Republik Österreich
Datenschutz behörde

NEWSLETTER 2/2017

Datenschutzgrundverordnung Kapitel IV („Verantwortlicher und Auftragsverarbeiter“) -Überblick

Das Kapitel IV gliedert sich in fünf Abschnitte und umfasst die Artikel 24 bis 43. In diesem Kapitel werden die allgemeinen Pflichten der für die Verarbeitung Verantwortlichen (so der künftige Terminus für den „Auftraggeber“-Begriff des DSG 2000) sowie der Auftragsverarbeiter (jetzt: „Dienstleister“) geregelt; es beinhaltet Bestimmungen hinsichtlich der Sicherheit personenbezogener Daten, die sogenannte „Datenschutzfolge-Abschätzung“ sowie die „vorherige Konsultation“ und alle relevanten Bestimmungen im Zusammenhang mit dem für Österreich neuen Datenschutzbeauftragten. Schließlich umfasst das Kapitel auch Bestimmungen über die Schaffung von Verhaltensregeln und die Verleihung von Zertifizierungen.

Eine der Pflichten des Verantwortlichen (auch des Auftragsverarbeiters) ist das Führen eines Verzeichnisses seiner Verarbeitungsvorgänge gemäß Artikel 30: dieses umfasst alle Verarbeitungsvorgänge, die seiner Zuständigkeit unterliegen und hat jedenfalls zu enthalten: die eigenen Kontaktdaten, die Daten des Datenschutzbeauftragten, die Zwecke der Verarbeitung, die Betroffenenkreise, die Datenarten, die Übermittlungsempfänger sowie gegebenenfalls auch Übermittlungen in Drittländer; weiters wenn möglich: Löschungsfristen und die Beschreibung technischer und organisatorischer Maßnahmen im Zusammenhang mit der Verarbeitung der Daten. Der Verantwortliche (bzw. sein Auftragsverarbeiter) hat der Datenschutzbehörde auf deren Anfrage das Verzeichnis zur Verfügung zu stellen. Ausnahmen können für Unternehmen oder Einrichtungen bestehen, die weniger als 250 Mitarbeiter beschäftigen. Diese trifft die Pflicht zur Führung eines solchen Verzeichnisses nur, wenn die Verarbeitung ein Risiko für die Rechte und Freiheiten der Betroffenen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder besondere Datenkategorien im Sinne des Artikel 9 Abs. 1 (Verwendung von sensiblen, genetischen, biometrischen Daten) bzw. des Artikel 10 (Verwendung von strafrechtlichen Verurteilungen, Straftaten) umfasst.

Weitere Pflichten ergeben sich aus den Artikeln 33 und 34: Verletzungen des Schutzes personenbezogener Daten sind unverzüglich und möglichst binnen 72 Stunden samt den notwendigen Informationen (Beschreibung der Verletzung, Anzahl der Betroffenen bzw. der Datensätze, getroffene Maßnahmen, wahrscheinliche Folgen, Dokumentation etc.) der Datenschutzbehörde zu melden, wenn ein Risiko für Rechte und Freiheiten der Betroffenen besteht. Darüber hinaus hat der Verantwortliche die Betroffenen (natürliche Personen) über Datenschutzverletzungen zu benachrichtigen, wenn ein hohes Risiko für Rechte und Freiheiten der Betroffenen besteht.

Eine weitere Pflicht ist die sogenannte Datenschutz-Folgeabschätzung gemäß Artikel 35: wenn durch die Verarbeitung von Daten (insbesondere bei der Verwendung neuer Technologien oder nach Art bzw. Zweck der Verarbeitung) ein hohes Risiko für Rechte und Freiheiten natürlicher Personen besteht, ist vom Verantwortlichen eine Abschätzung der Folgen durchzuführen. Eine Folgenabschätzung muss zumindest die Beschreibung (Zwecke) der Verarbeitungsvorgänge, die Bewertung der Notwendigkeit, die Verhältnismäßigkeit und Risiken, Abhilfemaßnahmen (Garantien, Sicherheitsvorkehrungen etc) enthalten.

