EU-CON BERATERFORUM GMBH

Verbindliche Vorgaben & Zweck der Vorgaben

Die DSGVO hat unmittelbare Auswirkung auf jede Unternehmensorganisation und setzt auf eine Selbstverpflichtung in Form einer **Rechenschaftspflicht** (ordinäre Compliance). Dabei führt die Rechenschaftspflicht zu einer **Beweislastumkehr** für jedes datenverarbeitende Unternehmen dahingehend, dass es darlegen muss, angemessene Maßnahmen ergriffen zu haben, um eine rechtskonforme Datenverarbeitung zu gewährleisten. Daraus ergibt sich aus Beweissicherungsgründen eine umfassende **Dokumentationspflicht**.

Das Unternehmen muss eigenverantwortlich eine Datenschutz-Folgen-Abschätzung (vgl. Vorabkontrolle), also eine **Risikoanalyse** vornehmen, und mögliche Schwachstellen bei der Datenverarbeitung identifizieren.

Der Datenschutzbeauftragte muss deshalb unbedingt **alle Datenverarbeitungsprozesse**, also **Datenströme** in einem Unternehmen kennen (wann, wie, durch wen, in welchem System, werden welche Daten verarbeitet und weitergegeben).

Ziel bzw. Best Practice für jedes Unternehmen soll sein:
Zusammenspiel von **QM + DS-Management + IT-Sicherheitsmanagement** (vgl. TOM´s), um absolute **Transparenz** des Datenflusses sowie ein schnelles Handeln bei DS-Vorfällen und in Fällen von Auskunftsbegehren durch Betroffene und Behörden zu garantieren. Kurz: Das Unternehmen muss umfassend **reaktionsfähig** sein.

Das Unternehmen trifft die Pflicht zur regelmäßigen **Kontrolle** der getroffenen Maßnahmen, zur Überprüfung der Risikobereiche und zur Durchführung von Penetrationstests.

Darüber hinaus trifft das Unternehmen eine umfassende **Informationspflicht**:
Informationen über die Datenverarbeitung (konkret: über den Zweck der Verarbeitung, die Speicherdauer, Empfänger von Daten usw.) müssen präzise, transparent, verständlich, in leicht zugänglicher Form und in klarer und einfacher Sprache vorliegen (z.B. Datenschutzerklärung, Einwilligungserklärung, AGB usw.)

Kurzinfo & Checkliste zur Umsetzung der EU-DSGVO

EU-CON BERATERFORUM GMBH

1	**ÜBERSICHT DER DATENSTRÖME SCHAFFEN**
	Erfassung aller externen Dienstleister
	Erfassung aller Datenverarbeitungssysteme (Systemübersicht)
	Verfahrensverzeichnisse erstellen bzw. Verzeichnis von Verarbeitungstätigkeiten (VVT)
	Sofern noch nicht geschehen: Erst-Audit (Bestandsaufnahme des Ist-Zustandes)
2	**PRÜFUNG (U.U. DURCH / MIT HILFE DES DATENSCHUTZBEAUFTRAGTEN)**
	Rechtsgrundlagen der Datenverarbeitung: ADV, SCC usw. notwendig?
	Verpflichtung auf Daten-, Fernmelde-, Bank-, Firmengeheimnis o.ä. notwendig?
	Vorabkontrolle / Risikofolgenabschätzung (kritischer) Systeme
	Privacy by Design / Privacy by Default (verbraucher- und datenschutzfreundliche Voreinstellungen) notwendig und ggf. prüfen
	Löschfristen definieren
3	**(RISIKO-)BERICHT**
	Zusammenführung der Ergebnisse der Vorabkontrollen/Risikofolgenabschätzungen, der Verfahrensverzeichnisse/Verzeichnis von Verarbeitungstätigkeiten und der Vor-Ort-Audits zu einem (Risiko-) Bericht, der alle datenschutzrechtlich relevanten Bereiche umfasst (u.a. eingesetzte Systeme, verantwortliche Personen, Rollen- & Berechtigungskonzept, TOM´s, Löschkonzept, Transparenz der Datenströme usw.)
4	**MAßNAHMENPLAN & -UMSETZUNG AUF GRUNDLAGE DES (RISIKO-) BERICHTS**
	Technisch-organisatorische Maßnahmen anpassen
	Vertragliche / rechtliche Maßnahmen (Datenschutzerklärung/ AGB´s/ Einwilligungen usw.)
	Notfallplan
	Erstellung einer Datenschutz-Leitlinie/ DS-Handbuch/ Policies
5	**VERBINDLICHE INFORMATIONEN UND SENSIBILISIERUNG DER MITARBEITER**
	Arbeitsanweisungen
	Datenschutzhandbuch/ Policy
	Live-/ Online-Schulungen
	Datenschutzbeauftragten als Ansprechpartner bekannt machen
6	**REGELMÄSSIGE KONTROLLEN DER BESTEHENDEN MAßNAHMEN (PDCA-ZYKLUS)**
	Penetrationstests / Testweise Rückspielung von Datensicherungen
	Re-Audits (auch Niederlassungen)
	Einbeziehung des DSB in neue Maßnahmen
	Kontrollen der Lieferanten, Auftraggeber, Auftragnehmer