Republik Österreich
Datenschutz behörde

NEWSLETTER 4/2018

100 Tage DSGVO aus Sicht der Datenschutzbehörde

Mag. Dr. Matthias Schmidl

Bereits im Vorfeld des 25. Mai 2018 war bei der DSB ein signifikanter Anstieg an Rechtsauskünften zu verzeichnen. Gleichzeitig waren viele Unternehmen, Vereine und Betroffene verunsichert, was die DSGVO bringen und wie die DSB den Vollzug gestalten wird. Die DSB hat dazu bereits lange vor Ingeltungtreten der Verordnung einen „Leitfaden" zur DSGVO auf ihrer Website publiziert, der über die wichtigsten Fragen Auskunft geben soll und vor allem für Nichtjuristinnen und Nichtjuristen konzipiert ist. Dieser Leitfaden wird ständig aktualisiert.

Am 25. Mai 2018 trat die DSGVO in Geltung. An diesem Tag wurde der Europäische Datenschutzausschuss (EDSA), der Nachfolger der Gruppe nach Art. 29 der Datenschutzrichtlinie, konstituiert und die Leiterin der Österreichischen Datenschutzbehörde zur Vorsitzenden gewählt.

Der 25. Mai selbst war in der DSB ein ruhiger Tag. Entgegen allen Erwartungen hielt sich die Anzahl der Eingangsstücke in Grenzen. Seit diesem Zeitpunkt ist allerdings ein merklicher Anstieg zu verzeichnen.

So langten seit 25. Mai alleine mehr Beschwerden (konkret mehr als 750) ein als im gesamten Jahr 2017 (489). Ein Gutteil dieser Beschwerden bezieht sich auf grenzüberschreitende Sachverhalte, somit auf Sachverhalte, in welchen die DSB eine Partnerbehörde zu verständigen und einzubeziehen hat oder in welchen die DSB von einer ausländischen Partnerbehörde kontaktiert wird. Es wurden seit dem Ingeltungtreten der DSGVO mehr als 60 amtswegige Prüfverfahren eingeleitet (2017: 93), es langten mehr als 250 Meldungen über die Verletzung des Schutzes personenbezogener Daten („Data Breach Notifications") ein, mehr als 110 Verwaltungsstrafverfahren wurden anhängig gemacht und in bisher 4 Fällen wurden Verhaltensregeln beantragt.

Die Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) wurde noch am 25. Mai im BGBl. II Nr. 108/2018 kundgemacht. Das Gegenstück – die Verordnung über die Datenschutz-Folgenabschätzung (DSFA-V) – wurde im Sommer 2018 einer öffentlichen Begutachtung unterzogen, im EDSA behandelt und wird zeitnahe veröffentlicht werden.

Der Personalstand der DSB hat sich erhöht: Seit Juni 2018 versehen 4 zusätzliche juristische Bedienstete ihren Dienst in der DSB. Aus derzeitiger Sicht kann der Arbeitsanfall mit dem bestehenden Personalstand knapp abgedeckt werden. Sollte der Anstieg im Verfahrensbereich nicht abebben, wird jedenfalls zusätzliches Personal erforderlich sein.

Die DSB hat seit dem 25. Mai bereits einige weitreichende Entscheidungen erlassen, die Verletzungen in den Rechten auf Geheimhaltung, Auskunft und Löschung zum Inhalt haben. Auch eine mangelhafte Einwilligungserklärung war bereits Gegenstand einer Entscheidung der DSB, in bisher zwei Fällen wurde eine Verwaltungsstrafe verhängt und in zwei Fällen wurde mit Bescheid aufgetragen, die Betroffenen von einer Sicherheitsverletzung in Kenntnis zu setzen.

Die ersten 100 Tage DSGVO waren für die DSB durchaus arbeitsintensiv und ereignisreich.

Im Fokus

Erste Erfahrungen mit Data Breach Notfications

Mag. Michael Suda

Bis zum 25. Mai 2018 gab es nur für Unternehmen der IKT-Branche (Anbieter von Telekommunika-

tions- und Internetdiensten) eine im Unionsrecht und in nationalen Durchführungsbestimmungen (§ 95a TKG 2003) verankerte Pflicht, Datenschutzverletzungen bei der DSB zu melden (auch Data Breach Notification, kurz: DBN). Die Praxis hierzu war sehr unterschiedlich und reichte von der Meldung jeder Brief-Fehlzustellung bis hin zu großen Marktteilnehmern, die nie eine DBN vorgenommen haben.

Seit 25. Mai 2018 kann die DBN-Pflicht jeden treffen. Geregelt ist dies in den Artikeln 33 und 34 der DSGVO. Wie der Name schon sagt, handelt es sich um eine Pflicht eines Verantwortlichen oder eines Auftragsverarbeiters. Es gibt kein durchsetzbares Recht einer betroffenen Person auf Einhaltung der entsprechenden Bestimmungen oder auf Verhängung von Strafen.

Eine Missachtung der DBN-Bestimmungen kann jedoch gemäß Artikel 83 Abs. 4 DSGVO von der DSB mit Geldbußen bis zu 10 Millionen Euro (bis zu 2 % des weltweiten Jahresumsatzes bei Unternehmen) geahndet werden.

