„Datenschutzgrundverordnung Lessons learned bis 3/2019„

CON.ECT Informunity Veranstaltung
Security, Risk- and Compliance-Management
9. April 2019 in Wien

CON●ECT INFORMUNITY papers4you

FRANKLAW OFFICE@FRANK-LAW.AT

RA Dr Markus Frank, LLM.

Spezialisierung: Datenschutz-Recht, Immobilien- und Wirtschafts-Recht, Wien

DS-Schwerpunkt:
- DSGVO-Umsetzung im KMU – effiziente Branchenlösungen
- DS-Compliance

2017 Ausbildung Datenschutzbeauftragter, bag Arbeit e.V., Hannover

2016 EU-Data Protection and Privacy Rights (HELP-EU-Programm for Legal Professionals)

Seit 2004 Vortragender zu Datenschutz-Recht für ISM-Personenzertifizierungen

Neustiftgasse 3/5
A-1070 Wien
Tel: +43 1 523 44 02
Email: office@frank-law.at
Web: www.frank-law.at

FRANKLAW OFFICE@FRANK-LAW.AT

„Datenschutzgrundverordnung – Lessons learned bis 3/2019“

1. Was der Europäische Datenschutzausschuss (EDSA = EDPB) 9 Monate nach Wirksamwerden der DSGVO am 25. Mai 2018 über deren Umsetzung in der EU berichtet?

2. Was in Österreich seit 25. Mai 2018 im Datenschutz (nicht) geschehen ist?

3. Beispiel-Thema: Löschen von Daten - Entscheidungen der Datenschutzbehörden seit 25. Mai 2018 – siehe https://www.frank-law.at/news/

4. Bisherige Bußgeldbescheide der Datenschutzbehörden und die Rolle der Kartellbehörden im Datenschutzrecht – siehe https://www.frank-law.at/news/

5. DatDOK – Wirtschaftlich vertretbare Umsetzung der DSGVO – ist das für KMUs und EPUs überhaupt möglich – auch unter Berücksichtigung der umfangreichen Dokumentationspflichten gemäß der DSGVO?

RA Dr. Markus Frank, LLM

FRANKLAW
OFFICE@FRANK-LAW.AT

Bericht des EDSA 2/19

206.326 Verfahren in EU seit 25.5.2018

52% entschieden, 1% angefochten

Anlass:
- ca. 46% Beschwerden
- ca. 31% Data-Breach-Meldungen

Häufigste Themen der Verfahren:
- Betroffenenrechte, besonders Löschen
- rechtliche Basis für Verarbeitung
- Data Breach

Grenzüberschreitende Fälle:
- 642 Verfahren zur Bestimmung der federführenden Behörde
- 45 „One-Stop-Shop“-Entscheidungen der federführenden Behörde
- Abstimmung EDSA mit nationalen Behörden -> einheitliche Rechtsprechung

Arbeiten des EDSA:
- bisher: Liste der Verarbeitungen, für die eine DSFA erforderlich ist
- in Arbeit:
  - Standardvertragsklausel controller – processor
  - Verhältnis DSGVO zur e-privacy-VO (für digitale Medien + elektronische Kommunikationsdienste!)
  - Regeln für BCR – Verbindliche interne Datenschutz-Vorschriften (Art 47 DSGVO)

FRANKLAW
OFFICE@FRANK-LAW.AT

Was ist in Österreich (nicht) passiert?

Fake News:
- „Keine Strafen“
- „99,9% der Firmen haben die DSGVO ausreichend umgesetzt“ - oder doch nicht (in KMUs und EPUs)?

Gesetzes-Änderungen: DSG i.d.F. BGBl. I Nr. 14/2019 + 100e Bundes- und Landes-Gesetze

DSFA-AV und DSFA-V:
- siehe Verarbeitungstätigkeiten im VVT => Anwendbarkeit prüfen!
- Risiko für hohe Strafen?

DSB 3/19: 28 Mitarbeiter, weitere 16 Bedarf

§ 1 DSG: Grundrecht von „jedermann“ auf Geheimhaltung, Auskunft und Richtigstellung

Mitarbeiter-Daten?

