keeen

Anlage Datenschutz

GEGENSTAND UND ZWECK DER VERARBEITUNG

Je nach Beauftragung werden durch den Auftragnehmer folgende Arbeiten und/oder Leistungen erbracht:

- Hosting, Administration und Weiterentwicklung der Webportale des Auftraggebers
- Hosting, Administration und Weiterentwicklung von Mobile Apps oder digitalen Ökosystemen für den Auftraggeber
- Administration und Einrichtung von Marketing Automation Systemen
- Bereitstellung eines Consent-Management-Tools in den Webportalen des Auftraggebers
- Versand von Newslettern für den Auftraggeber
- Versand von Direktmarketing für den Auftraggeber (z. B. Kundenmagazin)

I. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Logfiles, Nutzungs- und Protokolldaten
- Nutzerberechtigungen und Zugangsdaten
- E-Mail-Adressen
- Name, Kontaktdaten, Versandadressen
- Analyse- und Trackingdaten

II. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

- Websitebesucher
- Nutzer
- Mitarbeiter des Auftraggebers
- Interessenten und Kunden des Auftraggebers
- ggf. sonstige Dritte

III. Unterauftragnehmer

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).
Je nach Umfang der Beauftragung handelt es sich dabei um nachfolgende Unternehmen:

Hosting:

- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen

Administration:

- Mitting UG, Ostseeallee 100a, 23946 Boltenhagen

Consent-Management-Tool:

- Usercentrics A/S, Havnegade 39, 1058 Copenhagen, Dänemark

IV. Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

Grundlegende Informationen:

Das Hosting von Servern erfolgt bei zertifizierten Dienstleistern, mit denen ein Auftragsverarbeitungsvertrag abgeschlossen wurde. In den Unternehmensräumen werden keine Server betrieben.

1. Zutrittskontrolle

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

- Schlüsseldokumentation
- Manuelles Schließsystem

- Sicherheitsschlösser
- Besucherprotokollierung (Standort Wolfsburg)
- Videoüberwachung (Standort Wolfsburg)
- Alarmanlage (Standort Wolfsburg)
- Grundstück nur durch verriegeltes Tor zu betreten (Standort Wolfsburg)

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Individuelle Zugangsberechtigungen
- Zentrales Berechtigungsmanagement
- Dokumentation der Berechtigungen
- Sperrung von Benutzeraccounts bei wiederholter Falscheingabe
- Hardware-Firewall
- Anti-Viren-Software
- Software-Firewall
- Administration von Geschäftshandys
- Automatische Bildschirmsperre mit Passwortschutz

3. Zugriffskontrolle

Maßnahmen, die 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.

- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Authentifikation mit individueller Nutzer-/Passwortkombination
- Zentrales Berechtigungsmanagement
- Differenzierte Berechtigungen
- Dokumentation der Berechtigungen

- Mindestanforderungen Passwörter
- Passwortmanager
- Verschlüsselung mobiler Datenträger
- Verschlüsselung mobiler IT-Systeme
- Regelmäßige Updates und Patches
- Regelmäßige Überprüfung von Benutzerrollen
- Aktenschredder bzw. Aktenentsorgung durch Dienstleister
- Clean Desk Policy

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.

- Einrichtung von Standleitungen bzw. VPN-Tunneln
- Beim physischen Transport: sichere Transportbehälter/-verpackungen
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen, Nachverfolgung

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.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen

6. Auftragskontrolle

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

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Abschluss von Auftragsverarbeitungsverträgen nach Art. 28 DSGVO
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datenschutz und Vertraulichkeit
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

7. Verfügbarkeitskontrolle

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

- Unterbrechungsfreie Stromversorgung (USV)
- Notfallplan
- Verschlüsselung von Datensicherungen
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Feuerlöschgeräte werden regelmäßig gewartet, zusätzlicher Feuerlöscher in Serverräumen (Netzwerkanlagen)
- Feuer- und Rauchmeldeanlagen (Standort Wolfsburg)
- Backup- & Recoverykonzept
- Datenhosting in zertifizierten deutschen Rechenzentren

8. Trennungsgebot

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

- Festlegung von Datenbankrechten
- Logische Mandantentrennung
- Trennung von Produktiv- und Testsystem
- In allen DEV-Environments werden grundsätzlich Testdaten genutzt.

9. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Schulungen
- Benennung Datenschutzbeauftragter
- Leitlinie Datenschutz
- Verarbeitungsverzeichnis
- Datenschutzrichtlinie
- Vertraulichkeitsverpflichtung der Mitarbeiter

10. Maßnahmen im Homeoffice

- Keine lokale Datenspeicherung
- Keine Papierunterlagen
- komplexe Password-Policy und/oder biometrische Verfahren (2FA wo möglich)
- Einsatz von zentral gesteuerter Endpoint-Überwachung
- Einsatz von zentral gesteuerter Sicherheitssoftware
- Verschlüsselung von SSDs
- VPN-Tunnel für kritische Verbindungen