DATENSCHUTZBEAUFTRAGTER
Büro für Datenschutz & Datensicherheit

Mehr Pflichten und neue Aufgaben im Datenschutz Management für die Geschäftsleitung

27.4.2017 – OÖ Datenschutztag

Felix Hörlsberger

DORDA

WIR SCHAFFEN KLARHEIT.

Ansprechpartner

MMag Dr Felix Hörlsberger

- Partner bei DORDA
- Universität Wien (Dr iur 2003; Ranking Top 1%) und der Wirtschaftsuniversität Wien (Mag rer soc oec 2003)
- Fachliche Schwerpunkte: Restrukturierungen, Versicherungsrecht, Datenschutzrecht, Zivilprozessrecht, Compliance
- Empfohlen von den renommierten internationalen Handbüchern „Chambers Global“ und „Legal 500“ für seine Expertise in Restrukturierungen und für seine Expertise in Dispute Resolution
- Autor zahlreicher Fachpublikationen in den Bereichen Versicherungsrecht, Datenschutz, Gesellschafts- und Bankrecht
- Regelmäßig Vortragender bei Fachseminaren
- Mitglied der IBA (Insurance, Litigation)
- Gründungsmitglied und Vizepräsident der YACLA (Young Austrian Commercial Litigation Association)

Datenschutz-Grundverordnung (DSGVO)

- Vollharmonisierung angestrebt
  - geringerer nationaler Umsetzungsspielraum
  - einheitliche Verfahren (Kooperations- und Kohärenzmechanismus)
- Anwendbarkeit ab 25.5.2018
  - bis dahin interne Prozesse umstellen
  - innerhalb von zwei Jahren nach Inkrafttreten (ErwG 171)
- neue Terminologie (Art 4)
  - Verantwortlicher, Auftragsverarbeiter, Einwilligung
  - aber weiterhin technologieneutral
- Ausweitung der Betroffenenrechte
  - Informationsrechte; Recht auf Vergessen; Datenportabilität
- umfangreiche Pflichten der Verantwortlichen
- erhöhtes, einheitliches Strafmaß

→ Datenschutz wird zu echtem Compliance Thema

Dokumentation (statt Meldung)

VERPFLICHTUNG

Risiko für Rechte / Freiheiten

Verarbeitung nicht nur gelegentlich

sensible / strafrechtliche Daten

VERPFLICHTUNG

>250 Mitarbeiter

DOKUMENTATION

INHALT

Name / Kontaktdaten des Verantwortlichen

Zweck der Verarbeitung

Kategorien der Betroffenen, Daten, Empfänger

Beschreibung geeigneter Garantien bei Übermittlungen in Drittländer

Fristen für Löschung der Daten

Beschreibung der Sicherheitsmaßnahmen

KEINE VERPFLICHTUNG

<250 Mitarbeiter

und keine besondere Verarbeitung

Dokumentation (statt Meldung)

- Zusätzliches Verzeichnis für Auftragsverarbeiter
  - Name und Kontaktdaten des Auftragsdatenverarbeiters und aller Verantwortlichen
  - Kategorien der Verarbeitungen je Verantwortlichen
  - Beschreibung der geeigneten Garantien bei Übermittlungen in Drittländer
  - allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen
- Verzeichnis ist schriftlich zu führen
  - elektronisches Format aber erlaubt
- Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung stellen

Privacy by design and by default (Art 25 DSGVO)

Setzung geeigneter technischer und organisatorischer Maßnahmen, um Datenschutzgrundsätze und –sicherheitsmaßnahmen, Verordnung sowie Betroffenenrechte wirksam umzusetzen

- Berücksichtigung
  - Stand der Technik
  - Implementierungskosten
  - Art, Umfang, Umstände und Zweck der Verarbeitung
  - Eintrittswahrscheinlichkeit und Schwere der Risiken

Privacy by design and by default (Art 25 DSGVO)

Pflicht zur Sicherstellung, dass durch Voreinstellung nur für den Zweck erforderliche Daten verarbeitet werden

- Menge der erhobenen Daten
- Umfang der Verarbeitung
- Speicherfrist
- Zugänglichkeit

Praxistipp: Einhaltung der datenschutzrechtlichen Prinzipien bereits in frühem Projektstadium sicherstellen

- zB bei Produktentwicklungen und –einführungen (Leistungsdefinition!)

