dsb
Republik Österreich
Datenschutz behörde

NEWSLETTER 1/2020

Die DSB wünscht allen Leserinnen und Lesern des Newsletters ein gutes Jahr 2020 und viel Freude beim Lesen!

Bildverarbeitung und Dashcams

Dr. Matthias Schmidl

Das DSG regelt in den §§ 12 und 13 die Bildverarbeitung im privaten Bereich (einschließlich der Privatwirtschaftsverwaltung durch Gebietskörperschaften). Nicht im DSG, sondern in den jeweiligen Materiengesetzen, ist die Bildverarbeitung für hoheitliche Zwecke geregelt (z.B. im SPG und im MBG).

Das BVwG hat in zwei rezenten (nicht rechtskräftigen) Entscheidungen die Gültigkeit von §§ 12 und 13 DSG im Lichte der DSGVO in Zweifel gezogen und ausgesprochen, dass – in den konkreten Fällen - für § 13 DSG sowie § 12 Abs. 4 Z 1 DSG keine Öffnungsklausel besteht und diese Bestimmungen daher nicht anzuwenden sind (siehe dazu BVwG, Beschluss vom 20.11.2019, W256 2214855-1, und BVwG, Erkenntnis vom 25.11.2019, W211 2210458-1).

Diese Entscheidungen haben weitreichende Auswirkungen.

So wird die DSB, sofern im Einzelfall nicht besondere Gründe dafürsprechen, die §§ 12 und 13 DSG nicht mehr anwenden, sondern Bildverarbeitungen ausschließlich auf Basis der Art. 5 und 6 DSGVO prüfen. Dass eine Bildverarbeitung (in einem Mehrparteienhaus) auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden kann, hat der EuGH in einem rezenten Urteil (zur Rechtslage nach der Richtlinie 95/46/EG) bestätigt (EuGH, Urteil vom 11.12.2019, C-708/18).

Eine Bildverarbeitung entspricht demgemäß nur dann der DSGVO, wenn sie zumindest auf einen Tatbestand gemäß Art. 6 Abs. 1 DSGVO (im Regelfall wird nur lit. f in Betracht kommen) gestützt werden kann und alle Vorgaben gemäß Art. 5 Abs. 1 DSGVO erfüllt sind. Dies wird im Rahmen einer Einzelfallbeurteilung zu prüfen sein.

Soweit es so genannte „Dashcams" betrifft – also Kamerasysteme, die am Armaturenbrett oder am Heck eines Kfz angebracht sind und das Verkehrsgeschehen dokumentieren –, vertritt die DSB nachstehende, vorläufige Rechtsmeinung:

Dashcams sind nicht per se unzulässig und einer Einzelfallbewertung zugänglich. Sie können gemäß Art. 5 und 6 Abs. 1 lit. f DSGVO insbesondere dann zulässig sein, wenn folgende Parameter eingehalten werden (siehe dazu im Detail https://www.dsb.gv.at/fragen-und-antworten > Dashcams/Autokameras):

- Die Datenverarbeitung erfolgt zum ausschließlichen Zweck der Dokumentation eines Unfallherganges.
- Die Aufnahme des öffentlichen Raumes (= Straße) wird auf das erforderliche Maß beschränkt.
- Im Falle einer Speicherung werden Daten nur im unbedingt erforderlichen zeitlichen Ausmaß gespeichert (zum Beispiel 1 Minute vor dem Unfallgeschehen bis wenige Sekunden nach einem Unfall). Daten werden kontinuierlich überschrieben, soweit es zu keinem Unfall gekommen ist. Auch Unfalldaten dürfen nicht endlos gespeichert werden, sondern nur bis zur Zweckerreichung.

– Wenn die dauerhafte Speicherung von Bilddaten (= Stopp des Überschreibungsprozesses) von einer willentlichen Handlung des Verantwortlichen abhängig ist (etwa durch das manuelle Betätigen eines Speicherknopfes oder durch Entfernen einer SD-Karte), wird im Zweifelsfall von einer Unzulässigkeit der Dashcam auszugehen sein.
– Gewährleistung von Integrität und Vertraulichkeit durch Einsatz von Verschlüsselungstechniken und Zugriffsbeschränkungen.

