DSGVO – Technische und organisatorische Anforderungen und Herausforderungen

Die Umsetzung der EU-Datenschutz-Grundverordnung (DSGVO) verlangt von Unternehmen, insbesondere solchen, die personenbezogene Daten in größerem Umfang verarbeiten, die Einhaltung verschärfter Datenschutz- und Sicherheitsvorgaben. Ziel ist es, bestehende IT- und Geschäftsprozesse auf ein höheres Schutzniveau zu heben und die Rechte von betroffenen Personen umfassend zu wahren.

Ein zentrales Element der DSGVO-Anforderungen ist der Schutz personenbezogener Daten auf technischer und organisatorischer Ebene. Dazu gehört unter anderem die systematische Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen, die Identifikation sensibler Datenbestände und die kontinuierliche Analyse potenzieller Gefährdungen. Es müssen Verfahren implementiert werden, mit denen Datenschutzverletzungen erkannt, bewertet und behoben werden können. Technisch bedeutet das u. a. den Einsatz von Verschlüsselung, Pseudonymisierung, Zugriffskontrollen sowie regelmäßige Sicherheitsüberprüfungen.

Ein weiteres wesentliches Ziel der DSGVO ist die Gewährleistung von Integrität, Verfügbarkeit und Vertraulichkeit bei der Verarbeitung personenbezogener Daten. Hierzu zählen Maßnahmen wie rollenbasierte Zugriffskonzepte, Multi-Faktor-Authentifizierung (MFA), Verschlüsselung bei der Speicherung und Übertragung sowie ein zentrales Identitäts- und Berechtigungsmanagement.

Die DSGVO fordert eine lückenlose Dokumentation von Verarbeitungstätigkeiten (Art. 30 DSGVO) und die Überwachung von Datenschutz-relevanten Ereignissen. Die daraus gewonnenen Informationen müssen nicht nur für interne Prozesse genutzt werden, sondern auch im Rahmen der Rechenschaftspflicht gegenüber Aufsichtsbehörden verfügbar sein.

Protokoll- und Verarbeitungsdaten erzeugen hohe Anforderungen an Speicher, Datenmanagement und insbesondere den Datenschutz. Es muss sichergestellt werden, dass Daten rechtmäßig, transparent und zweckgebunden verarbeitet werden (Art. 5 DSGVO). Dies gilt umso mehr, wenn besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO betroffen sind.

Auch die Zusammenarbeit mit Auftragsverarbeitern oder Drittanbietern erfordert klare vertragliche Regelungen (Art. 28 DSGVO) sowie laufende Kontrollen der Einhaltung der Datenschutzpflichten.

Darüber hinaus verlangt die DSGVO wirksame Vorkehrungen gegen Datenpannen. Technisch bedeutet das unter anderem regelmäßige Backups, Notfallpläne, Tests der Wiederherstellbarkeit sowie klare Vorgaben für die Meldewege im Fall einer Datenschutzverletzung. Verantwortliche müssen Verstöße innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde melden (Art. 33 DSGVO) und gegebenenfalls auch die betroffenen Personen informieren (Art. 34 DSGVO).

Ein weiterer Schwerpunkt liegt auf der Gewährleistung der Betroffenenrechte (Art. 12–22 DSGVO). Unternehmen müssen Prozesse und technische Lösungen vorhalten, um Auskunfts-, Lösch-, Berichtigungs- oder Widerspruchsanfragen effizient und fristgerecht umzusetzen.

Die Herausforderung liegt nicht nur in der Einführung neuer technischer Maßnahmen, sondern vor allem in der nachhaltigen, datenschutzgerechten und integrierten Umsetzung innerhalb des gesamten Unternehmens. Eine langfristig erfolgreiche DSGVO-Compliance erfordert deshalb ein Zusammenspiel aus technischem Know-how, Prozessverständnis, rechtlicher Expertise und interdisziplinärer Zusammenarbeit.

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg

DSGVO-Betroffenheits-Checkliste

Ziel: Herausfinden, ob Ihr Unternehmen unter die Regelungen der DSGVO fällt – und damit verpflichtet ist, umfassende Datenschutzmaßnahmen umzusetzen.

1. Verarbeitung personenbezogener Daten

Fragen:	Ja	Nein
Verarbeiten wir personenbezogene Daten von Kunden, Beschäftigten oder Dritten?	☐	☐
Verarbeiten wir besondere Kategorien personenbezogener Daten (Gesundheitsdaten, biometrische Daten etc.)?	☐	☐
Nutzen wir Systeme, die personenbezogene Daten automatisch verarbeiten (z. B. CRM, ERP, HR-Software)?	☐	☐

---

2. Rolle des Unternehmens

Fragen:	Ja	Nein
Sind wir Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO?	☐	☐
Treten wir als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO auf?	☐	☐
Arbeiten wir mit externen Auftragsverarbeitern zusammen (Cloud-Dienste, Hosting, Outsourcing)?	☐	☐

---

3. Unternehmensgröße und Umfang der Verarbeitung

Fragen:	Ja	Nein
Beschäftigen wir ≥ 250 Mitarbeitende?	☐	☐
Verarbeiten wir regelmäßig Daten von mehr als 5.000 betroffenen Personen im Jahr?	☐	☐
Sind wir gesetzlich verpflichtet, einen Datenschutzbeauftragten zu benennen (Art. 37 DSGVO)?	☐	☐

---

4. Risiken und Auswirkungen

Fragen:	Ja	Nein
Würde ein Verlust oder Missbrauch unserer Daten erhebliche Risiken für Betroffene nach sich ziehen?	☐	☐
Führen wir Verarbeitungstätigkeiten durch, die eine Datenschutz-Folgenabschätzung (DSFA) erfordern (Art. 35 DSGVO)?	☐	☐
Sind unsere Systeme potenziell Ziel von Cyberangriffen oder Datenlecks?	☐	☐

Auswertung der Checkliste

Anzahl "Ja" Antworten	Einschätzung
0–2	Wahrscheinlich nicht betroffen / geringes Risiko – dennoch Grundpflichten beachten
3–5	Möglicherweise betroffen – detaillierte Prüfung dringend empfohlen
6 oder mehr	Sehr wahrscheinlich betroffen – umfassende DSGVO-Compliance zwingend erforderlich

---

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg