Stand: 15.05.2021

Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Der Auftragsverarbeiter setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

I. Zweckbindung und Trennbarkeit

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Durch Virtualisierung (sowie teilweise physikalisch) getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Berechtigungskonzept
- Trennung von Produktiv- und Testsystem

II. Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragsverarbeiters:

1. Verschlüsselung

Die im Auftrag verarbeiteten Daten bzw. Datenträger werden in folgender Weise verschlüsselt:

Alle Arbeitsrechner werden nach dem Stand der Technik vollverschlüsselt. Backups der Arbeitsrechner sind ebenfalls verschlüsselt, sodass ein Diebstahl der Datenträger keine sensiblen Daten offenlegen würde. Verbindungen zu unseren Servern, Verwaltungsoberflächen und sonstigen Systemen finden ausschließlich verschlüsselt statt (Einsatz von SSH, HTTPS, allgemein TLS / SSL).

Für unsere Kunden erreichbare Verwaltungsoberflächen sind ausschließlich über verschlüsselte Verbindungen erreichbar.

2. Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern **(Zutrittskontrolle)**:

2.1 Maßnahmen in den Rechenzentren

- Alarmanlage
- Absicherung von Gebäudeschächten
- Automatisches Zugangskontrollsystem
- Chipkarten-/Transponder-Schließsystem

- Schließsystem mit Codesperre
- Manuelles Schließsystem
- Biometrische Zugangssperren (Venenscanner) kombiniert mit schriftlichen Zutrittslisten und Ausweiskontrolle bei jedem Zutritt
- Erfassung neuer Venenscans zur Ergänzung permanenter Zutrittsberechtigungen ausschließlich über Zwei-Faktor-Authentifizierung (die Vorlage eines gültigen Personalausweises ist nicht ausreichend)
- Videoüberwachung der Zugänge
- Lichtschranken / Bewegungsmelder
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Empfang
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Besucherausweisen
- Zutrittskonzept / Besucherregelung

2.2 Maßnahmen am Firmensitz

- Sorgfältige Auswahl von Reinigungspersonal
- Sicherung des Businessparks über einen Sicherheitsdienst
- Ein Zutritt zu unseren Büroflächen ist grundsätzlich nur bei Anwesenheit mindestens eines Geschäftsführers möglich. Etwaige Gespräche mit Kunden, Lieferanten, Bewerbern etc. finden ausschließlich in einem Konferenzraum statt, in dem keine Support-Tätigkeiten wie Telefonate und Ticketbearbeitung ausgeführt werden. Weitere „Gäste“ werden nicht empfangen. Die Räumlichkeiten innerhalb des Büros sind gesondert abschließbar, sodass auch bei Anwesenheit weiterer autorisierter Personen keine Berührung mit personenbezogenen Daten (beispielsweise auf Bildschirmen oder in Form von Schriftstücken) stattfindet. Zu entsorgende Dokumente werden in einem Aktenvernichter geschreddert, aufzubewahrende Dokumente in einem Aktenschrank verschlossen, der nur von der Geschäftsführung geöffnet werden kann.

3. Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern **(Zugangskontrolle)**:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge und Komplexitätsanforderungen nach dem Stand der Technik)
- Authentifikation mit Benutzername / Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Verschlüsselung mobiler IT-Systeme
- Verschlüsselung mobiler Datenträger
- Verschlüsselung der Datensicherungssysteme
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Pförtner / Empfang

- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Besucherausweisen
- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Software-Firewall

4. Es wurden folgende Maßnahmen getroffen, 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 **(Zugriffskontrolle):**

   - Berechtigungskonzept
   - Verwaltung der Rechte durch Systemadministrator
   - regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)
   - Anzahl der Administratoren ist auf das „Notwendigste“ reduziert
   - Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel, Komplexitätsanforderungen
   - Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
   - Sichere Aufbewahrung von Datenträgern
   - physische Löschung von Datenträgern vor Wiederverwendung
   - ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
   - Einsatz von Aktenvernichtern
   - Verschlüsselung von Datenträgern

5. Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind **(Eingabekontrolle).**

   - Protokollierung der Eingabe, Änderung und Löschung von Daten
   - Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
   - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

6. Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können **(Auftragskontrolle).**

   - Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
   - vorherige Prüfung der und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen

- schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart
- laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten

7. Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können **(Transport- bzw. Weitergabekontrolle)**:

    - Einsatz von SSH-Jump-Hosts
    - Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des E-Mail-Verkehrs)
    - Verschlüsselung physischer Datenträger bei Transport

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

- Unterbrechungsfreie Stromversorgung (USV)
- Klimatisierung der Serverräume
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Server- und Büroräumen
- Feuer- und Rauchmeldeanlagen in Serverräumen
- Feuerlöschgeräte in Server- und Büroräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Einsatz von RAID-Systemen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort (Speicherung auf physikalisch getrenntem System)
- Serverräume nicht unter sanitären Anlagen
- Betrieb von regelmäßig erweiterten Echt- und Langzeitmonitoringsystemen
- DDoS-Protection
- Überkapazitäten im Netzwerk
- Hochverfügbares Rechenzentrum: maincubes FRA01
- ISO 27001-Zertifizierung des vorgenannten Rechenzentrums
- TÜV-Zertifizierung Verfügbarkeitsklasse 3 nach DIN EN 50600 des vorgenannten Rechenzentrums

IV. Besondere Datenschutzmaßnahmen

Es liegen schriftlich vor:

- Zertifikat: ISO 27001-Zertifizierung maincubes FRA01

- Zertifikat: Verfügbarkeitsklasse 3 nach DIN EN 50600, auditiert durch den TÜV Saarland maincubes FRA01

V. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von einem Jahr und anlassbezogen prüfen, evaluieren und bei Bedarf anpassen.

Die aktuelle Liste der Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO wird unter https://php-friends.de/tom bereitgestellt.