Anlage – Technisch-organisatorische Maßnahmen – Brunner & Schmidt Datentechnik GmbH (Büro-Standorte)

[Stand: 2023]

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a. Zutrittskontrolle

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

Technische Maßnahmen:

- Festlegung der Sicherheitsbereiche
- Digitales Schließsystem (Berechtigungsverwaltung), Chipkarten / Transponder-Schließsystem, Sicherheitsschlösser
- Lichtschranken / Bewegungsmelder
- Automatisches Zutrittskontrollsystem
- Videoüberwachung der Zugänge

Organisatorische Maßnahmen:

- Personenkontrolle beim Empfang
- Schlüsselregelung / Schlüsselbuch (Digital)
- Personelle und organisatorische Zutrittskontrollmaßnahmen

b. Zugangskontrolle

Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen:

- Authentifikation mit Benutzer + Passwort, Zwei-Faktor Authentifizierung, Authentifikation mit biometrischen Daten
- Einsatz von Anti-Viren-Software
- Einsatz von Managed-Firewalls
- Einsatz von VPN-Technologie
- Einsatz von Mobile Device Management
- Verschlüsselung von Datenträgern

Organisatorische Maßnahmen:

- Benutzerberechtigungen verwalten, Erstellen von Benutzerprofilen
- Passwortvergabe / Passwortvorgaben erzwungen
- Personenkontrolle beim Empfang
- Schlüsselregelung / Schlüsselbuch (Digital)
- Sorgfältige Auswahl von Reinigungspersonal

c. Zugriffskontrolle

Gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten

ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen:

- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Verschlüsselung von Datenträgern
- Einsatz von Anti-Viren-Software
- Einsatz von Managed-Firewalls
- Einsatz von Mailschutzsystemen
- Einsatz Mail-Archivierung
- Zwei-Faktor Authentifizierung
- Ordnungsgemäße Vernichtung von Daten-trägern (DIN 66399), Einsatz von Aktenvernichtern
- Physische Löschung von Datenträgern vor deren Wiederverwendung
- Protokollierung der Vernichtung von Daten

Organisatorische Maßnahmen:

- Anzahl der Administratoren auf das „Notwendigste“ reduzieren
- Berechtigungskonzept
- Passwortrichtlinie inkl. Länge, Komplexität und Wechsel
- Regelmäßige Kontrolle der Benutzerrechte durch Systemadministratoren
- Einsatz von Dienstleistern zur Akten- und Datenvernichtung (mit Zertifikat)

d. Trennungskontrolle

Gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen:

- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Trennung von Produktiv- und Testsystem
- Verschlüsselung von Datensätzen
- Verschlüsselung von Datensätzen

Organisatorische Maßnahmen:

- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Logische Mandantentrennung (softwareseitig)
- Versehen der Datensätze mit Zweckattributen/Datenfeldern

e. Pseudonymisierung

Gewährleisten, dass die Pseudonymisierung, nach Art. 4 Nr. 5 DSGVO, die Identität der verarbeiteten Daten der Personen schützt, sodass keine Rückschlüsse auf eine konkrete Person möglich sind. Pseudonymisieren ist das Ersetzen des Namens und anderer

Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Organisatorische Maßnahmen:

- Prinzip der Datenminimierung wird ergriffen, d.h. Daten werden für die Zwecke der Verarbeitung notwendiger Maß beschränkt sein

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

a. Weitergabekontrolle

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.

Technische Maßnahmen:

- Einrichtungen von VPN-Technologie
- E-Mail-Verschlüsselung (Zertifikatsbasiert)
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Einsatz von Mailschutzsystemen

Organisatorische Maßnahmen:

- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

b. Eingabekontrolle

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

Technische Maßnahmen:

- Einsatz von revisionssicheren Archivsystemen, z.B. Mailarchivierung, DMS, DATEV-Belegarchiv

Organisatorische Maßnahmen:

- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

a. Verfügbarkeitskontrolle

Gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen:

- Feuerlöschgeräte in Serverräumen
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Unterbrechungsfreie Stromversorgung (USV)
- Redundante Daten / Datenträger / Datenverarbeitungssysteme
- Monitoring
- Archivierungssysteme intern/extern
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Einsatz von Datensicherung

Organisatorische Maßnahmen:

- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Erstellen eines Backup- & Recoverykonzepts
- Erstellen eines Notfall-Konzepts
- Testen von Datenwiederherstellung
- Serverräume nicht unter sanitären Anlagen

b. Rasche Wiederherstellbarkeit

Gewährleistet, dass nach einem physischen oder technischen Zwischenfall die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen rasch wiederhergestellt werden kann. Sowie, dass die Wiederherstellbarkeit in regelmäßigen Abständen getestet wird.

Organisatorische Maßnahmen:

- Aktuelle Datensicherung und Kontrolle
- Errichtung eines Notfall-Konzepts
- Erstellung von Notfallplänen, sowie Handlungsanweisungen (Leitfäden)
- Regelmäßiger Termin der Datensicherung
- Datenrücksicherungstests
- Penetrationstest
- Verfügbarkeit von Ersatzhardware

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

a. Datenschutz-Management

Gewährleistet, dass die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicher zu stellen.

Organisatorische Maßnahmen:

- Nachweis, dass das Unternehmen angemessene und wirksame Maßnahmen ergreift, um datenschutzrechtliche Verpflichtungen und Grundsätze umzusetzen (Datenschutzkonzept)
- Erstellung des Datenschutzkonzeptes Soll-Ist-Abgleich (Datenschutz-Audit)
- Verantwortliche der Bereiche festlegen
- Mitarbeiterschulung zum Thema Datenschutz
- Regelmäßige Überprüfung des Datenschutzes im laufenden Betrieb

b. Incident-Response-Management

Gewährleistet, dass Maßnahmen und Prozesse auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT-Bereichen ergriffen werden. Das IT-Störungsmanagement berücksichtigt dabei technische Probleme, sowie konkrete Angriffe auf die IT-Infrastruktur. Ziel ist die möglichst rasche Wiederherstellung des Systems.

Organisatorische Maßnahmen:

- Festlegung von Verantwortungsbereichen und Ansprechpartnern in allen Abteilungen/Bereichen des Unternehmens
- Mechanismen zur frühzeitigen Erkennung und Meldung von Sicherheitsvorfällen
- Vorliegen eines Notfall-Konzepts

c. Datenschutzfreundliche Voreinstellungen

Gewährleistet, dass Grundeinstellungen von Produkten und Diensten so gestaltet sind, dass möglichst wenig personenbezogene Daten erhoben oder verarbeitet werden. Sind Voreinstellungen schon vorhanden so ist zu gewährleisten, dass beim Zeitpunkt der Verarbeitung geeignete technische und organisatorische Maßnahmen ergriffen werden, z.B. Pseudonymisierung, Datenminimierung

Organisatorische Maßnahmen:

- Prinzip der Datenminimierung wird ergriffen, d.h. Daten werden für die Zwecke der Verarbeitung notwendiger Maß beschränkt sein

d. Auftragskontrolle

Gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Organisatorische Maßnahmen:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Schriftliche Weisungen an den Auftragnehmer durch Auftragsdatenverarbeitungsvertrag gemäß Art. 28 DS-GVO
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Verpflichtung der Mitarbeiter des Auftrag-nehmers auf das Datengeheimnis (§ 53 BDSG)
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbaren

Anlagen:

– Technisch-organisatorische Maßnahmen –
Hetzner RZ