Republik Österreich
Datenschutzbehörde

NEWSLETTER 2/2020

Die Anwendbarkeit des § 11 DSG

Muss die Datenschutzbehörde bei erstmaligen Verstößen verwarnen statt strafen?

Mag. Ali Zanjani

Der im Zuge des Datenschutz-Deregulierungs-Gesetzes 2018 neu eingeführte § 11 DSG (Verwarnung durch die Datenschutzbehörde) normiert, dass die Datenschutzbehörde (DSB) den Katalog des Art. 83 Abs. 2 bis 6 DSGVO so anzuwenden hat, dass (1) die Verhältnismäßigkeit gewahrt wird und (2) dass insbesondere bei erstmaligen Verstößen gegen die DSGVO die Datenschutzbehörde im Einklang mit Art. 58 DSGVO von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen wird. Dieser Beitrag setzt sich mit der Anwendbarkeit des § 11 DSG auseinander und zeigt im Ergebnis auf, dass die Normen der Datenschutzgrundverordnung diese Bestimmung verdrängen.

Die DSB ist eine nach Art. 51 DSGVO eingerichtete unabhängige Aufsichtsbehörde, die für die Festsetzung von Sanktionen zuständig ist. Nach Art. 58 Abs. 2 lit. i DSGVO kann die DSB Geldbußen gemäß Art. 83 DSGVO „zusätzlich zu oder anstelle von“ anderen in Art. 58 Abs. 2 DSGVO bestimmten Befugnissen verhängen. Zu diesen anderen Befugnissen gehört auch die Verwarnung nach Art. 58 Abs. 2 lit. b DSGVO. Den Aufsichtsbehörden wird somit ein Ermessen eingeräumt. Es stellt sich daher die Frage, inwieweit der nationale Gesetzgeber dieses Ermessen der Aufsichtsbehörden durch nationale Bestimmungen einschränken kann und auf Grund welcher Öffnungsklausel oder Berechtigung im Rahmen der DSGVO diese Einschränkung erfolgt. In Bezug auf die Anwendbarkeit des § 11 DSG ist zunächst festzuhalten, dass diese Bestimmung im ersten Satz keinen normativen Mehrwert im Verhältnis zur DSGVO darstellt. Die Wahrung der Verhältnismäßigkeit im Zuge der Verhängung von Sanktionen wird bereits in Art. 83 Abs. 1 und 2 DSGVO normiert und zudem im Erwägungsgrund 129 angeführt. Hierzu wird auf die Rsp des EuGH zu Art. 288 AEUV verwiesen (Verbot der Wiederholung von unmittelbar anwendbarem Unionsrecht in nationalen Rechtsvorschriften der einzelnen Mitgliedstaaten, vgl EuGH 7.2.1973, Rs C-39/72, Kommission/Italien, Rz 17; 28.3.1985, Rs C-272/83, Kommission/Italien, Rz 26f).

Die Bestimmung des § 11 DSG erweckt, insbesondere durch die Überschrift „Verwarnung durch die Datenschutzbehörde“ in Verbindung mit dem zweiten Satz, beim Normadressaten den Eindruck, dass die Datenschutzbehörde als unabhängige Aufsichtsbehörde in ihrem Ermessen über die Bestimmungen der DSGVO hinaus insofern gebunden wird, dass bei erstmaligen Verstößen gegen die DSGVO

eine Verwarnung verhängt werden muss. Eine solche Auslegung widerspräche jedoch klar dem durch die DSGVO im Rahmen der Abhilfebefugnisse nach deren Art. 58 eingeräumten Ermessen (vgl hierzu Art. 58 Abs. 2 lit. b und i iVm Art. 83 Abs. 2 leg. cit.; siehe hierzu auch die Erwägungsgründe 129 und 148). Zudem ist für eine derartige nationale Bestimmung keine Öffnungsklausel im Rahmen der DSGVO gegeben. Die einschlägige Rsp des EuGH legt fest, dass Mitgliedstaaten die unmittelbare Wirksamkeit von Unionsrecht, durch den Erlass von verbindlichen Auslegungsregelungen in ihrem nationalen Recht, nicht verhindern oder sonst beschränken können (vgl hierzu EuGH 10.10.1973, Rs 34/73, Fratelli Variola, Rz 10,11; vgl auch mwN Kunnert in Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl, DSG (2018) § 11 Rz 3 ff).

