DataAgenda - das Informationsportal zum Datenschutzrecht

Präsentiert von DATAKONTEXT

www.DataAgenda.de

@dataagenda

Checkliste Datenschutzorganisation

Der Begriff „Datenschutzorganisation“ findet sich nicht in der Datenschutz-Grundverordnung (DS-GVO). Der Gesetzgeber hat aber vorgesehen, dass die jeweilige Organisation nachweisen muss, dass gesetzliche und weitere Vorgaben eingehalten werden. Ein systematisches und strukturiertes Vorgehen und Auseinandersetzen mit den Anforderungen sind daher unerlässlich.

Mit der folgenden Checkliste können Sie im Sinne eines Best-Practise-Ansatzes prüfen, ob eine wirksame Datenschutzorganisation implementiert ist bzw. in welchen der vier Bereiche

(1) Struktur und Aufbauorganisation
(2) Ordnungsrahmen und Führung
(3) Prozesse / Ablauforganisation
(4) Systeme und Support

ggf. Handlungsbedarf besteht.

(1) Struktur und Aufbauorganisation

- Datenschutz ist Aufgabe der gesamten Organisation; Bestimmung einer geeigneten Form der Organisation des Datenschutzes (zentral, dezentral, hybrid) unter Berücksichtigung des generellen Organisationsmodells und der Risikoerwartung – insbesondere in größeren / internationalen Organisationen.
- Eindeutige und nachvollziehbare Festlegung und Dokumentation der Gesamtverantwortung (Accountability), der Durchführungsverantwortung (Responsibility) sowie der Unterstützungs- und Beratungsfunktionen (Rollen und Aufgaben) in der Datenschutzorganisation.
- Empfehlung, eine Funktion in der Organisation zu etablieren, die die fachbereichsübergreifende (Weiter-)Entwicklung und Führung der Datenschutzorganisation steuert und koordiniert, z.B. einen Datenschutzmanager oder ein (institutionelles oder virtuelles) Datenschutz-Team.
- Transparente Dokumentation und Kommunikation der Stellen, Teams und/oder Gremien, die mit den Steuerungs-, Durchführungs-, Koordinations-, Unterstützungs- und Beratungsaufgaben in der Datenschutz-Organisation betraut sind.
- Benennung eines Datenschutzbeauftragten (DSB), sofern die gesetzlichen Voraussetzungen gem. DS-GVO und Bundesdatenschutzgesetz (BDSG) gegeben sind, bzw. freiwillig, wenn die Organisation bspw. zur Risikominimierung einen kompetenten Ansprechpartner für alle Datenschutzfragen zur Verfügung stellen will.
- Ausreichende Dimensionierung der einzelnen mit Datenschutzaufgaben befassten Stellen/ Teams und/oder Gremien (personelle, finanzielle, materielle und zeitliche Ressourcen).

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

(2) Ordnungsrahmen und Führung

- Festlegung von Datenschutzzielen und einer Datenschutzkultur, die sich am Geschäftsmodell und der Strategie der Organisation orientieren, und Dokumentation in einer Datenschutz-Leitlinie.
- Etablierung eines Rahmenregelwerks (z.B. in Form einer oder mehrerer Datenschutz-Richtlinien), dass den Datenschutz in der erforderlichen Detaillierung regelt und den Beschäftigten zur Verfügung gestellt wird.
- Bereitstellung von arbeits- und aufgabenspezifischen Materialien (z.B. Handlungsanweisungen, Maßnahmenpläne, Muster, Checklisten) für die Beschäftigten inkl. regelmäßigen Trainings.
- Führungskräfte fördern die weitgehende Integration der Umsetzung datenschutzrechtlicher Anforderungen in die „normalen“ betrieblichen Arbeitsprozesse (Datenschutz ist kein add on).
- Erarbeitung, Umsetzung und regelmäßige Aktualisierung eines Schulungs- und Awareness-Konzepts, mit dem die Beschäftigten der Organisation regelmäßig und wirksam im Datenschutz unterwiesen werden.
- Verpflichtung der Beschäftigten zur Vertraulichkeit.

(3) Prozesse

- Beschreibung und Etablierung eines Prozesses zur Dokumentation neuer bzw. geänderter Verarbeitungen im Verzeichnis der Verarbeitungstätigkeiten des Verantwortlichen und des Auftragsverarbeiters inkl. regelmäßigem Training der involvierten Beschäftigten.
- Festlegung und Dokumentation der Prozesse zur Erfüllung der Informationspflichten und Betroffenenrechte inkl. regelmäßigem Training der involvierten Beschäftigten.
- Einrichtung und Dokumentation eines Prozesses zum Umgang mit Datenschutzverletzungen inkl. der Schnittstelle zur Informationssicherheit. Regelmäßige Sensibilisierung aller Beschäftigten auf potenzielle Risikobereiche.
- Beschreibung, Kommunikation und praktische Umsetzung der Dokumentationsprozesse zum Nachweis der Einhaltung der gesetzlichen und betrieblichen Anforderungen.
- Definition und Kommunikation der Einbindung des DSB und/oder weiterer Unterstützungs- und Beratungsfunktionen in den betreffenden Prozessen und regelmäßige Anwendung in der Praxis.
- Etablierung einer Systematik (Datenschutzmanagementsystem), mit der die Einhaltung der aktuellen betrieblichen, organisatorischen und gesetzlichen Vorgaben und Ziele regelmäßig überwacht, kontrolliert und weiterentwickelt werden.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

(4) Systeme und Support

- Einrichtung eines dokumentierten IT-Sicherheitsmanagements nach dem Stand der Technik inkl. der Schnittstellen und redundanzfreien Regelungen zum Datenschutz und Umsetzung in der Praxis.
- Einhaltung der Grundsätze des Privacy by Design und des Privacy by Defaults bei der Entwicklung bzw. der Beschaffung und dem Einsatz von IT-Systemen, Apps, IT-Tools etc.
- Organisation des Zugangs zu IT-Systemen und Zugriff auf personenbezogene Daten nach dem „need-to-know"-Prinzip.
- Festlegung und Kommunikation der Nutzung der dienstlichen IT-Infrastruktur (insbesondere Abgrenzung der privaten Internet- und E-Mail-Nutzung) sowie Regelungen für das Arbeiten im Homeoffice/Mobiles Arbeiten.
- Löschung von personenbezogenen Daten aus IT-Systemen auf Basis der von den Fachbereichen erstellten Löschkonzepte; klare Regelungen zur Entsorgung von IT-Komponenten und Dokumenten.
- Zusammenarbeit mit Dienstleistern, Partnern und Lieferanten mit Zugang zu personenbezogenen Daten unter Einhaltung der gesetzlichen Anforderungen an eine Auftragsverarbeitung (Art. 28 DS-GVO), ein Joint Controllership (Art. 26 DS-GVO) oder den Regelungen zur Übermittlung personenbezogener Daten (Art. 40 ff. DS-GVO).

Autor

Uwe Bargmann
Freiberuflicher Berater Datenschutzmanagement, Kooperationspartner der DMC Datenschutz Management + Consulting GmbH & Co KG