EU-DSGVO.at
Der Datenschutzblog

ALIX FRANK
Rechtsanwälte GmbH

BUSINESS BREAKFAST - DATENSCHUTZ

DIE VERANTWORTUNG VON GESCHÄFTSFÜHRER_INNEN, VORSTAND UND VEREINSOBLEUTEN

RA Prof. Franz J. Heidinger, LL.M. (Virginia)
RAA Mag. Laurin Maran

INHALT

- Aktuelle Situation
- Behördliche Entscheidungen
- Risiken für Unternehmen
- Haftungsrisiken der Organe
- Prävention

DSGVO-NOVELLE SEIT 25. MAI 2018 ANWENDBAR

- noch keine neuen Strafverfahren eingeleitet
  - aber > 80 laufende Verwaltungsstrafverfahren übernommen
- 424 Beschwerden eingereicht (2017: 531)
- 911 Rechtsauskünfte eingeholt (2017: 2.192; 2018 bis 28.5.: 1.299)
- 147 Data Breach Notifications gemeldet (2017: 89)
- 4.182 Datenschutzbeauftragte gemeldet

DATENSCHUTZ-FOLGENABSCHÄTZUNG

- Verarbeitung mit hohem Risiko für Rechte & Freiheiten natürlicher Personen

☒ Blacklist: erfordert Datenschutz-Folgenabschätzung

- VO im Herbst erwartet

☑ Whitelist: Datenschutz-Folgenabschätzung nicht erforderlich

BEHÖRDLICHE ENTSCHEIDUNGEN

SEIT INKRAFTTRETEN DER DSGVO

ANHÄNGIGE VERFAHREN

- Fortführung nach den neuen Bestimmungen
- 3 Entscheidungen auf Grundlage von DSGVO

1. GESETZLICH ZULÄSSIGER SPEICHERZEITRAUM VON STAMMDATEN

- Telekom-Unternehmen: Speicherung von Stammdaten für 10 Jahre
- Argument: Verjährungsfrist von 10 Jahren bei Abgabenhinterziehung (BAO)
- Datenschutzbehörde: Aufbewahrungsfrist von Büchern und Belegen ist 7 Jahre (BAO)

➔ **Daten dürfen <u>min 7 Jahre</u> aufbewahrt werden**

- Rechtsgrundlage: § 132 BAO

ALIX FRANK
Rechtsanwälte GmbH

EU-DSGVO.at

2. KEINE DATENSPEICHERUNG ZUM ZWECK EINER EVENTUELL ZUKÜNFTIGEN KONTAKTAUFNAHME

- Betroffener verlangt Löschung → Unternehmen löscht, speichert aber gleichzeitig Vor- & Zuname, Geburtsdatum, Adresse neu → Betroffener verlangt abermals Löschung
- Unternehmen verweigert:
  - Speicherung aus „*sicher amtsbekannten Gründen*" („*zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen*")
  - Notwendigkeit für Dokumentations- & Kommunikationszwecke
- Datenschutzbehörde:
  - Kein ausreichender Beweis der **Erforderlichkeit**
  - Bei Antrage auf Löschung sämtlicher Daten ist **Speicherung für eventuell zukünftige Kontaktaufnahme nicht notwendig**
  - Widerspricht Grundsatz der **Speicherbegrenzung**

AD 2) LÖSCHUNGSBEGEHREN BERECHTIGT WENN:

a. Daten **nicht mehr notwendig für Zwecke, für die** sie **erhoben / verarbeitet** wurden
b. **Person widerruft Einwilligung + keine andere Rechtsgrundlage für Verarbeitung**
c. **Widerspruch gegen die Verarbeitung**
d. Daten wurden unrechtmäßig verarbeitet
e. Rechtliche Verpflichtung zur Löschung
f. Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft erhoben

➔**Einwilligung + anderer Rechtfertigungsgrund!**

3. PFLICHT ZUR KOSTENLOSEN ZURVERFÜGUNG-STELLUNG HISTORISCHER BANKBELEGE

- Bank verlangt EUR 30 für Bankauszüge, die älter als 12 Monate sind → Kunde stellt datenschutzrechtliches Auskunftsbegehren → keine Beantwortung durch Bank
- Bank: personeller & monetärer Aufwand; schikanöses Begehren
- Behörde: Auskunft muss innerhalb von 2 Wochen erteilt werden
  - Je nach Intensität kann Auskunftsbegehren unzumutbar sein

→ **Einzelfallprüfung notwendig**

→ **klare & strukturierte Prozesse zur Erfüllung der Betroffenenrechte**

RISIKEN FÜR UNTERNEHMEN

SANKTIONEN – HAFTUNG & SCHADENERSATZ – IMAGESCHADEN

SANKTIONEN

- bis zu EUR 20 Mio / bis zu 4% des gesamten Jahresumsatzes
  - Art, Schwere und Dauer des Verstoßes
  - Vorsätzlichkeit oder Fahrlässigkeit
  - Wie erlangt Behörde Kenntnis?
  - technische und organisatorische Maßnahmen
- Österreich: **Verhältnismäßigkeit**
- Handelnde Person hat in juristischer Person **Führungsfunktion**:
  - Vertretungsbefugnis / Entscheidungsbefugnis / Kontrollbefugnis
- Unterhalb der Führungsebene: **Versagen der internen Kontrolle**