Im Ergebnis ist daher festzuhalten, dass die DSB den – neu eingeführten – § 11 DSG auf Grund der Rsp des EuGH zum Anwendungsvorrang des Unionsrechts, der sowohl Gerichte als auch Verwaltungsbehörden zur Nichtanwendung nationaler Rechtsvorschriften verpflichtet, wenn diese Bestimmungen im Widerspruch zu unmittelbar anwendbarem Unionsrecht stehen (vgl EuGH 15.7.1964, Rs 6/64, Costa/ENEL, Rz 12 iVm EuGH 9.3.1978, Rs 196/77, Simmenthal, Rz 17/18 ff; siehe auch Ruffert in Callies/Ruffert, EUV/AEUV-Kommentar 4, Art. 1 AEUV Rz 19 ff), unionsrechtskonform anzuwenden hat, sodass sie in ihrem Ermessen im Rahmen der Verhängung von Sanktionen nicht beschränkt wird und daher auch bei erstmaligen Verstößen Geldbußen nach Art. 83 DSGVO verhängen kann. Dieses Ergebnis wird nicht nur durch die herrschende Meinung der Literatur (siehe Baumgartner, Öffentliches Recht (2018) S 65 f; Roth, Vorrang der Verwarnung bei erstmaligen Datenschutzverstößen: Der neue § 11 DSG im Konflikt mit dem Unionsrecht, ZTR 2018, 79; Kunnert in Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl, DSG § 11), sondern auch durch die Judikatur des Bundesverwaltungsgerichts (BVwG) bestätigt. Das BVwG hat in einer – noch nicht rechtskräftigen – Entscheidung (GZ: W211 2217212-1/9E) festgehalten, dass § 11 DSG auf Grund der bereits oben erläuterten Gründe nicht in dem Sinne anzuwenden ist, dass die DSB bei erstmaligen Verstößen in ihrem Ermessen beschränkt wird. Der Beschwerdeführer brachte im gegenständlichen Fall unter anderem vor, dass die DSB § 11 DSG ignoriert hätte, da im konkreten Fall ein erstmaliger Verstoß vorliegen würde, der von der DSB ursprünglich per Verwarnung zu ahnden gewesen wäre. Das BVwG führt hierzu aus: „Ein Vorrang des Vorgehens nach § 11 DSG lässt sich der Systematik und dem Anwendungsvorrang der DSGVO jedenfalls nicht entnehmen; betreffend einen möglichen Versuch, die belangte Behörde (oder das Gericht) über die DSGVO hinaus zu binden, fehlt es an einer entsprechenden Öffnungsklausel bzw. Ermächtigung in der DSGVO."

Im Fokus

Mag. Andreas Zavadil

Information der Datenschutzbehörde zum Coronavirus (Covid-19)

Aufgrund der derzeitigen Epidemie stellt sich für Unternehmen, Behörden und auch für ArbeitnehmerInnen die Frage, unter welchen Umständen Daten (insbesondere Gesundheitsdaten) verarbeitet und ausgetauscht werden können und dürfen. Darüber hinaus bringt der steigende Umstieg auf Home-Office und die erhöhte Cyberkriminalität einige Herausforderungen mit sich.

Die Datenschutzbehörde weist einleitend darauf hin, dass Daten über Infektionen mit dem Coronavirus (Covid-19) sowie über Verdachtsfälle zu jenen sensiblen Daten zählen, für die das Datenschutzrecht einen besonderen Schutz vorsieht.

