TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

1. Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten

Pseudonymisierung von nicht mehr im Klartext benötigten personenbezogenen Daten
Verschlüsselung von Webseiten (SSL)
E-Mail-Verschlüsselung (TLS 1.2 oder 1.3)

2. Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

Vertraulichkeitsvereinbarungen mit Mitarbeitern
NDAs mit Dritten
Datenschutzverpflichtung der Mitarbeiter
Firewall
Antivirenprogramm
Regelmäßige Datensicherungen

3. Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Regelmäßige Backups des gesamten
Regelmäßiger Test Backup/Recovery
Regelmäßige Schulung des IT-Personals

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Interne Kontrollen
Regelmäßige Überprüfung der IT-Prozesse
Regelmäßige Audits (z.B. durch den DSB)

5. Maßnahmen zur Identifizierung und Autorisierung der Nutzer

Authentisierung mit Benutzername / Passwort

Regelmäßige Prüfung von Berechtigungen
Passwort-Richtlinie
Begrenzung der Anzahl der Admins
Verwaltung der Rechte durch einen Admin

6. Maßnahmen zum Schutz der Daten während der Übermittlung

Einsatz von Verschlüsselungstechnologien
Protokollierung von Aktivitäten und Ereignissen
E-Mail-Verschlüsselung (TLS 1.2 oder 1.3)
Verwendung nicht öffentlicher Laufwerke

7. Maßnahmen zum Schutz der Daten während der Speicherung

Protokollierung von Aktionen und Ereignissen
Begrenzung der Anzahl der Administratoren
Firewall

8. Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden

Manuelles Schließsystem
Sicherheitsschlösser
Verfahren zur Schlüsselausgabe

9. Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen

Protokollierung auf Applikationsebene
Regelmäßige manuelle Überprüfung der Protokolle

10. Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

Prozess zu Konfigurationsänderungen
Datenschutzgerechte Voreinstellungen
Konfiguration durch Systemadministrator
Regelmäßige Schulung der IT-Mitarbeiter

11. Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit

IT-Sicherheitsrichtlinie
Schulung der Mitarbeiter zur Datensicherheit
IT-Team mit klaren Rollen / Verantwortlichkeiten

12. Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten

Klarer Überblick über die für Produkte/Dienstleistungen/Prozesse geltenden Bestimmungen
Regelmäßige interne und/oder externe Audits
Zuweisung von Audit-Verantwortlichkeiten an zertifizierte Experten

13. Maßnahmen zur Gewährleistung der Datenminimierung

Identifikation des Zwecks der Verarbeitung
Bewertung des Zusammenhangs zwischen Verarbeitung und Zweck
Identifikation der geltenden Aufbewahrungsfristen
Sichere Löschung der Daten nach Ablauf der Aufbewahrungsfrist

14. Maßnahmen zur Gewährleistung der Datenqualität

Protokollierung Eingabe/Änderung Daten
Rechtevergabe zur Dateneingabe
Nachvollziehbarkeit der Benutzer bei Eingabe,

15. Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

Regelmäßige Schulungen
Regelmäßige Prüfung und Bewertung der gespeicherten Daten

16. Maßnahmen zur Gewährleistung der Rechenschaftspflicht

Schulungen / Sensibilisierung
Regelmäßige Kontrollen und Prüfungen
Angemessene Richtlinien zum Datenschutz
Abschluss von Standardvertragsklauseln

17. Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

Speicherung in einem strukturierten Format
Überwachung gesetzlicher Fristen
Einhaltung von Aufbewahrungsfristen
Ermöglichung der Datenübertragbarkeit
Richtiger Umgang mit Betroffenenrechten
Sichere Datenlöschung und Datenträgervernichtung gewährleistet durch Beauftragung der Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Deutschland, E-Mail: info@notebook12.com

18. **Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-) Auftragsverarbeiter zur Unterstützung des Verantwortlichen und (bei Datenübermittlungen von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter) zur Unterstützung des Datenexporteurs ergreifen muss.**

Standardvertragsklauseln (SCCs) werden unterzeichnet oder vereinbart
UK IDTAs oder Addendums zu den SCCs werden unterzeichnet oder vereinbart
Vertraglich vereinbarte, wirksame Kontrollrechte
Vertraglich vereinbarte Unterstützung des Verantwortlichen