Technisch-Organisatorische Maßnahmen

Raiffeisen Rechenzentrum GmbH (RRZ)

Dokument Eigentümer	Raiffeisen Rechenzentrum GmbH
Version	1.1
Versionsdatum	06.12.2024
Status	Freigegeben
Vertraulichkeitsklassifizierung	Öffentlich

Dokumentenkontrolle

Dokumentenkontrolle	
Titel	Technisch-Organisatorische Maßnahmen
Version	1.1
Status (Entwurf / Freigegeben)	Freigegeben
Ersetzt Version	
Eigentümer	Raiffeisen Rechenzentrum GmbH
Revisionsdatum	
Datum der nächsten Revision	-
Dateiname	RRZ-DSGVO-techn-org-Massnahmen.docx

Dokumenten Historie

Revisions-datum	Version Nr.	Änderungen	Autoren
12.03.2018	1.0	Initialversion	DI Markus Hefler
06.12.2024	1.1	Anpassung an neue RRZ-CI	Prok. Matthias Bauernberger, MSc

Dokumenten Freigabe

Freigabe-datum	Version Nr.	Name	Position
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

Raiffeisen Rechenzentrum GmbH - Firmensitz: Radetzkystraße 15, 8010 Graz - Zentrale: Raiffeisen-Platz 1, 8074 Raaba-Grambach, Firmenbuchgericht: Landesgericht für ZRS Graz, FN: 315298 z, UID: ATU64479157 - Betriebsstätte Linz: Goethestraße 84, 4020 Linz - Kontakt E-Mail: office@rrz.co.at, Tel.: +43 316 4002 8880

1 VERTRAULICHKEIT (ART 32 ABS 1 LIT B DSGVO)

- Zutrittskontrolle
  Schutz vor unbefugten Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Sicherheitspersonal, Portier, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
  Schutz vor unbefugter Systembenutzung, z.B.: (sichere) Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis", Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb. von administrativen Benutzerkonten;
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art 32 Abs 1 lit a DSGVO; Art 25 Abs 1 DSGVO)
  Sofern für die jeweilige Datenverarbeitung erforderlich oder zweckmäßig, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, sodass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer konkreten betroffenen Person zugeordnet werden können, und diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen entsprechenden technischen und organisatorischen Maßnahmen;
- Klassifikationsschema für Daten Beachtung der vom Verantwortlichen vorgegebenen Klassifikationsschemata (zB: geheim / vertraulich/ intern / öffentlich);
- Technische Löschkonzept-Einstellungen Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.;

Raiffeisen Rechenzentrum GmbH - Firmensitz: Radetzkystraße 15, 8010 Graz - Zentrale: Raiffeisen-Platz 1, 8074 Raaba-Grambach, Firmenbuchgericht: Landesgericht für ZRS Graz, FN: 315298 z, UID: ATU64479157 - Betriebsstätte Linz: Goethestraße 84, 4020 Linz - Kontakt E-Mail: office@rrz.co.at, Tel.: +43 316 4002 8880

2 INTEGRITÄT (ART 32 ABS 1 LIT B DSGVO)

- Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

- Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

3 VERFÜGBARKEIT UND BELASTBARKEIT (ART 32 ABS 1 LIT B DSGVO)

- Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;

- Rasche Wiederherstellbarkeit (Art 32 Abs 1 lit c DSGVO);

4 VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (ART 32 ABS 1 LIT D DSGVO; ART 25 ABS 1 DSGVO)

- Datenschutz-Management; einschließlich regelmäßiger Mitarbeiter-Schulung;
- Incident-Response-Prozesse;
- Datenschutzfreundliche Voreinstellungen (Art 25 Abs 2 DSGVO);
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Verantwortlichen, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrolle

Raiffeisen Rechenzentrum GmbH - Firmensitz: Radetzkystraße 15, 8010 Graz - Zentrale: Raiffeisen-Platz 1, 8074 Raaba-Grambach, Firmenbuchgericht: Landesgericht für ZRS Graz, FN: 315298 z, UID: ATU64479157 - Betriebsstätte Linz: Goethestraße 84, 4020 Linz - Kontakt E-Mail: office@rrz.co.at, Tel.: +43 316 4002 8880