Im Fokus

Mag. Matthias Wildpanner-Gugatschka

PNR-Gesetz

Am 27. April 2016 verabschiedeten die Gesetzgeber der Union die Richtlinie (EU) 2016/681 über die Verwendung von Fluggastdatensätzen (Passenger Name Records oder PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (PNR-Richtlinie).

Unter PNR-Daten werden personenbezogene Daten verstanden, die von einer Fluggesellschaft im Zuge der Buchung eines Fluges erfasst und gespeichert werden. Zu diesen Daten gehören etwa Informationen wie der Name des Fluggasts, seine Reisedaten, die gebuchte Reiseroute, seine zugewiesene Sitznummer, Gepäcksangaben, Kontaktangaben oder die vom Fluggast verwendete Zahlungsart.

Die Fluggesellschaften werden durch die PNR-Richtlinie verpflichtet, die bei der Buchung erhobenen Fluggastdatensätze an eine nationale Fluggastdatenzentralstelle, die von jedem Mitgliedstaat einzurichten ist und der die Verarbeitung der PNR-Daten obliegt, zu übermitteln. Die nationale Fluggastdatenzentralstelle soll ihrerseits die übermittelten Fluggastdatensätze zur Überprüfung der Fluggäste vor deren Ankunft oder vor deren Abflug verwenden, um so Personen zu finden, die im Verdacht stehen an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein. Nach der Vorstellung des Unionsgesetzgebers sollen anhand von PNR-Daten jedoch auch Personen gefunden werden, die bislang nicht im Verdacht stehen, an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein und somit nicht in entsprechenden Datenbanken gespeichert sind. Während sich der Anwendungsbereich der PNR-Richtlinie grundsätzlich auf Flüge in die Union oder aus der Union erstreckt, eröffnet die Richtlinie den Mitgliedstaaten die Möglichkeit, den Anwendungsbereich auch auf Flüge innerhalb der Union zu erstrecken.

Mit dem am 17. August 2018 erlassenen Bundesgesetz über die Verarbeitung von Fluggastdaten zur Vorbeugung, Verhinderung und Aufklärung von terroristischen und bestimmten anderen Straftaten (PNR-Gesetz) setzte der österreichische Gesetzgeber die PNR-Richtlinie um. Mit der (wiederverlautbarten) Verordnung des Bundesministers für Inneres vom 15. Februar 2019 wurde der Anwendungsbereich des PNR-Gesetzes auch auf jene innereuropäischen Flüge erstreckt, mit denen Personen von einem Mitgliedstaat der Union nach Österreich oder aus Österreich in einen Mitgliedstaat der Union befördert werden. Die nationale Fluggastdatenzentralstelle ist beim Bundesministerium für Inneres eingerichtet und organisatorisch im Bundeskriminalamt angesiedelt. Die von den Fluggesellschaften zu übermittelnden PNR-Daten sind im PNR-Gesetz aufgelistet und entsprechen dem Anhang I der PNR-Richtlinie. Sollten von einer Fluggesellschaft Fluggastdaten übermittelt werden, die nicht dem PNR-Gesetz bzw. der PNR-Richtlinie entsprechen, hat die nationale Fluggastdatenzentralstelle diese unverzüglich zu löschen. Die nationale Fluggastdatenzentralstelle ist ermächtigt, die PNR-Daten mit den Fahndungsevidenzen und sicherheitspolizeilichen Datenbanken sowie anhand bestimmter Kriterien abzugleichen. Der Abgleich mit den von der Fluggastdatenzentralstelle festgelegten Kriterien soll die Identifizierung von Personen ermöglichen, die den Sicherheitsbehörden bzw. den Strafverfolgungsbehörden bislang noch nicht bekannt sind, jedoch mit einer strafbaren Handlung im Sinne des PNR-G in Zusammenhang stehen könnten.

