RMPRIVACY
Datenschutz für Unternehmen

Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO

Dokumentenkontrolle

Ablageort: 3. Datenschutzkonzept (TOM)

Datum	Verfasser / Bearbeiter	Änderung
06.07.2022	RMPrivacy	Zusammenfassung aller TOMs

Die nachfolgend gelisteten technischen und organisatorischen Maßnahmen im Sinne vom Art. 32 Datenschutzgrundverordnung (DSGVO) haben für die gesamte **FinanzGeek GmbH**, **Frauenbergstrasse 31 – 33, 35039 Marburg** sowie für deren Unterauftragsdatenverarbeiter 1&1 IONOS SE und Telehouse Deutschland GmbH Gültigkeit.

A. Vertraulichkeit

1. Zutrittskontrolle

Maßnahmen, die verhindern, dass Unbefugte Zutritt (räumlich) zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden.

a. FinanzGeek GmbH

- Gebäude und Zu- und Ausgangssicherung
    - Alarmanlage

    - Bewegungsmelder
    - Schließanlage
    - Sicherheitsschlösser
- funktions- und rollenbasierte Zutrittsberechtigung

b. 1&1 IONOS SE

- Gebäude und Zu- und Ausgangssicherung
    - Alarmanlage
    - Einbruchmeldeanlage (EMA)
    - Bewegungsmelder
    - Schließanlage
    - Sicherheitsschlösser
    - Pförtner
    - Wachpersonal/Werkschutz
- funktions- und rollenbasierte Zutrittsberechtigung
- Videoüberwachungsanlage
- Firmenausweis
- Besucherregelung
    - persönliche Besucherführung

c. Telehouse Deutschland GmbH

- Gebäude und Zu- und Ausgangssicherung
    - Alarmanlage
    - Bewegungsmelder
    - Schließanlage
    - Sicherheitsschlösser
    - Schlüsselkonzept
- funktions- und rollenbasierte Zutrittsberechtigung
- unterteilte Bereiche in verschiedene Sicherheitszonen

2. Zugangskontrolle

Maßnahmen, die eine unbefugte Systembenutzung verhindern

a. FinanzGeek GmbH

- biometrischen Authentifizierung
- Zwei-Faktor-Authentifizierung
- Authentifizierung mit Benutzername und Passwort
    - automatische Sperrmechanismen, z.B. Passwortwiederholungssperre nach Fehlversuchen
    - Verschlüsselung von abgelegten Passwörtern
- Anti-Viren-Software
- Anti-Spam-Gateway
- Hardware-Firewall (IDS/IPS)
- Software-Firewall
- Verschlüsselung von Datenträgern und/oder externen Schnittstellen (USB, HDMI etc.)
- Verschlüsselung von mobilen Endgeräten
- Virtual Private Networks (VPN)
- Absicherung WLAN

- Netzwerksegmentierung

b. 1&1 IONOS SE

- biometrischen Authentifizierung
- Zwei-Faktor-Authentifizierung
- Authentifizierung mit Benutzername und Passwort
  - automatische Sperrmechanismen, z.B. automatische Sperre des Desktops nach wenigen Minuten Inaktivität
  - Verschlüsselung von abgelegten Passwörtern
  - Passwortrichtlinie zur Gewährleistung eines sicheren und vertraulichen Passworts
- Verschlüsselung von Datenträgern und/oder externen Schnittstellen (USB, HDMI etc.)
- Verschlüsselung von mobilen Endgeräten
- Virtual Private Networks (VPN)
- Mobile Device Policy
- Allgemeine Mitarbeiterrichtlinie zum Datenschutz und zur IT-Sicherheit (z.B. Clean-Desk-Policy)

c. Telehouse Deutschland GmbH

- Authentifizierung mit Benutzername und Passwort
  - Verschlüsselung von abgelegten Passwörtern
  - Passwortrichtlinie zur Gewährleistung eines sicheren und vertraulichen Passworts
- Verschlüsselung von Datenträgern und/oder externen Schnittstellen (USB, HDMI etc.)
- Verschlüsselung von mobilen Endgeräten
- Anti-Viren-Software
- Anti-Spam-Gateway
- Hardware-Firewall (IDS/IPS)
- Software-Firewall
- Virtual Private Networks (VPN)
- Mobile Device Policy
- Netzwerksegmentierung
- Allgemeine Mitarbeiterrichtlinie zum Datenschutz und zur IT-Sicherheit (z.B. Clean-Desk-Policy)

