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.

1. Zweckbindung

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

physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ✓ Logische Mandantentrennung (softwareseitig)
- ✓ Berechtigungskonzept
- ✓ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ✓ Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen
- ✓ Trennung von Produktiv- und Testsystemen

Sonstiges:

Bei pseudonymisierten Daten:
- ✓ Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten und abgesicherten IT-System

2. Vertraulichkeit und Integrität

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

2.1 Verschlüsselung

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

- ✓ Microsoft® Bit-Locker
- ✓ AES 256-Bit

2.2 Pseudonymisierung

„Pseudonymisierung“ bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z.B. Verwendung von Fantasienamen, die ohne zusätzliche Informationen keiner bestimmten Person zugeordnet werden können).

- ✓ Nein
  Ja, und zwar in folgender Art und Weise:

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

- ✓ Alarmanlage
  Absicherung von Gebäudeschächten
- ✓ Automatisches Zugangskontrollsystem
- ✓ Chipkarten- / Transponder-Schließsystem
- ✓ Manuelles Schließsystem
- ✓ Biometrische Zugangssperren
- ✓ Videoüberwachung der Zugangswege
  Lichtschranken / Bewegungsmelder
- ✓ Sicherheitsschlösser
- ✓ Schlüsselregelung
  Personenkontrolle beim Pförtner / Empfang
  Protokollierung der Besucher
- ✓ Sorgfältige Auswahl von Reinigungspersonal

Sorgfältige Auswahl von Wachpersonal
Tragepflicht von Berechtigungsausweisen
✓ Zutrittskonzept / Besucherregelung

Sonstiges: ----

2.4 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, Komplexität etc.)
Authentifikation mit biometrischen Verfahren
✓ Authentifikation mit Benutzername / Passwort
✓ Zuordnung von Benutzerprofilen zu IT-Systemen
✓ Gehäuseverriegelungen
✓ Einsatz von VPN-Technologie bei der Übertragung von Daten
✓ Verschlüsselung mobiler IT-Systeme
✓ Verschlüsselung mobiler Datenträger
✓ Verschlüsselung der Datensicherungssysteme
Sperren externer Schnittstellen (USB etc.)
✓ Sicherheitsschlösser
✓ Schlüsselregelung (Schlüsselausgabe etc.)
Personenkontrolle beim Pförtner / Empfang
✓ Sorgfältige Auswahl von Reinigungspersonal
Sorgfältige Auswahl von Wachpersonal
Tragepflicht von Berechtigungsausweisen
✓ Einsatz von Intrusion-Detection-Systemen
✓ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
✓ Einsatz von Anti-Viren-Software
✓ Verschlüsselung von Datenträgern in Laptops / Notebooks
✓ Einsatz einer Hardware-Firewall
Einsatz einer Software-Firewall

Sonstiges: ----

2.5 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 das „Notwendigste“ reduziert
✓ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
✓ 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
✓ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
✓ Protokollierung der Vernichtung
✓ Verschlüsselung von Datenträgern

Sonstiges: ----

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

- ✓ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ✓ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, >>
- >> geändert und gelöscht werden können
- ✓ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen >>
- >> (nicht Benutzergruppen)
- ✓ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitung übernommen worden sind
- ✓ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Sonstiges: ----

2.7 Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die von Unterauftragnehmern / Subunternehmern des Auftragnehmers verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers und des Auftragnehmers verarbeitet werden können (Auftragskontrolle).

- ✓ Auswahl des Subunternehmers unter Sorgfaltsgesichtspunkten
- ✓ vorherige Prüfung der und Dokumentation der beim Subunternehmer getroffenen Sicherheitsmaßnahmen
- ✓ schriftliche Weisungen an den Subunterehmer (z.B. durch Auftragsverarbeitungsvertrag)
- ✓ Verpflichtung der Mitarbeiter des Subunternehmers auf das Datengeheimnis
- ✓ Subunternehmer hat Datenschutzbeauftragten bestellt
- ✓ Sicherstellung der Vernichtung von Daten von den Systemen des Subunternehmers nach Beendigung des Auftrags
- ✓ Wirksame Kontrollrechte gegenüber dem Subunternehmer vereinbart
- ✓ laufende Überprüfung des Subunternehmers und seiner Tätigkeiten
- ✓ Vertragsstrafen bei Verstößen

Sonstiges: ----

2.8 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 VPN-Tunneln
- ✓ Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des EMail-Verkehrs)
- ✓ Verschlüsselung physischer Datenträger bei Transport

Sonstiges: ----

3. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen Datenverarbeitungssysteme gewährleisten, jederzeit dass einwandfrei die eingesetzten funktionieren 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 Serverräumen
- ✓ Feuer- und Rauchmeldeanlagen in Serverräumen
- ✓ Feuerlöschgeräte in Serverräumen
- ✓ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ✓ Erstellen eines Backup- & Recoverykonzepts
- ✓ Testen von Datenwiederherstellung
- ✓ Erstellen eines Notfallplans und
- ✓ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ✓ Serverräume nicht unter sanitären Anlagen

4. Besondere Datenschutzmaßnahmen

---

5. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

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