Wie setzt man TOM am besten DSGVO-konform um?

Da die DSGVO bei der konkreten Definition der TOM für den Datenschutz eher vage bleibt, hilft ein Blick ins Bundesdatenschutzgesetz (BDSG). § 9 BDSG (alte Fassung) definiert technisch-organisatorische Maßnahmen und benennt konkret folgende Bereiche:

- **Zutrittskontrolle:** Der physische Zutritt zu Datenverarbeitungsanlagen wie einem Serverraum muss durch Zutrittskontrolle verhindert werden. Mögliche Mittel sind elektronische Zugangssysteme oder Pförtner.

- **Zugangskontrolle:** Dritte dürfen auch keinen digitalen Zugriff auf Datenverarbeitungsanlagen erhalten. Dies kann durch Verschlüsselungen, Mehr-Faktor-Authentifizierungen oder strenge Passwortverfahren erfolgen.

- **Zugriffskontrolle:** Durch strenge Berechtigungskonzepte wird sichergestellt, dass unbefugte Dritte keinen Schreib- oder Lesezugang zu sensiblen Daten erhalten. Auch die Möglichkeit, Daten unbefugt zu kopieren oder zu löschen darf nicht gegeben sein.

- **Weitergabekontrolle:** Durch ausreichende Verschlüsselungen wird sichergestellt, dass sensible Daten unbefugten Dritten auch dann nicht offengelegt werden, wenn diese z.B. gerade übertragen werden. Hier dürfen unberechtigte Dritte ebenfalls weder die Möglichkeit zum Lesen, Verändern, Kopieren oder Löschen der Daten erhalten.

- **Eingabekontrolle:** Protokollierungssysteme erfassen jeden Zugriff auf personenbezogene Daten und ermöglichen jede Änderung oder Löschung nachzuvollziehen.

- **Auftragskontrolle:** AV-Verträge regeln die Datenverarbeitung durch auf diese Weise befugte Dritte den Regelungen des Auftraggebers entsprechend.

- **Verfügbarkeitskontrolle:** Firewalls und Backups sind nur zwei der Möglichkeiten, um Daten vor ungewünschten Verlusten und Angriffen zu schützen und zudem zu gewährleisten, dass die Daten im Verlustfall wiederhergestellt werden können.

- **Trennungsgebot:** Der Einsatz separater Systeme soll gewährleisten, dass für unterschiedliche Zwecke erhobene Daten nur für den jeweiligen Erhebungszweck verwendet werden.

Natürlich müssen nicht alle Maßnahmen von allen Unternehmen umgesetzt werden, aber wichtig ist, dass mittels Risikoanalyse abgeklärt wird, für welche Unternehmen bestimmte Maßnahmen relevant sind.
Die Mustervorlage (siehe PDF in Teams) für technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO bietet ebenfalls konkrete Beispiele zur geeigneten Umsetzung.

Aufgabenstellung:

Nennen Sie jeweils zwei konkrete technische und organisatorische Maßnahmen für folgende Bereiche! Geben Sie auch das betroffene Schutzziel an!

Zutrittskontrolle:

Technisch: Chipkarten, Manuelles Schließsystem

Organisatorisch: Empfang/Rezeption, Mitarbeiter- / Besucherausweise

Vertraulichkeit

Zugangskontrolle:

Technisch: Login mit Benuzername + Passwort, Sperre externer Schnittstellen

Organisatorisch: Zentrale Passwortvergabe, "Clean desk"

Vertraulichkeit

Zugriffskontrolle:

Technisch: Aktenschredder, Physische Löschung von Datenträgern

Organisatorisch: Berechtigungskonzepte, Verwaltung Benutzerrechte durch Admins

Vertraulichkeit

Weitergabekontrolle:

Technisch: Einsatz von VPN, Protokollierung der Zugriffe und Abrufe

Organisatorisch: Weitergabe annonymisierter oder pseudonymisierter Form,

Persönliche Übergabe mit Protokoll

Integrität

Eingabekontrolle:

Technisch: Techn. Protokollierung der Änderungen, Manuelle / autom. Kontrolle der Protokolle

Organisatorisch: Klare Zuständigkeiten für Löschungen, Übersicht mit welchen Programmen änderungen gemacht werden können

Integrität

Auftragskontrolle:

Technisch: -

Organisatorisch: Schriftliche Weisung an den Auftragsnehmer, Sicherstellung der Vernichtung von Daten nach Beenden eines Auftrags

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Verfügbarkeitskontrolle:

Trennungskontrolle: