TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

der eurodata AG

Großblittersdorfer Straße 257-259, 66119 Saarbrücken

(Stand: 15.03.2018)
nach DS-GVO Art. 32, ergänzt durch §64 BDSG-neu

eurodata hat in ihrem Rechenzentrum u.a. folgende technische und organisatorische Maßnahmen getroffen:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DS-GVO, (§64 Abs. 3) BDSG-neu

1.1 Zutrittskontrolle.

Der unbefugte Zutritt wird verhindert. Die Zutrittskontrolle wird im Empfang durch Empfangsmitarbeiter sichergestellt. Zusätzlich werden die folgenden technischen Maßnahmen insbesondere auch zur Legitimation der Berechtigten getroffen:

- Zutrittskontrollsystem (z.B. durch Ausweisleser, Magnetkarte, Chipkarte)
- Schlüssel/Schlüsselvergabe
- Türsicherung (elektronische Türöffner usw.)
- Überwachungseinrichtung (Alarmanlage, Video-/ Fernsehmonitor)

1.2 Zugangskontrolle.

Zugang zu den DV-Anlagen erhalten ausschließlich berechtigte Personen. Das Eindringen Unbefugter in die DV-Systeme wird verhindert durch technische (Kennwort-/Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Kennwortverfahren (z.B. Mindestlänge und regelmäßiger Wechsel des Kennworts)
- Automatische Sperrung
- Einrichtung eines Benutzerstammsatzes pro User
- Verschlüsselung von Datenträgern

1.3 Zugriffskontrolle.

Der Zugriff wird administrativ mittels Benutzerauthentifizierung über die Domain-Richtlinien geregelt. Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen werden durch bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung verhindert durch:

- Differenzierte Berechtigung (Profile, Rollen, Transaktionen und Objekte)
- Auswertung
- Kenntnisnahme
- Veränderung
- Löschung

1.4. Trennungskontrolle.

Daten, die zu unterschiedlichen Zwecken erhoben werden, werden auch getrennt verarbeitet. Folgende Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken werden ergriffen:

- Zweckbindung
- Funktionstrennung

1.5 Datenträgerkontrolle

Daten werden ausschließlich auf verschlüsselten Speichersystemen in den speziell abgesicherten Rechenzentren der eurodata gespeichert.

1.6 Speicherkontrolle

Durch ein umfangreiches Berechtigungskonzept wird sichergestellt, dass nur befugte Personen Zugang zu personenbezogenen Daten erhalten.

1.7 Benutzerkontrolle

Die Datenübertragung erfolgt ausschließlich über verschlüsselte Datenverbindungen, Virtual Private Networks (VPN).

2 Integrität /Art. 32 Abs. 1 lit. b) DS-GVO

2.1 Weitergabekontrolle.

Die Aspekte der Weitergabe personenbezogener Daten werden durch Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträgern (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung geregelt:

- Transportsicherung
- Protokollierung
- elektronische Signatur
- Verschlüsselung/Tunnelverbindung

2.2. Eingabekontrolle.

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege wird durch Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, gewährleistet:

- Protokollierungssysteme
- Protokollauswertungssysteme

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DS-GVO

3.1 Verfügbarkeitskontrolle (Art. 32 Abs. 1 lit. c)

Die Daten sind gegen zufällige oder mutwillige Zerstörung durch umfangreiche Backup-Strategien geschützt:

- Spiegeln von Festplatten (z.B. RAID- Verfahren)
- regelmäßiges Backup aller relevanten Daten.
- Spiegelung der Backups in ein Off-Site Rechenzentrum.
- Unterbrechungsfreie Stromversorgung (USV) und Notstromgeneratoren.
- Firewall
- Meldewege und Notfallpläne

3.2 Rasche Wiederherstellung (Art. 32 Abs1 lit. c) DS-GVO

Durch den Einsatz einer virtuellen Systemumgebung innerhalb einer redundanten Infrastruktur können personenbezogene Daten jederzeit rasch wiederhergestellt werden.

3.3 Zuverlässigkeit (§64 Abs. 3 Nr. 10) BDSG-neu

Die Verfügbarkeit und Funktion der für die Datenverarbeitung erforderlichen Systeme werden rund um die Uhr überwacht. Fehlfunktionen werden unverzüglich an den eurodata Bereitschaftsdienst gemeldet.

4. Verfahren zur regelmäßigen Überprüfung und Evaluierung (Art. 32 Abs. 1 lit. d; Art. 25 Abs. 1) DS-GVO

4.1 Datenschutz-Management

Durch regelmäßige interne und externe Audits der ISO 27001 Zertifizierung wird die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung überprüft.

4.2 Incident-Response-Management

Durch die ISO 22301 Zertifizierung wird ein effektives Managementsystem nachgewiesen um sich gegen Vorfälle mit Betriebsunterbrechung zu schützen, die Wahrscheinlichkeit ihres Auftretens zu vermindern, sich auf diese vorzubereiten, auf diese zu reagieren und sich von diesen zu erholen, sollten sie auftreten.

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Die Voreinstellungen in den einzelnen Programmen stellen sicher, dass nur solche personenbezogenen Daten verarbeitet werden können, die für den jeweiligen Verarbeitungszweck erforderlich sind.

4.4. Auftragskontrolle.

Die weisungsgemäße Auftragsdatenverarbeitung wird durch technische und organisatorische Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer gewährleistet:

- Eindeutige Vertragsgestaltung
- Formalisierte Vertragserteilung (Auftragsformular)
- Kriterien zur Auswahl des Auftragnehmers
- Kontrolle der Vertragsausführung
- Statusbericht des Auftragnehmers