Vorherige Konsultation gemäß Artikel 36: der Verantwortliche konsultiert vor der Verarbeitung der Daten die Datenschutzbehörde, wenn aus seiner Datenschutz-Folgeabschätzung hervorgeht, dass durch die Verarbeitung der Daten ein hohes Risiko gegeben wäre, sofern er keine Maßnahmen zur Eindämmung des Risikos trifft. Gelangt

die Datenschutzbehörde zur Auffassung, dass die Verarbeitung nicht im Einklang der DSGVO steht (weil das Risiko nicht genug ermittelt bzw. eingedämmt wurde), spricht sie innerhalb von acht Wochen nach Erhalt des Ersuchens - die Frist kann noch einmal um sechs Wochen verlängert, aber auch ausgesetzt werden - schriftliche Empfehlungen aus. Dafür benötigt sie Informationen über die Verarbeitung samt der bereits zuvor durchgeführten Datenschutz-Folgeabschätzung.

Die Artikel 37, 38 und 39 beschäftigen sich mit der Benennung, der Stellung und den Aufgaben des Datenschutzbeauftragten. Verantwortlicher und Auftragsverarbeiter müssen unter bestimmten Umständen einen Datenschutzbeauftragten bestellen:

- Behörden/öffentliche Stellen (Ausnahme: Gerichte im Rahmen ihrer justiziellen Tätigkeit),
- Verantwortliche/Auftragsverarbeiter mit der Kerntätigkeit einer umfangreichen, regelmäßigen und systematischen Überwachung von betroffenen Personen,
- Verantwortliche/Auftragsverarbeiter mit Kerntätigkeit im Zusammenhang mit der umfangreichen Verarbeitung von sensiblen Daten, strafrechtlichen Verurteilungen bzw. Straftaten,
- Verantwortliche/Auftragsverarbeiter, wenn es ihnen durch Unions- oder nationales Recht vorgeschrieben wird.

Alle anderen Verantwortlichen/Auftragsverarbeiter können einen Datenschutzbeauftragten auf freiwilliger Basis bestellen. Eine Gruppe von Unternehmen oder öffentlicher Einrichtungen kann einen gemeinsamen Datenschutzbeauftragten benennen. Der Datenschutzbeauftragte muss entsprechendes Fachwissen aufweisen und nicht in beruflichen Interessenskonflikten stehen. Er ist vom Verantwortlichen/Auftragsverarbeiter in datenschutzrechtliche Angelegenheiten einzubinden, hat Beratungsfunktion gegenüber Betroffenen und berät und informiert die oberste Managementebene. Er führt Schulungen durch, überwacht die Einhaltung der Datenschutzvorschriften. Er muss in seinem Bereich weisungsfrei sein und darf nicht abberufen werden. Er ist an Geheimhaltung und Vertraulichkeit gebunden und fungiert als Ansprechpartner für die Datenschutzbehörde. Der Datenschutzbeauftragte kann ein Bediensteter des Verantwortlichen/Auftragsverarbeiters sein, aber auch ein Externer. Seine Kontaktdaten sind zu veröffentlichen und der Datenschutzbehörde mitzuteilen.

Artikel 40 ermöglicht Verbänden und Interessensvertretungen Verhaltensregeln für Kleinst-, Klein- und Mittelbetriebe auszuarbeiten, welche die Anwendung der DSGVO präzisieren sollen. Die Einhaltung dieser Verhaltensregeln kann von einer fachlich geeigneten unabhängigen Stelle überwacht werden, die von der Datenschutzbehörde zuvor akkreditiert wurde; die Datenschutzbehörde übt in diesem Kontext auch eine Kontrollfunktion aus.

Artikel 42 führt Zertifizierungsverfahren, Datenschutzsiegel bzw. Prüfzeichen ein, durch die ein Verantwortlicher oder ein Auftragsverarbeiter nachweisen kann, dass er die Bestimmungen der DSGVO einhält. Zertifizierungen werden entweder von der Datenschutzbehörde oder von einer akkreditierten Zertifizierungsstelle erteilt.

Die DSGVO ist auf der Website der Datenschutzbehörde unter https://www.dsb.gv.at/datenschutz-grundverordnung abrufbar.

