Anhang III: Technisch-organisatorische Maßnahmen (TOM)

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen **treffen der Verantwortliche und der Auftragsverarbeiter gemäß Art. 32 DS-GVO („Sicherheit der Verarbeitung“) geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a.) Zutrittskontrolle

Maßnahmen mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

[X] Alarmanlage
[X] Zugangskontrollsysteme
[ ] Personenkontrolle durch Empfang/Pförtner
[X] Sicherheitsschlösser
[X] Absicherung von Gebäudeschächten
[ ] Chipkarten/Transponder-Schließsystem
[ ] Protokollierung der Besucher
[X] Videoüberwachung der Zugänge

b.) Zugangskontrolle

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

[X] Zuordnung von Benutzerrechten
[X] Passwortvergabe nach BSI
[X] Auth. mit Benutzername/Passwort
[ ] Gehäuseverriegelung
[X] Schlüsselregelung
[X] Einsatz von Anti-Viren Software
[ ] USB-Sperren
[ ] Erstellen von Benutzerprofilen
[ ] Auth. mit biometrischem Verfahren
[X] Zuordnung von Benutzerprofilen zu IT-Sys.
[X] Einsatz von VPN-Technologie
[ ] Einsatz von Intrustion-Detection-Systemen
[X] Verschlüsselung von mobilen Datenträgern
[X] Zuordnung Mitarbeiter <-> Kunde

c.) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung 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.

[X] Berechtigungskonzept
[X] Einschränkung Adminzugriffe
[ ] Protokollierung Zugriff auf Anwendung
[X] Einsatz von Aktenvernichtern
[X] Verwaltung der Rechte durch Systemadmin
[X] Passwortrichtlinie nach BSI
[X] Sichere Aufbewahrung von Datenträgern
[ ] Protokollierung der Vernichtung Standard Admin-Konto wird nicht verwendet. Adminzugriffe nur für Admin Mitarbeiter.

Fernwartung von Kundenservern über 2-Faktor Auth. und verschlüsselte Ablage von Passwörtern.

---

d.) Weitergabekontrolle

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

[X] Einrichtung von Standleitungen bzw. VPN-Tunneln

[X] Weitergabe von Daten in anonymisierter Form

[X] E-Mail-Verschlüsselung

[ ] Dokumentation der Empfänger von Daten und der Zeitspanne bis zur Löschung

[ ] Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen

---

e.) Eingabekontrolle

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

[X] Protokollierung der Eingabe, Änderung und Löschung von Daten

[X] Nachvollziehbarkeit von Datenmanipulationen auf Benutzerebene

[X] Vergabe der Rechte aufgrund eines Berechtigungskonzepts

[X] Vorhandensein einer Übersicht welche Applikation die personenbezogenen Daten verändert werden.

---

f.) Auftragskontrolle

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

[X] Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gem. Art. 28 Abs. 1 DS-GVO)

[X] Schriftliche Unterweisung an den Auftragnehmer i.S. gem. Art. 28 Abs. 1 DS-GVO

[X] Auftragnehmer hat Datenschutzbeauftragen bestellt, sofern vom BDSG gefordert

[X] Wirksame Kontrollrechte gegenüber dem Auftragnehmer sind vereinbart

[X] Vertragsstrafen bei Verstößen

[X] Vorherige Prüfung und Dokumentation der beim Subunternehmer getroffenen Sicherheitsmaßnahmen.

[X] Verpflichtung der Mitarbeiter auf das Datengeheimnis (gem. Art. 6 DS-GVO und §53 BDSG)

[X] Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags.

[X] Laufende Überprüfung des Subunternehmers und seiner Tätigkeiten.

[X] Lfd. Schulungen und Einführung / Verbesserungen von Prozessen VdS 10000 / 10100

---

g.) Verfügbarkeitskontrolle

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

[X] Unterbrechungsfreie Stromversorgung (USV)
[ ] Geräte zur Überwachung von Serverraumklima
[X] Feuer- und Rauchmelder
[ ] Alarmmeldung bei Zutritt Serverraum
[X] Regelmässige Recoverytests
[X] Datensicherung an sicherem Ort
[X] Klimatisierte Serverräume
X] Schutzsteckdosen in Serverräumen
[X] Feuerlöschgeräte neben Serverraum
[ ] Backup- Recoverykonzept
[ ] Notfallmanagementplan vorhanden
[X] Notfallhandbuch wird nach BSI erstellt.

---

h.) Trennungsgebot

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

[X] Physikalisch getrennte Speicherung auf gesonderten Systemen

[X] Logische Mandantentrennung (Software)

[X] Trennung durch Berechtigungskonzept

[ ] Versehen der Datensätze mit Zweckattributen

[X] Festlegung von Datenbankrechten

[X] Trennung von Produktiv- und Testsystem

[X] Generische Testdaten

[X] statistische Profildaten unpersonalisiert oder pseudonymisiert.

---

i.) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

☒	Datenschutz-Managementsystem
☐	Datenschutzkonzept
☒	Datenschutzfreundliche Voreinstellungen
☐	Incident-Response-Management (Vorfallreaktionsplan)