Republik Österreich
Datenschutzbehörde

Rechtsprechung der Datenschutzbehörde und der Gerichte zu geeigneten Datensicherheitsmaßnahmen

Vortrag 23. Salzburger Telekom-Forum am 05.09.2022

Dr. Matthias Schmidl

Vorstellung

- Dr. Matthias Schmidl
- stv. Leiter der Datenschutzbehörde seit Jänner 2014 (wiederbestellt im Dezember 2018 für weitere 5 Jahre)
- November 2012-Dezember 2013 Referent in der Geschäftsstelle der Datenschutzkommission
- April 2011-November 2012: Bundeskanzleramt-Verfassungsdienst (Abt. V/1 und V/3)
- September 2007-März 2011: wissenschaftlicher Mitarbeiter am Verwaltungsgerichtshof

Grundsätzliches

Soweit es Fragen betrifft, die noch nicht (abschließend) geklärt wurden, stellen die Ausführungen dazu die **Privatmeinung des Vortragenden** dar und binden die Datenschutzbehörde nicht.

Verordnung (EU) 2016/679 – DSGVO

- **Artikel 32: Sicherheit der Verarbeitung** (Auszug)

(1) 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

Verordnung (EU) 2016/679 – DSGVO

- **Artikel 32: Sicherheit der Verarbeitung** (Auszug)

(2) Bei der **Beurteilung des angemessenen Schutzniveaus** sind insbesondere die **Risiken** zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3) Die Einhaltung genehmigter **Verhaltensregeln gemäß Artikel 40** oder eines genehmigten **Zertifizierungsverfahrens gemäß Artikel 42** kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Verordnung (EU) 2016/679 – DSGVO

- **Artikel 32: Sicherheit der Verarbeitung** (Auszug)

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Verordnung (EU) 2016/679 – DSGVO

- Artikel 32 normiert eine Pflicht des Verantwortlichen/Auftragsverarbeiters
- Artikel 32 normiert einen risikobasierten Ansatz
- Datensicherheitsmaßnahmen können/müssen variieren, je nachdem, wie die Verarbeitung erfolgt (kein „Schema F“)
- Wirtschaftliche Überlegungen (Implementierungskosten) können eine Rolle spielen, sind aber nur einer von mehreren zu beachtenden Faktoren
- Programme, mit denen bspw. Gesundheitsdaten verarbeitet werden, unterliegen folglich anderen Datensicherheitsmaßnahmen als Programme, die bspw. lediglich der Rechnungslegung dienen

Verordnung (EU) 2016/679 – DSGVO

Republik Österreich
Datenschutzbehörde

Mangelnde Datensicherheitsmaßnahmen können Gegenstand

a) einer **Beschwerde** an die DSB gemäß Art. 77 DSGVO
b) eines **amtswegigen Prüfverfahrens** nach Art. 57 Abs. 1 lit. h DSGVO
c) eines **Verwaltungstrafverfahrens** nach Art. 58 Abs. 2 lit. i iVm Art. 83 DSGVO
d) eines **Zivilverfahrens (einschließlich Schadenersatz, auch immerateriell!)** nach Art. 79 und Art. 82 DSGVO

sein.

Republik Österreich
Datenschutzbehörde

Rechtsprechung der DSB zu Art. 32 DSGVO

Rechtsprechung DSB – 1

Bescheid vom 13.09.2018, GZ DSB-D123.070/0005-DSB/2018 (RIS):

- Beschwerde nach Art. 77 DSGVO
- Beschwerdeführerin (Bfin) behauptete unzureichende Datensicherheitsmaßnahmen zu ihrem Nachteil (keine Pseudonymisierung ihrer Daten)
- Abweisung der Beschwerde
- Bfin konnte keine sie betreffende Rechtsverletzung nachweisen (potentielle Hackerangriffe sind unzureichend)
- Kein subjektives Recht auf Ergreifung spezifischer Datensicherheitsmaßnahmen

Rechtsprechung DSB – 2

Bescheid vom 16.11.2018, GZ DSB-D213.692/0001-DSB/2018 (RIS):

- Amtswegiges Prüfverfahren
- Verantwortlicher verlangte von Betroffenen u.a. eine „Einwilligungserklärung“, dass Gesundheitsdaten per E-Mail (also unverschlüsselt) übermittelt werden können
- Bescheid der Datenschutzbehörde, Feststellung einer objektiven Rechtsverletzung + Leistungsauftrag
- Pflicht des Verantwortlichen, geeignete Datensicherheitsmaßnahmen (von sich aus) zu ergreifen
- mit Einwilligung kann das erforderliche Niveau nicht unterschritten werden

Rechtsprechung DSB – 3

Bescheid vom 09.10.2019, GZ DSB-D130.073/0008-DSB/2019 (RIS):

- Beschwerde nach Art. 77 DSGVO
- Mj. Beschwerdeführer (Bf), vertreten durch den Vater, behauptete unzureichende Datensicherheitsmaßnahmen, weil er E-Mail-Nachrichten von einer Datingplattform erhält, ohne dort angemeldet zu sein
- Stattgabe der Beschwerde
- Bf wurde in seinem subjektiven Recht auf Geheimhaltung (§ 1 DSG) verletzt, weil es die Beschwerdegegnerin (= Betreiberin der Datingplattform) verabsäumt hat, adäquate Datensicherheitsmaßnahmen zu ergreifen
- Hier: Kein „double opt-in Verfahren“, obwohl es geboten gewesen wäre

