Technisch- Organisatorische Maßnahmen

Energy Services Handels- und Dienstleistungs G.m.b.H.

(in der Folge kurz „Energy Services“ genannt)

Dokument Eigentümer	Energy Services Handels- und Dienstleistungs G.m.b.H.
Version	1.0
Versionsdatum	22.05.2018
Status	
Vertraulichkeitsklassifizierung	Öffentlich

Ausgedruckte Dokumente unterliegen nicht der Dokumentenlenkung und erheben keinen Anspruch auf Gültigkeit. Gültigkeit hat ausschließlich die jeweils aktuelle elektronische Version der Dokumente, welche jederzeit unter https://www.energy-services.at/kontakt/ abrufbar ist

Dokumentenkontrolle

Dokumentenkontrolle	
Titel	Technische-organisatorische Maßnahmen
Version	1.0
Status (Entwurf / Freigegeben)	FREIGEGEBEN
Ersetze Version	-
Eigentümer	Energy Services Handels- und Dienstleistungs G.m.b.H.
Revisionsdatum	22.05.2018
Datum der nächsten Revision	-
Dateiname	DSGVO_tech-org-massnahmen_V1.docx
Anzahl Seiten	6
Druckdatum	23.05.2018 11:38

Dokumentenhistorie

Revisions-datum	Version	Änderungen	Autor	Editor	Begutachter	Genehmiger
11.05.2018	0.1	Erstellung	Czelecz	Czelecz		
18.05.2018	0.2	Überarbeitung	Czelecz	Czelecz	Brunner	
22.05.2018	1.0	Finales Review	Czelecz	Czelecz	Brunner, Pfeiler, Ulrich	Czelecz, Brunner

Inhaltsverzeichnis:

1 Präambel

Die Daten werden vorrangig in einem externen Rechenzentrum (Raiffeisen Rechenzentrum GmbH) verarbeitet. Die Energy Services bedient sich hierbei eine Housinglösung. Der Zugriff auf die im externen Rechenzentrum betriebene Infrastruktur erfolgt Engery Services seitig von einem Bürogebäude am Gelände des E Werk Gösting (via. einer Point2Point Verbindung). Die Kunden der Energy Services greifen via. VPN auf die - auf der Infrastruktur gehosteten – Softwarelösungen zu.

Die Technisch Organisatorischen Maßnahmen des Raiffeisen Rechenzentrums sind jederzeit unter https://www.rrz.co.at/datenschutz/ abrufbar.

In weitere Folge werden in diesem Dokument ergänzend die technisch organisatorischen Maßnahmen für

- Die IT Infrastruktur und Programme der Energy Services im externen Rechenzentrum
- den Zugriff auf die IT Infrastruktur sowie den
- Bürostandort der Energy Services

beschrieben. Dies Maßnahmen werden tlw. im Zuge der jährliche ISAE 3402 Typ 2 Überprüfung gebenchmarkt.

2 Vertraulichkeit (Art 32 Abs 1 lit b DSGVO)

2.1 Zutrittskontrolle

Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen:

- Schlüssel inkl. zentrale Schlüsselverwaltung und Dokumentation
- Schließregelung für Türen
- Sicherheitstüren mit Tür Knauf an Außenseite
- Besucher nur in Begleitung von Mitarbeitern
- Alarmanlagen
- Videoanlagen

2.2 Zugangskontrolle

Schutz vor unbefugter Systembenutzung:

- Kennwörter (einschließlich entsprechender Policy wie z.B. Passwortlänge, erzwungene Passwortänderung, Passwortkomplexität, etc.)
- Verwaltung von Benutzerbrechtigungen
- Automatische Sperrmechanismen und Anleitung „manuelle Desktopsperre“
- Verschlüsselung von Datenträgern

2.3 Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems:

- Standard-Berechtigungsprofile auf „need to know-Basis“
- Standardprozess für Berechtigungsvergabe inkl. Minimierung der Anzahl an Administratoren
- Protokollierung von Zugriffen
- Periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten
- Externer Aktenvernichter

2.4 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden. Basierend auf einer logischen / physikalischen Trennung auf IT Ebene und eine Mandantentrennung in der Software (über eine entsprechende Mandanten ID).

2.5 Pseudonymisierung

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.

2.6 Klassifikationsschema für Daten

Klassifikation aufgrund gesetzlicher Verpflichtungen oder Vorgabe durch den Verantwortlichen:

- Geheim
- Vertraulich
- Intern
- Öffentlich

3 **Integrität** (Art 32 Abs 1 lit b DSGVO)

3.1 Weitergabekontrolle

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

3.2 Eingabekontrolle

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

4 **Verfügbarkeit und Belastbarkeit** (Art 32 Abs 1 lit b DSGVO)

4.1 Verfügbarkeitskontrolle

N.a. für die Energy Services Büro Infrastruktur. Auszug aus den technisch organisatorischen Maßnahmen des externen Rechenzentrums sowie der Energy Services eigenen IT Infrastruktur.
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:

- Backup-Strategie (online/offline; on-site/off-site)
- Unterbrechungsfreie Stromversorgung (USV)
- 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;

4.2 Rasche Wiederherstellbarkeit

Betrieb einer redundant ausgelegten Lösung in zwei physikalisch getrennten Rechenzentren inkl. einer redundant ausgelegten Internetanbindung.

5 **Verfahren zur regelmäßigen Überprüfung und Evaluierung** (Art 32 Abs 1 lit d DSGVO; Art 25 Abs 1 DSGVO)

5.1 Datenschutz-Management

- Regelmäßige Mitarbeiter-Schulungen (inkl. Lernzielüberprüfung) im Zuge der Quartals Jour Fixe
- Laufenden Mitarbeitersensibilisierung
- Verpflichtung der Mitarbeiter zur Vertraulichkeit;

5.2 Incident-Response-Prozess

Unterstützung bei der Reaktion auf Sicherheitsverletzungen unter Einsatz von

- Firewalls
- Spam Filter
- Virenscanner
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
  inkl. regelmäßige Aktualisierung.

Weiters werden Sicherheitsvorfälle und Datenpannen in einem Ticketsystem dokumentiert und unterliegen einem formalen Prozess (auch in Hinblick auf Meldepflicht gegenüber Verantwortlichen und Aufsichtsbehörde).

5.3 **Datenschutzfreundliche Voreinstellung** (Art 25 Abs 2 DSGVO)

Bottom Up Prinzip bei der Rechtevergabe von neuen Usern. Weiters werden bei Energy Services nur jene personenbezogenen Daten erhoben die für den jeweiligen Zweck (insbesondere den Zugriff auf die IT Systeme durch die Verantwortlichen) erforderlich sind.

5.4 Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers:

- Eindeutige Vertragsgestaltung
- Formalisiertes Auftragsmanagement
- Strenge Auswahl des Auftragsverarbeiters
- Vorabüberzeugungspflicht, Nachkontrollen