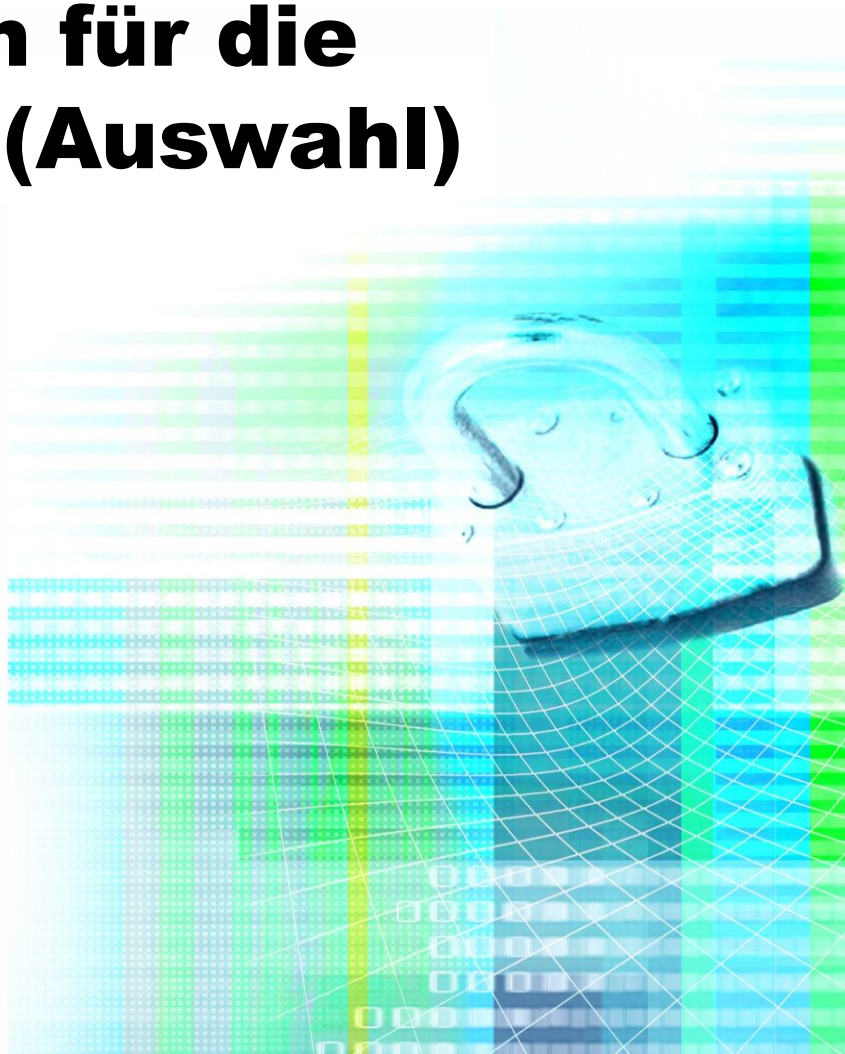
EU-Datenschutzgrundverordnung – Anforderungen für die Verantwortlichen (Auswahl)

RA Dr. Jan K. Köcher
Datenschutzauditor, DFN-CERT
koecher@dfn-cert.de



Überblick EU-DSGVO

- **Ziel: Europaweite Vereinheitlichung der Vorgaben zum Datenschutz**
- **Unmittelbare Geltung ab dem 25.5.2018**
- (Grund-)Verordnung
- Anwendungsvorrang
- Zahlreiche relevante Änderungen, u.a.:
- Aufgaben des behördlichen Datenschutzbeauftragten
- Recht auf Auskunft
- Verzeichnis der Verarbeitungstätigkeiten
- Schadenersatz
- Meldepflicht
- Rechenschaftspflicht

Verantwortlichkeit für die Umsetzung des Datenschutzes

- **Verantwortliche Stelle**
- Muss alle Anforderungen aus der EU-DSGVO erfüllen
- Grundsätzlich keine Option zur Übertragung der Umsetzung an den behördlichen DSB

- **Behördlicher Datenschutzbeauftragter (bDSB)**
- Überwachung der Umsetzung des Datenschutzes
- Unterstützung der Leitung bei der Umsetzung auf Anfrage
- Unterstützung der mit der Umsetzung beauftragten Mitarbeiter
- Beratung von Projekt- und Prozessverantwortlichen
- Ansprechpartner für die Aufsichtsbehörden

Recht auf Auskunft

Art. 15 Recht auf Auskunft

- **Auskunft ob personenbezogene Daten verarbeitet werden**
- **Anspruch auf kostenlose Kopie eigener Daten**

➢ Problematische Formulierung in Art. 15 Abs. 3: „Der Verantwortliche stellt **eine Kopie** … zur Verfügung.

- **Weitere Informationen zur Verarbeitung:** Zwecke, Empfänger, Speicherdauer, Betroffenenrechte, Ggf. Auskunft zur Datenquelle, Ggf. automatisierte Entscheidungen, Ggf. Übermittlung Drittland
- **Frist zur Auskunfterteilung:** Innerhalb eines Monats nach Eingang des Antrags, Ausnahmsweise Fristverlängerung um zwei Monate

Verfahrensverzeichnis

Gibt es als solches nicht mehr:

Nach Außen, Art. 13 - 15:

- **Erweiterte Informationspflichten**
- Inhaltlich ähnlich wie bisher Verfahrensverzeichnis
- Anforderungen an Form ähnlich wie bisher Datenschutzerklärungen auf Webseiten

Nach Innen, Art. 30:

- **Verzeichnis von Verarbeitungstätigkeiten**
- **Verpflichtet:** Verantwortlicher und Auftragsverarbeiter
- **Einsicht:** Aufsichtsbehörde auf Anfrage
- **Form:** Schriftlich, kann auch im elektronischen Format erfolgen

