Anlage zur Auftragsdatenverarbeitung

V2.0

Technische und organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, treffen der Auftraggeber und der Auftragnehmer die nachfolgenden technischen und organisatorischen Maßnahmen (TOM). Diese gelten für die im Hauptvertrag definierten IT-Leistungen, welche durch den Auftragnehmer erbracht werden.

Bei der Auswahl der Maßnahmen wurden die vier Schutzziele des Art. 32 Abs. 1 b) DSGVO, namentlich die Vertraulichkeit, die Integrität, die Verfügbarkeit, sowie die Belastbarkeit der Systeme berücksichtigt. Eine schnelle Wiederherstellung nach physischen, oder technischen Zwischenfällen ist gewährleistet. Alle technischen und organisatorischen Maßnahmen werden regelmäßig gemäß Art. 32 Abs 1 d) DSGVO auf Ihre Wirksamkeit hin geprüft.

1. Pseudonymisierung

Die Pseudonymisierung oder Anonymisierung von personenbezogenen Daten ist kein Bestandteil der vom Auftragnehmer für den Auftraggeber erbrachten Leistugen, sofern dies nicht anderlautend im Hauptvertrag festgehalten wurde. Werden vom Aufragnehmer „Analytics“ Daten mit Hilfe von „Matomo“ für den Auftraggeber gesammelt, so werden alle Daten durch Entfernen des letzten IP Octetts anonymisiert.

2. Verschlüsselung

Alle Arbeitsgeräte des Auftragnehmers sind verschlüsselt. Zugriffe auf Server und Systeme durch den Auftragnehmer erfolgen ausschließlich über verschlüsselte Kanäle (VPN / SSL).

3. Vertraulichkeit

a. Zutrittskontrolle

Maßnahmen, die Unbefugte den Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren:

Der Zutritt zu den Servern erfolgt ausschließlich zu notwendigen Wartungszwecken. Physischen Zugang zu den Servern haben ausschließlich Mitarbeiter des Auftragnehmers, sowie Mitarbeiter des beauftragten Rechenzentrums, oder von diesen beauftragten Unternehmen, zu notwendigen Wartungstätigkeiten. Das beauftragte Rechenzentrum sorgt für Zutrittskontrollen gemäß ISO27001 und PCI-DSS, sowie für die Einhaltung aller relevanten Kriterien zur Erfüllung der DSGVO.

b. Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- **Verbindungssicherheit:**
  - Der Zugriff auf Server erfolgt ausschließlich per verschlüsselter SSH Verbindung
  - In öffentlichen Netzwerken wird vor einer Verbindung zu Servern oder Unternehmenssystemen erst ein sicherer, verschlüsselter VPN Kanal zum Firmennetzwerk des Auftragnehmers aufgebaut
- **Kennwortverfahren:**
  - Der Login am Server findet primär per sicherem Public-Key-Verfahren statt. Die unsichere Übermittlung eines Passwortes im Klartext findet nicht statt.
  - Alle verwendeten Schlüssel weisen eine Mindestlänge von 2048 bits auf. Alle neuen Schlüssel weisen eine Mindestlänge nach aktuellem Stand der Technik auf. Die Verschlüsselung erfolgt mit dem RSA Algorhythmus
- **Hardwaresicherheit:**
  - Alle eingesetzten Arbeitsgeräte des Arbeitnehmers sind mit hardwareseitig verschlüsselten Festplatten ausgestattet, die über Microsoft Bitlocker verschlüsselt werden
  - Tragbare Geräte sind darüber hinaus per TPM oder vergleichbare Sicherheitschips gesichert, die selbst bei einem Verlust der Hardware einen Zugriff auf die Daten ohne Passwort unmöglich machen
  - Tragbare Geräte werden darüber hinaus mit biometrischen Merkmalen abgesichert und mit alphanumerischen Passwörtern > 10 Zeichen versehen
- **Berechtigungskonzept:**

- Jeder Mitarbeiter und Dienstleister, der Zugriff auf die Server benötigt, bekommt einen persönlich zugeordneten Account mit den minimal erforderlichen Rechten für seinen Einsatzzweck
- Mitarbeiter erhalten über technisch geeignete Maßnahmen Zugriff auf erweiterte Rechte, so wie diese benötigt werden. Ein genereller Zugriff mit vollen Rechten wird keinem persönlichen User eingeräumt.

c. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungs-systeme 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:

