Technische und organisatorische Maßnahmen
Anlage 2

EWERK Group

Brühl 24

04109 Leipzig

Inhaltsverzeichnis

Technische und organisatorische Maßnahmen

zur Gewährleistung der Ausführung des Bundesdatenschutzgesetzes, insbesondere die in der Anlage zu § 9 BDSG genannten Anforderungen

1. Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren

1.1 Lage der Räume

- DataCenter Leipzig; envia TEL GmbH; Leipziger Str.116 b; 04425 Taucha

1.2 Absicherung der Zugänge

- es findet ein mehrstufiges Zutrittssystem Verwendung. Zutritte zum DataCenter sind 24h im Voraus anzukündigen. Zutritt wird nur im Vorhinein autorisierten, bekannten Personen gewährt. Ein Live-Videobildabgleich mit hinterlegtem Foto findet beim Wachschutz statt.

1.3 Schließsysteme

- Zutritt zur Schleuse kann nach erfolgter Fotoidentifizierung nur mit Zutrittskarte und PIN erfolgen. Ein zweiter PIN ist erforderlich, um in den Serverhousingbereich zu gelangen. Die EWERK Kollokation ist nur mittels erneuter PIN-Eingabe zu betreten.

1.4 Überwachungseinrichtung

- Alarmanlage
- 24h Videoüberwachung

1.5 Zutrittskontrolle

- Zutritt zum Datacenter wird durch ein gesondertes Zutrittskonzept mit Durchführung personalisierter Zutritte gewährt. Bei Beendigung des Arbeitsverhältnisses erfolgt unmittelbarerer Entzug der Zutrittsberechtigung.
- Schriftliche Festlegung zur Zugangsberechtigung
- Ausweisregelung
- Trennung von Bearbeitungs- und Publikumszonen

- mehrstufiges Sicherheitszonenkonzept
- Besucherdokumentation, Aufzeichnung der Zutritte im Zutrittserfassungssystem
- Homeoffice-Richtlinie
- Reinigungsarbeiten nur bei Anwesenheit eines Mitarbeiters; kein Zutritt zu Serverräumen
- Es bestehen Regelungen bzgl. der Entziehung von Gebäudezutrittsberechtigungen und Zugriffsrechten zu Computersystemen inkl. Dokumentation für Mitarbeiter bei Beendigung des Arbeitsverhältnisses.

2. Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können

2.1 Firewall

- Zentral auf Router und Server
  Je nach konzeptioneller Ausführung kommen jeweils eine virtuelle interne Firewall (OpnSense) und eine externe Firewall (Cisco ASA 5545-X mit IPS) zum Einsatz
- Dezentral an jedem Arbeitsplatz

2.2 Virenschutz

- Dezentral an jedem Arbeitsplatz

2.3 Benutzeridentifikation und Passwortverfahren

- Anforderungen an Passwort in Passwort-Richtlinie geregelt; Passwort-Wechsel – soweit möglich – technisch erzwungen

2.4 Sperrung der Bildschirme mit Passwort in Pausen

- Anweisung Sperrung nach Verlassen des Arbeitsplatzes/Raumes
- Automatische Sperrung der Bildschirme der PC-Arbeitsplätze bei Nichtbenutzung des PC

2.5 Einrichtung eines Benutzerstammsatzes pro User

- pro User ein Account

2.6 Serverräume

- Täglich 24 Stunden verschlossen

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können

3.1 Berechtigungskonzept und Zugriffsrechte

- technische Umsetzung über Gruppen-Rollen-System

3.2 Schutz gegen unberechtigte Zugriffe

- technische Umsetzung über Gruppen-Rollen-System
- Firewall dezentral und zentral

3.3 Datenträger

- Clean-Desk-Policy
- Lagerung der Sicherungsdatenträger nach Dienstschluss außerhalb der Geschäftsräume in verschlossenen Schränken

3.4 Entsorgung/Vernichtung

- Vernichtung von IT-Datenträger durch IT-Verantwortlichen

- Entsorgung und Vernichtung der geschredderten Papierdatenträger (Schnittbreite 4mm; bei HR und Buchhaltung Partikelgröße) durch zertifiziertes Entsorgungsunternehmen gegen Entsorgungsbescheinigung