Die nationale Fluggastdatenzentralstelle darf die Fluggastdatensätze für fünf Jahre speichern, wobei die Daten nach sechs Monaten depersonalisiert werden müssen. Das bedeutet, dass nach einem Zeitraum von sechs Monaten die Identität der betroffenen Person nicht mehr unmittelbar festgestellt werden kann. Eine Aufhebung einer solchen Depersonalisierung ist nur auf Grund eines begründeten Ersuchens einer zuständigen Behörde und nach Ermächtigung des jeweiligen Rechtsschutzbeauftragten oder auf Anordnung der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung oder auf Anordnung des Gerichts nach den Bestimmungen der Strafprozessordnung möglich.

Die unmittelbare Kontrolle über die Rechtmäßigkeit sämtlicher Verarbeitungsvorgänge in der PNR-Datenbank obliegt dem Datenschutzbeauftragten beim Bundesministerium für Inneres und in weiterer Folge der Datenschutzbehörde. Das

PNR-Gesetz sieht ein spezielles Auskunftsrecht für Betroffene vor. Demnach können sich Fluggäste mit einem Auskunftsersuchen an die nationale Fluggastdatenstelle wenden, um Auskunft über die zu ihrer Person verarbeiteten Daten zu erhalten, wobei sich das Auskunftsrecht nicht auf jene Daten erstreckt, die bereits depersonalisiert wurden.

Ob die PNR-Richtlinie und damit das PNR-Gesetz in der gegenwärtigen Ausgestaltung mit dem Grundrecht auf Datenschutz vereinbar ist, wird durch den Europäischen Gerichtshof bzw. den Verfassungsgerichtshof zu klären sein.

Ausgewählte Entscheidungen der DSB

DSB-D124.352/0003-DSB/2019, Abwägung zwischen dem Recht auf Geheimhaltung und dem Recht auf freie Meinungsäußerung

Im Bescheid vom 2. Dezember 2019, GZ: DSB-D124.352/0003-DSB/2019, hatte sich die Datenschutzbehörde mit einer Abwägung des Rechts auf Geheimhaltung (§ 1 DSG) gegen das Recht auf freie Meinungsäußerung auseinander zu setzen.

Die Beschwerdeführerin ist Polizistin in Tirol und war Teil eines Einsatzes zur Weihnachtszeit 2018. Ein 12-jähriger Minderjähriger – untergebracht in einem Wohnheim – war abgängig. Er hatte seine Familie und zwei Schwestern zu Weihnachten 2018 - besucht. Die Eltern hatten aufgrund der bekannten Abgängigkeit im Wohnheim die Polizei verständigt, die – von der Bezirksleitstelle beauftragt – mit zwei Streifenwagen und 6 Mann uniformierter Besatzung bei dem Einfamilienhaus vorgefahren war, um den Minderjährigen abzuholen.

Der Vater des Minderjährigen – Beschwerdegegner des Verfahrens vor der Datenschutzbehörde - hatte vom Dachgeschoß aus Fotos angefertigt, die die in der Auffahrt geparkten Einsatzfahrzeuge samt mehrerer Polizisten zeigten und auf Facebook mit dem Zusatz „So werden 12jährige Kinder mit der Polizei gegen ihren Willen von zuhause weggezogen. Bitte teilen“ gepostet.

Die Beschwerdeführerin forderte daraufhin den Beschwerdegegner telefonisch auf, das Facebook-Posting zu entfernen. Kurz darauf veröffentlichte der Beschwerdegegner nochmals dieselben Fotos auf Facebook, diesmal unter dem Titel „Auf ein neues Frau Müller“ (Name der Beschwerdeführerin von der Datenschutzbehörde geändert).

Die Beschwerdeführerin fühlte sich durch die beiden Facebook-Postings in ihrem Recht auf Geheimhaltung verletzt.

