Technische und organisatorische Maßnahmen

Folgende technische und organisatorische Maßnahmen wurden getroffen:

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

1. Technische Maßnahmen

- ☐ Alarmanlage
- ☐ Türsicherung (elektrischer Türöffner, Zahlenschloss usw.)
- ☐ Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.)
- ☑ Sicherheitsschlösser
- ☐ _____

2. Organisatorische Maßnahmen

- ☐ Protokollierung der Besucher / Besucherbuch
- ☐ Schlüsselregelung / Schlüsselbuch
- ☑ Videoüberwachung der Zugänge
- ☐ _____

B. Zugangskontrolle
Maßnahme, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können

1. Technische Maßnahmen

- ☑ Authentifikation mit Benutzer + Passwort
- ☑ Aktuelle Anti-Viren-Software
- ☑ Aktuelle Firewall
- ☐ VPN-Technologie
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung
- ☐ E-Mail-Verschlüsselung

☐ Verschlüsselung von Datenträgern

☐ _____

2. Organisatorische Maßnahmen

☑ Zuordnung und Verwaltung der Benutzerberechtigungen

☐ Erstellen von Benutzerprofilen

☑ Passwortvergabe / Passwortregeln (inkl. regelmäßigen Änderungen)

☑ Automatische Sperrung des Arbeitsplatzes

☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

☑ Protokollierung von Übermittlungen

☐ Erstellung einer Übersicht von Datenträgern, Aus- und Eingang

☐ _____

C. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass Personen nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können

1. Technische Maßnahmen

☑ Einsatz von Aktenvernichter

☐ Einsatz von Datenträgervernichter

☐ Einsatz von Dienstleistern unter Beachtung von DIN 66399

☐ Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

☐ Verschlüsselung von Datenträgern

☐ Verschlüsselung von Smartphones

☐ _____

2. Organisatorische Maßnahmen

☑ Verwaltung der Benutzerrechte durch System-Administrator

☑ Anzahl der Administratoren auf das "Notwendigste" reduziert

- [ ] Erstellung eines Berechtigungsplans
- [ ] Passwortrichtlinie inkl. Länge und Wechsel
- [x] Sichere Aufbewahrung von Datenträgern
- [x] Ordnungsgemäße Vernichtung von Datenträgern
- [x] Löschungskonzept für Daten
- [x] Protokollierung der Vernichtung von Daten
- [x] Protokollieren von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- [ ] _____

D. 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 werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist

1. Technische Maßnahmen

- [ ] Einrichtungen von VPN-Tunneln
- [ ] E-Mail-Verschlüsselung
- [ ] _____

2. Organisatorische Maßnahmen

- [ ] Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- [ ] Erstellung einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgänge
- [ ] Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- [ ] _____

E. Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

1. Technische Maßnahmen:

- ☐ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☐ _____

2. Organisatorische Maßnahmen:

- ☑ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
- ☐ Protokollauswertungsroutinen/-systeme vorhanden
- ☐ Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden
- ☐ _____

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

1. Technische Maßnahmen:

- ☐ _____

2. Organisatorische Maßnahmen:

- ☑ Vorhandene Vereinbarungen zur Auftragsverarbeitung
- ☑ Kontrolle der Vertragsausführung
- ☑ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ _____

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

1. Technische Maßnahmen:

- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Überspannungsschutz
- ☐ Schutz gegen Umwelteinflüsse (Sturm, Wasser)
- ☑ Feuer- und Rauchmeldeanlagen
- ☐ Feuerlöscher in Serverraum
- ☐ Klimaanlage in Serverraum
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverraum
- ☑ Schutzsteckdosen in Serverraum
- ☐ _____

2. Organisatorische Maßnahmen:

- ☐ Erstellen eines Notfallplans
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverraum
- ☑ Testen von Datenwiederherstellung
- ☐ Serverraum nicht unter sanitären Anlagen
- ☐ Serverraum über Wassergrenze (in Hochwassergebiet)
- ☑ Erstellen eines Backup- (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort) und Recoverykonzepts
- ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☑ Spiegelung von Festplatten (z. B. RAID-Verfahren)
- ☐ _____

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

1. Technische Maßnahmen:

- [x] Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- [ ] Bei pseudonymisierten Daten: Trennung der Zuordnungsdaten und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- [ ] _____

2. Organisatorische Maßnahmen:

- [x] Festlegung Technologie von Datenbankrechten
- [x] Festlegung von Datenbankrechten
- [ ] Erstellung eines Berechtigungskonzepts
- [ ] _____

I. Dokumentationskontrolle
Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können

1. Technische Maßnahmen:

- [x] Zulässigkeit eines Datentransfers in Drittländer ist gegeben
- [ ] _____

2. Organisatorische Maßnahmen

- [ ] Führung eines Verarbeitungsverzeichnisses
- [x] Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration
- [ ] _____

J. Allgemeine Maßnahmen

☐ Ist ein betrieblicher Datenschutzbeauftragter bestellt?

☑ Nein

☐ Ja

Name: _____

Funktion: _____

E-Mail: _____

Telefon: _____

☐ Mitarbeiter wurden über Datenschutzrecht und Datensicherheit geschult.
Am: _____ / Vom: _____

☑ Alle Mitarbeiter sind auf das Datengeheimnis, ggf. auf das Fernmeldegeheimnis, verpflichtet.

☐ Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen (z.B. technisch unterstützt oder durch Externe).

☐ Ein Datensicherheitskonzept / Informationssicherheitsmanagement ist vorhanden.

☑ Ein Datenschutzkonzept ist vorhanden.

☐ Eine Auditierung/Zertifizierung ist vorhanden (Prüfung der Einhaltung am _____und Bestätigung s. Anlage ____).

☐ Verhaltensregeln nach Art. 40 DSGVO sind vorhanden (Unterwerfung am _____und Bestätigung s. Anlage ____).