Im Fokus

„Vorschlag der Europäischen Kommission für eine ePrivacy Verordnung“

Mag. Christiane Lackner

Nach einer so genannten ex-post REFIT Evaluierung (Gewährleistung der Effizienz und Leistungsfähigkeit in der Rechtssetzung) veröffentlichte die europäische Kommission am 10. Jänner 2017 unter COM(2017) 10 final[1] einen Vorschlag (kurz „ePrivacy Verordnung“) für einen Verordnungsentwurf des europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG.

Wie sich im Rahmen der REFIT Evaluierung herausstellte, nutzen Verbraucher und Unternehmen immer stärker anstatt herkömmlicher Kommunikationsdienste neue Internet Dienste, die eine interpersonelle Kommunikation erlauben (etwa VoiceOver IP, Instant Messaging und Web unterstützte E-Mail Dienste). Solche so genannten „Over the top“ Kommunikationsdienste werden jedoch von der e-Datenschutzrichtlinie grundsätzlich nicht erfasst, da diese auf „öffentlich zugängliche elektronische Kommunikationsdienste in öffentlichen Kommunikationsnetzen“[2] abstellt, also auf eine klassische Signalübertragung über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen zugeschnitten war, sodass im wesentlichen Telekommunikationsbetreiber[3] adressiert waren. Die e-Datenschutzrichtlinie hat „mit der technischen Entwicklung nicht Schritt gehalten, was zu einem man-

1 http://eur-lex.europa.eu/procedure/EN/2017_3, deutsche Fassung: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

2 Siehe dazu Art. 3 von RL 2002/58/EG: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:de:PDF

3 Zur schwierigen Abgrenzung, wenn ein Telekombetreiber zumindest teilweise einen webbasierten SMS Dienst betreibt, siehe EFTA – Court E 6-16: http://www.eftacourt.int/uploads/tx_nvcases/6_16_Judgment_EN.pdf

gelnden Schutz der über solche neuen Dienste abgewickelten Kommunikation führte“[4].

Folgende wesentliche Neuerungen sind im Vorschlag zur ePrivacy Verordnung (Stand Jänner 2017) zu finden:

- Verordnung statt Richtlinie
- New player: Die ePrivacy Verordnung gilt für alle elektronischen Kommunikationsdienste ohne Rücksicht auf deren Übertragungstechnik
- Einheitliche Rechtsdurchsetzung europaweit durch Datenschutzbehörden
- Geschützt ist u.a. der Inhalt der Kommunikation und Metadaten (z.B. Zeit und Standort der Kommunikation)
- Einfachere Regeln für Cookies
- Schutz vor unerbetener Werbung „Spam“, sofern der Nutzer nicht eingewilligt hat
- Die ePrivacy Verordnung ist als lex specialis zur DSGVO angelegt
- Geschützt sind nach dem derzeitigen Entwurf auch juristische Personen
- Inkrafttreten ist gemeinsam mit DSGVO geplant

4 Zitat aus der Begründung der EU-Kommission zum Proposal „ePrivacy“

Ausgewählte Entscheidungen der DSB

Bilddokumentation oder Videoüberwachung?

Im Bescheid vom 15.7.2016, GZ: DSB-D122.453/0008-DSB/2016, hatte die DSB die Frage zu beurteilen, ob das anlassbezogene Filmen von Starts und Landungen auf einem Hubschrauberlandeplatz (Heliport) durch einen Anrainer eine Videoüberwachung (9a. Abschnitt DSG 2000) darstellt. Der Beschwerdeführer, der Flugbetriebsleiter des Heliports, hatte vom Verantwortlichen eine datenschutzrechtliche Auskunft verlangt. Diese war ihm im Umfang einer Kopie der gespeicherten Bilddaten (§ 50e Abs. 1 DSG 2000) verweigert worden. Hintergrund war, dass der Verantwortliche diese Bilddaten regelmäßig als Beweismittel dazu verwendete, behauptete Missstände im Flugbetrieb und mögliche Verwaltungsübertretungen bei verschiedenen Behörden anzuzeigen. Nach Einsichtnahme in die Bilddaten (MP4-Files) kam die Datenschutzbehörde zu dem Schluss, dass keine Videoüberwachung durchgeführt wurde. Die Aufnahmen wurden anlassbezogen, mittels einer von Hand geführten Kamera und von verschiedenen Standpunkten aus angefertigt. Sie zeigten den Beschwerdeführer nicht. Die Bilddaten dienten hier dem Zwecke der Dokumentation von Ereignissen (Flugbewegungen) und der Sicherung von Beweisen. Die Datenverwendung erfolgte nicht systematisch, insbesondere nicht mittels einer fest installierten Anlage, und auch nicht fortlaufend. Daher kam dem Beschwerdeführer, der auch nicht Betroffener der Bilddokumentation war, kein besonderes Auskunftsrecht nach § 50e DSG 2000 zu. Die Beschwerde wurde rechtskräftig abgewiesen.

