

Da mich dazu immer wieder Fragestellungen erreichen, hier ein kurze Schilderung, welche Gemeinsamkeiten haben der Datenschutzbeauftragte (DSB) und der Informationssicherheitsbeauftragte (ISB) und was trennt sie auf der anderen Seite?

Im Standard-Datenschutz-Modell (SDM)[1] ist in der Einleitung festgehalten, dass DSB und ISB eine gemeinsame Sprache finden müssen, um rechtliche Anforderung des Datenschutzes zur Verwendung von Daten und deren Aufbewahrung sicherzustellen. Aus Sicht des Datenschutzes ergeben sich aus den 7 Gewährleistungszielen mehrfache Überschneidungen.

i. Datenschutz



Transparenz

In unterschiedlichem Maße müssen Betroffene, Betreiber von Systemen und Kontrollinstanzen erkennen können, welche Daten wann, für welchen Zweck erhoben, verarbeitet werden, welche Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung in den einzelnen Phasen besitzt. Transparenz von der Entstehung bis zur Löschung.



Nichtverkettung

Die Vermeidung einer Zusammenführung / Verkettung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, ist durch technische und organisatorische Maßnehmen sicherzustellen (Pseudonymisierung, Anonymisierung, Berechtigungskonzepte). Eine rechtliche zu-lässige Verkettung ist nur unter eng definierten Umständen möglich.



Datenminimierung

Das Minimierungsgebot erstreckt sich nicht nur auf die Menge der verarbeiteten Daten, sondern auch auf den Umfang der Verarbeitungen, die Speicherfristen und die Zugänglichkeit (je weniger und je kürzer, desto besser).



Intervenierbarkeit

Erfüllung der den Betroffenen zustehenden Rechten auf Benachrichtigung, Auskunft, Berichtigung, Löschung, Einschränkung, Übertragbarkeit, Widerspruch und Eingriff in automatisierte Bewertungs- und Entscheidungsprozesse, Profiling, sowie Maßnahmen zur Identifizierung bzw. Authentisierung. Zwecks Erfüllung der Betroffenenrechte und möglichen, behördlichen Anordnungen muss der Verantwortliche jederzeit Eingriff in die Prozesse nehmen können.

ii. Datenschutz und Datensicherheit



Vertraulichkeit

Kein Zugriff, Kenntnisnahme oder Nutzung der Daten durch unbefugte Dritte, ob externe, Beschäftigte oder alle Arten von Dienstleistern. Dies gilt auch bei allen Arten von Zwischenfällen.

1 *Quelle: Datenschutzkonferenz der Länder DSK: „Standard Datenschutz Modell“*

CC BY SA

Integrität

Sicherstellung der technischen Prozesse und Systeme in Bezug auf die kontinuierliche Einhaltung der festgelegten Spezifikationen, sowie der Erhalt der Vollständigkeit, Richtigkeit, Unversehrtheit und Aktualität der Daten. Angemessene und regelmäßige Überwachung der Einhaltung, um Abweichungen festzustellen und anzupassen, wo es erforderlich ist. Neben der Fehlerfreiheit ist die Diskriminierungsfreiheit bei automatisierten Bewertungs- und Entscheidungsprozessen IM VORFELD zu prüfen, festzulegen und im Prozess sicherzustellen.

Verfügbarkeit

Unverzüglicher Zugriff auf und Auffindbarkeit der (personenbezogenen) Daten und der Verarbeitung im ordnungsgemäß vorgesehenen Prozess, einschließlich einer angemessenen, gut verständlichen Darstellung für die Person (Datenmanagement – Systeme, Datenbanken, Suchfunktionen). Ein Schutz und zügiger Zugriff auch bei physischen oder technischen Zwischenfällen und bei hoher Systemlast. Bei Ausnahme eines Störfalles sind und werden Maßnahmen zur Behebung getroffen.

iii. Datenschutzbeauftragte[2]:

Aufgaben

Ein Datenschutzbeauftragter überwacht und unterstützt die Einhaltung der Datenschutzgesetze im Unternehmen. Seine Tätigkeit umfasst unter anderem:

- Beratung der Geschäftsführung und Mitarbeitenden zu Datenschutzfragen.
- Überwachung der Einhaltung der DSGVO und anderer Datenschutzvorschriften.
- Prüfung und Dokumentation von Datenverarbeitungsprozessen.
- Durchführung oder Koordination von Schulungen zum Datenschutz.
- Ansprechpartner für Betroffene und Aufsichtsbehörden.
- Meldung und Bewertung von Datenschutzvorfällen.