HAFTUNG & SCHADENERSATZ

- **materieller** oder **immaterieller** Schaden

➔ Vermögensschaden

➔ Art von Schmerzengeld

➔ Beweislastumkehr

IMAGESCHADEN

- Datenschutz = Wettbewerbsfaktor
  - ☒ Datenpannen
  - ☒ Geldbußen

HAFTUNGSRISIKEN DER ORGANE

REGRESS UND DIREKTE STRAFEN

REGRESS FÜR STRAFEN NACH ART. 82 DSGVO

- Geschäftsführer_innen einer Gesellschaft:
  - Sorgfalt eines ordentlichen Geschäftsmannes
  - Haftung zur ungeteilten Hand
- Aber:
  - Verhältnismäßigkeitskorrektiv
  - Auswahlverantwortung bei der Wahl der Führungskräfte

☒ **Regress von Unternehmensgeldbußen wohl nicht möglich**

REGRESS FÜR SCHADENERSATZZAHLUNGEN DER GESELLSCHAFT

- Sorgfalt eines ordentlichen Geschäftsmanns
- branchen-, größen- und situationsadäquate Bemühung
- mangelnde Kompetenz in einem bestimmten Bereich = Einlassungsfahrlässigkeit

➔ Mangelnde Sorgfalt → **Regress für eigenes Verhalten**

➔ Schuldhafte Verletzung von Organisations- und Überwachungspflichten → **Haftung für Fehler von Arbeitnehmer_innen**

DIREKTE BESTRAFUNG DES ORGANS GEM § 9 VSTG NACH ART. 82 DSGVO

- DSGVO-Geldbuße = Verwaltungsstrafe
- Verantwortliche gem § 9 VStG
  - zur Vertretung nach außen berufen = strafrechtlich verantwortlich

☒ keine Bestrafung, wenn bereits Verwaltungsstrafe gegen juristische Person

SONSTIGE DATENSCHUTZVERSTÖßE

- Keine strengere Strafe gem DSGVO / Verwaltungsstrafbestimmungen
- Geldstrafe: bis EUR 50.000
- zB § 62 DSG: Übermittlung von Daten mit dem Vorsatz der Verletzung des Datengeheimnisses

PRÄVENTION

VERMEIDUNG VON STRAFEN UND HAFTUNGEN

PRÄVENTION – GESELLSCHAFT 1

- Strafe nur aufgrund von:
  - Verstoß durch Person in Führungsposition
  - mangelnde Überwachung oder Kontrolle

➔ Delegierung an Person/Abteilung/Externe ohne Führungsposition

➔ Entwicklung von Internem Kontrollsystem (IKS)

➔ Integration von Datenschutz in bestehendes IKS

ALIX FRANK
Rechtsanwälte GmbH

EU-DSGVO.at

PRÄVENTION – GESELLSCHAFT 2

- Schadenersatz
  - Schaden entsteht wegen Verstoß gegen DSGVO
  - Unabhängig von verursachender Person

➔Versicherungsdeckung klären:

- ➔ Rechtsschutz: Abwehr solcher Schadenersatzklagen
- ➔ Betriebshaftpflicht: Zahlung von Schadenersatzansprüchen

PRÄVENTION – LEITUNGSORGAN

- Vermeidung von Strafen gegen die Gesellschaft → kein Regress
- Ressortverteilung
- Einholen von Weisungen
- Entlastung

→ Abschluss von Haftpflichtversicherung („Manager-Haftpflicht“)

PRÄVENTION – WAS WIR FÜR SIE TUN KÖNNEN

- Unterstützung bei der Einhaltung datenschutzrechtlicher Regelungen
- Vermeidung und Abwehr von Schadenersatzansprüchen und Geldbußen
- Professionelle datenschutzrechtliche Betreuung als Wettbewerbsfaktor
- Nachweis der Datenschutzkonformität im Falle einer beabsichtigten Veräußerung der Gesellschaft (due diligence)

EU-DSGVO.at
Der Datenschutzblog

ALIX FRANK
Rechtsanwälte GmbH

WIR UNTERSTÜTZEN SIE BEIM DATENSCHUTZ!

RA PROF. FRANZ J. HEIDINGER, LL.M. (VIRGINIA)
RAA MAG. LAURIN MARAN

Alix Frank Rechtsanwälte GmbH
Schottengasse 10
1010 Wien
Tel: 01 / 523 27 27
Fax: 01 / 523 33 15
f.heidinger@alix-frank.co.at