Republik Österreich
Datenschutz behörde

NEWSLETTER 4/2017

DATENSCHUTZ-GRUNDVERORDNUNG KAPITEL VI – UNABHÄNGIGE AUFSICHTSBEHÖRDEN

Nach den Vorgaben der DSGVO ist in jedem Mitgliedstaat der EU zumindest eine Datenschutz-Aufsichtsbehörde einzurichten, die in der Erfüllung ihrer Aufgaben und Befugnisse völlig unabhängig handelt.

Die DSGVO räumt den Aufsichtsbehörden eine besondere Stellung ein.

Sie sind Erstanlaufpunkt für Personen, die sich in Datenschutzrechten verletzt erachten, und auch für Verantwortliche bzw. Auftragsverarbeiter, die sich in bestimmten Fällen zwingend an die Aufsichtsbehörden zu wenden haben. Darüber hinaus kommt ihnen insofern eine „entscheidende" Bedeutung zu, weil sie die ersten sind, die datenschutzrechtliche Sachverhalte zu prüfen und damit die – teilweise unbestimmten – Begriffe der DSGVO auszulegen haben.

Gegen verbindliche Entscheidungen der Aufsichtsbehörden steht der Rechtsweg an ein Gericht offen.

Ein Vergleich mit der Richtlinie 95/46/EG (Datenschutz-Richtlinie) zeigt, dass Aufgaben und Befugnisse der Aufsichtsbehörden ausgeweitet und vereinheitlicht wurden: Zukünftig werden allen Aufsichtsbehörden in Europa die gleichen Aufgaben und Befugnisse zustehen. Sie sind verpflichtet, eng zusammenzuarbeiten und in bestimmten Fällen eine harmonisierte Entscheidung herbeizuführen.

Die Aufgaben der Aufsichtsbehörden umfassen u.a. die Beratung von Regierung und Parlament(en) in Datenschutzfragen, die Gewährleistung eines effektiven Rechtsschutzes von Betroffenen, die Prüfung so genannter „Data Breach Notifications" (Meldungen von Verletzungen des Schutzes personenbezogener Daten) sowie die Billigung von Verhaltensregeln und Prüfzeichen/-siegeln.

Die Befugnisse der Aufsichtsbehörden lassen sich in drei Gruppen zusammenfassen:

- Untersuchungsbefugnisse (wie bspw. das Anfordern von Unterlagen und das Betretungsrecht von Räumlichkeiten);
- Abhilfebefugnisse (wie bspw. die verbindliche Anordnung, Datenverarbeitungen in Einklang mit der DSGVO zu bringen oder auch Geldbußen zu verhängen);
- Beratungs- und Genehmigungsbefugnisse (wie bspw. im Konsultationsverfahren bei Datenschutz-Folgeabschätzungen).

Das Datenschutz-Anpassungsgesetz 2018 bestimmt die Datenschutzbehörde als die für Österreich zuständige Aufsichtsbehörde und überträgt ihr alle Aufgaben und Befugnisse nach der DSGVO (einschließlich der Verhängung von Geldbußen). Eine Zuständigkeit der Zivilgerichte in Datenschutzangelegenheiten (vgl. dazu § 32 DSG 2000) wird es – mit Ausnahme von Fällen des Schadenersatzes – nicht mehr geben.

Im Fokus

Fluggastdaten (PNR) Abkommen der EU mit Kanada. Gutachten 1/15 des EuGH vom 26. Juli 2017.

Mag. LL.M. Marcus Hild

Dem von der EU und Kanada am 25. Juni 2014 unterzeichneten Abkommen zur Übermittlung von Fluggastdaten (PNR, passenger name records) an Kanada hatte das EU Parlament nicht zugestimmt, sondern am 30. Jänner 2015 ein Gutachten des EuGH angefordert. Der EuGH hat in diesem Gutachten vom 26. Juli 2017 nun erstmals zur Frage, ob ein internationales Abkom-

men der EU mit dem EU-Recht vereinbar ist, Stellung genommen.

