

## **Anforderungen TOMs**

### **Allgemeine Voraussetzungen:**

- Eingesetzte Rechenzentren/Datenstandorte befinden sich in Deutschland oder Europa
- Im Idealfall keine Beteiligungen von Firmen aus Drittländern (z.B. USA, Indien, China) oder Vorlage von geeigneten Schutzmaßnahmen zur Verarbeitung in Drittländern (BCR sind zu bevorzugen).

### **Vertraulichkeit**

#### **Zutrittskontrolle**

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen und Zutrittskontrollsysteme inkl. dazugehöriger Regelungen, z.B. durch:

- Nachweise der Zutrittskontrollen bei Bedarf
- Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner
- Besucherregelungen
- Einbruchs- und Diebstahlsicherung
- Pförtner oder Werksschutz
- Alarmanlage
- Videoanlagen

#### **Zugangskontrolle**

Keine unbefugte Systembenutzung, sichergestellt z.B. durch:

- Sichere Passwortmaßnahmen und –Regelungen nach Stand der Technik auf allen Geräten
- Regelmäßige Kontrolle von Zugangsberechtigungen
- automatische Sperrmechanismen
- Zwei-Faktor-Authentifizierung
- Verschlüsselung von Datenträgern
- Verschlüsselung mobiler Endgeräte der Mitarbeiter

#### **Zugriffskontrolle**

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, sichergestellt z.B. durch:

- Abgestuftes und verbindliches Zugriffs-konzept/Berechtigungskonzept
- Durchgehende Protokollierung und regelmäßige Kontrolle der Zugriffe auf Daten
- Vergabe von minimalen Zugriffsrechten (Need-to-know Prinzip)
- Datenschutzkonforme Vernichtung von Datenträgern; bspw. gem. Din 66399
- Ggfs. Sichtschutz bei betroffenen Geräten (z.B. Sichtschutzfolien bei Laptops)
- Einsatz von Verschlüsselungsverfahren nach Stand der Technik bei der Speicherung von Daten

## **Trennungskontrolle**

- Logische oder physische Trennung der Daten unterschiedlicher Kunden der DAkkS (Mandantenfähigkeit)
- Logische/physische Trennung der unterschiedlichen Systemebenen (Entwicklung/Test/Produktiv)
- Ggfs. Trennung der Daten der DAkkS von denen anderer Kunden des Anbieters (Mandantenfähigkeit)

## **Pseudonymisierung**

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

## **Integrität**

### **Weitergabekontrolle**

- Einsatz von Verschlüsselungsverfahren nach Stand der Technik bei der Übertragung von Daten (Transportverschlüsselung)
- Firewall- und IT-Sicherheitslösungen nach aktuellem Stand der Technik (jedenfalls Endpoint Detection and Response und nicht nur legacy AV)
- Datenschutzkonforme Vernichtung von Datenträgern sämtlicher Art inkl. Protokollierung nach DIN 66399
- Verschlüsselte Datenspeicherung in allen mobilen Systemen

### **Eingabekontrolle**

- Dokumentation der Daten- und Dateiänderungen
- Stichprobenartige Überprüfung der Änderungsprotokollierung
- Regelmäßige Überprüfung anhand des Berechtigungskonzepts

## **Verfügbarkeit und Belastbarkeit**

### **Verfügbarkeitskontrolle**

- Unterbrechungsfreie Stromversorgung (USV)
- Virenschutz (siehe oben)
- Firewall (Next Generation)
- Notfallplan
- Verfügbarkeitsüberwachung (u.a. Auslastung, Temperatur)

### **Wiederherstellbarkeit**

- Backupkonzept (Backups müssen entweder offline oder unveränderbar (immutable) gespeichert werden),
- Regelmäßige Prüfung der Backups auf Funktionsfähigkeit
- Sichere Aufbewahrung der Backups

### **Belastbarkeit**

- Virtualisierung/Containerstrukturen
- Regelmäßige Penetrationstests
- Eingerichtete Redundanzen

## **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

### **Datenschutzmanagement**

- Verpflichtung auf die Einhaltung datenschutzrechtlicher Normen
- Benennung einer/eines Datenschutzbeauftragten
- Etabliertes Datenschutz-Managementsystem inkl. Risikoeinschätzung
- Incident-Response-Management;
- Ggfs. Bestätigung der Datenschutzkonformität durch Audit (von Dritten)

### **Beurteilung des angemessenen Schutzniveaus**

- Regelmäßige datenschutzrechtliche Risikobewertung der Verarbeitungstätigkeiten
- Datenschutz-Folgenabschätzung falls notwendig
- Implementierung Privacy by Design & Default

### **Auftragskontrolle**

- Ausschluss der Datenverarbeitungen in Drittländern
- DSGVO-konforme Vertragsgestaltung mit Unterauftragnehmern
- Regelmäßige Überprüfung der Unterauftragnehmer
- Eindeutige Regelungen zur Erteilung von Weisungen an Unterauftragnehmer