

# Technical and Organizational Measures

Raiffeisen Rechenzentrum GmbH (RRZ)

Document owner	Raiffeisen Rechenzentrum GmbH
Version	1.1
Version date	06.12.2024
Status	Released
Confidentiality classification	Public

## Document control

Document control	
Title	Technical and Organizational Measures
Version	1.1
Status (draft / released)	released
Replaces version	
Owner	Raiffeisen Rechenzentrum GmbH
Revision date	06.12.2024
Date of the next revision	-
Dateiname	RRZ-DSGVO-techn-org-Massnahmen_EN.docx

## Document history

Revision date	Version Nr.	Changes	Authors
12.03.2018	1.0	Creation	DI Markus Hefler
06.12.2024	1.1	Adaptation to the new RRZ corporate identity (CI)	Prok. Matthias Bauernberger, MSc

## Dokumenten Freigabe

Release date	Version Nr.	Name	Role
12.03.2018	1.0	Dipl.-Ing. (FH) Dietmar Schlar, MBA	Geschäftsführung Raiffeisen Rechenzentrum GmbH
06.12.2024	1.1	Dipl.-Ing. (FH) Dietmar Schlar, MBA Dipl.-Ing. Wilfried Seyruck	Geschäftsführung Raiffeisen Rechenzentrum GmbH

## 1 CONFIDENTIALITY (ART 32 (1) LIT B DSGVO)

- **Entry control**

Protection against unauthorized entry to data processing systems, e.g. magnetic or chip cards, keys, electric door owners, security personnel, porters, alarm systems, video systems

- **Admission control**

Protection against unauthorized system use, e.g. (secure) passwords (including corresponding policy), automatic locking mechanisms, twofactor authentication, encrypting data carriers;

- **Access control**

No unauthorized reading, copying, changing or deletion within the system, e.g.: Standard authorization profiles on a "need-to-know basis", standard process for issuing authorizations, logging access, periodic review of the authorizations issued, especially administrative user accounts;

- **Separation control**

Separate processing data that has been collected for different purposes, e.g. multi-client capability, sand-boxing;

- **Pseudonymization (Art 32 (1) lit a DSGVO; Art 25 (1) DSGVO)**

If necessary or appropriate for the respective data processing, the primary identification features of the personal data are removed in the respective data application, so that the data can no longer be attributed to a concrete, respective person without adding additional information, and this additional information is stored separately and is subject to corresponding technical and organizational measures;

- **Classification scheme for data**

Complying with the classification scheme prescribed by the person responsible (e.g.: secret/confidential/internal/public); • Technical deletion concept settings Both for data and also for metadata such as log files, etc.;

- **Technical deletion concept settings**

Both for data and also for metadata such as log files, etc.;

## **2 INTEGRITY (ART 32 (1) LIT B DSGVO)**

- **Forwarding control**

No unauthorized reading, copying, changing or deletion during electronic transmission or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;

- **Input control**

Determining whether and by whom personal data has been input, changed or deleted in data processing systems, e.g.: Logging, document management;

## **3 AVAILABILITY AND CAPACITY (ART 32 (1) LIT B DSGVO)**

- **Availability control**

Protection against inadvertent or malicious destruction or loss, e.g.: Backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS, diesel generator), virus protection, firewall, reporting paths and emergency plans; security checks at the infrastructure and application level, multi-stage security concept with encrypted storage of backups in a different in computer center, standard processes for change/departure of employees;

- **Quick restorability (Art 32 (1) lit c DSGVO);**

## **4 PROCEDURE FOR REGULAR REVIEW, ANALYSIS AND EVALUATION (ART 32 (1) LIT D DSGVO; ART 25 (1) DSGVO)**

- **Data protection management**

Including regular employee training;

- **Incident response processes**

- **Data protection-friendly presets (Art 25 (2) DSGVO)**

- **Contract control**

No contract data processing as defined in Art 28 DSGVO without corresponding instruction from the person responsible, e.g.: Clear contractual structure, formalized control management, strict selection of the service provider, requirement to check in advance, follow-up checks.