3.5 Regelung und Kontrolle von externer Wartung und Fernwartung

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist

4.1 Transportsicherung

- E-Mail-Verschlüsselung
- VPN (Virtual Private Network)

4.2 Lieferscheine/Quittierverfahren von Datenträgern

- Erfassung Ein- und Ausgang von Datenträgern

4.3 Dokumentation der Abruf- und Übermittlungsprogramme

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

5.1 Einsatz von revisionssicherer Software

5.2 Dokumentation sämtlicher Eingabeverfahren

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (vgl. § 11 BDSG).

6.1 Festlegung von Kriterien zur Auswahl der Auftragnehmer

- Sitz in Deutschland, Zertifizierung, möglichst nicht cloudbasiert

6.2 Regelungen in ADV-Verträgen

6.3 Formalisierte Auftragserteilung

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

7.1 Brandschutzeinrichtungen

- Feuerlöscher
- Rauchmelder
- Rauchverbot

7.2 Getrennte Aufbewahrung von Sicherungsdatenträgern

- Je nach konzeptioneller Ausführung: nächtlicher Bandabzug und räumlich getrennte Lagerung im Bankschließfach

7.3 Back Up Verfahren

- Backup aller Server im lfd. Betrieb auf externen NAS (Network Attached Storage)

- nächtlicher Bandabzug

7.4 Spiegeln von Festplatten

7.5 Virenschutz

- Je nach gewählter konzeptioneller Ausführung kommen Virenscanner für Server und zentrale Dienste wie E-Mail / FTP / Web zum Einsatz

7.6 Firewall

7.7 Wartung und Aktualisierung der Datenverarbeitungsanlagen

- Hardware-Reinigung
- Software-Aktualisierung nach Bereitstellung von Updates
- Einsatz konservativer Systeme

7.8 Service und Desaster Recovery

- Wiederherstellungskonzept: Je nach konzeptioneller Ausführung kann nach völliger Zerstörung des DataCenters ein Wiederanlauf innerhalb 4 Stunden (redundante Auslegung der Services) erfolgen. Bei nicht redundanter Auslegung ist die Wiederanlaufzeit abhängig vom gewählten Backupkonzept. Alle Betriebs- / Notfallhandbücher der Services sind einzeln einsehbar.

8. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

8.1 Regelungen/Maßnahmen zur Sicherstellung der getrennten Speicherung, Veränderung, Speicherung, Löschung, Übermittlung

- Jeder Auftrag wird separat angelegt, bearbeitet und abgelegt
- Keine Zusammenlegung von Daten

8.2 Interne Mandantenfähigkeit/Zweckbindung

8.3 Funktionstrennung

- Produktiv- und Testsystem laufen auf unterschiedlichen Servern
- Mitarbeiter werden schriftlich dazu verpflichtet, Informationen aus Datenbeständen des Auftraggebers nicht in andere Projekte/Zwecke mit einzubringen.

9. Organisation

Maßnahmen, die gewährleisten, dass die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird

9.1 it-sicherheitskonzept

- Schriftliche Regelungen über Betrieb und Abläufe der Datenverarbeitung

9.2 Standards für die IT-Sicherheit bzw. Abwicklung von IT-Projekten

- IT-Grundschutz
- Mitarbeiter werden schriftlich dazu verpflichtet, Informationen aus Datenbeständen des Auftraggebers nicht in andere Projekte/Zwecke mit einzubringen.
- Geregelt in „O I-RL 1 Datenschutz“ und „O I-VA 8-1 Regelwerk IT-Sicherheit“

9.3 Urlaubs- und Krankheitsvertretung der Geschäftsführung und des IT-Verantwortlichen

9.4 DV-Revision durch IT-Sicherheitsbeauftragten

9.5 Schriftliches Programmfreigabeverfahren

9.6 Regelungen über Sicherung des Datenbestands

9.7 Regelmäßige Hinweise und Ermahnungen, um Problembewusstsein zu fördern

9.8 Gelegentliche unvermutete Kontrolle der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen