Aufstellung der TOMs im Datenschutz gem. DSGVO

id newmedia **Stand Januar 2021**

Vorwort

Diese Auflistung der getroffenen TOMs im Datenschutz orientiert sich an den Vorgaben des § 64 BDSG-Neu. Diese Angaben dokumentieren auch die Forderungen des § 78a SGB X und des Art. 32 der DSGVO. Die getroffenen Maßnahmen unterliegen den technischen Fortschritt und werden somit fortlaufend aktualisiert, wobei das bisher vorhandene Sicherheitsniveau nicht verringert wird.

Beschreibung der Technische und organisatorische Maßnahmen (TOMs)

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle)

- ►*Closed-Shop-Betrieb*
- ►unsere *Serverräume werden per Video überwacht, sobald diese betreten werden*
- ►*Zutritt in die IT-Räume nur über programmierten elektronischen Schlüssel*
- ►*Token zur Entschärfung der Alarmanlage notwendig*
- ►*Besucher müssen sich anmelden*
- ►*Besucher der IT-Bereiche dürfen nur in Begleitung agieren sofern sie nicht per NDA (Non-Disclosure-Agreement) akkreditiert sind*
- ►es kann n*achvollzogen werden welche Tür wann und von wem geöffnet wurde (Logfiles in den Türzutrittssystemen)*

2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle)

- ►*elektronische und optische Datenträger werden in der IT-Abteilung in einem verschlossenen Raum gesammelt und vor der Entsorgung einzeln unbrauchbar gemacht*
- ►*magnetische Datenträger (Festplatten) sind gelistet und der „Lebenszyklus“ wird dokumentiert*

3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle)

- ►*Benutzername und Kennwort*
- ►*automatische Sperrung (Pausenschaltung)*
- ►*Sperrung des Accounts bei wiederholter Falschanmeldung*
- ►*datenschutzgerechte Passwortrichtlinien gem. BSI werden vorgegeben/generiert*
- ►*Benutzerverzeichnis mit Zugangsprotokoll*
- ►*Server mit zusätzlichen Administrator Passwörtern*
- ►*geschützte WLAN Netzwerke*
- ►*keine Hardware in nicht produktiven Räumen*
- ►*dokumentierte Prozesse bei der Benutzerverwaltung*

4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle)

- ►*2-schichtiges Modell : Sophos in den Security Appliances (WEB- und email-Services), Microsoft Virenscanner auf Servern und Clients für das Dateisystem sowie zweite Instanz für WEB und email, alle Systeme mit automatischem Update und automatischer Verteilung an die Clients*
- ►*Home Office Arbeitsplätze sind ausschließlich über Sophos RED angebunden administrierte Firewalls*
- ►*Server für Zugriffe von außen stehen in geschichteter DMZ*
- ►*Echtzeit- Network- und Server-Monitoring der Zugriffe im Innen und Außen*

5. Gewährleistung, daß die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfaßten personenbezogenen Daten Zugang haben (Zugriffskontrolle)

►*nur die jeweiligen Programmierer bzw. Systembetreuer haben Zugriff auf „ihr" System*
►*durch differenzierte Berechtigungen, gesteuert durch die Anmeldung*
►*extra Administrationspasswörter für die Server die nur den entsprechenden IT-Technikern bekannt sind und zusätzlich in einem verschlossen Umschlag in einem Tresor aufbewahrt werden*

6. Gewährleistung, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle)

►verfahrensabhängige Dokumentation im eShop

7. Gewährleistung, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle)

►verfahrensabhängige Dokumentation im eShop

8. Gewährleistung, daß bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle)

►alle *ein- und ausgehende Mails werden vom Virenscanner gescannt*

9. Gewährleistung, daß eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit)

►*„Reserve" Server stehen bei Ausfall in anderem Brandschutzabschnitt*
►*Datensicherungskomponenten werden in anderem Brandschutzabschnitt aufbewahrt*
►redundante *Linux Firewall in anderem Brandschutzabschnitt*
►*IT-Notfallpläne*

10. Gewährleistung, daß alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit)

►*Raid-Systeme überbrücken und melden Plattenausfälle in den Servern*
►*Systemüberwachung meldet Störungen*
►*Echtzeit- Überwachung von Leistung und Temperatur in den IT-Räumen*
►*IT-Räume mit Brand- und Rauchmelder, Alarmanlage und Videoüberwachung*

11. Gewährleistung, daß gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)

►*keine Datenhaltung auf lokalen Endgeräten*
►*Patchmanagement*

12. Gewährleistung, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

►verfahrensabhängige Dokumentation im eShop

13. Gewährleistung, daß personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)

►*Backupverfahren mit Protokollen (Hardware: 3-fach QNAP RAID1 (räumlich getrennt)*
►*redundante IT-Räume sind vorhanden*
►*alle Server sind mit Raid-Systemen ausgestattet die die Daten permanent spiegeln*
►*alle Server sind an ausreichend dimensionierte USVs angeschlossen*

14. Gewährleistung, daß zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit)

►*verfahrensabhängig*
►*verschiedene Systeme sind auf unterschiedlichen Servern installiert*
►*Trennung von Produktiv- und Testsystemen (z.B. Finanzwesen HKR)*