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass ausschließlich berechtigte Nutzung auf die betreffenden Daten zugreifen können. Der Zugriff auf die Daten wird so geschützt, so dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich ist.

a. FinanzGeek GmbH

- Begrenzung der Administratoren auf das erforderliche Minimum
- Funktions- und rollenbasiertes Berechtigungskonzept
  - Leseberechtigung
  - Schreibberechtigung
- bedarfsgerechte Zugriffsrechte

b. 1&1 IONOS SE

- Begrenzung der Administratoren auf das erforderliche Minimum
- Nutzung kryptografischer Verfahren (z.B. Verschlüsselung)

- Funktions- und rollenbasiertes Berechtigungskonzept
    - Leseberechtigung
    - Schreibberechtigung
- Verwaltung der Zugriffsberechtigung unter Beachtung der Funktionstrennung und des 4-Augenprinzips
- bedarfsgerechte Zugriffsrechte
- Einrichtung von Administratorarbeitsplätzen
- Protokollierung von Zugriffsversuchen
- Nutzung von Dokumentenvernichtung

c. Telehouse Deutschland GmbH

- Funktions- und rollenbasiertes Berechtigungskonzept
    - Leseberechtigung
    - Schreibberechtigung
- Verwaltung der Zugriffsberechtigung unter Beachtung der Funktionstrennung und des 4-Augenprinzips
- bedarfsgerechte Zugriffsrechte
- Protokollierung von Zugriffen
- Protokollierte Datenvernichtung
    - Ordnungsgemäße Vernichtung von Datenträgern
    - Ordnungsgemäße Vernichtung von Papier
    - Richtlinie zum Homeoffice/telearbeit

4. Trennungskontrolle

Maßnahmen die sicherstellen, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden getrennt verarbeitet werden.

a. FinanzGeek GmbH

- Festlegung von Datenbankrechten
- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung
- Trennung von Produktiv- und Testsystem

b. 1&1 IONOS SE

- Trennung von Produktiv- und Testsystem
- Personenbezogene Daten dürfen nicht für Testzwecke verwendet werden
- Logische Mandantentrennung
- Festlegung von Datenbankrechten
- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- **Pseudonymisierung**[1] (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO), d.h. die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

c. Telehouse Deutschland GmbH

- Trennung von Produktiv- und Testsystem
- Festlegung von Datenbankrechten
- **Pseudonymisierung**[2] (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO), d.h. die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.
    - Auswahl eines Verfahrens zur Pseudonymisierung

B. Integrität

1. Weitergabekontrolle

Wie gewährleisten Sie, dass ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei einer elektronischen Übertragung oder einem Transport verhindert wird?

a. FinanzGeek GmbH

- Verschlüsselung
    - Einsatz eines kryptographischen Verfahrens nach dem Stand der Technik
    - Verschlüsselung von Datenträgern und Laptops/Notebooks
    - Verschlüsselung von Inhalten auf Smartphones
    - Verschlüsselung von Passwörtern
- Datenaustausch über gesicherte Downloadplattform
- Virtual Private Networks (VPN)
- Verpflichtung der Mitarbeiter zur Verschwiegenheit

b. 1&1 IONOS SE

- Verschlüsselung
    - Einsatz eines kryptographischen Verfahrens nach dem Stand der Technik
    - Verschlüsselung von Datenträgern und Laptops/Notebooks
    - Verschlüsselung von Inhalten auf Smartphones
    - Verschlüsselung von Passwörtern
- Datenaustausch über gesicherte Kommunikationswege
- Weitergabe von Papierdokumenten mit personenbezogenen Daten in einem verschlossenen undurchsichtigen Umschlag
- Dokumentation der Weitergabe von physischen Speichermedien
- Virtual Private Networks (VPN)
- Verpflichtung der Mitarbeiter auf das Fernmeldegeheimnis (§ 88 TKG)

c. Telehouse Deutschland GmbH

- Verschlüsselung
    - Einsatz eines kryptographischen Verfahrens nach dem Stand der Technik
- Datenaustausch über gesicherte Downloadplattform
- Richtlinie zum Homeoffice/Telearbeit
- Verpflichtung der Mitarbeiter zur Verschwiegenheit

2. Eingabekontrolle

Können Sie feststellen, ob und von wem personenbezogene Daten in Ihr Datenverarbeitungssystem eingegeben, verändert oder entfernt worden sind?