Das Datenschutzrecht sieht jedoch ebenso vor, dass diese Gesundheitsdaten in jenem Ausmaß verwendet werden können, das notwendig ist, um die Verbreitung des Virus einzudämmen und um die Mitmenschen zu schützen. Dazu zählt insbesondere die Datenerhebung von Personen, bei denen eine Infektion festgestellt wurde oder bei denen ein Verdachtsmoment aufgrund eines Kontakts mit einer infizierten Person oder aufgrund eines Aufenthalts in einer Risikoregion besteht.

Im arbeitsrechtlichen Kontext kommt als konkrete Rechtsgrundlage der Datenverarbeitung Art. 9 Abs. 2 lit. i Datenschutz-Grundverordnung (DSGVO) in Betracht (Verarbeitung zum Zwecke der Gesundheitsvorsorge). Darüber hinaus ist jeder Arbeitgeber gegenüber seinen ArbeitnehmerInnen zur umfassenden Fürsorge verpflichtet, wozu der Ausschluss von Gesundheitsrisiken am Arbeitsplatz zählt. Vor diesem Hintergrund kann diese Datenverarbeitung auch auf Art. 9 Abs. 2 lit. b DSGVO (Verarbeitung zum Zwecke der Erfüllung arbeits- und sozialrechtlicher Pflichten) gestützt werden. Für die Übermittlung der Gesundheitsdaten an die Gesundheitsbehörden normiert Art. 9 Abs. 2 lit. i DSGVO eine entsprechende Rechtsgrundlage (Verarbeitung aus Gründen des

öffentlichen Interesses im Bereich der öffentlichen Gesundheit). Weiters kann auf Verlangen der Bezirksverwaltungsbehörden ebenso eine Pflicht des Arbeitgebers zur Auskunftserteilung (über Verdachtsfälle und Infektionen) nach § 5 Abs. 3 Epidemiegesetz 1950 bestehen. Bitte wenden Sie sich bei Fragen, wem festgestellte Infektionen oder Verdachtsfälle zu melden sind, an die Gesundheitsbehörden.

Zur Risikoprävention ist es ferner zulässig, dass Arbeitgeber die private Handynummer der ArbeitnehmerInnen erfragen und temporär speichern, um diese kurzfristig über eine Infektion im Betrieb oder in der Behörde warnen zu können und damit diese nicht am Arbeitsplatz erscheinen müssen. Die ArbeitnehmerInnen können zu dieser Bekanntgabe jedoch nicht gezwungen werden. Deshalb ist es ratsam, die Datenverarbeitung der privaten Kontaktdaten auf die Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO zu stützen. Die Freiwilligkeit einer solchen Einwilligung ist zu bejahen, da die Datenverarbeitung im Interesse der ArbeitnehmerInnen erfolgt.

Die Datenverarbeitung hat unter Einhaltung des Zweckbindungsgrundsatzes gemäß Art. 5 Abs. 1 lit. a DSGVO zu erfolgen. Eine Verwendung der Gesundheitsdaten für andere Zwecke als der Gesundheitsvorsorge, der Eindämmung des Virus und der Heilbehandlung ist daher unzulässig. Darüber hinaus ist auf den Grundsatz der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e DSGVO hinzuweisen. Nach Ende der Epidemie sind daher jene Daten, die nicht mehr notwendig sein werden, (wie insbesondere die privaten Kontaktdaten der ArbeitnehmerInnen) zu löschen. Aufgrund des Umstands, dass vermehrt Home-Office zum Einsatz kommt, ist schließlich auf die Sicherheitsvorgaben gemäß Art. 5 Abs. 1 lit. f iVm Art. 32 Abs. 1 DSGVO hinzuweisen. Die Arbeitgeber sollten Ihre Mitarbeiter insbesondere darauf hinweisen, dass Hardware (wie Dienstlaptops und Diensthandys) sicher aufzubewahren und dass eine geschützte WLAN-Verbindung mit einem starken Passwort (optimalerweise auch eine verschlüsselte VPN-Verbindung) zu verwenden ist (so diese vorhanden) sowie, dass erhöhte Aufmerksamkeit gegenüber Phishing-Nachrichten mit angeblich neuen Informationen über das Coronavirus bestehen sollte.

