Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Informationen zum Dokument	
Version	1.0
Datum	07.02.2019
Dokumentenklassifikation	Öffentlich
Genehmigungsstatus	Genehmigt
Ursprungsversion freigegeben durch	Datenschutzbeauftragter 1&1
Aktuelle Version freigegeben durch	Konzerndatenschutzbeauftragter United Internet AG
Freigegeben am	07.02.2019

Hinweis

Dieses Dokument enthält Informationen, welche Geschäftspartnern, Kunden sowie weiteren externen Stellen, die ein gesetzliches oder sonstig begründetes Einsichtsrecht haben, zur Verfügung gestellt werden.

Aus Gründen der Lesbarkeit wurde im Text die männliche Form gewählt, nichtsdestoweniger beziehen sich die Angaben auf Angehörige aller Geschlechter.

Präambel

Der Verantwortliche hat geeignete Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert.

Der allgemeine Teil beschreibt technische und organisatorische Maßnahmen die unabhängig von den jeweiligen Dienstleistungen und Services, Standorten und Kunden gelten. In den Anhängen sind Maßnahmen beschrieben, die über die im allgemeinen Teil dokumentierten Maßnahmen hinaus gelten.

1. Vertraulichkeit

Vertraulichkeit ist die Eigenschaft, dass personenbezogene Daten unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.

Zutrittskontrolle

- Empfangs- und Sicherheitsdienst
- Individuelle, dokumentierte und rollenabhängige Zutrittsberechtigungen (Karten, Transponder und Schlüssel)
- Mitarbeiter- und Besucherausweise
- Besucher dürfen sich grundsätzlich nur in Begleitung eines Mitarbeiter im Gebäude aufhalten
- Alarm- und Einbruchmeldeanlage
- Büroräume sind außerhalb der Arbeitszeit verschlossen

Zugangskontrolle

- Formale Benutzer- und Berechtigungsverfahren
- Login nur mit Benutzername, Passwort und wo erforderlich 2-Faktor-Authentifizierung
- Systemisch forcierte Passwortrichtlinien
- VPN bei Remotezugriff und durch vom Verantwortlichen verwaltete Geräte
- Mobile Device Management
- Mobile Datenträger sind verschlüsselt
- Automatische Sperre von Desktops nach wenigen Minuten Inaktivität
- Clean Desk-Policy

Zugriffskontrolle

- Führen von Assetregistern und Ableitung von Maßnahmen anhand der Datenklassifikation
- Nutzung kryptografischer Verfahren (z.B. Verschlüsselung)
- Umsetzung von Berechtigungskonzepten nach dem Need-to-Know-Prinzip
- Trennung von Anwendungs- und Administrationszugängen
- Protokollierung von Zugriffsversuchen
- Einrichtung von Administratorarbeitsplätzen
- Minimale Anzahl an Administratoren
- Nutzung von Dokumentenvernichtung

Pseudonymisierung

- Sofern möglich oder erforderlich werden personenbezogene Daten pseudonymisiert verarbeitet (Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem System)

Trennungskontrolle

- Trennung von Entwicklungs-, Test- und Produktivumgebung
- Personenbezogene Daten dürfen nicht für Testzwecke verwendet werden

- Mandantenfähigkeit / logische Trennung von Daten bei relevanten Anwendungen: Separate Datenbanken, Schema-Trennung in Datenbanken, Berechtigungskonzepte und/oder strukturierte Dateiablage

2. Integrität

Die Integrität personenbezogener Daten ist dann gewahrt, wenn sie richtig, unverändert und vollständig sind.