Die Datenschutzbehörde wies die Beschwerde hinsichtlich des ersten Postings ab, weil davon auszugehen war, dass damit ein Beitrag zu einer Debatte von öffentlichem Interesse (namentlich die Angemessenheit der Abholung Minderjähriger mit zwei Streifenwägen und 6 Mann uniformierter Besatzung) vorlag und das Recht auf freie Meinungsäußerung überwog.

Anders stellte sich der Sachverhalt in Bezug auf das zweite Posting dar: Dieses Posting lieferte keinen Beitrag zu einer Debatte im öffentlichen Interesse. Der Beschwerdegegner bezweckte damit vielmehr seinem Unmut öffentlich Ausdruck zu verleihen und nannte zudem auch noch den Nachnamen der Beschwerdeführerin, weswegen das schutzwürdige Geheimhaltungsinteresse der Beschwerdeführerin überwog und der Beschwerde in diesem Punkt stattzugeben war.

DSB-D130.073/0008-DSB/2019, Fehlendes „Double-Opt-In-Verfahren“ bei Onlinedating-Portalen

Im vorliegenden Fall ging es um ein Unternehmen, das Onlinedating-Portale betreibt. Der Beschwerdeführer erhielt Sex-Spams von diesem Unternehmen, obwohl er sich nicht bei dessen Onlinedating-Portalen angemeldet hatte. Die DSB entschied für den Beschwerdeführer und sprach aus, dass das Unternehmen den Beschwerdeführer wegen fehlender Datensicherheitsmaßnahmen – konkret wegen eines fehlenden „Double-Opt-In-Verfahrens“ – in seinem Recht auf Geheimhaltung gemäß § 1 Absatz 1 DSG verletzt hat.

Beim „Double-Opt-In-Verfahren“ gibt ein User die Zustimmung zur Verwendung seiner personenbezogenen Daten doppelt („double“): Zunächst meldet sich der User auf der Website des Unternehmens, dessen Services er nutzen will, mit seiner E-Mail-Adresse an. Danach schickt ihm das Unternehmen auf die angegebene E-Mail-Adresse ein Bestätigungs-E-Mail. Erst wenn der User seine Anmeldung – etwa durch Anklicken eines Aktivierungslinks im Bestätigungs-E-Mail - nochmals bestätigt, hat das Unternehmen eine DSGVO-konforme Zustimmung zur Verwendung der personenbezogenen Daten des Users erlangt.

Im vorliegenden Fall reichte die Bekanntgabe einer beliebigen E-Mail-Adresse, um sich bei den Onlinedating-Portalen des Unternehmens anzumelden. Das Unternehmen schickte dem User zwar ein Bestätigungs-E-Mail an die angegebene E-Mail-Adresse, wartete aber nicht darauf, dass der User seine Anmeldung nochmals durch Anklicken eines Aktivierungslinks im Bestätigungs-E-Mail bestätigte. Das Unternehmen verwendete also kein „Double-Opt-In-Verfahren“, vielmehr erlaubte es dem User, der sich auf der Website des Unternehmens anmeldete, sofort – das heißt mit Bekanntgabe der E-Mail-Adresse – die Nutzung seiner Onlinedating-Portale. Das führte - wie im vorliegenden Beschwerdefall - dazu, dass eine fremde Person die E-Mail-Adresse des Beschwerdeführers dazu nutzte,

sich für die Onlinedating-Portale des Unternehmens anzumelden, sodass diese fremde Person sofort die Onlinedating-Portale des Unternehmens selbst nutzen konnte und der Beschwerdeführer auf seine E-Mail-Adresse Sex-Spams erhielt, ohne sich jemals auf dessen Onlinedating-Portalen angemeldet zu haben.

Der Bescheid ist rechtskräftig.