Dieses Abkommen sieht vor, dass Fluglinien die meisten personenbezogenen Daten, die sie über ihre Passagiere verarbeiten – das sind bis zu 60 Daten die von der Fluglinie und dem Flughafen erfasst werden (z.B. Reiseroute, Kontaktdaten, Zahlungsdaten, Sitzplatz, Vielfliegerinformationen, Gepäckinformationen, Diätwünsche und spezielle Betreuungsangaben) vor dem Abflug an die kanadischen Behörden übermitteln müssen und die kanadischen Behörden diese Daten 5 Jahre lang zum Zweck der Terrorismusbekämpfung und zur Aufklärung schwerer Verbrechen verwenden dürfen.

Grundsätzlich hat der EuGH die Möglichkeit der systematischen Überwachung aller Flugpassagiere, die mit dem Flugzeug nach Kanada reisen, mit dem Hinweis auf Art. 13 des Abkommens über die internationale Zivilluftfahrt (Chicagoer Abkommen) bejaht, weil diese automatisierte Verarbeitung der Fluggastdaten die Sicherheitskontrollen erleichtere und beschleunige, denen sämtliche Fluggäste unterlägen, die nach Kanada einreisen oder aus Kanada ausreisen möchten.

Auch die Auswertung der für kommerzielle Zwecke erhobenen Daten dieser Passagiere für Zwecke der Strafrechtsverfolgung hat er nicht beanstandet.

Die Auswertung von 28 Millionen an Kanada übermittelten Datensätzen innerhalb eines Jahres (April 2014 bis März 2015) ist auch ein zur Aufrechterhaltung der öffentlichen Sicherheit verhältnismäßiger Eingriff, zumal die Ergebnisse der Analysen unter anderem zu 178 Verhaftungen geführt haben.

Der EuGH hat in seinem Gutachten jedoch inhaltliche Anforderungen als Bedingung für die Zulässigkeit des Abkommens ausdrücklich vorgeschrieben.

Klare Definition der Datenarten. Die aus der Europäischen Union nach Kanada zu übermittelnden Fluggastdatensätze müssen klar und präzise definiert sein. Als unzureichend klar definiert, sieht der EuGH die im Annex des Abkommens genannten Vielfliegerdaten, „alle verfügbaren" Kontaktinformationen und „generelle Anmerkungen".

Keine sensiblen Daten ohne besondere Rechtfertigung. Die Übermittlung und Verarbeitung sensibler Daten bedarf einer präzisen und besonders fundierten, auf andere Gründe als den Schutz der öffentlichen Sicherheit vor Terrorismus und grenzübergreifender schwerer Kriminalität gestützten Rechtfertigung.

Festgelegte Methoden der automatisierten Auswertung. Die im Rahmen der automatisierten Verarbeitung von Fluggastdatensätzen verwendeten Modelle und Kriterien müssen „spezifisch und zuverlässig sowie nicht diskriminierend" sein und es dürfen nur Datenbanken verwendet werden, die von Kanada im Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität betrieben werden.

Pflicht zur Überprüfung automatisch erzeugter Ergebnisse. Bevor Maßnahmen ergriffen werden, die in die Rechte eines durch automatische Auswertung verdächtigen Flugpassagiers eingreifen, muss das Ergebnis manuell überprüft werden.

Objektiv überprüfbare Verwendung. Die Verwendung von Fluggastdatensätzen durch die kanadischen Behörden während des Aufenthalts der Fluggäste in Kanada und nach ihrer Ausreise sowie jede Weitergabe der Daten an andere Behörden muss materiell- und verfahrensrechtlichen Voraussetzungen unterworfen sein, die sich auf objektive Kriterien stützen.