Die Datenschutzbehörde stellt auf ihrer Startseite unter www.dsb.gv.at ein Musterformular (Erhebung privater Kontaktdaten von Mitarbeitern) und ein Informationsblatt zu Datensicherheit und Home-Office zur freien Verwendung zur Verfügung.

Ausgewählte Entscheidungen der DSB

DSB-D123.815/0002-DSB/2019, Patientenbogen frei zugänglich mit Diagnose/Medikation

Im Bescheid vom 16. Jänner 2020, GZ: DSB-D123.815/0002-DSB/2019, hatte sich die Datenschutzbehörde mit einer Beschwerde im Recht auf Geheimhaltung (§ 1 DSG) auseinander zu setzen.

Der Beschwerdeführer wurde von seinem Arbeitgeber zu einer periodischen Untersuchung bei der Beschwerdegegnerin (einem Arbeitsmedizinischen Zentrum) geladen. Vor der Untersuchung hat der Beschwerdeführer ein Patientenblatt ausgefüllt und Angaben zu seinem Gesundheitszustand und seinen Medikamenten gemacht. Einige Tage später wurde der Beschwerdeführer von einem ehemaligen Arbeitskollegen kontaktiert (der selbst zu einer Untersuchung bei der Beschwerdegegnerin geladen war) und darauf aufmerksam gemacht, dass der Patientenbogen des Beschwerdeführers offen herumliegen würde. Der ehemalige Kollege konnte namentlich die Medikamente sowie die Wohnadresse des Beschwerdeführers nennen.

Im gegenständlichen Fall war es so, dass eine Mitarbeiterin der Beschwerdegegnerin die Unterlagen des Beschwerdeführers auf ihrem Schreibtisch abgelegt hatte. Im Zuge einer kurzfristen Abwesenheit der Mitarbeiterin war es dem ehemaligen Arbeitskollegen möglich, Einsicht zu nehmen. Wie genau es diesem gelang, Einsicht in die Unterlagen zu nehmen und ob – wie von der Beschwerdegegnerin vorgebracht, eine bewusste und absichtliche Handlung dazu führte – konnte im Ermittlungsverfahren nicht mehr festgestellt werden. Festgestellt werden konnte aber, dass die Mitarbeiterin der Beschwerdegegnerin sensible Unterlagen des Beschwerdeführers in unmittelbarer Nähe von Dritten offen abgelegt hatte.

Rechtlich ergab sich daher, dass die Beschwerdegegnerin den Beschwerdeführer im Recht auf Geheimhaltung verletzt hatte, indem Unterlagen, die Angaben zum Gesundheitszustand und Medikamentengebrauch des Beschwerdeführers enthielten, offen liegen gelassen wurden, womit es einem Dritten möglich war, Einsicht in selbige zu nehmen.

Der Bescheid ist rechtskräftig.

DSB-D123.685/0009.DSB/2019, Veröffentlichung von Bildaufnahmen der Polizei während einer Amtshandlung

Im Bescheid vom 28. Februar 2020, GZ: DSB-D123.685/0009.DSB/2019, hatte sich die Datenschutzbehörde mit der Frage zu befassen, inwiefern das Filmen von Organen des öffentlichen Sicherheitsdienstes während einer Amtshandlung, und das anschließende Veröffentlichen dieser Bildaufnahmen auf sozialen Medien, gegen das Recht der Polizisten auf Geheimhaltung verstößt. Hierbei hatte die Datenschutzbehörde den Schutz auf personenbezogene Daten gegen das Recht auf freie Meinungsäußerung abzuwägen und gelangte zu einer teilweisen Stattgabe der Beschwerde.