DSB-D122.970/0004-DSB/2019, Löschung eines pseudonymen Nutzerprofils

Im Bescheid vom 8.11.2019, GZ: DSB-D122.970/0004-DSB/2019 (RIS), hatte sich die DSB mit der Verarbeitung pseudonymisierter Daten (Art. 4 Z 5 DSGVO) zu befassen. Der Beschwerdeführer hatte beim Anbieter eines Internet -Kleinanzeigenportals ein Nutzerprofil angelegt, das nur durch einen (wählbaren) Nutzernamen und eine E- Mail- Adresse als „unique identifier" gekennzeichnet war. Dieses Nutzerprofil wollte er nun löschen lassen. Eine Möglichkeit zur Selbstlöschung wurde nicht angeboten. Das verantwortliche Unternehmen reagierte auf den per E-Mail-Adresse gesendeten Löschungswunsch mit der Aufforderung, einen umfassenden Löschungsantrag auszufüllen und darin u.a. den vollständigen (Real -) Namen und die Wohnadresse bekanntzugeben. Die Datenschutzbehörde gab der Beschwerde Folge, stellte eine Verletzung des Löschungsrechts fest und trug der Beschwerdegegnerin auf, das Profil zu löschen. Begründet wurde dies u.a. mit einem Verstoß gegen die Pflicht gemäß Art. 12 Abs. 2 DSGVO, der betroffenen Person die Ausübung ihrer Rechte zu erleichtern, und der fehlenden Möglichkeit, die im verlangten Löschungsantrag zusätzlich erhobenen Daten zwecks Feststellung der Identität mit bereits verarbeiteten Daten zu vergleichen. Bei einem pseudonymen Nutzerprofil reiche es aus, wenn sich der Nutzer etwa durch Kenntnis der Login -Daten (User-ID, Passwort), durch Angaben zum gespeicherten Dateninhalt des Profils oder durch die nachgewiesene Verfügungsgewalt über die Mailbox, deren E -Mail-Adresse anlässlich der Registrierung angegeben worden ist, identifizieren könne.

Der Bescheid ist rechtskräftig.

DSB-D124.285/0005-DSB/2019, Unzulässige Offenlegung von Gesundheitsdaten in einer WhatsApp-Chatgruppe

Mit Bescheid vom 7. Oktober 2019 zur GZ: DSB-D124.285/0005-DSB/2019 hatte sich die Datenschutzbehörde mit der Frage zu beschäftigen, ob eine Arbeitsunfähigkeitsmeldung (ohne Diagnose) als Gesundheitsdatum im Sinne von Art. 9 Abs. 1 DSGVO zu qualifizieren ist und ob die Offenlegung einer solchen Arbeitsunfähigkeitsmeldung in einer WhatsApp-Chatgruppe zu Unrecht erfolgt ist.

Bei der Beschwerdegegnerin handelt es sich um die ehemalige Arbeitgeberin des Beschwerdeführers. Dieser meldete sich krank und übermittelte die Arbeitsunfähigkeitsmeldung an einen Vorgesetzten der Beschwerdegegnerin. Dieser Vorgesetzte, der der Beschwerdegegnerin zuzurechnen ist, teilte die genannte Arbeitsunfähigkeitsmeldung unter Verwendung des Kurznachrichtendienstes WhatsApp in einer WhatsApp-Chatgruppe, an welcher neben dem Beschwerdeführer auch weitere ArbeitnehmerInnen der Beschwerdegegnerin teilgenommen haben.

Die Datenschutzbehörde wies zunächst auf die Judikatur des EuGH in der Rechtssache C-101/01 (Lindqvist) hin, wonach der Begriff „Daten über Gesundheit" weit auszulegen sei und hielt fest, dass diese Judikatur auch auf die neue Rechtslage übertragbar ist. Zwar befand sich auf der gegenständlichen Arbeitsunfähigkeitsmeldung kein konkreter Grund für die Arbeitsunfähigkeit, allerdings besitzt nach Auffassung der Datenschutzbehörde die Information über den konkreten Zeitraum einer Arbeitsunfähigkeit (Beginn der Arbeitsunfähigkeit und Termin für die Wiederbestellung beim behandelnden Arzt) eine ausreichende Aussagekraft über den körperlichen oder geistigen Gesundheitszustand einer Person, um als „Gesundheitsdatum" nach nunmehr Art. 4 Z 15 DSGVO qualifiziert zu werden.