Unabhängige Kontrolle. Die Verwendung und Weitergabe – außer in hinreichend begründeten Eilfällen – muss einer vorherigen Kontrolle durch ein Gericht oder einer unabhängige Verwaltungsstelle unterworfen sein. Zusätzlich muss auch die Einhaltung der Bestimmungen des Abkommens durch eine unabhängige Behörde überwacht werden.

Löschung nach Ausreise. Die Speicherung von Fluggastdaten nach der Ausreise der Fluggäste muss auf jene Personen beschränkt werden, für die objektive Anhaltspunkte vorliegen, dass von ihnen eine Gefahr im Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität ausgehen könnte.

Recht auf Information, Auskunft und Richtigstellung. Die Flugpassagiere haben ein Recht auf allgemeine Information im Zuge der Datenerhebung über die Auswertung ihrer Daten bei der Einreise, sowie das Recht auf Auskunft und Richtigstellung falsch erfasster Daten.

Besondere Informationspflichten nach der Einreise und Ausreise. Falls die Daten während des Aufenthalts in Kanada oder auch nach ihrer Ausreise verwendet werden, muss das Abkommen vorsehen, dass die betroffenen Fluggäste darüber individuell informiert werden.

Übermittlung an Drittstaaten nur bei angemessenem Datenschutzniveau. Nur an Staaten, bei denen es eine Entscheidung der Europäischen Kommission über das angemessene Datenschutzniveau gibt, oder ein internationales Abkommen mit der EU, in dem die Übermittlung dieser Daten geregelt ist, dürfen (einzelne) vorhandene Daten weitergegeben werden.

Schließlich hat der EuGH eine möglicherweise für die Bewertung anderer EU Abkommen wichtige rechtliche Frage, die vom EU Parlament ausdrücklich gestellt wurde, geklärt. Dieses Abkommen fällt nicht unter Artikel 82 Abs 1 lit d (Zusammenarbeit zwischen Justizbehörden) des Vertrags über die Arbeitsweise der Europäischen Union. Damit folgt der EuGH der Ansicht des Generalanwalts und des EDPS der dies

bereits in seiner Stellungnahme vom 15.7.2011 zum Fluggastdatenabkommen mit Australien kritisiert hat.

Zusammengefasst hat der EuGH zwar diese intensive und flächendeckende Überwachungsmaßnahme zugelassen, aber sehr hohe Standards bei den Informationspflichten, den zulässigen Datenarten, der Methodik der Auswertung, der Löschung und bei der vorabkontrollpflichtigen zweckgebundenen Datenverwendung gesetzt.

Ausgewählte Entscheidungen der DSB

Auskunft über Bonitätsprüfung eines Zahlers

Im rechtskräftigen Bescheid vom 8. Juni 2017, GZ: DSB-D122.641/0006-DSB/2017, hatte sich die Datenschutzbehörde wieder einmal mit einer Frage der datenschutzrechtlichen Auskunftserteilung über Bonitätsdaten zu befassen.