Weitergabekontrolle

- Bereitstellung von Daten über verschlüsselte Verbindungen (z.B. SFTP)
- Weitergabe von personenbezogenen Daten im Sinne des Need-to-Know / Need-to-Do-Prinzips
- Personenbezogene Daten werde nach ihrem Schutzbedarf klassifiziert, wobei vertrauliche Daten nur über sichere Kommunikationswege übertragen werden dürfe
- Wo möglich wird E-Mailverschlüsselung eingesetzt
- Wo möglich werden personenbezogene Daten nur in pseudonymisierter oder anonymisierter Form übermittelt
- Dokumentation der Weitergabe von physischen Speichermedien
- Weitergabe von Papierdokumenten mit personenbezogenen Daten in einem verschlossenen undurchsichtigen Umschlag

Eingabekontrolle

- Technische Protokollierung der Eingabe, Änderung und Löschung von personenbezogenen Daten sowie Kontrolle der Protokolle
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
- Rollenbasiertes Berechtigungskonzept (Lese-, Schreib-, und Löschrechte)
- Protokollierung von administrativen Änderungen

3. Verfügbarkeit und Belastbarkeit

Die Verfügbarkeit von personenbezogenen Daten ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können

- Einsatz von Hardware- und Softwarefirewalls
- Intrusion Detection Systeme
- Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag
- Unterbrechungsfreie-Stromversorgung (USV)
- Notfallhandbücher für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust
- Durchführung von Wiederherstellungstests
- Wo notwendig Nutzung redundanter Systeme (z.B. RAID)
- Regelmäßiger Test von Datensicherungen
- Externe Audits und Sicherheitstests

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?

Datenschutz-Management

- Datenschutzbeauftragte und ein Informationssicherheitsbeauftragter sind benannt

- Etablierung einer Datenschutz- und Informationssicherheitsorganisation
- Alle Mitarbeiter sind auf die Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet und werden auf das Telekommunikationsgeheimnis hingewiesen
- Mitarbeiter sind im Umgang mit personenbezogenen Daten sensibilisiert
- Neue Mitarbeiter erhalten Informationsmaterial bezüglich dem Umgang mit personenbezogenen Daten
- Ein Verzeichnis von Verarbeitungstätigkeiten wird gepflegt und Datenschutzfolgenabschätzungen werden bei Bedarf durchgeführt
- Prozesse zur Wahrnehmung von Betroffenenrechten sind etabliert

Auftragskontrolle

- Daten die im Auftrag verarbeitet werden, werden nur nach Weisungen des Auftraggebers verarbeitet
- Auftragnehmer werden im Hinblick auf getroffene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten sorgfältig ausgewählt
- Weisungen zum Umgang mit personenbezogenen Daten werden in Textform dokumentiert
- Sofern erforderlich werden Auftragsverarbeitungsvereinbarungen bzw. geeignete Garantien zur Übermittlung von Daten an Drittländer geschlossen

Datenschutzfreundliche Voreinstellungen

- Es wird prozessual sichergestellt, dass Systeme und Produkte datenschutzfreundlich entwickelt werden
- Es werden nur diejenigen personenbezogenen Daten erhoben, die für den jeweiligen Zweck erforderlich sind

Incident-Response-Management

- Dokumentierter Prozess zur Erkennung, Meldung und Dokumentation von Datenschutzverletzungen unter Einbindung des Datenschutzbeauftragten
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen unter Einbindung des Informationssicherheitsbeauftragten

Anhang 1: Besondere technische und organisatorische Maßnahmen für Rechenzentren

- Alle Rechenzentren sind nach dem ISO 27001 Standard zertifiziert
- Elektronische Zutrittskontrollsysteme überwachen und gewährleisten den Zutritt zum jeweiligen Rechenzentrum nur für autorisierte Personen
- Sicherheitsschleuse
- Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes
- Definierte Sicherheitszonen
- Hochredundante Netzwerkinfrastruktur
- Feuer und/oder Rauchmelder verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr
- Kühlsystem im Rechenzentrum / Serverraum
- Serverraumüberwachung Temperatur und Feuchtigkeit
- Keine sanitären Anschlüsse im oder oberhalb von Rechenzentren
- Alarmmeldung bei unberechtigtem Zutritt zu Rechenzentren