Eine Rechtsgrundlage für die Offenlegung der Arbeitsunfähigkeitsmeldung, auf der neben den Gesundheitsdaten auch weitere Informationen wie die Sozialversicherungsnummer und die vollständige Anschrift des Beschwerdeführers enthalten waren, war nicht ersichtlich. Vor diesem Hintergrund war mangels Rechtsgrundlage eine Verletzung im Recht auf Geheimhaltung aufgrund einer unzulässigen Offenlegung von Gesundheitsdaten in einer WhatsApp-Chatgruppe festzustellen.

Neben diesem Verfahren wurden auch zwei weitere, parallel geführte Beschwerden gegen die Beschwerdegegnerin aufgrund desselben Sachverhalts eingebracht. Die Datenschutzbehörde machte daher zusätzlich amtswegig von ihrer Befugnis nach Art. 58 Abs. 2 lit. f DSGVO Gebrauch und hat gegen die Beschwerdegegnerin ein Verbot mit der Maßgabe verhängt, die Offenlegung von Daten ihrer ArbeitnehmerInnen im Zusammenhang mit einer Arbeitsunfähigkeitsmeldung unter Verwendung des Kurznachrichtendienstes WhatsApp zu unterlassen.

Dieser Bescheid sowie das ausgesprochene Verbot gegen die Beschwerdegegnerin sind nicht rechtskräftig.

Ausgewählte Entscheidungen der Gerichte

Vorabentscheidungsersuchen des Landesgerichts Bukarest (TK/Asocieta de Prorietari bloc M5A ScaraA)

Urteil des EuGH vom 11.12.2019, Rs C-708/18

Der zugrundeliegende Fall des vorlegenden Gerichts betraf die Frage der Rechtmäßigkeit einer Videoüberwachung (VÜ) in einem Mehrparteienhaus. Ein Miteigentümer hatte der Videoüberwachung nicht zugestimmt. Das System mit mehreren Kameras wurde aufgrund mehrerer Delikte gegen das Eigentum (Sachbeschädigung, Vandalismus etc.) eingerichtet, da sich andere Maßnahmen, wie ein davor installiertes Zutrittskontrollsystem als unwirksam erwiesen hatten. Der Beschwerdeführer TK forderte die Demontage bzw. Außerbetrieb-Setzung der Anlage, sie verstoße gegen das Recht auf Achtung des Privatlebens: Er habe der Anlage nicht zugestimmt und sehe das nationale Recht die Zustimmung zwingend vor. Bei der Beurteilung des Falls formulierte das Gericht vier Vorlagefragen zum EuGH betreffend die RL 95/46EG (DS-RL).

Der EuGH wiederholte in weiten Teilen seine Rechtsprechung zum Anwendungsbereich der DS-RL (C-212/13, C-131/12) und sprach weiter aus, dass für eine VÜ keine Einwilligung erforderlich ist (Art. 7 lit. f der DS-RL (nunmehr Art. 6 Abs. 1 lit. f DSGVO). Weiter, dass jede Datenverarbeitung den Grundsätzen nach Art. 6 der DS-RL (nunmehr Art. 5 DSGVO) genügen muss und zumindest in einem Eingriffstatbestand nach Art. 7 der DS-RL (nunmehr Art. 6 DSGVO) Deckung zu finden hat. Art. 7 lit. f der DS-RL gestattet die Verarbeitung unter drei kumulativen Voraussetzungen:

a. Wahrnehmung eines berechtigten Interesses;
b. Erforderlichkeit der Verarbeitung und
c. kein Überwiegen der Rechte und Freiheiten anderer.