Der Beschwerdeführer bezahlte im Lastschriftverfahren die von einem Dritten zu leistenden Entgelte für die Dienste eines Mobilfunkunternehmens (Beschwerdegegnerin). Anlässlich einer Änderung des Lastschriftmandats (anderes Bankkonto) kam es zu einem fehlgeschlagenen Geldeinzug, Reklamationen und in weiterer Folge zur Einholung von Bonitätsauskünften über den Beschwerdeführer durch die Beschwerdegegnerin bei einem Wirtschaftsauskunftsdienst. Danach forderte die Beschwerdegegnerin den Beschwerdeführer zur Erbringung eines Identitäts- und Einkommensnachweises auf. Dieser antwortete, anwaltlich vertreten, mit einem datenschutzrechtlichen Auskunftsverlangen. Die Beschwerdegegnerin verneinte zunächst die Durchführung einer „Bonitätsabfrage“ zu Gänze, ergänzte die Auskunft aber schließlich im bereits laufenden Beschwerdeverfahren dahingehend, dass „negative“ Bonitätsauskünfte „vermerkt“ worden seien. Damit gab sich der Beschwerdeführer jedoch nicht zufrieden. Das Ermittlungsverfahren, in dem u.a. eine verantwortliche Mitarbeiterin der Beschwerdegegnerin als Zeugin befragt wurde, ergab, dass das Ergebnis der Bonitätsprüfung (nach dem Ampelsystem grün-gelb-rot) im CRM-System (Kundenbetreuungssystem) gespeichert wurde. Außerdem war über den Wirtschaftsauskunftsdienst (als Dienstleister) nicht korrekt Auskunft erteilt worden (Angabe der Firma einer Holding anstatt jener der operativen Tochtergesellschaft). Die Datenschutzbehörde gab daher der Beschwerde teilweise Folge und trug der Beschwerdegegnerin auf, eine inhaltliche Auskunft über die verarbeiteten Bonitätsdaten und eine korrekte Auskunft über die Firma des Dienstleisters zu geben. Die Datenschutzbehörde betonte dabei, dass bei gespeicherten Bonitätsdaten ein berechtigtes Interesse des Betroffenen besteht, den genauen Inhalt dieser Daten zu erfahren.

Hinsichtlich eines Auskunftsverlangens zur Logik der automatisierten Entscheidungsfindung der Bonitätsprüfung (§ 49 DSG 2000) wurde der Beschwerdeführer hingegen von der Beschwerdegegnerin zu Recht an den Wirtschaftsauskunftsdienst verwiesen, da die Beschwerdegegnerin nicht für die im „Ampelsignal“ ausgedrückte Bonitätsbeurteilung sondern nur für daran anknüpfende wirtschaftliche Entscheidungen verantwortlich war.

Gesetzesbegutachtung – Stellungnahmen

Die DSB hat zu folgenden Gesetzesvorhaben eine Stellungnahme abgegeben:

- Privatstiftungsgesetz- Novelle 2017
- Strafprozessrechtsänderungsgesetz 2017
- Entwurf für ein BG Änderung SPG, BStMG 2002, StVO, TKG 2003
- Datenschutz-Anpassungsgesetz 2018

Weblink:

- Parlament aktiv: alle Stellungnahmen

DVR-Online Tipps und Tricks

NEU: EXPORT-FUNKTION IN DVR-ONLINE

Mit dem In-Geltung-Treten der EU-Datenschutz-Grundverordnung am 25. Mai 2018 entfällt die Verpflichtung zur Erstattung von DVR-Meldungen an die Datenschutzbehörde. Das Datenverarbeitungsregister wird ab diesem Zeitpunkt (bis zum 31. Dezember 2019) zu Archivzwecken fortgeführt werden. Um einem Auftraggeber die Möglichkeit zu bieten, seine vorhandenen DVR-Meldungen zu sichern, ist es ab sofort möglich, in der Internet-Applikation DVR-ONLINE elektronisch verfügbare Meldungsinhalte sowohl als PDF-Dokumente als auch als XML-Dateien zu exportieren. Hierfür wurden im DVR-ONLINE-Meldebereich des Auftraggebers entsprechende Funktionen (rote Buttons, siehe Screenshot) eingefügt. Bitte beachten Sie: für Informationsverbundsysteme besteht diese Möglichkeit nicht.

Auftraggeber (AG)

DVR-Nummer	0000027 (Registriert)
Auftraggeber	Datenschutzbehörde
Adresse	Hohenstaufengasse 3, 1010 Wien, Österreich

AG-Daten ändern | AG-Daten lesen | Streichen | Exportiere PDF | Exportiere XML

Datenanwendungen (DAN)

