring audits

3.4.2. Incident Response Management

Support for security breach response and data breach process.

Technical Measures	Organizational Measures
Use of firewall and regular updating	Documented process for detecting and reporting security incidents / data breaches (also with regard to reporting obligation to supervisory authority)
Use of spam filter and regular updating	Formalized procedure for handling security incidents
Use of virus scanner and regular updating	Involvement of DPO and ISO in security incidents and data breaches
Intrusion Detection System (IDS)	Documentation of security incidents and data breaches via ticket system
Intrusion Prevention System (IPS)	A formal process for following up on security incidents and data breaches
	Information Security Policy
	Data Protection Policy
	Work instruction operational security

3.4.3. Data Protection by Design and by Default

Measures pursuant to Art 25 GDPR that comply with the principles of data protection by design and by default.

Technical Measures	Organizational Measures
No more personal data is collected than is necessary for the respective purpose	Data Protection Policy (includes principles "privacy by design / by default")
Use of data protection-friendly default settings in standard and individual software	OWASP Secure Mobile Development Security Checks are performed
	Perimeter analysis for web applications

3.4.4. Order Control (outsourcing, subcontractors and order processing)

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

Technical Measures	Organizational Measures

Monitoring of remote access by external parties, e.g. in the context of remote support	Work instruction supplier management and supplier evaluation
Monitoring of subcontractors according to the principles and with the technologies according to the preceding chapters 1, 2	Prior review of the security measures taken by the contractor and their documentation where applicable
	Selection of the contractor under due diligence aspects (especially with regard to data protection and data security) where applicable
	Conclusion of the necessary data processing agreement on commissioned processing or EU standard contractual clauses
	Framework agreement on contractual data processing within the group of companies
	Written instructions to the contractor
	Obligation of the contractor's employees to maintain data secrecy
	Agreement on effective control rights over the contractor
	Regulation on the use of further subcontractors
	Ensuring the destruction of data after termination of the contract
	In the case of longer collaboration: ongoing review of the contractor and its level of protection

3.5. Organization and Data Protection at Welocalize

Welocalize has set itself the goal, among other things, of providing its customers with the products and services to be delivered at the highest possible level of information security in compliance with the law.

In this context, Welocalize has established a distinctive cross-sectional security organization to ensure comprehensive protection of its own corporate information and data as well as protection of the data of its customers and clients. The functions of Information Security Officer (ISO), Data Protection Officer (DPO), Quality Officer (QO), Risk Officer (RO) and Legal Compliance Officer (LCO) with group-wide responsibility and direct authority in these areas of activity have been established.

Employees are continuously informed and trained in the area of data protection. In addition, all employees are contractually bound to data secrecy and confidentiality. External parties who may come into contact with personal data in the course of their work for Welocalize are obligated to maintain secrecy and confidentiality as well as to comply with data protection and data secrecy by means of a so-called NDA (Non-Disclosure Agreement) before they begin their work.

Any subcontractors entrusted with further processing (as “other processors”) are only used after approval by the Client as the “controller” and after conclusion of a Data Processing Agreement (DPA) in accordance with Art 28 GDPR, with which they are fully bound by all data protection obligations to which Welocalize itself is subject.

All of these organizational measures are flanked by Welocalize current, high technical security standards, and both dimensions are periodically reviewed.

Technical & Organizational Measures

3.6. Certifications

Overview:

Measure	GDPR compliant implemented	Comments
Physical Access Control	✓	
Logical Access Control	✓	
Authorization Control	✓	
Separation Control	✓	
Pseudonymization	✓	
Transfer Control	✓	
Input Control	✓	
Availability Control	✓	
Recoverability Control	✓	
Data Protection Management	✓	
Incident Response Management	✓	
Privacy by Design and by Default	✓	
Order Control	✓	
Organization	✓	