Der Schutz des Eigentums, der Gesundheit und des Lebens der Miteigentümer eines Gebäudes können demnach als berechtigte Interessen angesehen werden. Diese müssen zum Zeitpunkt der Verarbeitung entstanden und vorhanden sein und dürfen zu diesem Zeitpunkt nicht nur hypothetisch sein - es ist jedoch nicht zwingend, dass die Sicherheit des Eigentums der Personen bereits zuvor beeinträchtigt wurde. Die Erforderlichkeit der Verarbeitung (als zweite Voraussetzung nach Art. 7 lit. f der DS-RL) verlangt, dass das angestrebte Ziel nicht mit weniger eingriffsintensiven Datenverarbeitungen erreicht werden kann (Datenminimierungspflicht nach Art. 6 Abs. 1 lit. c der DS-RL, nunmehr Art. 5 Abs. 1 lit. c DSGVO). Es ist zu unterscheiden, ob Daten aus öffentlich zugänglichen Quellen stammen oder aus nicht öffentlich zugänglichen Quellen. Für eine Abwägung der Interessen iSd Art. 7 lit. f der DS-RL sind die berechtigten Erwartungen der betroffenen Person zu berücksichtigen, dass ihre Daten nicht verarbeitet werden, wenn diese Person unter den konkreten Umständen vernünftigerweise nicht mit einer Weiterverarbeitung der Daten rechnen kann.

BVwG-Erkenntnis vom 25.11.2019, W211 2210458-1 (Videoüberwachung)

Der Betreiber eines Kebab-Standes in Niederösterreich wurde von der Polizei angezeigt, da seine Videokameras Bereiche gefilmt haben, die nicht in seiner Verfügungsbefugnis gestanden sind. Im Konkreten wurden auch Teile einer naheliegenden Bundesstraße und eine benachbarte Tankstelle von den Kameras erfasst. Überdies war die Speicherdauer unverhältnismäßig lange (14 Tage), Hinweisschilder fehlten.

Die Datenschutzbehörde verhängte daraufhin eine Geldbuße in einer Gesamthöhe von € 1.800 (€ 1.200 für das Filmen von Fremdgrund und jeweils € 300 wegen der Verstöße gegen Speicherdauer und Kennzeichnungsverpflichtung), dazu kamen Kosten in der Höhe von 10 % bzw. 5 Tage Ersatzfreiheitsstrafe.

Als Rechtsgrundlagen hierfür hat die DSB im Wesentlichen Art. 5 Abs. 1 lit. a und c sowie Art 6 Abs. 1 DSGVO (Filmen von Fremdgrund), § 13 Abs. 3 DSG (Speicherdauer) und § 13 Abs. 5 DSG (Kennzeichnung) herangezogen.

Der Beschuldigte erhob gegen das Straferkenntnis eine Beschwerde an das Bundesverwaltungsgericht.

Dieses bestätigte im Grunde die Entscheidung der DSB.

Die Strafen bezüglich Speicherdauer und fehlender Kennzeichnung wurden um die Hälfte auf € 150 reduziert, die Ersatzfreiheitsstrafe auf vier Tage.

Die Tatbestände des DSG hinsichtlich der zu langen Speicherdauer und der fehlenden Kennzeichnung wurden durch folgende Bestimmungen der DSGVO ersetzt:

- Speicherdauer: Art. 5 Abs. 1 lit. e sowie Art 6 abs. 1 lit. f DSGVO
- Kennzeichnung: Art. 5 Abs. 1 lit. a iVm Art. 12 und 13 DSGVO

Das BVwG geht - nicht nur in dieser Entscheidung - davon aus, dass die Bestimmungen zur Bildverarbeitung des Datenschutzgesetzes aufgrund fehlender Öffnungsklauseln in der DSGVO nicht anzuwenden sind.

Die ordentliche Revision wurde für zulässig erklärt.