Recht auf Datenübertragbarkeit (Datenportabilität)

- Betroffenenrecht wirkt sich auf Verarbeitungsvorgang bei Verantwortlichen direkt aus
- vom Betroffenen bereitgestellte Daten müssen vom Verantwortlichen in einem
  - strukturierten
  - gängigen und
  - maschinenlesbaren Format
- an
  - Betroffenen selbst oder
  - an einen anderen Verantwortlichen (soweit technisch möglich)
- übergeben werden, wenn Rechtmäßigkeit der Verarbeitung durch
  - Einwilligung oder
  - Vertragserfüllung hergestellt wird; oder
  - Verarbeitung mithilfe automatisierter Verfahren erfolgt

Informationspflicht bei Datenmissbrauch

Data Breach Notification Duty (§ 24 Abs 2a DSG)

- Auftraggeber muss den Betroffenen informieren
  - ab Kenntnis tatsächlicher, systematischer, schwerwiegender, unrechtmäßiger Verwendung (Datenmissbrauch) und bei
  - drohendem Schaden für Betroffenen
  - in geeigneter Form

- Ausnahme bei
  - drohenden geringfügigen Schäden
  - unverhältnismäßigem Aufwand

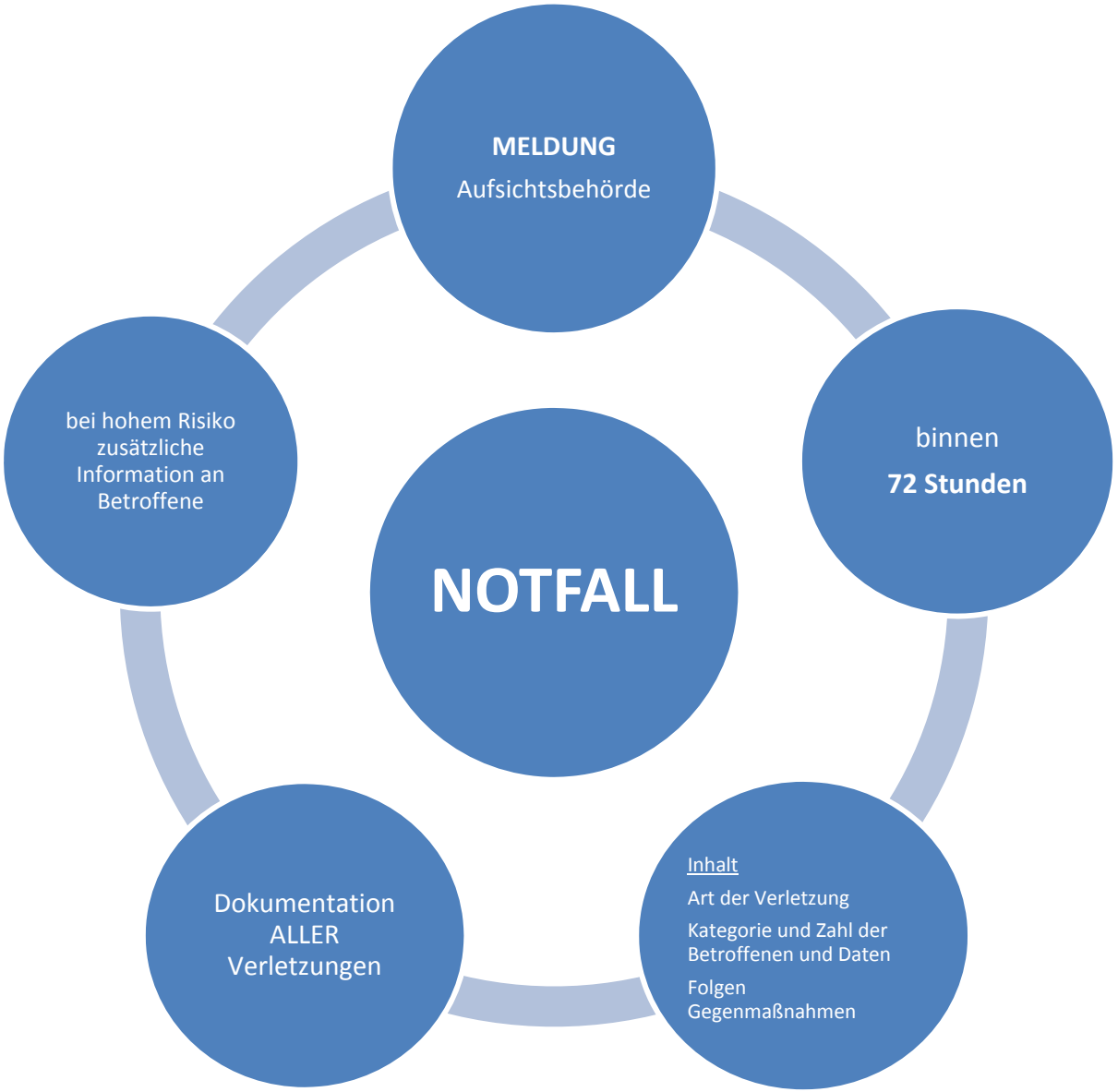
Informationspflicht bei Datenmissbrauch

Meldung von Datenschutzverstößen (Art 33 ff DSGVO)

Verletzung der Sicherheit, die zur Vernichtung, Verlust, Veränderung, unbefugten Offenlegung oder unbefugten Zugang führt (Art 4 Z 12)

- unverzügliche (möglichst binnen 72 Stunden) Meldung an Aufsichtsbehörde
  - Beschreibung Art der Verletzung
  - Angabe Kategorien und Zahl der Betroffenen und Daten