Der Fokus liegt auf dem Schutz personenbezogener Daten und der Wahrung der Rechte der Betroffenen. Aufsichtsbehörde: BfDI – Bundesbeauftragte/r für den Datenschutz und die Informationsfreiheit und deren Vertretern in den Ländern.

Erforderlichkeit

Ein Datenschutzbeauftragter lohnt sich spätestens, wenn die gesetzlichen Schwellen erreicht oder sensible Daten verarbeitet werden. Oft lohnt er sich aber schon früher, weil er Risiken minimiert, Prozesse sauber aufsetzt und Vertrauen schafft. 😉

iv. Informationssicherheitsbeauftragte[3]:

Aufgaben

Ein Informationssicherheitsbeauftragter ist für die Sicherheit aller Informationen im Unternehmen verantwortlich – unabhängig davon, ob personenbezogen oder nicht. Seine Aufgaben beinhalten:

- Aufbau, Pflege und Weiterentwicklung eines Informationssicherheitsmanagementsystems (ISMS).
- Analyse von Risiken für IT-Systeme und Geschäftsprozesse.
- Definition und Überwachung von Sicherheitsmaßnahmen (technisch und organisatorisch).
- Sensibilisierung und Schulung der Mitarbeitenden zur Informationssicherheit.
- Koordination bei Sicherheitsvorfällen und Unterstützung im Incident Management.
- Beratung der Unternehmensleitung zu Sicherheitsstrategien.

2 Quelle: Management-Info zum Standard-Datenschutz-Modell
3 Quelle: Management-Info BSI / IT Grundschutz Basiswissen

CC BY SA

Der Fokus liegt auf Vertraulichkeit, Integrität und Verfügbarkeit aller Unternehmensinformationen. Aufsichtsbehörde: BSI – Bundesamt für Sicherheit in der Informationstechnik.

Erforderlichkeit

Ein Informationssicherheitsbeauftragter lohnt sich spätestens, wenn ein ISMS (Informations-Sicherheits-Management-System eingeführt, NIS-2-Pflichten zu erfüllen sind oder ein erhöhtes Cyberrisiko besteht. In der Praxis setzen viele Unternehmen bereits früher auf einen ISB, um Haftungsrisiken zu reduzieren, Prozesse zu professionalisieren und Angriffe zu verhindern.

v. Fazit:

- ✔ Datenschutzbeauftragter (DSB): Überwacht die Einhaltung von Datenschutzgesetzen, berät Mitarbeiter und Geschäftsführung beim Umgang mit Kund- oder Mitarbeiterdaten und dokumentiert Verarbeitungsprozesse.
- ✔ Informationssicherheitsbeauftragter (ISB): Schützt das Unternehmen vor Ausfällen, Spionage oder Datenklau durch die Sicherung der Vertraulichkeit, Verfügbarkeit und Integrität aller Daten und Systeme.
- ✔ Beide Rollen ergänzen sich ideal, sollten aber wegen möglicher Interessenkonflikte (z. B. bei Überwachungsmaßnahmen am Arbeitsplatz) in der Organisation möglichst nicht von derselben Person in Personalunion ausgeübt werden.

Weiterführende Informationen

Bei Bedarf, einfach einmal sprechen!

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtigkeit und Vollständigkeit übernehmen kann. Aus Gründen der besseren Lesbarkeit Verwendung der männlichen Form, die alle Geschlechter mit einbezieht.

CC BY SA