a. FinanzGeek GmbH

- Funktions- und rollenbasiertes Berechtigungskonzept
    - Schreibberechtigung
- Dokumentenmanagement
- Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) → Benutzeridentifikation
- Klare Zuständigkeiten für Löschungen

b. 1&1 IONOS SE

- Funktions- und rollenbasiertes Berechtigungskonzept
    - Schreibberechtigung
- Dokumentenmanagement
- Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) → Benutzeridentifikation
- Klare Zuständigkeiten für Löschungen
- Nachvollziehbarkeit von Eingaben

c. Telehouse Deutschland GmbH

- Protokollierung der Eingabe, Veränderung und Löschung von Daten
- Funktions- und rollenbasiertes Berechtigungskonzept
- Dokumentenmanagement
- Klare Zuständigkeiten für Löschungen

C. Verfügbarkeit und Belastbarkeit

3. Verfügbarkeitskontrolle

Gewährleisten Sie den Schutz der Daten gegen mutwillige oder zufällige Zerstörung?

a. FinanzGeek GmbH

- Backup-Strategie (online/offline; on-site/off-site) [Bsp. NAS- System: verschlüsseltes Back UP Auslagerung bei einem externen Anbieter]
- Verschlüsselte Backupdatenträger
- Virenschutz
- Firewall
- Überwachung Zustand/Funktionen relevanter Systeme (Monitoring)

b. 1&1 IONOS SE

- unterbrechungsfreie Stromversorgung (USV)
- Überspannungsschutz-Stromversorgung
- Festplatten im RAID-Verbund
- Redundantes Netzteil
- Cluster
- Intrusion Detection System

- Überwachung Zustand/Funktionen relevanter Systeme (Monitoring)
- Regelmäßige Updates / Patchmanagement
- Externe Audits und Sicherheitstests
- Feuer- und/oder Rauchmelder verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr
- Definierte Sicherheitszonen
- Kühlsystem im Rechenzentrum/Serverraum
- Serverraumüberwachung Temperatur und Feuchtigkeit
- Keine sanitären Anschlüsse im oder oberhalb von Rechenzentren
- Alarmmeldung bei unberechtigtem Zutritt zu Rechenzentren

c. Telehouse Deutschland GmbH

- Virenschutz
- Firewall

4. Rasche Wiederherstellbarkeit

Setzen Sie Maßnahmen ein, welche die **Verfügbarkeit** der personenbezogenen Daten und den **Zugang** zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen?

a. 1&1 IONOS SE

- dokumentiertes Notfallkonzept

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Welche Prozesse und Abläufe haben Sie auf organisatorischer Ebene im Unternehmen umgesetzt, um die Sicherheit der Datenverarbeitung zu gewährleisten?

a. FinanzGeek GmbH

- Datenschutz-Management
    - Bestellung eines Datenschutzbeauftragten
- Datenschutzinformationen gemäß Art. 13, 14 DSGVO (Datenschutzerklärung)
- strenge Auswahl des Dienstleisters

b. 1&1 IONOS SE

- Datenschutz-Management
    - Bestellung eines Datenschutzbeauftragten
    - Richtlinie für Mitarbeiter zum Umgang mit Datenpannen
    - Richtlinie für Mitarbeiter zum Umgang mit Betroffenenrechten
    - zentrale Dokumentation aller Verarbeitungstätigkeiten
    - Durchführung von Datenschutz-Folgenabschätzungen bei Bedarf
- IT-Sicherheitsbeauftragter
- Etablierung einer Datenschutz- und Informationssicherheitsorganisation
- Schulungskonzept zum Datenschutz
- Auftragskontrolle, d.h. keine Auftragsdatenverarbeitung im Sinne von Art. 28, 29 DSGVO ohne entsprechende Weisung des Auftraggebers
- strenge Auswahl des Dienstleisters
- Weisungen zum Umgang mit personenbezogenen Daten werden in Textform dokumentiert

- Zertifizierung[3] der Rechenzentren nach dem ISO 27001 Standard
- Incident-Response-Management

c. Telehouse Deutschland GmbH

- Datenschutz-Management
    - Bestellung eines Datenschutzbeauftragten
    - Schulungskonzept zum Datenschutz
- IT-Sicherheitsbeauftragter
- Etablierung einer Datenschutz- und Informationssicherheitsorganisation
- Datenschutzinformationen gemäß Art. 13, 14 DSGVO (Datenschutzerklärung)
    - Zertifizierung nach ISO 27001 und ISO 27002
- Auftragskontrolle, d.h. keine Auftragsdatenverarbeitung im Sinne von Art. 28, 29 DSGVO ohne entsprechende Weisung des Auftraggebers
- Eindeutige Vertragsgestaltung
- Nachkontrollen