HEUKING KÜHN LÜER WOJTEK

Was passiert, bei keinem oder unzureichendem Schutz? Haftungsfragen und Organisationsverschulden

15.02.2022 - Digital.Kommunal.Sicher - Informationssicherheit

Dr. Lutz M. Keppeler
Fachanwalt für IT-Recht

RECHTSANWÄLTE UND STEUERBERATER

DSGVO als Haftungsgrundlage

- Haftung des „Verantwortlichen“ für Verstöße gegen die DSGVO und/oder das DSG NRW

- Fast jeder „Hacking-Vorfall“ führt auch zu Datenschutzverstößen
  - Anforderung an IT-Sicherheit (Art 32 DSGVO, § 15 DSG NRW)
  - Meldepflichten an Datenschutzaufsichtsbehörde (Art 33 DSGVO)
  - Information der Betroffenen (Art 34 DSGVO)
    - Häufig kommen in diesem Rahmen allgemeine Datenschutz-Versäumnisse ans Licht
    - Dokumentation?
    - DSFA

- Aktueller Durchschnittsstand der Datenschutzcompliance

IT-Sicherheit ist Schwerpunkt im Datenschutzrecht

- Erste DSGVO Bußgeld in ganz Europa (400.000 EUR) => Art. 32: Zugriffsberechtigung

- Erste DSGVO Bußgeld in Deutschland (20.000 EUR) => Art. 32: Kundendaten unverschlüsselt

ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
Filter Column	Filter Column		Filter Column	Filter Column		Insufficient technical and organisat	
ETid-1068	ITALY	2022-01-13	14,000	Azienda sanitaria unica regionale Marche	Art. 5 (1) f) GDPR, Art. 32 GDPR, Art. 35 GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-1050	GERMANY	2020	Fine amount between EUR 50 and EUR 100	Restaurant	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-1049	GERMANY	2020	Fine amount between EUR 50 and EUR 100	Restaurant	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-1048	GERMANY	2020	Fine amount between EUR 50 and EUR 100	Restaurant	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-1014	SWEDEN	2022-01-26	152,000	Uppsala hospital board	Art. 5 (1) f) GDPR, Art. 32 (1) GDPR	Insufficient technical and organisational measures to ensure information security	link link
ETid-1013	SWEDEN	2022-01-26	28,500	Uppsala regional board	Art. 32 (1) GDPR	Insufficient technical and organisational measures to ensure information security	link link

howing 1 to 10 of 211 entries (filtered from 1,068 total entries)

Previous 1 2 3 4 5 ... 22 Next

Tatsächliches Risiko für Kommunen?

- § 33 Abs. 4 DSG NRW:

  („*Gegen öffentliche Stellen […] werden Geldbußen nach Absatz 2 oder einer anderen Rechtsvorschrift über den Schutz personenbezogener Daten nicht verhängt.*“)

- Aber
  - Reputationsverlust
  - Neues Risiko: Schadensersatz!
    - Art. 82 DSGVO gilt auch gegen staatliche Stellen
    - 85 veröffentliche Entscheidungen zu Art. 82 DSGVO
    - Gilt auch für immaterielle Schäden
    - Problem: Feststellung des Schadens?

Rechtliche Anforderungen an IT-Sicherheit

Anforderung an IT-Sicherheit

- Art 32 DSGVO

> „*Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten*“

Möglichkeiten der Konkretisierung

- Rechtsprechung ?
- § 9 DSG NRW
- ISMS (im Idealfall nach ISO 27001); Bei der Umsetzung konkreter Maßnahmen Orientierung an ISO 2700x oder an
- Kausalität !
- Praxisfälle die zu Bußgeld oder Schadensersatz führen sind meistens „Eindeutig“

Rechtliche Risiken außerhalb der DSGVO

Rechtliche Risiken außerhalb der DSGVO

- Vertragliche Ansprüche (Nutzungsbedingungen)
- Deliktische Ansprüche (839 BGB i.v.m. Art 34 GG)
  - Haftungsmaßstab „Fahrlässigkeit“ („die im Verkehr erforderliche Sorgfalt außer acht gelassen“)
    - Letztlich die gleichem Maßstäbe wie bei Art 32 DSGVO
    - ISMS verhindert „Organisationsverschulden“

Sonderfälle für Betreiber Kritischer Infrastrukturen

Lösung über Cyber Policen?

Regressansprüche

Welches Maß an IT-Sicherheit ist geschuldet, wenn hierzu nichts im Vertrag steht?

Ansprechpartner

Dr. Lutz M. Keppeler

Fachanwalt für IT-Recht

Magnusstraße 13

50672 Köln

T +49 221 2052-426

F +49 221 2052-1

l.keppeler@heuking.de

Kompetenzen

- IT-Recht mit Spezialisierung auf IT-Sicherheitsrecht und Open Source Lizenzen
- Datenschutzrecht
- Telekommunikationsrecht

Mitgliedschaften

- Fellow der European Free Software Foundation (FSFE)
- International Bar Association (IBA)

Veröffentlichungen (Auszug)

- § 9 und 13 TTDSG in Schwartmann/Jaspers/Eckardt TTDSG (im Erscheinen)
- § 21-24 TTDSG in Riechert/Wilmer TTDSG (im erscheinen)
- Erläuterung zum IAB TCF 2.0 in Beck Handbuch Datenschutz im Internet (im Erscheinen)
- § 2, 4a,4b,5b,7a-c,9b BSIG, § 11 EnWG, § 109 TKG in Ritter, Kommentar zum IT-Sig. 20
- „Objektive Theorie“ des Personenbezugs und “berechtigtes Interesse“ als Untergang der Rechtssicherheit?, CR 2016, 360 ff.
- „Datenschutz und SSL-Decryption“ K&R 2017, 453 ff.
- Technische und rechtliche Probleme bei der Umsetzung der DSGVO Löschpflichten ZD 2017, 314 ff.

HEUKING KÜHN LÜER WOJTEK

Vielen Dank
für Ihre Aufmerksamkeit

www.heuking.de

Berlin
Kurfürstendamm 32
10719 Berlin
T +49 30 88 00 97-0
F +49 30 88 00 97-99

Düsseldorf
Georg-Glock-Straße 4
40474 Düsseldorf
T +49 211 600 55-00
F +49 211 600 55-050

Hamburg
Neuer Wall 63
20354 Hamburg
T +49 40 35 52 80-0
F +49 40 35 52 80-80

München
Prinzregentenstraße 48
80538 München
T +49 89 540 31-0
F +49 89 540 31-540

Chemnitz
Weststraße 16
09112 Chemnitz
T +49 371 38 203-0
F +49 371 38 203-100

Frankfurt
Goetheplatz 5-7
60313 Frankfurt am Main
T +49 69 975 61- 0
F +49 69 975 61-200

Köln
Magnusstraße 13
50672 Köln
T +49 221 20 52-0
F +49 221 20 52-1

Stuttgart
Augustenstraße 1
70178 Stuttgart
T +49 711 22 04 579-0
F +49 711 22 04 579-44

Zürich
Bahnhofstrasse 69
8001 Zürich/Schweiz
T +41 44 200 71-00
F +41 44 200 71-01