Datenschutz-Frühstück
dataprotect_at

Datenschutz-Frühstück - ein Datenschutz-Event in Linz - dataprotect_at

Der **25.05.2018** ist nur mehr **weniger als 300 Tage entfernt**; einen aktuellen Countdown finden Sie unter www.dataprotect.at.

Mit diesem Tag ändert sich vieles im Bereich Datenschutz in Österreich. Beim **Datenschutz-Frühstück** erfahren Sie mehr über die DSGVO und die Umsetzung in Österreich durch das am 31.07.2017 im BGBl I 120/2017 veröffentlichte Datenschutz-AnpassungsG 2018.

@dataprotect_at folgen

dataprotect 13h
@dataprotect_at

DSFA -Datenschutz-Folgenabschätzung ... bei hohem Risio für Rechte u Freiheiten natürl Personen notwendig .. Risiko... t.co/BFGFvitpyS

RA Dr. Thomas Schweiger, LL.M. (Duke)

- Rechtsanwalt in Linz seit 09.09.1999
- vorwiegend im Bereich Beratung tätig
- diverse Publikationen im Bereich Informationstechnologierecht
- Spezialgebiet: Datenschutz
- www.dataprotect.at

EMRK -> DSRL (95) -> DSG 2000 -> DSGVO -> DSG

- Art 8 EMRK
- Richtlinie 95/46/EG (Datenschutzrichtlinie)
- Datenschutzgesetz 2000
- VO 2016/679 (Datenschutzgrundverordnung)
- direkt anwendbar
- umzusetzen bis 25.5.2018 (Art. 99 Abs. 2 DSGVO)
- 31.07.2017: Datenschutz-AnpassungsG 2018 (BGBl I 120/2017; in Kraft: 25.05.2018)

DSGVO <> DSG (ab 25.05.2018)

- Öffnungsklausel: Kinder – ab 14
- keine Geldbußen für Behörden / öff Stellen
- Ergänzungen:
  - Bildverarbeitung
  - Straftatbestand

DSGVO – Herausforderungen

- Compliance
- Rechenschaftsverpflichtung
- Nachweispflicht
- umfassende Informationspflichten
- Schulung & Training
- Dokumentation
- Revision & Review

Recht-
mäßigkeit

Transparenz

Zweck(e)

Datenmini-
mierung

Richtigkeit

Speicher-
begrenzung

Integrität & Vertraulichkeit

Rechtmäßigkeit

- „*the processing shall be lawful only …*“ (lawfulness)
- Grundsatz: die Verarbeitung ist verboten
- Grundlage für die (erlaubte) Verarbeitung
  - Einwilligung
  - Vertrag / Vertragsanbahnung
  - rechtliche Verpflichtung
  - lebenswichtige Interessen
  - Wahrnehmung einer Aufgabe im öff Interesse
  - überwiegend berechtigte Interessen

Transparenz

- für die betroffene Person nachvollziehbar
- was geschieht mit „meinen Daten“
- umfassende Informationspflichten
  - bei der Erhebung von pb Daten
  - bei der Verwendung von pb Daten
- Datenschutzpolicy & -erklärung
- Rechte der Betroffenen

Zweck(e) der Verarbeitung

- jede Verarbeitung verfolgt einen Zweck
- Zweckfestlegung
- Zweckbindung (ieS)
- Informationspflichten
  - individuell nach Art 13 / 14: Zweck
  - Verzeichnis von Verarbeitungstätigkeiten: Zweck
- Datenschutz-Folgenabschätzung: Zweck

Datenminimierung

- ausgehend vom Zweck
- angemessen
- erforderlich
- auf das notwendige Maß beschränkt

Richtigkeit

- sachlich richtige Daten
- aktuelle Daten
- Löschung / Berichtigung unrichtiger Daten

Speicherbegrenzung

- zeitlicher Bezug
- Relevanz für den Zweck der DV
- Löschroutinen (-fristen)
- Aufbewahrungspflichten (gesetzliche)
- Recht auf Löschung / Vergessenwerden

Vertraulichkeit & Integrität

- Datensicherheit
- Schutz vor
  - unbefugter / unrechtmäßiger Verarbeitung
  - unbeabsichtigtem Verlust
  - unbeabsichtigter Zerstörung
  - unbeabsichtigter Schädigung
- technische & organisatorische Maßnahmen (TOMs)

- VV (Verz. von Verarbeitungstätigkeiten) / ROPA – Art 30
- DSFA (Datenschutz-Folgenabschätzung) / (D)PIA– Art 35 ff
- DSB (Datenschutzbeauftragter) / DPO - Art 37 ff
- DBN (Data Breach Notification) – Art 33 ff
- Geldbußen (gg Unternehmen) – Art. 83 / § 11 DSG

DSMS – was sollte es abdecken?