Rechtsprechung DSB – 4

Straferkenntnis vom 17.02.2021, GZ 2020-0.675.335 (D550.325) (nicht rechtskräftig):

- Strafe: **4 Mio. EUR** wegen unzureichender Datensicherheitsmaßnahmen durch ein Kreditinstitut
- ungesicherte Excel-Liste mit Kundendaten (einschließlich Kontoinformationen) wurde verwendet
- Auszüge dieser Liste wurden versehentlich an (andere) Kunden versendet und damit unbefugten Dritten offengelegt
- Verantwortlicher hat es verabsäumt, adäquate Datensicherheitsmaßnahmen (hier: zumindest Verschlüsselung der Excel-Liste) zu ergreifen und dadurch gegen seine Pflicht nach Art. 32 DSGVO verstoßen
- Verstöße gg. Art. 32 DSGVO werden nach Art. 83 Abs. 4 lit. a mit Geldbuße bis zu 10 Mio. Euro bzw. bis zu 2% des gesamten weltweiten Jahresumsatzes des Vorjahres bestraft, je nachdem, welcher Betrag höher ist

dsb
Republik Österreich
Datenschutz
behörde

Rechtsprechung des BVwG zu Art. 32 DSGVO

Rechtsprechung BVwG – 1

Erkenntnis vom 09.12.2021, GZ W214 2225733-1 (RIS):

- Bf behauptet Verletzung von Art. 32 DSGVO, weil ihm Zugangsdaten mittels einfachem Brief übermittelt wurden
- BVwG bestätigt Rsp. der DSB, dass die betroffene Person kein subjektives Recht hat, einzelne konkrete Datensicherheitsmaßnahmen vom Verantwortlichen einzufordern
- allfällige Verletzung von Art. 32 DSGVO hat keine Auswirkungen auf Rechtmäßigkeit der Datenverarbeitung

Rechtsprechung BVwG – 2

Erkenntnis vom 20.01.2022, GZ W214 2239688-1 (RIS):

- Beschwerde wurde abgewiesen und Bescheid der DSB bestätigt
- Teile eines Gesundheitsgutachtens (zur Überprüfung der Dienstfähigkeit) wurden fotografiert und mittels Messengerdienst an eine nicht feststellbare Anzahl an (Erst-)Empfänger übermittelt (wodurch sich die betroffene Person in ihren Recht verletzt erachtete)
- Rechtsverletzung wegen mangelnder Datensicherheitsmaßnahmen festgestellt, weil es die Behörde unterließ, den Zugang zum Gutachten entsprechend abzusichern (Gutachten lag in einem unversperrten Zimmer offen auf dem Tisch)

Rechtsprechung– Zusammenfassung

- aus Art. 32 DSGVO ist kein subjektives Recht betroffener Personen auf Ergreifung ganz bestimmter Datensicherheitsmaßnahmen ableitbar
- Ergreifung von Datensicherheitsmaßnahmen ist eine objektive Pflicht des Verantwortlichen, die im Rahmen von amtswegigen Prüfverfahren und Verwaltungsstrafverfahren aufgegriffen werden kann
- mittels Einwilligung betroffener Personen kann nicht von notwendigen Datensicherheitsmaßnahmen abgewichen werden

dsb
Republik Österreich
Datenschutz
behörde

Rechtsprechung des EuGH zu Art. 32 DSGVO

Rechtsprechung EuGH – 1

- Anhängiges Vorabentscheidungsersuchen zu **C-340/21:**

1. Sind Art. 24 und Art. 32 der Verordnung (EU) 2016/679 dahin auszulegen, dass es ausreicht, wenn eine unbefugte Offenlegung von beziehungsweise ein unbefugter Zugang zu personenbezogenen Daten […] durch Personen erfolgt ist, die keine Bediensteten der Verwaltung des Verantwortlichen sind und nicht seiner Kontrolle unterliegen, um anzunehmen, dass die getroffenen technischen und organisatorischen Maßnahmen nicht geeignet sind?

Rechtsprechung EuGH – 2

- Anhängiges Vorabentscheidungsersuchen zu **C-340/21:**

2. Falls die erste Frage verneint wird, welchen Gegenstand und Umfang sollte die gerichtliche Rechtmäßigkeitskontrolle bei der Prüfung haben, ob die vom Verantwortlichen getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 der Verordnung (EU) 2016/679 geeignet sind?

4. Ist Art. 82 Abs. 3 der Verordnung (EU) 2016/679 dahin auszulegen, dass die unbefugte Offenlegung von oder der unbefugte Zugang zu personenbezogenen Daten […] wie vorliegend mittels eines „Hackerangriffs" […] einen Umstand darstellt, für den der Verantwortliche in keinerlei Hinsicht verantwortlich ist und der zur Befreiung von der Haftung berechtigt?

Republik Österreich
Datenschutzbehörde

Danke für Ihre Aufmerksamkeit!