Datenschutzbeauftragte nach der DSGVO

Herausforderungen in der Praxis

Mag. DI Dr. Bernhard Horn, CIPP/E
Oesterreichische Nationalbank

Herausforderung 1

Feststellung der Bestellungspflicht

- Jedenfalls bestellungspflichtig (Art 37 Abs 1)
  - Behörden (organisatorischer Behördenbegriff)
  - Öffentliche Stellen (Legaldefinition: § 4 Z 1 IWG)
- Andere nur unter bestimmten Voraussetzungen (Art 37 Abs 1)
  - *Kerntätigkeit* erfordert eine *umfangreiche* regelmäßige und systematische Überwachung betroffener Personen
  - *Kerntätigkeit* erfordert eine *umfangreiche* Verarbeitung von Daten nach Art 9 oder 10

Herausforderung 1

Feststellung der Bestellungspflicht

- Freiwillige Bestellung jederzeit möglich (Art 37 Abs 4)
  - Im Zweifel: Sichere Variante, ansonsten Begründung dokumentieren
    - *DSGVO muss ohnedies erfüllt werden*
    - *Milderungsgrund*
  - Löst alle Rechtsfolgen der Art 37 – 39 aus
    - *Falls nicht erwünscht: Andere Bezeichnung wählen („Datenschutzmanager“)*
- Risiko einer Fehlbeurteilung
  - Geldbuße, Unterlassungsklage nach § 1 UWG (Kontaktdatenveröffentlichung)

Herausforderung 2

Neues Rollenbild und Ressourcen

- Aufgaben und Verantwortlichkeiten (Art 38 und 39)
  - Beratungs- und Kontrollorgan
  - Kontaktperson für und Zusammenarbeit mit Datenschutzbehörde
  - Ansprechperson für betroffene Personen (Art 38 Abs 4)
    - *Direkte und vertrauliche Erreichbarkeit erforderlich, kein „Anwalt der Betroffenen“*
  - Geheimhaltungspflicht (Art 38 Abs 5, § 5 DSG)

Herausforderung 2

Neues Rollenbild und Ressourcen

- Unterstützung durch den Verantwortlichen - Ressourcen (Art 38 Abs 2)
  - Zeitliche Ressourcen
  - Infrastruktur (Büro, Arbeitsmittel, Literatur)
  - Aus- und Weiterbildung, beruflicher Austausch
  - Zugang zu Datenanwendungen
- Nebentätigkeiten oder Teilzeit-DSBA möglich (Art 38 Abs 6)
  - Kein Interessenkonflikt + hinreichend zeitliche Ressourcen!

Herausforderung 3

Verankerung der Position in der Aufbauorganisation

- Stellung von Datenschutzbeauftragten (Art 38 Abs 3)
  - Weisungsfreiheit und Unabhängigkeit (§ 5 Abs 3 DSG)
  - Keine Interessenskonflikte = keine Selbstkontrolle (4-Augen-Prinzip!)
  - Direkte Berichtslinie an die oberste Organisationsleitung
  - Kündigungsschutz (Verbot der Benachteiligung oder Abberufung)
- De facto Stabsstellenfunktion
- Anpassung von Prozessen erforderlich

Herausforderung 3

Verankerung der Position in der Aufbauorganisation

- Konzern- bzw. Behördengruppen-DSBA sind möglich (Art 37 Abs 2 und 3)
  - Leichte Erreichbarkeit für Verantwortliche, Betroffene und Behörde
    - *Sicherstellung einer effizienten Kommunikation*
  - Ordnungsgemäße Aufgabenerfüllung muss möglich sein
- Interne oder externe Bestellung (Art 37 Abs 6)
  - Situationsabhängige Abwägung der Vor- und Nachteile (Kombination?)
  - Externe DSBA: Klare Verantwortlichkeiten! Nur Rechtsanwälte?

Herausforderung 4

Finden einer geeigneten Person

- Berufliche Qualifikation und Fachwissen (Art 37 Abs 5)
  - Kenntnisse im Datenschutzrecht und der Datenschutzpraxis
  - Eignung zur Erfüllung aller Aufgaben nach Art 39
  - Komplexität der Organisation und der Verarbeitungen ausschlaggebend
- Verfügbarkeit geeigneter Personen?
- Verfügbarkeit gewillter Personen?
  - Keine Haftung nach § 9 VStG als beauftragter Verantwortlicher (Art 24)
  - Aber: Haftung nach DHG bzw. Vertrag

Herausforderung 5

Inbetriebnahme eines funktionierenden DSMS

- Klärung von Prozessen und Verantwortlichkeiten (Ablauforganisation)
  - Sicherstellung der frühzeitigen Einbindung des/der DSBA in alle Angelegenheiten mit Datenschutzbezug (Art 38 Abs 1)
  - Behandlung von Betroffenenrechten (Kapitel III)
  - Behandlung von Data Breaches (Art 33 f)
- Weitere Aufgaben möglich
  - Beispiel: Führung des Verarbeitungsverzeichnisses
  - Kein Interessenkonflikt, keine Selbstkontrolle!

Herausforderung 5

Inbetriebnahme eines funktionierenden DSMS

- Kontinuierliche Verbesserung: Plan – Do – Check – Act
  - Im gesamten DSMS (Art 24)
  - Für jede Verarbeitungstätigkeit (Art 25)
- Schulungs- und Awarenessmaßnahmen
- DSBA-seitig
  - Erstellung eines Audit- und Berichtsplans
  - Risikoorientierte Priorisierung der Tätigkeiten (Art 39 Abs 2)

De-facto Aufgaben von DSBA

- Aufbau einer Datenschutzkultur – Schulung und Awareness
- Auffinden von Verarbeitungen → Behandlung und Dokumentation
- Umsetzung der Grundsätze (Art 5)
- Sicherstellung der Rechtsgrundlagen (Art 6, 9, 10 + Materiengesetze)
- Formulierung der Datenschutzinformation (Art 13, 14)
- Umsetzung der Betroffenenrechte (Kapitel III)
- Durchsetzung von Privacy by Design (Art 25)
- Verarbeitungsverzeichnis (Art 30)
- Sicherheit der Verarbeitung (Art 32)

De-facto Aufgaben von DSBA

- Data-Breach-Notification (Art 33, 34)
- Outsourcing/Cloud Computing (Art 28)
- Internationale Datentransfers (Kapitel V)
- Mitwirkung bei Prozess- und Regelungsgestaltung (Art 24 Abs 2)
- Verfassung von Stellungnahmen und Leitlinien
- Monitoring der gesetzlichen Entwicklungen
- Keep DSMS alive!

- **Dokumentation der eigenen Tätigkeit und von Dissenting Opinions!**

Vielen Dank für die Aufmerksamkeit!