Gesetzesbegutachtung – Stellungnahmen

Die DSB hat zu folgenden Gesetzesvorhaben eine Stellungnahme abgegeben:

- Transparenzdatenbank-Abfrageverordnung 2019
- Novelle des WTBG 2017 und des BiBuG 2019 zur Umsetzung der 5. Geldwäsche-Richtlinie
- Novelle der GewO 1994 zur Umsetzung der 5. Geldwäsche-Richtlinie (Geldwäschenovelle 2019)
- Wr. Veranstaltungsgesetz 2020
- Forschungsrahmennovelle (BMVIT) 2019

Weblink:

- Parlament aktiv: alle Stellungnahmen

Nachruf auf Mag[a]. Samraa El Fohail

(von Mag. Thomas Sonnenschein und Dr. Matthias Schmidl)

Mit großer Trauer müssen wir bekannt geben, dass unsere liebe und allseits geschätzte Kollegin Mag[a]. Samraa El Fohail Ende Dezember völlig überraschend verstorben ist.

Mag[a]. El Fohail ist im Zuge des In-Geltung-Tretens der Datenschutz-Grundverordnung im Mai 2018 vom Bundesministerium für Verkehr, Innovation und Technologie zur Datenschutzbehörde gewechselt. Die Juristin hat sowohl im Büro 1 (Präsidialangelegenheiten/Legistik) als auch im Büro 5 (Verwaltungsstrafsachen) gearbeitet und konnte dort ihre unbestrittene Expertise einbringen. So war sie unter anderem für die Ausarbeitung der Verordnung über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V) und die Verordnung über die Anforderungen an eine Stelle für die Überwachung der Einhaltung von Verhaltensregeln (Überwachungsstellen-akkreditierungs-Verordnung (ÜstAkk-V) maßgeblich verantwortlich. Mag[a]. El Fohail hat darüber hinaus etliche Verwaltungsstrafverfahren geführt und dabei stets ein gerechtes und verhältnismäßiges Augenmaß bei der Beurteilung des jeweiligen Sachverhaltes bewiesen.

Durch ihr tragisches Ableben verliert die Datenschutzbehörde nicht nur eine äußerst fachkundige, engagierte und hilfsbereite Mitarbeiterin, sondern auch einen hochgeschätzten Menschen.

Liebe Samraa, wir werden dich schmerzlich vermissen. Mögest Du in Frieden ruhen!

News

Folgende neue Mitarbeiterinnen und Mitarbeiter nahmen ihre Tätigkeit in der DSB auf:

Frau **Mag. Katharina Mayrhofer** studierte Rechtswissenschaften an der Universität Wien und absolvierte den Diplomlehrgang an der Diplomatischen Akademie. Nach diversen Praktika im In- und Ausland unterstützt sie das Team der Juristinnen und Juristen in den Bereichen nationales und internationales Verfahren.

Frau **Mag. Hannah Sprickler** studierte Rechtswissenschaften an der Universität Wien und unterstützt nun als Verwaltungspraktikantin das Team der Juristinnen und Juristen in den Bereichen nationales und internationales Verfahren.

Herr **Mag. Clemens Trauner** studierte Rechtswissenschaften an der Universität Wien und unterstützt nun nach Absolvierung seiner Gerichtspraxis als Verwaltungspraktikant in der Datenschutzbehörde das Team der Juristinnen und Juristen in den Bereichen nationales und internationales Verfahren.

Herr **Mag. Ali Zanjani** studierte Rechtswissenschaften an der Karl-Franzens-Universität Graz und unterstützt nach vorhergehender Tätigkeit als Rechtsanwaltsanwärter im Bereich IP/IT und Datenschutz das Team der Juristinnen und Juristen im Bereich des Verwaltungsstrafverfahrens.

Folgende Mitarbeiterinnen und Mitarbeiter beendeten ihre Tätigkeit in der DSB:

Frau Antonia Reininger, LL.B., Frau Christina Niederhametner, Frau Marlene Neichl, Herr Mag. Michael Brückner, Frau Mag. Christina Schwaiger.

Impressum:
Medieninhaber, Herausgeber und Redaktion: Österreichische Datenschutzbehörde (DSB), Barichgasse 40-42, 1030 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.