Übersicht Technische und organisatorische Maßnahmen

Anlage 1

Vertraulichkeit

a) **ZUTRITTSKONTROLLE** (für Gebäude und Räume; an Schränke und Schächte) Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, wo personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

- Werkschutz, Pförtner, Sicherheitspersonal
- Zutrittskontrollsystem
  (z.B. Ausweisleser, Schleusen, Magnetkarte)
- Überwachungseinrichtungen
  (Alarmanlage, Video, Bewegungsmelder an Türe und fenstern)
- Schlüsselregelung und Quittung bei Schlüsselausgabe
- Gesicherte Türen, Sicherheitsschlösser, Fenster
- Kontrolle Reinigungs- und Wartungsarbeiten
- Besonderer Zutrittsschutz Serverräume
  (elektronische Zutrittskontrolle/ Protokollierung)

b) **ZUGANGSKONTROLLE/NUTZUNGSKONTROLLE**
(Anmelden im System, unerlaubtes Hochfahren und Eindringen in das DV-System verhindern) Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert werden kann:

- Passwort-Management
  (mind. 8 Stelliges Passwort, Passwortkomplexität, regelmäßiger Wechsel)
- Automatisches Sperren, Log-out
- Berechtigungsregelungen/ Terminals
- Spezielle Benutzermenüs
- Firewall, Virenschutz, DMZ
- Intrusion Detection/ Intrusion Prevention
- Sicherung externer Schnittstellen (USP-Ports, CD/DVD-Laufwerke)

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:

- Protokollierung von Zugriffen
- Differenzierte Berechtigungen (Profile, Rollen)
- Dokumentation von Berechtigungen
- Lagerung der Datenträger in abschließbaren Schränken
- On-Boarding/ Off-Boarding-Prozess

d) **TRENNUNGSKONTROLLE**
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die zu unterschiedlichen Zwecken und für verschiedene Auftraggeber erhoben wurden, getrennt voneinander verarbeitet werden.

e) **PSEUDONYMISIERUNG UND ANONYMISIERUNG**
(Bei der Pseudonymisierung wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym ersetzt bei der Anonymisierung verändert, um die Feststellung der Identität des Betroffenen ohne Hinzuziehung zusätzlicher Informationen auszuschließen oder wesentlich zu erschweren.)

- Verwendung eines Pseudonyms für den Namen möglich
- Dem Kommunikationspartner ist die reale Identität nicht bekannt, wohl aber dem Dienstanbieter

Integrität

f) **WEITERGABEKONTROLLE UND VERSCHLÜSSELUNG**
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 und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Verschlüsselte Kommunikation/ Datentransfer (https: VPN, SSL etc.)
- Passwortgeschützte Übertragung von Dokumenten

g) **EINGABEKONTROLLE** (Nachvollziehbarkeit, Dokumentation)
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 und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- ✔ Zugriffsregelungen/ Rollen
- ✔ Protokollierung von Zugriffen
- ✔ Speicherung 1 Monat

h) **SICHERSTELLUNG DER AUTHENTIZITÄT & INTEGRITÄT**
(Schutz von unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung sowie unbefugter Änderung.)

- ✔ Dokumentation von Berechtigungen
- ✔ Verschlüsselung der Datenübertragung
- ✔ Überwachungseinrichtungen der Datenverarbeitungs-Anlagen

i) **DATENSCHUTZMANAGEMENT**
(Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.)

- ✔ Regelmäßige Datenschutzaudits
- ✔ Auftragskontrolle & Eindeutige Vertragsgestaltung
- ✔ Strenge Auswahl der Dienstleister
- ✔ Vorab- und Nachkontrollen
- ✔ Datenschutzfreundliche Voreinstellungen
- ✔ Datenschutzbeauftragte

Verfügbarkeit und Belastbarkeit

k) **VERFÜGBARKEITSKONTROLLE**
(Nachvollziehbarkeit, Dokumentation) Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust, gegen technische Störungen durch Versagen von Betriebs-/Anwendungssoftware, vor fahrlässigen/-vorsätzlichen Handlungen, vor schadenstiftender Software geschützt sind:

- Schaffung von Redundanzen (Bestandssicherungskonzept, Sicherungskopien, Backups, Datenspiegelung)
- Getrennte Datenaufbewahrung
- Notfallkonzept/ Notfallplan
- Unterbrechungsfreie Stromversorgung/ (USV)
- Kontrolliertes Herunterfahren der Systeme im Notfall
- Monitoring
- Automatische Abwehrsysteme
- Regelmäßige PEN-Tests

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

l) **DATENSCHUTZMANAGEMENT**
(Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.)

- Regelmäßige Datenschutzaudits
- Auftragskontrolle & Eindeutige Vertragsgestaltung
- Strenge Auswahl der Dienstleister
- Vorab- und Nachkontrollen
- Datenschutzfreundliche Voreinstellungen
- Datenschutzbeauftragte

Rheinberg,

Richard Zelzer Andreas Feldmann
newclicks UG (haftungbeschränkt) & Co. KG