Das Hinterfragen der Verhältnismäßigkeit von polizeilicher Befehls- und Zwangsgewalt – hier zum Thema „Ethnic Profiling durch die Polizei" – stellt einen Beitrag zu einer Debatte von öffentlichem Interesse dar. Es lag daher nach Ansicht der Datenschutzbehörde grundsätzlich eine zulässige Veröffentlichung vor und war die Beschwerde dahingehend abzuweisen.

Anders verhält es sich jedoch bei zwei konkreten Bildaufnahmen: Zum einen wurde ein Polizist, unter Verwendung eines Snapchat-Filters, mit Hasenohren und Hasennase dargestellt, zum anderen wurde eine Polizistin abgelichtet, wobei diese Bildaufnahme mit anzüglichem Text und sexualisiertem Emoji versehen war. Diese beiden Veröffentlichungen stellen keinen geeigneten Beitrag zu einer Debatte von öffentlichem Interesse dar. Insbesondere liegt in letzterer Bildaufnahme der Fokus nicht auf einem Organ der Polizei, sondern bezieht sich direkt auf eine Person in ihrer Rolle als Frau. Im Hinblick auf diese beiden Bildaufnahmen überwiegt daher das Recht auf Geheimhaltung und war der Beschwerde dahingehend stattzugeben.

Der Bescheid ist nicht rechtskräftig.

DSB-D124.1090/0005-DSB/2019, Verletzung im Recht auf Geheimhaltung: Führerschein und Bankomatkarte fotografiert und auf WhatsApp versendet

Im Bescheid vom 3.1.2020, GZ: DSB-D124.1090/0005-DSB/2019, hatte sich die DSB mit der Verarbeitung personenbezogener Daten im Zusammenhang mit Maßnahmen in Bezug einer nicht bezahlten Beförderungsdienstleistung auseinanderzusetzen. Der Beschwerdeführer hatte eine Beförderungsdienstleistung des Beschwerdegegners, der ein Taxi-Unternehmen betreibt, in Anspruch genommen. Da der Beschwerdeführer nicht über genügend Bargeld verfügte, um bezahlen zu können, fertigte der Beschwerdegegner ohne Einwilligung des Beschwerdeführers ein Foto von dessen Führerschein und Bankomatkarte an, wobei er das Führerschein-Foto per „Whatsapp" an zumindest eine dritte Person (einen Bekannten des Beschwerdegegners) weiterleitete.

Die Datenschutzbehörde gab der Beschwerde statt und stellte eine Verletzung im Recht auf Geheimhaltung des Beschwerdeführers iSd. § 1 DSG fest, da weder die Datenerhebung (Fotografieren) noch die Datenübermittlung (Weiterleiten per Whatsapp) rechtmäßig war. Der Beschwerdegegner konnte sich diesbezüglich weder auf ein lebenswichtiges Interesse des Betroffenen noch dessen Zustimmung stützen. Eine Verarbeitung im überwiegenden berechtigten Interesse des Beschwerdegegners war ebenfalls zu verneinen, da das Fotografieren des Führerscheins und der Bankomatkarte sowie das Weiterleiten des Führerschein-Fotos an einen Bekannten des Beschwerdegegners unverhältnismäßig war und gegen den Grundsatz der Datenminimierung iSd. Art. 5 Abs. 1 lit. c verstoßen hat.

Dieser Bescheid ist nicht rechtskräftig.

DSB-2020-0.059.515 (D124.1579), Datenweitergabe von Mieterdaten von der Hausverwaltung an einen Subdienstleister gesetzlich gedeckt

Im Bescheid vom 20.02.2020, GZ: DSB-2020-0.059.515(D124.1579), hatte sich die DSB mit der Datenweitergabe von Namens- und Telefondaten eines Mieters von der Hausverwaltung an einen Subdienstleister zur Konfliktlösung zu befassen.