Schadenersatz

Art. 82:

- **Materielle und immaterielle Schäden durch Verletzung EU-DSGVO**
- **Ersatzpflichtig:**
- Verantwortliche
- Auftragsverarbeiter
- **Außenverhältnis: Gesamtschuldnerische Haftung jedes Verantwortlichen/ Auftragsverarbeiters**

Weitere Folgen bei Verstößen

- **Bußgelder**
  - ➢ Für öffentliche Stellen niedriger oder sogar ausgeschlossen
  - ➢ Aber für die An-Institute weiter relevant
- **Anweisungen durch die Aufsichtsbehörde (Art. 58)**
- **Reputationsverlust**
- **Eigene Schäden**

Meldepflicht Art. 33 EU-DSGVO

- **Innerhalb von 72 Stunden nach Bekanntwerden an die zuständige Aufsichtsbehörde**
- Auftragsverarbeiter hat eine Verletzung unverzüglich an den Verantwortlichen zu melden
- **Ausnahme:** Verletzung führt voraussichtlich nicht zu einem Risiko für Rechte und Freiheiten natürlicher Personen

Inhalt:

- Beschreibung Art der Verletzung, Kategorien, ungefähre Anzahl Betroffener, ungefähre Zahl betroffener Datensätze
- Name und Kontaktdaten des Datenschutzbeauftragten
- Beschreibung der wahrscheinlichen Folgen
- Beschreibung der ergriffenen und vorgeschlagenen Maßnahmen zur Behebung oder Abmilderung

Rechenschaftspflicht

Neu:

Art. 5 Abs. 2: „Der Verantwortliche ist für die Einhaltung des Absatzes 1 [Datenschutzgrundsätze] verantwortlich und muss dessen Einhaltung nachweisen können."

Art. 24 Abs. 1: „Der Verantwortliche setzt … geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt."

Datenschutzmanagement erforderlich!
Dokumentation von Maßnahmen!

Datenschutzmanagement (1)

Datenschutzorganisation

- **Bekenntnis der Leitungsebene zum Datenschutz, Förderung einer Datenschutz- und Sicherheitskultur**
- **Strukturelle Gewährleistung der Anforderungen**
- **Effektive Datenschutzkontrolle**
- Datenschutzbeauftragte(r) (DSB)
- Einbindung DSB in die Geschäftsprozesse und IT-Strategie / Vorabkontrolle
- IT-SiBe/DSB: Abgestimmte Sicherheitsstrategie
- Durchsetzung in allen Organisationseinheiten
- Gewährleistung einer Grundsicherheit
- Strukturelle Gewährleistung der Betroffenenrechte
- Information und Schulung der Mitarbeiter

Datenschutzmanagement (2)

Verarbeitungsbezogen:

- **Verarbeitungsverzeichnis**
- **Dokumentierte Maßnahmen zur Datensicherheit**
- **Dokumentierte Beurteilung neuer Verarbeitungen und wesentlicher Änderungen (Vorabkontrolle)**
- Rechtmäßigkeit, Datensparsamkeit, Zweckbindung, Informationspflichten, Betroffenenrechte, besondere Umstände
- **Gegebenenfalls: Ergänzende Maßnahmen zur Gewährleistung des Datenschutzes.**
- **Gegebenenfalls: Durchführung eine Datenschutz-Folgeabschätzung**
- **Gewährleistung der regelmäßigen/anlassbezogenen Überprüfung (Audits) von Maßnahmen auf ihre Wirksamkeit, ggf. Anpassung und Dokumentation (Plan, Do, Check, Act)**

Vorstellung

Eines Entwurfs für eine neue Datenschutzleitlinie

Struktur

Festlegung Ziele und Verantwortlichkeiten

1. Grundlage
   - Bedeutung des Grundrechts
   - Bekenntnis der Leitungsebene zur datenschutz-gerechten Aufgabenwahrnehmung und Förderung
2. Zielsetzung
   - Anhand der materiellen gesetzlichen Anforderungen
   - Einhaltung der Rechenschaftspflicht
3. Verantwortlichkeiten
4. Verstöße
5. Inkrafttreten

Vorstellung

Erforderlichkeit von Datenschutz-Koordinatoren

Ausgangspunkt

- **Verantwortliche Stelle**
- Muss alle Anforderungen aus der EU-DSGVO erfüllen
- Grundsätzlich keine Option zur Übertragung der Umsetzung an den behördlichen DSB

- **Behördlicher Datenschutzbeauftragter (bDSB)**
- Überwachung der Umsetzung des Datenschutzes
- Überwachung der Schulung
- Unterstützung der Leitung bei der Umsetzung auf Anfrage
- Unterstützung der mit der Umsetzung beauftragten Mitarbeiter
- Beratung von Projekt- und Prozessverantwortlichen
- Ansprechpartner für die Aufsichtsbehörden

Erforderlichkeit

- **Datenschutz-Koordinatoren zur Umsetzung des Datenschutzes**
  - Bereiche benennen Personen, die in ihrem Bereich IT-Verfahren und damit verbunden Datenschutz- und Sicherheitsmaßnahmen koordinieren
- **Datenschutzteam/Datenschutzlenkungs-kreis**
  - Informationsaustausch, einheitlicher Umsetzungsstand, Anpassung von Prozessen
  - Regelmäßige Treffen mit der behördlichen Datenschutzbeauftragten und dem IT-Sicherheitsbeauftragten

DFN CERT®

DFN Deutsches Forschungsnetz

Vielen Dank
für die Aufmerksamkeit

RA Dr. Jan K. Köcher
koecher@dfn-cert.de