  - Namen und Kontaktdaten des Datenschutzbeauftragten
  - Beschreibung der wahrscheinlichen Folgen
  - Beschreibung der ergriffenen oder vorgeschlagenen Gegenmaßnahmen

Informationspflicht bei Datenmissbrauch



Datenschutz-Folgenabschätzung

Datenschutz Folgenabschätzung (PIA)

sofern Verarbeitung	voraussichtlich hohes Risiko zur Folge hat	muss vorab ein PIA durchgeführt werden	**JEDENFALLS** erforderlich, wenn
-) insbesondere bei Verwendung neuer Technologien -) aufgrund Art, Umfang, Umstände, Zweck	für Rechte / Freiheiten der Betroffenen	-) bei ähnlichen Verarbeitungen genügt ein PIA -) laufende Überprüfung erforderlich	-) Bewertung auf Basis automatisierter Entscheidungen (Profiling) -) umfangreiche Verarbeitung sensible / strafrechtliche Daten -) systematische Überwachung öffentlicher Bereiche

Datenschutz-Folgenabschätzung

Mindestinhalt nach Art 35 DSGVO

1) systematische Beschreibung der Verarbeitung und Zwecke
2) Bewertung Notwendigkeit und Verhältnismäßigkeit
3) Bewertung der Risiken
4) Abwehrmaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren

Zuhilfenahme Leitlinien / Entscheidungshilfen

ISO/IEC 29134:2016 (derzeit DIS) → erweiterter Ermessensspielraum
CNIL, Privacy Impact Assessment (Guidelines)

Aufbau: Dokumentation → PIA → Risikomeldung

Schritt 1 → Erweiterung DVR Meldung auf Dokumentation
Schritt 2 → Erweiterung Dokumentation zu PIA
Schritt 3 → Ergebnisse als Basis für Risikomeldung an Aufsichtsbehörde