- Zugriffschutz per Unix Systemberechtigungen
- Feingranulare Zuweisung von Benutzern und Gruppen auf Dateisystemebene
- Einsatz von SELinux
- Überwachung auf anomale Zugriffmuster mittels Intrusion Detection

d. Weitergabekontrolle

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

- **Verschlüsselung:**
  - Einsatz kryptographischer Verfahren wie beispielsweise getunnelte Datenfernverbindungen (VPN) mit 256 AES Verschlüsselung oder elliptischer Kurven
  - Zugriff auf Webanwendungen über SSL Verbindung mit mindestens 2048bits
- **Protokollierung:**
  - Protokollierung von Logins und Zugriffen auf die Systeme

e. Eingabekontrolle

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

- **Protokoll aller Systemzugriffe**
  - Jeder Login auf den Servern wird protokolliert
  - Jeder Login in die Datenspeichernden Systeme wird protokolliert
  - Alle Aktionen der persönlichen Benutzer werden protokolliert

f. Trennungskontrolle

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

- Daten werden in Datenbanken und Dateisystem-Ordnern gespeichert, die einem dedizierten Benutzer zugeordnet sind und eine logische Trennung von Kundendaten und deren Verarbeitungszweck ermöglichen

4. Integrität

- Feingranulares Berechntigungsprinzip unter dem Minimalprinzip
- Automatische Sperrung aller PCs / Smartphones mit Kennwortschutz
- Protokollierung aller Zugriffe auf Anwendungen und IT-Systeme der Hive-IT

5. Verfügbarkeit

a. Verfügbarkeitskontrolle

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

- Tägliches Back-Up von Daten und Datenbanken
- Pull-Backup auf externe Systeme
- Redundante Auslegung kritischer Hardwarekomponenten (insb. Festplatten, Netzteile)
- Ausfallsicherer Betrieb von Festplatten (RAID)
- Backup aller Firmendaten auf verschlüsseltem lokalen Speicher, sowie zusätzlich verschlüsselt vor dem Upload in eine gesicherte Cloud als redundantes Backup
- Virenschutz / Firewall / Intrusion Detection auf allen Systemen

6. Belastbarkeit

Die unter Ziffer 5 („Verfügbarkeit“) aufgeführten Maßnahmen dienen zur Sichererstellung der Belastbarkeit der Kundensysteme. Penetrationstests der Systeme des Auftaggebers sind grundsätzlich nicht Bestandteil der vom Auftragneher zu erbringenden Leistungen, sofern dies nicht anderslautend im Hauptvertrag festgehalten wurde.

7. Wiederherstellbarkeit der Verfügbarkeit und des Zugangs

- Erstellung von Backups, sowie deren Tests auf Wiederherstellbarkeit
- Maßnahmen gem. Ziffer 5 („Verfügbarkeit“)
- Maßnahmen gem. Zifffer 3 b) („Zugangskontrolle“)

8. Verfahren zur regelmäßigen Überprüfung

Wir prüfen unsere Maßnahmen regelmäßig auf deren Angemessenheit, Funktionalität und gleichen diese mit dem Stand der Technik und den aktuellen Industriestandards ab. Angelehnt an den Prozess der Wirksamkeitskontrolle.

9. Unrechtmäßiger Zugang zu personenbezogenen Daten

Die unter Ziffer 3 b) („Zugangskontrolle“) und 3 c) („Zugriffskontrolle“) genannten Maßnahmen werden vom Auftragnehmer zur Verhinderung unberechtigten Zugangs zu personenbezogenen Daten unternommen.

10. Verarbeitung personenbezogener Daten nur nach Anweisung

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

- **Eindeutige Vertragsgestaltung:**
  - Schriftlicher Vertrag
  - Regelung der technisch-organisatorischen Maßnahmen
  - Verpflichtung der Mitarbeiter auf das Datengeheimnis
- **Formalisierte Auftragserteilung:**
  - Regelung der Rechte und Pflichten des Auftragnehmers und des Auftraggebers
  - Geordnete Führung der Dokumentation zur Einhaltung der Vereinbarung
- **Kriterien zur Auswahl des Auftragnehmers:**
  - Schriftliche Regelung der Rechte und Pflichten des Auftragnehmers und des Auftraggebers
- **Kontrolle der Vertragsausführung:**
  - Laufende Fortbildung der zugriffsberechtigten Mitarbeiter zum Thema Datenschutz

11. Sonstige Maßnahmen

Sonstige Maßnahmen, die geeignet sind, die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird:

- **Keine**