Einwilligung in unverschlüsselte Mails generell nicht gültig?

Behörde sah in der Einwilligung nicht Schaffung einer Rechtsgrundlage, sondern ein unzulässiges Abweichen von erforderlichen Datensicherheitsmaßnahmen zum Nachteil von Betroffenen, DSB-D213.692/0001-DSB/2018 vom 16.11.2018

Übermittlung an Drittland?

Zertifizierungsverfahren: Kriterien für Anerkennung gem. DSGVO (ISO 27001, ISO 29151, …)?

Vereinfachung durch Verhaltensregeln (Art 40 DSGVO) für KMUs – nach Branchen?

NIS: Netz- und Informations-Sicherheit in kritischen Infrastrukturen. Strafen max. 50 T (Großunternehmen!)

FRANKLAW
OFFICE@FRANK-LAW.AT

Was ist in Österreich (nicht) passiert?

Ursachen für viele offene Rechtsfragen:
- Dauer der Verfahren -> viele Video-Kamera-Entscheidungen § 12f DSG
- Abstimmung mit anderen Mitgliedsstaaten - nicht DSG, aber DSGVO
- Noch wenig veröffentlichte Entscheidungen
- Getrennte Verfahren: Bestimmung der federführenden DSB, Beschwerde-Verfahren, amtswegige Prüfung, Bußgeldverfahren
- nur 1% wird angefochten

Offene Themen:
- Details zu Zulässigkeitsgründen Art 6 – 10 DSGVO – Einwilligung, berechtigtes Interesse, Mitarbeiter, sensible Daten, …?
- Betroffenenrechte: **Informationspflichten**, Auskunft, Löschen, …?
  Information: Trennung nach Art 13 und 14 DSGVO; unvollständige Angabe der Rechtsgrundlagen und der Art der berechtigten Interessen (DSB-D213.692/0001-DSB/2018 vom 16.11.2018)
- Standards für Verzeichnis der Verarbeitungstätigkeiten?
- DSFA – Auslegung von DSFA-AV und DSFA-V?
- Datenschutz-Beauftragter
  „umfangreiche Verarbeitung sensibler Daten“ im Allergie-Labor - Ausnahme nur für einzelnen Arzt, DSB-D213.692/0001-DSB/2018 vom 16.11.2018
  („umfangreich“, daher hoch-riskant, war Verarbeitung von Daten von 150 Patienten in einem verlorenen Suchtgift-Buch, DSB-D084.133/0002-DSB/2018 vom 08.08.2018)
- Standards für Schulungen
- Umfang und Tiefe eines angemessenen DSMS
- Angemessene TOMs und welche Prüfungen wann erforderlich
- **Rechenschaftspflicht – Was ist alles wie detailliert zu dokumentieren?**
- **Detailliertheit der nachweisbaren Anweisungen an Mitarbeiter?**
- **Brexit**
- Interne Revision

-> Risiko: Bußgeld, Schadenersatz (Post AG?), Verarbeitungsverbote, Image

FRANKLAW
OFFICE@FRANK-LAW.AT

Löschen von Daten

Mehrere Entscheidungen der Datenschutzbehörde zum Löschen, vor allem auf Grund eines Antrags auf Löschen

Protokolldaten nur solange speichern, wie für Protokollierungszweck erforderlich (13.12.2017, DSB-D213.531/0009-DSB/2017)

Ausnahmen von Löschpflicht:

- Gesetzliche oder vertragliche Aufbewahrungspflichten
- zur Geltendmachung oder Abwehr von Rechtsansprüchen (z.B. Verjährung von Gewährleistungs- und Schadenersatz-Ansprüchen)

Frist zur Aufbewahrung von Bewerber-Daten 6 + 1 = 7 Monate – Begründung wichtig! (27.8.2018, DSB-D123.085/0003-DSB/2018)

ACHTUNG: Löschpflicht wg.