Datenschutz-Folgenabschätzung

Standardisierungsmöglichkeiten

Beschreibung der IT Landschaft (Hard-, Software, Systeme, Provider etc)
Beschreibung der IT Standards (Virenschutz, Firewall, Back Up etc)
Darstellung der personellen Struktur (Zugriffsrechte, Kontrolle, Berichtslinien etc)
Darstellung potentieller Risken und deren Eintrittswahrscheinlichkeit
Auflistung der Folgen und Gefahrenklassen
Ausarbeitung der Risikominimierung / Gegenmaßnahmen

Praktische Umsetzungsvorschläge

Verweis auf angepasste / aktualisierte IT Policy
Detaillierte Mustererstellung und (Teil-)Implementierung in jede PIA

! VORSICHT !

PIA für jede Datenanwendung – wenn nicht inhaltlich gleich – **separat** durchzuführen
Anpassungsbedarf in **jeden Einzelfall** prüfen
unterschiedliche Verarbeitungen führen de facto zu unterschiedlichen Risken

Datenschutz-Folgenabschätzung

Ergebnis der PIA

Grundlage für Entscheidung

- Umsetzung Projekt möglich?
- Umstellung einzelner Schritte erforderlich?
- Ausreichende Sicherheitsmaßnahmen etabliert?

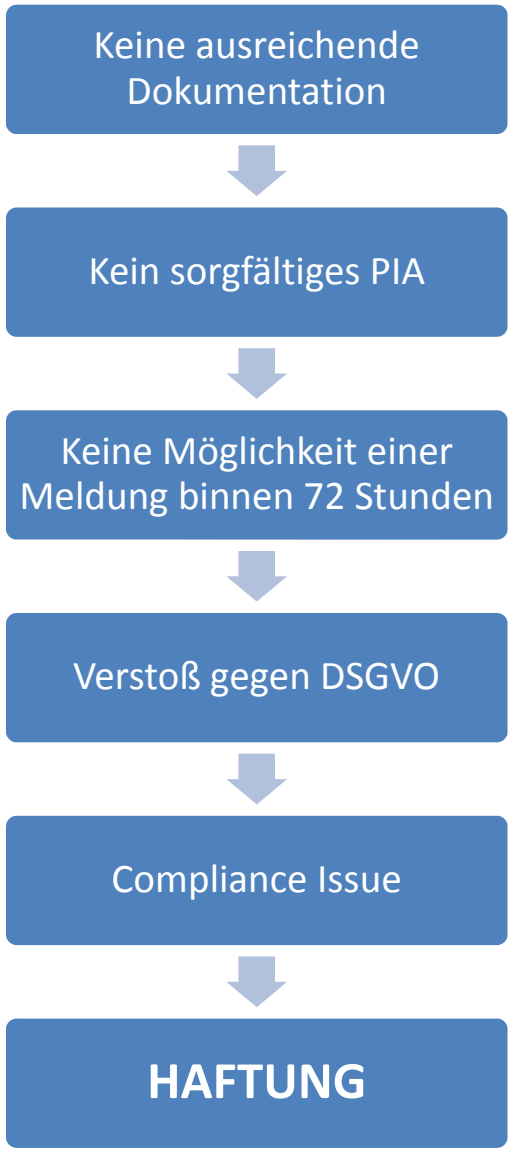
Zweck der PIA

- Erfüllung Art-35-DSGVO-Pflicht
- wichtigste Unterlage für Meldungen in Notfällen
- unverzichtbarer Nachweis der Einhaltung der Sorgfalt (**Entlastung**!)
- Erhöhung Transparenz innerhalb des Unternehmens

Aktualisierung der PIA

- bei Änderungen im Ablauf
- nach Eintritt eines bisher nicht bedachten Risikos
- bei Änderung internationaler / technischer Standards

V. Folgen / Risiken



Haftung der Unternehmensleitung

- Sorgfaltspflichten des Vorstandes bzw der GF
  - §§ 84 AktG, 25 GmbHG
  - Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters
  - bei schuldhafter Verletzung Schadenersatzpflicht
    - Beweislastumkehr

