Dokument: **TOM** Katalog ○ V ◉ AV

Erstellt am 29.11.2018

☐ Datum LVB

Letzte Änderung am ☐ durch ☐

☐ Prüfung LVB OK

1. Schutzziel: Pseudonymisierung

Regelungsgegenstand: Verwendungszusammenhänge innerhalb pbD sind zu zerstören oder deren Herstellbarkeit ist zu unterbinden, wenn technisch möglich und im übrigen vertretbar.

Es ist keine Pseudonymisierung im Einsatz.

2. Schutzziel: Verschlüsselung

Regelungsgegenstand: Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbefugte Offenlegung von bzw. unbefugten Zugang zu den Daten ist zu reduzieren.

Bei Übertragung von pbD zu | **finden folgende TOMs Anwendung:**

Betroffenem	Grundsätzliche Nutzung von verschlüsselter Kommunikation; https im Web bzw. TLS bei eMail, SSL bei allen übrigen.
Institutionen (iRv AV)	Grundsätzliche Nutzung von verschlüsselter Kommunikation; https im Web bzw. TLS bei eMail, SSL bei allen übrigen.
Dienstleister	Grundsätzliche Nutzung von verschlüsselter Kommunikation; https im Web bzw. TLS bei eMail, SSL bei allen übrigen.
Mitarbeiter	Grundsätzliche Nutzung von verschlüsselter Kommunikation; https im Web bzw. TLS bei eMail, SSL bei allen übrigen.
(Leer)	
(Leer)	

Mobile Endgeräte werden verschlüsselt ◉ ○

Notebooks werden verschlüsselt ● ◉

Remote Rechner werden verschlüsselt ● ◉

J / N

Device Management: ◉ ○

J / N

3. Schutzziel: Vertraulichkeit

Regelungsgegenstand: Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbefugte Offenlegung von bzw. unbefugten Zugang zu den Daten ist zu reduzieren. Unbefugten ist der Zutritt zu den Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten), mit denen Daten verarbeitet werden, zu verwehren.

3.1 TOMs für Physikalische Sicherheit: Bauliche Maßnahmen

Der Zugang zu informationstechnischen Systemen im Eigenbetrieb ist durch mehrere Zugangsebenen, Türen und Schlösser gegen unbefugten Zugang versperrt. Für diese existiert ein Schließkonzept. Im übrigen wird in diesem Zusammenhang für die nicht lokal betriebenen Systembestandteile auf das Sicherheitskonzept des Betreibers des Rechenzentrums verwiesen. Dieses ist auf Anfrage erhältlich.

3.2 TOMs für Physikalische Sicherheit: Objektschutz

Es existiert keine proaktive Bestreifung durch einen Sicherheitsdienst im Rahmen des Angemessenheitsgrundsatzes.

3.3 Authentifizierung

Es muss verhindert werden, dass Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten) von unbefugten Dritten genutzt werden können.

Durchgängige Nutzung von ActiveDirectory von Microsoft mit nach BSI BestPractice ausgeprägten Wechselintervallen von Passwörtern. Keine lokalen Benutzerhaltungen / Schatten-IT vorhanden.

3.4 Weitergabe von Daten

Daten dürfen bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Konsequenter Einsatz von Verschlüsselung auf der Transportebene und bei der Weitergabe auf Massendatenträgern, sofern diese nicht vermieden werden kann.

3.4 Löschkonzept

Regelungsgegenstand: Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Es existiert ein Löschkonzept, welches im Rahmen von Data Lifecycle Management die Erhebung, Nutzung und Löschung von personenbezogenen Daten unter den einschlägigen Vorschriften regelt. Durch regelmäßiges Anwenden der Löschroutine ist sichergestellt, daß die einschlägigen Vorschriften aus Art. 6 (1) DS-GVO und die nationalen Vorschriften berücksichtigt werden und eine anlasslose Verarbeitung i.S.d. Art. 4 DS-GVO nicht erfolgt.

3.4 Trennbarkeit

Regelungsgegenstand: Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können.

Es erfolgt keine Zweckerweiterung und keine Durchmischung von (Kunden)-Kerngeschäftsdaten und solchen für den Eigenbetrieb.