- Fehlen der Rechtsgrundlagen (zB. nicht gültige Einwilligung),
- Fehlen angemessener Datenschutz-Information an Betroffenen -> wider „Treu und Glauben“ -> unzulässige Verarbeitung (30.11.2018, DSB-D122.954/0010-DSB/2018) - vgl. Bußgeld-Bescheid über 50 Mio € von CNIL vom 21.1.2019 gegen Google wegen Fehlen von Information/Transparenz!

Österreich: § 4 Abs 2 DSG => Löschzyklen + Einschränkung der Verarbeitung - z.B. für Überschreiben von Datenträgern für Backup

Zeitlich unbegrenzte Speicherung von pb Daten für eventuelle künftige Kontaktaufnahme = Verletzung von Art 5 Abs 1 lit e DSGVO (= Grundsatz der Speicherbegrenzung, also Pflicht zum selbständigen Überwachen, dass die Daten nur solange mit Personenbezug gespeichert werden, als dies zur Erreichung eines konkreten zulässigen Zweckes erforderlich ist) – 28.5.2018, DSB-D216.580/0002-DSB/2018.

siehe auch Artikel Umsetzung von Löschpflichten https://www.frank-law.at/news/

FRANKLAW
OFFICE@FRANK-LAW.AT

Bußgeldverfahren in EU seit 28.5.2018

wegen:

- Data-Breach (verspätete Meldung!)
- unzureichende Sicherheitsmaßnahmen (abstraktes Risiko)
- Österreich: Videoüberwachung
- unzureichende Rechtsgrundlage (Einwilligung)
- Fehlen der Datenschutz-Information an Betroffene
- Schwerpunkt: Sensible Daten (Gesundheit)

Höhe:

- Kleinst-Unternehmen: wenige Tausend Euro (2%, 4%, max. 50T gem. § 62 DSG)
- größere Unternehmen: 20 – 600T
- Groß-Unternehmen:
  - Google - CNIL 50 Mio wg. Fehlen von DS-Information an Betroffene,
  - Facebook - Kartellbehörde Deutschland wg. Fehlen der DS-rechtlichen Einwilligung für Weitergabe von Daten für Werbeeinschaltungen

Ursache für derzeit geringe Anzahl an Bußgeld-Bescheiden:

- Bußgeldverfahren erst nach Klärung des Sachverhalts in vorangegangenem Prüfverfahren (rasche Klärung bei Video-Überwachung)
- Europäische Abstimmung - dzt. In Ö v.a. Video-Überwachungen gem. Österr. DSG § 12 f, nicht DSGVO
- Derzeit noch viel Rechtsunsicherheit –> Mangel an Verschulden => TIP: Beobachten der DS-Judikatur!

FRANKLAW
OFFICE@FRANK-LAW.AT

Wirtschaftlich vertretbare DSGVO-Umsetzung für KMUs

DSGVO-Know-How für Recht / Technik / Organisation im KMU?
Interne Arbeits-Zeit + externe Beratungs-Kosten für Compliance
Unklare Haftungsrisiken - Bußgeld, Schadenersatz (POST AG?), Verbote, Image

Aber: Unternehmen in einer Branche verwenden ähnliche Hard- und Software, erfassen ähnliche Daten und verarbeiten diese auf ähnliche Art und zu gleichen Zwecken, verursachen daher gleichartige Risiken für Betroffene …

=> Branchen-Lösungen für
Schulungen + Anweisungen
Daten-Sicherheits-Maßnahmen -> aus Sicht Betroffener!
Datenschutz-Grundsätze + privacy by design + by default
Betroffenenrechte v.a. DS-Information, Auskunft + Löschen
Rechtsgrund für Verarbeitung / Einwilligung / berechtigtes Interesse
VVT / AV-Verträge / Gemeinsam Verantwortliche / Datenschutzfolgenabschätzung / Datenschutzbeaufragter

Branchen-Lösung DatDOK: Schulung + Datenschutz-Ordner mit wichtigsten Mustern - (fast) fertig ausgefüllt, indiv. anzupassen - https://www.frank-law.at/datdok/

FRANKLAW
OFFICE@FRANK-LAW.AT

Viel Erfolg bei Ihrem Datenschutz!

RA Dr Markus Frank, LLM

10

FRANKLAW
OFFICE@FRANK-LAW.AT