Was sind technische und organisatorische Maßnahmen (TOM)?

Technische Maßnahmen sind alle angeschafften, montierten oder installierten Lösungen, die direkten Einfluss auf die Verarbeitung an sich haben. **Organisatorische** sind alle nicht-technischen Maßnahmen, um sichere Rahmenbedingungen für die Verarbeitung herzustellen – von Plänen über Richtlinien bis hin zu Arbeitsroutinen.

Als **technische und organisatorische Maßnahmen** gelten Lösungen und Vorgehensweisen, die gem. Art. 32 DSGVO ein angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten gewährleisten sollen.

Technische Maßnahmen umfassen solche Maßnahmen, mit denen die Datenverarbeitung insbesondere physisch, durch Hardware oder durch Software geschützt wird. Eine technische Maßnahme, die zur Datensicherheit auf einem Computer beiträgt, ist z.B. die Einrichtung eines Passwort-Schutzes.

Organisatorische Maßnahmen konzentrieren sich hingegen auf die Rahmenbedingungen der Datenverarbeitung und beinhalten Verfahrens- und Vorgehensweisen sowie Handlungsanweisungen. Eine passende organisatorische Maßnahme in Bezug zum genannten Passwort-Schutz wäre z.B. die Erstellung einer Richtlinie für die Anlage sicherer Passwörter und für die Aufbewahrung relevanter Unterlagen.

Welche TOM sind notwendig?

Um die Sicherheit der Verarbeitung personenbezogener Daten und damit auch die Effektivität und Angemessenheit der eingerichteten Schutzmaßnahmen – vor allem im Rahmen einer Überprüfung durch die Datenschutzaufsichtsbehörden – beurteilen zu können, enthält Art. 32 DSGVO nicht abschließend wesentliche Zielvorgaben bzw. Maßnahmenbereiche, die der Verantwortliche jedenfalls bei der Auswahl der konkreten TOM zu beachten hat. Dazu zählen insbesondere

- die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO),
- die Fähigkeit, die **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** und **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen (Art. 32 Abs. 1 lit. b DSGVO),
- die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall **rasch wiederherzustellen** (Art. 32 Abs. 1 lit. c DSGVO),
- ein Verfahren zur **regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzurichten (Art. 32 Abs. 1 lit. d DSGVO).

Diese noch recht abstrakten Begriffe werden wir uns nun im Detail ansehen und die zugehörigen praxisrelevanten Maßnahmen für das Home-Office ableiten.

TOM im Home-Office

Pseudonymisierung

Pseudonymisierung bedeutet, dass eine unmittelbare Zuordnung von Daten zu der spezifischen betroffenen Person nicht ohne Hinzuziehung weiterer Informationen möglich ist. Gängige **Arten** von Pseudonymen sind z.B. bei Kunden die Kundennummer, bei Mitarbeitern die Personalnummer, bei der Internetnutzung die IP-Adresse oder auch bei Online-Portalen der Nutzername (sofern dieser nicht den Klarnamen des Betroffenen enthält). Zu den TOM gehören dabei nicht nur die Möglichkeit der Pseudonymisierung an sich, sondern auch die Schutzmaßnahmen für die sichere, gesonderte **Aufbewahrung** der Information, die zur Zuordnung des Pseudonyms zum Betroffenen benötigt wird. Sie sollten z.B. dafür sorgen, dass Mitarbeiter als Login-Namen für ihren Zugang zu Programmen des Unternehmens (z.B. Anmeldung in Cloud, Datenbanken, etc.) nicht ihren Klarnamen, sondern z.B. eine eher zufällige Zeichenkombination verwenden. Zum Schutz von Kundendaten sollte – insbesondere für Arbeiten aus dem Home-Office – der Zugriff auf Kundendaten auf das nötige Mindestmaß beschränkt werden, sodass sich hier z.B. die Identifikation über die Kundennummer anbieten kann. Die pseudonymisierten Daten sollten dabei getrennt von den Informationen zur Identifizierung der einzelnen Personen gespeichert sein, z.B. in getrennten Datenbanken und in verschlüsselter Form.

Pseudonymisierung verhindert, dass Dritte ohne Weiteres personenbezogene Daten einzelnen Betroffenen zuordnen können.

Verschlüsselung

Mit der Verschlüsselung von personenbezogenen Daten bleibt im Gegensatz zur Pseudonymisierung der **Personenbezug** von Informationen bestehen. Allerdings werden diese bei einer ausreichend starken Verschlüsselung in eine derart unleserliche Zeichenfolge umgewandelt, dass die Gefahr der Offenlegung gegenüber einem Unbefugten minimiert wird. Grundsätzlich sollte die Speicherung aller personenbezogenen Daten – vor allem bei einer Online-Speicherung in z.B. der Cloud des Unternehmens oder auch bei einer lokalen Speicherung auf dem Computer im Home-Office – verschlüsselt erfolgen. Für eine sichere **E-Mail-Kommunikation** mit dem Mitarbeiter im Home-Office ist auch hier eine Verschlüsselung notwendig: Mithilfe einer Ende-zu-Ende-Verschlüsselung wird der Nachrichteninhalt an den Endpunkten der Übertragung ver- und wieder entschlüsselt. E-Mails werden folglich vom Versender verschlüsselt und müssen vom Empfänger erst entschlüsselt werden, um lesbar zu sein. Eine Ende-zu-Ende-Verschlüsselung ist z.B. über gängige Standards wie PGP und S/MIME möglich. Während die E-Mail bei der Ende-zu-Ende-Verschlüsselung auch am Ende der Leitung noch verschlüsselt ist, ist dies bei der häufig eingesetzten SSL/TLS-Verschlüsselung bzw. Transportverschlüsselung nicht der Fall: Die Übermittlung der E-Mail erfolgt zwischen dem Postausgangsserver des Senders und dem Posteingangsserver des Empfängers grundsätzlich unverschlüsselt.

Verschlüsselung verhindert, dass Dritte ungehindert personenbezogene Daten lesen und verwenden können.