4. Schutzziel: Integrität

Regelungsgegenstand: Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung oder unrechtmäßiges oder fahrlässiges Handeln von Daten ist zu reduzieren.

4.1 Protokollierung

Regelungsgegenstand: Es sind Maßnahmen zu wählen, mittels derer nachträglich überprüft und festgestellt werden kann, ob und von wem im Auftrag verarbeitete Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die personenbeziehbaren Bestandteile der verarbeiteten Datenkategorien unterliegen einer Historisierung; diese wiederum ist Teil des Löschkonzeptes.

5. Schutzziel: Verfügbarkeit
Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Nichtverfügbarkeit von Daten ist zu reduzieren.

5.1 Sicherstellung der Verfügbarkeit

Regelungsgegenstand: Daten sind gegen zufällige oder mutwillig herbeigeführte Zerstörung oder Verlust zu schützen.

5.1.1 Bauliche Maßnahmen

Es wird, zusammen in 3.1 diesem Zusammenhang auf das Sicherheitskonzept des Betreibers des Rechenzentrums verwiesen. Dieses ist auf Anfrage erhältlich.

5.1.2 Personelle Maßnahmen

Es wird IT-Fachpersonal beschäftigt, welches sicherstellt, daß bei Ausfällen unmittelbar auf die Schadenssituation angepasste Maßnahmen ergriffen werden können.

5.1.3 Organisatorische Maßnahmen

Es besteht eine definierte Rufbereitschaft für 5.1.2.

5.1.4 Stromversorgung

Die Stromversorgung aller betriebskritischen Systeme ist redundant aufgebaut. Es wird in diesem Zusammenhang für die nicht lokal betriebenen Systembestandteile auf das Sicherheitskonzept des Betreibers des Rechenzentrums verwiesen. Dieses ist auf Anfrage erhältlich.

5.1.5 Brandschutz

Es besteht eine Rauchgas- und Wärmeentwicklungsdetektion. Es wird in diesem Zusammenhang für die nicht lokal betriebenen Systembestandteile auf das Sicherheitskonzept des Betreibers des Rechenzentrums verwiesen. Dieses ist auf Anfrage erhältlich.

5.1.6 Klimatisierung

5.2 Zweckbindung

Regelungsgegenstand: Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden

Es erfolgt keine Zweckerweiterung.

6. Schutzziel: Resilienz

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung von Daten oder des unbefugten Zugangs zu Daten aufgrund von Systemüberlastungen oder –abstürzen ist zu reduzieren.

Die konsequent virtualisierte Systemarchitektur ist nach industriellen Best Practice Grundsätzen hinsichtlich Redundanz, Widerstandsfähigkeit und Ausfallsicherheit aufgebaut. Es wird in diesem Zusammenhang für die nicht lokal betriebenen Systembestandteile auf das Sicherheitskonzept des Betreibers des Rechenzentrums verwiesen. Dieses ist auf Anfrage erhältlich.

7. Schutzziel: Wiederherstellbarkeit

Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von Daten oder des unbefugten Zugangs zu diesen durch einen physischen oder technischen Zwischenfall ist zu reduzieren.

Es existiert eine ausreichend historisierte und verschlüsselte Datensicherung nach dem Großvater / Vater / Sohn Prinzip an mehreren Standorten und Brandabschnitten. Es wird in diesem Zusammenhang für die nicht lokal betriebenen Systembestandteile auf das Sicherheitskonzept des Betreibers des Rechenzentrums verwiesen. Dieses ist auf Anfrage erhältlich.

8. Schutzziel: Verfahren regelmäßiger Überprüfung, Evaluierung und Bewertung von TOMs

Regelungsgegenstand: Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu betreiben.

Es erfolgen regelmäßige Audits.

9. Dokumentation

Regelungsgegenstand: Es ist Dokumentation vorzuhalten, welche dazu geeignet ist, die Informationen in diesem Dokument zu flankieren.

- [ ] **interner Code of Conduct / Policy**
- [ ] **Risikoanalyse / FMEA / Schutzbedarfsfeststellung**
- [x] **Datensicherheitskonzept**
- [ ] **Wiederanlaufkonzept**
- [ ] **Notfallhandbuch**
- [ ] **Zertifikate:**
- [x] IT Sicherheitskonzept DHV E-Net
- [ ]
- [ ]