- Informationspflichten an Betroffene können implementiert werden (Vorgaben vorhanden)
- Verzeichnis von Verarbeitungstätigkeiten – Erstellung und Management (laufende Aktualisierung), durch Fachabteilungen (!) nicht Datenschutz-Compliance-Abteilung
- DSFA (Festlegung/Dokumentation: darüber, weshalb eine DSFA unterbleibt) die Analyse erfolgt aus Sicht des Betroffenen und im Hinblick auf die Risikofaktoren, die in der DSGVO genannt sind
- aus ISMS werden die Parameter für die „technische Sicherheit“ übernommen / TOMs können beschrieben werden

Verzeichnis von Verarbeitungstätigkeiten (VV)

- Ausnahme: < 250 MA, kein Risiko, Verarbeitung gelegentlich, keine Art. 9 / 10 Daten
- Inhalt:
  - Namen und Kontaktdaten des Verantwortlichen
  - Zweck(e) der Verarbeitung
  - Kategorien der betroffenen Personen & Daten
  - Kategorien der Empfänger
  - Löschungsfrist
  - technische u organisatorische Maßnahmen (TOMs)

Datenschutz-Folgenabschätzung

- Verarbeitung -> vorrausichtl hohes Risiko für Rechte u Freiheiten von natürlichen Personen:
  - Profiling (system. u umfassende Bewertung als Grundlage für Entscheidungen)
  - umfangreiche Verarbeitung von Art. 9 / 10 Daten
  - systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche
  - weiße Liste und schwarze Liste

Datenschutz-Folgenabschätzung

- Inhalt:
  - Beschreibung der geplanten Verarbeitungsvorgänge und des Zwecks
  - Notwendigkeit und Verhältnismäßigkeit
  - Maßnahmen zur Risikominderung
  - Risikobewertung
- hohes Risiko -> Konsultation mit Aufsichtsbehörde
- Reaktion: innerhalb von 8 Wochen -> Empfehlung oder Weisung

Datenschutzbeauftragter (DSB) 1/2

- Behörde / öffentliche Stelle (Ausnahme: Gerichte)
- gemeinsam möglich (Art 37 (3))
- beschäftigte Person / extern möglich
- Veröffentlichung von Kontaktdaten / Mitteilung an die Aufsichtsbehörde
- Einbindung in „Datenschutzfragen“
- weisungsfrei

Datenschutzbeauftragter (DSB) 2/2

- Aufgaben (Art. 39): - Berater & Auditor, nicht „verantwortliche Person“
  - Unterrichtung & Beratung des Verantwortlichen / der Beschäftigten -> Pflichten aus der DSGVO
  - Überwachung der Einhaltung / Strategien
  - Beratung iZhg mit PIA
  - Kooperation mit Aufsichtsbehörde
  - Anlaufstelle für die Aufsichtsbehörde
  - Anlaufstelle für betroffene Personen (Art. 38 (4))
- Sanktionsdrohung -> für Verantwortliche, nicht DSB

Data Breach Notification (DBN)

- Verletzung des Schutzes personenbezogener Daten
- Verantwortlicher / Auftragsverarbeiter
- Meldung an
  - Aufsichtsbehörde (unverzüglich, binnen 72 h)
  - betroffene Person (unverzüglich)

Data Breach Notification (Inhalt)

INHALT der Meldung	Behörde	Betroffene
Beschreibung der Verletzung, Datenkategorien, Anzahl der betroffenen Personen, betroffenen Kategorien, Zahl der Datensätze	X	-
Namen / Kontaktdaten des Datenschutzbeauftragten / Anlaufstelle	X	X
Beschreibung der Folgen	X	X
Beschreibung der ergriffenen / geplanten Maßnahmen	X	X

Geldbußen

- werden auf das 800-fache erhöht
- 4 % des weltweiten / jährlichen Gesamtvorjahresumsatzes bzw. EUR 20.000.000,--
- wirksam, verhältnismäßig & abschreckend
- Strafzumessungsgründe
- Geldbuße gg Unternehmen (wie § 99d BWG)
- keine Geldbußen gg Behörden / öffentliche Stellen