Amtswegige Prüfverfahren gegen Krankenanstaltenträger

Die DSB hat 2017 den zweiten Teil der Prüfverfahren gegen Krankenanstaltenträger abgeschlossen.

In Summe wurden 2015 bis 2017 die wesentlichen öffentlichen Krankenanstaltenträger in jedem Bundesland überprüft.

Die Überprüfungen ergaben, dass die Krankenanstaltenträger im überwiegenden Maß die Bestimmungen des DSG 2000 einhalten. Dennoch wurde in allen neun Fällen eine Empfehlung ausgesprochen.

Die den zweiten Teil der Überprüfung betreffenden Empfehlungen zu den Grundzahlen DSB-D213.468 bis DSB-D213.471 sind im RIS abrufbar.

Empfehlung der Datenschutzbehörde vom 07.12.2016, GZ DSB D216.175/0004 DSB/2016

Dieser Empfehlung liegt folgender Sachverhalt zugrunde:

Im Zuge einer Wahl zu einer gesetzgebenden Körperschaft glich eine politische Partei die Daten aus der Wählerevidenz mit den Daten des (nicht öffentlichen) Mitgliederverzeichnisses eines Vereins ab, um dessen Mitglieder gezielt mit politischem Werbematerial ansprechen zu können.

Während die Verwendung von Daten aus der Wählerevidenz zu Wahlwerbungszwecken gesetzlich gedeckt ist, ist eine Berechtigung zur Ermittlung von (in der Wählerevidenz allenfalls nicht enthaltenen) Daten (wie zB. Couleurname eines Vereinsmitgliedes) zum Zweck der Wahlwerbung nicht mit den Bestimmungen des DSG 2000 vereinbar.

Ausgewählte Entscheidungen der Gerichte

Verkehrspsychologische Untersuchung

Mit Erkenntnis vom 21. Jänner 2017, Zl. W214 2127320-1/35E, wurde eine Beschwerde gegen einen Bescheid der Datenschutzbehörde im Verfahren GZ D122.409 als unbegründet abgewiesen. Die Revision wurde für nicht zulässig erklärt. Der Beschwerdeführer war von einer Bezirkshauptmannschaft zu einer verkehrspsychologischen Untersuchung gemäß §§ 5 und 18 Führerscheingesetz-Gesundheitsverordnung (FSG-GV) zugewiesen worden. Das Formular für diesen Vorgang wies ein Feld „Anmerkungen zum Zuweisungsgrund“ auf, in dem der Amtsarzt Daten zu Diagnosen, Medikamenten und Therapieansätzen niederschrieb. Die Übermittlung dieser Daten erachtete der Beschwerdeführer als unzu-

lässig. Die Datenschutzbehörde hat die Beschwerde abgewiesen. Das Bundesverwaltungsgericht hat in dem Erkenntnis ausgesprochen, dass die Überweisung zu einer verkehrspsychologischen Untersuchung die Übermittlung von Gesundheitsdaten impliziert und daher zulässig war.

„EFTA Court" Entscheidung E-6/16

Der EFTA Gerichtshof hat jüngst (Entscheidung E-6/16 vom 22.12.2016) im Rahmen einer „advisory opinion" - angefordert durch das Bezirksgericht Reykjavík – hinsichtlich der Interpretation von Art. 2 „Begriffsbestimmungen" der RL 2002/21/EG (Rahmenrichtlinie für elektronische Kommunikationsnetze und –dienste) entschieden, dass

- Soweit sowohl die Software auf der Internetseite der Klägerin als auch ihr Telefonnetzwerk notwendig für die Übertragung einer SMS sind, diese einen Teil eines einzelnen elektronischen Kommunikationsnetzes bilden.
- Eine Dienstleistung dann als elektronische Kommunikationsdienstleistung nach Artikel 2(a) der Richtlinie 2002/21/EG einzustufen ist, wenn
  i. sie in der Regel gegen Vergütung angeboten wird,
  ii. ganz oder überwiegend in der Übertragung von Signalen in elektronischen Kommunikationsnetzen besteht und
  iii. nicht in der Bereitstellung oder redaktionellen Kontrolle von Inhalten besteht.

