R R
Z _

safe data,
great business.

TECHNISCH-ORGANISATORISCHE MASSNAHMEN IM RRZ

Raiffeisen Rechenzentrum GmbH

Dokument Eigentümer	RRZ GmbH
Version	1.0
Versionsdatum	14.03.2018
Status	FREIGEGEBEN
Vertraulichkeitsklassifizierung	Öffentlich

Dokumentenkontrolle

Dokumentenkontrolle	
Titel	Technisch-organisatorische Maßnahmen
Version	1.0
Status (Entwurf / Freigegeben)	FREIGEGEBEN
Ersetzt Version	-
Eigentümer	RRZ GmbH
Revisionsdatum	14.03.2018
Datum der nächsten Revision	-
Dateiname	DSGVO-techn-org-Massnahmen.docx
Anzahl Seiten	4
Druckdatum	22.05.2018 07:31:00

Dokumentenhistorie

Revisions-datum	Version	Änderungen	Autor	Editor	Begutachter	Genehmiger
12.03.2018	0.1	Erstellung	DI Markus Hefler	DI Markus Hefler	DI Ulfried Paier	DI Dietmar Schlar

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 (z.B.: geheim/vertraulich/intern/öffentlich);

- **Technische Löschkonzept-Einstellungen**
  Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.;

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, Nachkontrollen.