Datenschutz & IT-Sicherheit

Die Datenschutzgrundverordnung fordert Maßnahmen zur Gewährleistung der IT-Sicherheit. Datenschutz und IT-Sicherheit greifen ineinander, zum Beispiel durch TOMs (Technische und organisatorische Maßnahmen), durch Zugriffskonzepte und durch Schulungen.

So sind technische und organisatorische Maßnahmen nach Artikel 32 DSGVO zwingend erforderliche Sicherheitsvorkehrungen, um personenbezogene Daten vor unbefugtem Zugriff, Verlust oder Zerstörung zu schützen. Diese umfassen sowohl technische IT-Sicherheitslösungen wie Verschlüsselung und Firewalls als auch organisatorische Regelungen wie Zugriffskonzepte sowie Mitarbeiterschulungen. TOMs müssen dokumentiert werden. IT-Sicherheit bedeutet Risikomanagement, aber auch Effizienz und Kostenkontrolle. Eine Compliance zwingt zur sauberen Governance, indem Rollen, Prozesse und Kontrollen eingeführt werden.

Governance bedeutet dabei die Art und Weise der Steuerung, Führung und Kontrolle von Organisationen. Es umfasst die Strukturen, Prozesse und Regeln, die verantwortungsvolles Handeln, Transparenz und die Einhaltung von Normen sicherstellen. Klare Regeln für Auskünfte, Prozesse, Aufbewahrung und Löschungen schaffen Verantwortlichkeiten sowie Sicherheit im Arbeitsalltag.

Datenschutzverletzungen können vorab in IT-Systemen durch Privacy by Design verhindert werden. Dies meint Datenschutz durch Technikgestaltung bereits bei der Planung und Entwicklung von Systemen. Mittels technischer Maßnahmen wie Verschlüsselung und datenminimierenden Voreinstellungen (Privacy by Default) werden Verletzungen der Privatsphäre von Beginn an verhindert. Datenschutz ist gemäß Artikel 25 DSGVO ein integraler Bestandteil der Technikgestaltung und der Architektur von Hard- und Software.

Wichtige Konzepte sind hierbei:

- Anonymisierung und Pseudonymisierung: Daten werden so verarbeitet, dass sie nicht ohne Weiteres einer Person zugeordnet werden können.
- Verschlüsselung: Datenübertragungen und Speicherungen erfolgen verschlüsselt.
- Datenminimierung: Es werden nur Daten erhoben, die für den spezifischen Zweck unbedingt erforderlich sind.
- Zweckbindung: Nutzung der Daten nur für den ursprünglich definierten Zweck.
- Sensibilisierung: Dies senkt die Fehlerquote bei Themen wie Phishing oder Fehlversand.

Der Datenschutz unterstützt Governance- und Kontrollsysteme angrenzend an GRC (Governance, Risk and Compliance) und ISMS (Informationssicherheitsmanagementsystem). Diese sind eng verzahnt, um Informationssicherheit als Teil der Unternehmensführung nach ISO 27001 oder BSI IT-Grundschutz zu etablieren. Dies erhöht die Führungssicherheit und dient der Haftungserleichterung. Weniger Daten bei höherer Datenqualität führen zu verringerten Angriffsflächen, während eine saubere Datenhaltung Speicher- und Compliance-Folgekosten reduziert.

Abschließend reduziert Datenschutz Schadensersatz- und Prozessrisiken, verhindert behördliche Eingriffe und vermeidet Buß- oder Zwangsgelder. Compliance-Maßnahmen senken sowohl die Eintrittswahrscheinlichkeit als auch die Schadenshöhe von Datenpannen, die ansonsten schnell zu Management-Themen eskalieren.