Geldbußen

- siehe Art. 83 DSGVO – Höchstausmaß
- Strafzumessungsgründe sind maßgebend
- Österreich: Geldbußen gegen Unternehmen („Hauptadressat“):
  - Personen in Führungspositionen begehen die Tat
  - mangelnde Überwachung oder Kontrolle ermöglicht die Begehung des Verstoßes (Verstoß gegen Internes Kontrollsystem)

sonstige Sanktionen

- Warnung oder Verwarnung
- Anweisung:
  - Anträgen von Personen zu entsprechen
  - Herstellung der Compliance
  - Durchführung einer DBN
- Beschränkung der Verarbeitung
- Anordnung der Berichtigung oder Löschung von pb Daten

6-Schritte-Methode (frei nach CNIL)

1. Datenschutzbeauftragten bestellen (Pilot/in)
2. Datenstruktur erheben / Datenmapping
3. Maßnahmen priorisieren
4. Risiko managen / Toms & DSFA
5. Organisieren
6. Dokumentieren

1. Pilot/in für DSGVO-Compliance

- „Compliance-Verpflichtungs-Erklärung“ des Board
- verantwortliche Person als „Pilot/in“
- „Pilot/in“: Umsetzung der Verpflichtungen der DSGVO auf Basis einer Verpflichtungserklärung des Boards
- Unternehmen stellt die notwendigen Ressourcen zur Verfügung
- Informations-, Beratungs- und Kontrollaufgaben
- keine „Umsetzungsaufgabe“

2. Datenstruktur erheben | Datenmapping

- Verzeichnis von Verarbeitungstätigkeiten iSd Art 30 DSGVO
- Definition der Hauptzwecke der Verarbeitungen (HR-System, Lieferanten/Kundenmanagement, Newsletter-Marketing, Videoüberwachung ...)
- Erstellung eines Interviewleitfadens / Fragebogens für Konzernstellen & -töchter bzw. Abteilungen in der Organisation
- Erarbeitung der Kategorien (Datensubjekte, Daten, Empfänger)
- Identifikation von (Daten)-Lieferanten / Auftragsverarbeitern, die in die Verarbeitungsaktivitäten involviert sind
- Übermittlungsempfänger (auch im EU-Ausland)

3. Maßnahmen priorisieren

- Compliance-Maßnahmen unter Berücksichtigung des Risikos
- Maßnahmen bzw. Prinzipien :
  - Datenminimierung
  - Festlegung der Rechtsgrundlage der Verarbeitung
  - Review der bestehenden Datenschutzerklärungen,
  - Prüfung der Lieferanten / Auftragsverarbeiter auf DSGVO-Konformität
  - Prozessabläufe für Ausübung der Rechte einer betroffenen Person
  - Prüfung, ob Datensicherheitsmaßnahmen implementiert sind
  - Data Breach Notification – Prozesse implementieren

4. Risiko managen - DSFA

- aus den bisherigen Schritten
- Festlegung des Risikos (niedrig / hoch)
- für die Rechte und Freiheiten natürlicher Personen
- Datenschutz-Folgenabschätzung iSd Art. 35 DSGVO

5. Organisieren

- Datenschutzprinzipien bei der Einführung einer Verarbeitung
- Erhöhung des Bewusstseins von Mitarbeitern (Training, Kommunikationsleitlinien etc...)
- Richtlinien zur Behandlung von Datenschutzanfragen
- Antizipieren von Datenschutzverletzungen
- Sicherstellung, dass Data Breach Notifications durchgeführt und auch die Zeitlimits (z.B. 72 Stunden) eingehalten werden können

6. Dokumentieren

- Verzeichnis von Verarbeitungstätigkeiten iSd Art. 30 DSGVO
- Datenschutz-Folgenabschätzungen
- Dokumentation zu den Mechanismen der Datenübermittlungen
- Datenschutzerklärungen & Information an betroffene Personen
- Formulare für die Einwilligungserklärungen & Sicherstellung der Kontrolle von Widerrufen
- Prozesse für Betroffenenrechte
- Vereinbarungen mit Lieferanten und Auftragverarbeitern
- interne Prozesse bzgl. Datenschutzverletzung (inkl. Data Breach Notification)

Danke für die Aufmerksamkeit

nächster Termin: 28.09.2017 (8.15 Uhr)

voraussichtliches Thema:
Datenschutz & Marketingmaßnahmen:
Was darf man unter welchen Voraussetzungen?