Im gegenständlichen Fall ging es um einen isländischen Telekommunikationsprovider, der einen Web-basierten SMS Dienst auf seiner Homepage anbot. Dieser ermöglichte es „SMS-Gruppen" zu bilden, eine „Message – Historie" abzurufen und war (nicht nur) an eigene Telefon-Teilnehmer adressiert, sondern konnte jedermann (mit Telefonnummer und Passwort) den Dienst in Anspruch nehmen, unabhängig vom Endgerät (z.B. Smartphone oder Desktop). Kurz gesprochen, das angebotene Service näherte sich „funktional" den gängigen Messenger Diensten an. Der Sachverhalt hinter dieser Entscheidung des EFTA Court vermag zu zeigen, wie notwendig und wichtig es ist, durch die fortschreitende technische Entwicklung und die Konvergenz der Services einen einheitlichen Rechtsrahmen – unabhängig von der technischen Übertragungsart – zu schaffen, wie die europäische Kommission es mit der e-privacy Verordnung nun plant.

Erkenntnis des VwGH vom 21.12.2016, Zl. Ra 2016/04/0127

Der VwGH hob infolge einer Amtsrevision ein Erkenntnis des BVwG infolge Rechtswidrigkeit des Inhaltes auf.

Das BVwG hatte zuvor einen Bescheid der DSB (Spruchpunkte I bis III) ersatzlos behoben.

Dabei übersah das BVwG jedoch, dass Spruchpunkt III (eine Kostenentscheidung) überhaupt nicht vor dem BVwG angefochten worden war. Spruchpunkt III war nie Gegenstand des verwaltungsgerichtlichen Verfahrens. Die ersatzlose Behebung des gesamten DSB-Bescheides war daher rechtswidrig.

Urteil des EuGH vom 21.12.2016, C-203/15, Tele2, und C-698/15, Watson

Dieses Urteil betrifft die Zulässigkeit einer Vorratsdatenspeicherung von Kommunikationsdaten zum Zweck der Kriminalitätsbekämpfung.

Der EuGH hält in diesem Urteil einige wesentliche Punkte fest:

Zum einen fällt diese Vorratsdatenspeicherung in den Anwendungsbereich des Unionsrechts und unterliegt damit der Kontrolle durch den EuGH.

Eine generelle Speicherung von Kommunikationsdaten aller Nutzer verstößt gegen das Unionsrecht. Eine zielgerichtete und zeitlich begrenzte Speicherung von Kommunikationsdaten auf Vorrat zum Zweck der Bekämpfung schweren Verbrechens ist jedoch zulässig. Dazu sind klare gesetzliche Vorgaben erforderlich.

Gesetzesbegutachtung – Stellungnahmen

Die DSB hat zu folgenden Gesetzesvorhaben eine Stellungnahme abgegeben:

- Entwurf eines Bundesgesetzes, mit dem das Gesundheitsberuferegister-Gesetz, das Gesundheits- und Krankenpflegegesetz und das MTD-Gesetz geändert werden (GBRG-Novelle 2017)
- „kleine Ökostromnovelle"
- Novelle zum Polizeikooperationsgesetz
- Arbeitsmarktintegrationsgesetz
- Integrationsgesetz

Weblink:

- Parlament aktiv: alle Stellungnahmen

Impressum:
Medieninhaber, Herausgeber und Redaktion: Österreichische Datenschutzbehörde (DSB), Hohenstaufengasse 3, 1010 Wien, E-Mail: dsb@dsb.gv.at, Web: http://www.dsb.gv.at

Offenlegung gemäß § 25 Mediengesetz:
Der Newsletter der DSB ist ein wiederkehrendes elektronisches Medium (§ 1 Abs. 1 Z 5a lit. c MedienG); die gesetzlich gebotenen Angaben sind über folgenden Link abrufbar: https://www.dsb.gv.at/web/datenschutzbehorde/impressum-copyright