Auswahl	Nummer	Bezeichnung/Zweck	Datum	Status
○	0000027/001	REGISTERFÜHRUNG	02.09.1996 00:00	Registriert
○	0000027/002	Aktenverwaltung (Büroautomation)	30.04.2004 00:00	Registriert
○	0000027/003	Öffentlichkeitsarbeit und Informationstätigkeit	30.04.2004 00:00	Registriert
○	0000027/004	Ergänzungsregister für sonstige Betroffene (ERsB) im Sinne des § 6 Abs 4 E-GovG	14.10.2005 00:00	Registriert
○	0000027/005	Bezeichnung: Ergänzungsregister für natürliche Personen Zweck: Ergänzungsregister zur Errechnung von Stammz ahlen für natürliche Personen, die nicht im zentralen Melderegister eingetragen sind. Es dient der Aufzeichnung vo n Daten, die für den Nachweis einer eindeutigen Identität (§ 2 Z 2 E-GovG) notwendig sind.	14.04.2011 00:00	Registriert
○	0000027/006	Stammzahlenregister Zweck: Errechnung von Stammzahlen, bereichsspezifischen Personenkennzeichen und versc hlüsselten bereichspezifischen Personenkennzeichen. Es werden Identitätsdaten aus dem zentralen Melderegister und Identitätsdaten aus dem Ergänzungsregister für natürliche Personen verwendet, um Personen eindeutig zu id entifizieren. Es werden Identitätsdaten von öffentlichen und privaten Auftraggebern mit den Identitätsdaten des z entralen Melderegisters und den Identitätsdaten des Ergänzungsregisters für natürliche Personen verwendet, um P ersonen eindeutig zu identifizieren. Für eindeutig identifizierte Personen kann sowohl eine Stammzahl auf Grundla ge der ZMR Zahl oder der ERnP Ordnungsnummer als auch bereichsspezifische Personenkennzeichen und verschlü sselte bereichsspezifische Personenkennzeichen berechnet werden. Stammzahlen werden nur an Bürgerkartenregi strierungsstellen überlassen, die als Dienstleister der Stammzahlenregisterbehörde im Zuge der Eintragung der St ammzahl in ein geeignetes elektronisches Medium zur Aktivierung der Bürgerkartenfunktion tätig werden, oder an öffentliche Auftraggeber zur unverzüglichen Berechnung eines bereichsspezifischen Personenkennzeichens und/od er eines verschlüsselten bereichsspezifischen Personenkennzeichens übermittelt. Bereichsspezifische Personenken nzeichen und/oder verschlüsselte bereichsspezifische Personenkennzeichen werden nur an Auftraggeber übermitte lt, deren Berechtigung zum Bezug dieser Personenkennzeichen zuvor überprüft wurde. Das Stammzahlenregister s peichert keine Identitätsdaten, Stammzahlen oder bereichsspezifische Personenkennzeichen über den Zeitraum hi naus, der für die Errechnung dieser Kennzeichen erforderlich ist.	15.04.2011 00:00	Registriert
○	0000027/007	Vollmachtenservice Zweck: Register zur Aufzeichnung von erteilten und widerrufenen Vollmachten auf der Bürgerk arte. Es dient der Aufzeichnung von Daten, die für die Nachvollziehbarkeit und Beauskunftung von erteilten und wi derrufenen Vollmachten (§ 5 E-GovG) notwendig sind. Jedermann kann anhand der Seriennummer des Vertretung sdatensatzes den Status einer Vollmacht überprüfen. Die Applikation errechnet das bereichsspezifische Kennzeich en ZP („zur Person") anhand der aus den Bürgerkarten ausgelesenen Stammzahl. Die Stammzahlen von natürlich en Personen werden nicht gespeichert, sondern sofort nach der bPK Berechnung unwiderruflich gelöscht.	07.06.2011 00:00	Registriert
○	0000027/008	IVS vom 22.6.16	22.06.2016 13:27	Registriert

DAN-Daten ändern | DAN-Daten lesen | DAN-Erstmeldung | Streichen | Stornieren | Registerauszug | Exportieren aller DANs als PDF | Exportieren einzelner DAN als PDF
Exportieren aller DANs als XML | Exportieren einzelner DAN als XML

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: http://www.dsb.gv.at/impressum.