Der Beschwerdeführer setzte zunächst die Hausverwaltung telefonisch vom ungebührlichen Verhalten eines Mieters in Kenntnis. Eine Mitarbeiterin der Hausverwaltung nahm den Sachverhalt auf und informierte den Beschwerdeführer, dass sie einen Subdienstleister zur Konfliktlösung betrauen werde und sich dieser mit dem Beschwerdeführer in Verbindung setzen werde. Der Beschwerdeführer teilte der Mitarbeiterin daraufhin mit, dass seine Kontaktdaten nicht an den Subdienstleister übermittelt werden sollen und er auch keine Kontaktaufnahme durch Dritte wünsche. Da der Beschwerdeführer am nächsten Tag dennoch vom Subdienstleister telefonisch kontaktiert wurde, erachtete sich der Beschwerdeführer durch die Weitergabe seiner Namens- und Telefondaten von der Hausverwaltung in seinem Recht auf Geheimhaltung als verletzt und erhob Beschwerde bei der Datenschutzbehörde.

Im Rahmen des Verfahrens vor der Datenschutzbehörde brachte die Hausverwaltung vor, dass die Datenübermittlung an den Subdienstleister durch die einschlägigen landesgesetzlichen Bestimmun-

gen gedeckt gewesen wäre. Das entsprechende Gesetz sieht in der Tat vor, dass die Hausverwaltung sowie der Subdienstleister für die Erhebung eines Sachverhaltes bezüglich der Gewährleistung des friedlichen Zusammenlebens und der raschen Konfliktlösung berechtigt sind, einander Auskünfte zu erteilen bzw. in diesem Zusammenhang personenbezogene Daten der Mieterinnen und Mieter auszutauschen. Da die Übermittlung der Daten des Beschwerdeführers von der Hausverwaltung an den Subdienstleister somit gesetzlich gedeckt war, wies die Datenschutzbehörde die Beschwerde ab.

Der Bescheid ist nicht rechtskräftig.

News

Folgende neue Mitarbeiterin nahm ihre Tätigkeit in der DSB auf:

Frau **Haviseguel Kayayurt** verstärkt das Team der Kanzlei.

Ausgewählte Entscheidungen der Gerichte

Ersatz immaterieller Schäden nach Datenschutzverletzung

Wegen der Verarbeitung von Daten zur „Parteiaffinität" tausender Österreicherinnen und Österreicher durch die Österreichische Post AG (ÖPAG) hatte ein Betroffener die ÖPAG auf Schadenersatz gemäß Art. 83 DSGVO in Höhe von € 2.500,- geklagt und vom Erstgericht einen Betrag in Höhe von € 800,- zugesprochen erhalten (Landesgericht Feldkirch, 7.8.2019, AZ: 57 Cg 30/19b).

Über Berufung beider Streitparteien liegt nun das Berufungsurteil vor (Oberlandesgericht Innsbruck, 13.2.2020, AZ: 1 R 192/19b). Das Berufungsgericht ist den Anträgen der ÖPAG gefolgt und hat die Klage kostenpflichtig abgewiesen. Dieses Urteil ist rechtskräftig (zu niedriger Streitwert für Revision).

Der Kläger hatte immateriellen (nicht in Geld bezifferbaren) und ideellen Schaden durch Gefühle von Ärger, Ungemach und Kontrollverlust geltend gemacht. Das Berufungsgericht führte aus, dass ein solcher Schadenersatzanspruch gemäß Art. 83 DSGVO zwar möglich sei, der Kläger dafür aber das Eintreten des Schadens und dessen Höhe unter Beweis stellen hätte müssen. Die bloße Tatsache eines Verstoßes gegen Datenschutzrecht sei dafür nicht ausreichend. Der Verstoß müsse nachweislich ein über bloß „negative Gefühle" hinausgehendes „Mindestmaß an persönlicher Beeinträchtigung" des Geschädigten zur Folge gehabt haben. Der Kläger habe einen solchen Eingriff jedoch weder dargelegt, noch unter Beweis gestellt.

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.