- Haftung auch bei Delegation der Verantwortung auf Andere
  - unter Anleitung und Kontrolle des GF
  - Haftung für Auswahlverschulden

Haftung der Unternehmensleitung

- Organisationsverschulden
  - Berichtspflichten, rascher Zugriff auf Informationen
- Auswahlverschulden
  - Einsatz geeigneter Mitarbeiter, Dokumentation Mitarbeitergespräche, Know-How Transfer
- Instruktionsverschulden
  - Information der Mitarbeiter, unternehmensinterne Richtlinien
- Kontroll- und Überwachungsverschulden
  - effiziente Überwachung, Gegenmaßnahmen, Simulation von Risikosituationen, Whistleblowing-System

Rechtsfolgen (aktuell)

- Verwaltungsstrafen (DSG bis zu EUR 25.000)
- Beschwerde an Datenschutzbehörde
- Gesetz gegen unlauteren Wettbewerb (UWG)
  - Unterlassung
  - Einstweilige Verfügung
  - Kostenintensiv (Urteilsveröffentlichung)
- Auskunfts-/Richtigstellungsanspruch
- Unterlassungsanspruch
- Ideeller Schadenersatzanspruch
- Strafrecht
- Negativ PR!

Rechtsfolgen (neu nach DSGVO)

- Geldbußen (Art 83) – Adressat: Unternehmen (ähnlich KartG)
  - bis zu EUR 10 Mio / 2% des gesamten weltweit erzielten Jahresumsatzes des vorigen Geschäftsjahrs (höherer Wert gilt!)
    - Einwilligung eines Kindes (Art 8)
    - Verarbeitung für die Identifizierung nicht erforderlich (Art 11)
    - Pflichten der Verantwortlichen/Auftragsdatenverarbeiter (25-39)
    - Pflichten der Überwachungsstelle (Art 41)
    - Pflichten der Zertifizierung und Zertifizierungsstellen (42 und 43)
  - bis zu EUR 20 Mio / 4% des gesamten weltweit erzielten Jahresumsatzes des vorigen Geschäftsjahrs (höherer Wert gilt!)
    - Grundsätze der Verarbeitung, einschließlich Einwilligung (Art 5-7, 9)
    - Rechte der Betroffenen (Art 12-22)
    - Übermittlung an Empfänger im Drittland (Art 44-49)
    - Vorschriften über besondere Verarbeitungssituationen (Kapitel IX)
    - Nichtbefolgung Anweisung, Beschränkung, Aussetzung einer Datenübermittlung oder Nichtgewährung des Zugangs (Art 58)

CHECKLISTE

Deadline: **25.5.2018**

Anpassung Prozesse an DSGVO innerhalb von zwei Jahren (ErwG 171)

To Dos:

Dokumentation der Verarbeitungsvorgänge
Datenschutz-Folgenabschätzung (soweit erforderlich)
Vorbereitung Muster zur Meldung etwaiger Verstöße
Überarbeitung bestehender Verträge mit Auftragsverarbeitern
Anpassung Einwilligungserklärungen
Umstellung laufender, interner Prozesse
Sicherstellung Erfüllung neuer Informationspflichten
Überprüfung von Profiling/Scoring Anwendungen
Sicherstellung der Betroffenenrechte (zB Datenportabilität)
IT Sicherheitsmaßnahmen anpassen (zB Privacy by design)
Etablierung konzernübergreifender Verhaltensregeln?
Verbindliche interne Datenschutzvorschriften?
Zertifizierung?
Bestellung Datenschutzbeauftragter?

Kontakt

MMag Dr Felix Hörlsberger
T: +43 1 533 47 95 – 17
E: felix.hoerlsberger@dorda.at

DORDA Rechtsanwälte GmbH · Universitätsring 10 · 1010 Wien

International Law Office - Austrian Client Choice Award 2012, 2013 & 2014
IFLR European Awards - Austrian Law Firm of the Year 2013