Zu melden ist unverzüglich, möglichst binnen 72 Stunden nach Bekanntwerden, jede in den Anwendungsbereich der DSGVO fallende Datenschutzverletzung. Folgende alternative Ausnahmen von der Meldepflicht gelten:

1. Nur juristische Personen (z.B. Unternehmen, Vereine, Gebietskörperschaften) sind betroffen.
2. Die Datenverarbeitung erfolgt durch natürliche Personen ausschließlich für persönliche oder familiäre Zwecke (z.B. Verlust eines Handys mit privatem Kontaktverzeichnis).
3. Es besteht voraussichtlich kein Risiko für die Rechte und Freiheiten natürlicher Personen.

Es ist derzeit noch schwer zu sagen, wann der dritte Ausnahmetatbestand erfüllt ist. Dafür fehlen noch entsprechende Präzedenzfälle. Derzeit ist es daher ratsam, im Zweifel zu melden.

Die DSB stellt auf ihrer Website ein PDF-Formular zur Verfügung. Dieses enthält die Angaben, die gemäß Artikel 33 Abs. 3 DSGVO in einer Meldung gemacht werden müssen. Die Verwendung ist freiwillig.

Können nicht alle Angaben sofort gemacht werden, so muss die Meldung im Zuge der Aufarbeitung der Datenschutzverletzung ergänzt werden. Jeder Vorfall muss überdies intern dokumentiert werden. Dies dient auch dem Selbstschutz, da so die Abhilfemaßnahmen nachgewiesen werden können. Die Erfüllung der Meldepflicht bedeutet nicht, dass Abhilfemaßnahmen (z.B. das Einspielen neuer Software zur Schließung einer Sicherheitslücke) bis zu einer Anweisung der DSB aufgeschoben werden dürfen.

Es kann auch notwendig sein, alle Betroffenen einzeln von der Datenschutzverletzung und den getroffenen Maßnahmen zu benachrichtigen. Grundsätzlich gilt dies, wenn ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Folgende alternative Ausnahmen von der Benachrichtigungspflicht gelten:

1. Der Verantwortliche hat vorab geeignete technische und organisatorische Vorkehrungen getroffen (z.B. sind die gehackten Daten verschlüsselt, sodass sie absehbar unzugänglich bleiben).
2. Der Verantwortliche hat nach der Datenschutzverletzung Maßnahmen ergriffen, die das hohe Risiko für die Rechte und Freiheiten wahrscheinlich beseitigen (z.B. die Passwörter aller betroffenen Kunden-Accounts zurückgesetzt).
3. Die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden; in diesem Fall ist eine öffentliche Bekanntmachung oder ähnliche Maßnahme geboten.

Auch kann es bei Fehlen einer Benachrichtigungspflicht, ja sogar bei Fehlen einer DBN-Pflicht überhaupt, dennoch erforderlich sein, die Betroffenen zu verständigen, etwa im Rahmen einer Warn- und Schadensminderungspflicht.

Vom 25. Mai bis Anfang September 2018 sind 235 DBN nach Art. 33 DSGVO und 16 DBN nach § 95a TKG 2003 eingelangt. Zwei davon betrafen internationale Fälle (Verfahren nach Art. 56 ff DSGVO, Zuständigkeit mehrerer Aufsichtsbehörden). In bisher 2 Fällen (Zlen. DSB-D084.110 und DSB-D084.133) war es notwendig, den Verantwortlichen durch Bescheid Anweisungen zu erteilen. In beiden Fällen ging es um die Frage der Benachrichtigung gemäß Art. 34 DSGVO. In einem Fall ist dabei eine öffentliche Bekanntmachung oder gleichwertige Maßnahme angeordnet worden. Die weit überwiegende Mehrzahl der bisher abgeschlossenen Fälle konnte durch eine Einstellungsmitteilung beendet werden.

Ausgewählte Entscheidungen der DSB

Benachrichtigung von betroffenen Personen im Zuge einer Sicherheitsverletzung

Im Bescheid vom 8. August 2018, GZ: DSB-D084.133/0002-DSB/2018, hatte sich die DSB mit den Voraussetzungen, unter welchen die Datenschutzbehörde von datenschutzrechtlich Verantwortlichen verlangen kann, eine nach Art. 34 Abs. 1 DSGVO gebotene Benachrichtigung nachzuholen, zu befassen.

Der Verantwortliche meldete der Datenschutzbehörde, dass ein Suchtmittelbuch verloren worden sei, in dem von ca. 150 Patienten in unverschlüsselter Form der Name, der körperliche Gesundheitszustand sowie die verabreichte Menge des Suchtgiftes enthalten waren. Der Verantwortliche ging im vorliegenden Fall davon aus, dass die betroffenen Patienten nicht zu benachrichtigen

seien, weil kein hohes Risiko für diese vorläge. Insbesondere könnten die verarbeiteten Daten in den „falschen Händen“ eine Bloßstellung bzw. einen Identitätsdiebstahl-/betrug nur mit großem Rechercheaufwand ermöglichen. Die DSB sah dies anders und trug dem Verantwortlichen die Benachrichtigung der Betroffenen auf. Begründet wurde dies damit, dass im Suchtgiftbuch auch Gesundheitsdaten gemäß Art. 4 Z 15 DSGVO enthalten waren.
Ein hohes Risiko für die Rechte und Freiheiten betroffener Personen besteht nämlich jedenfalls, bei umfangreicher Verarbeitung besonderer Kategorien von Daten, worunter auch Gesundheitsdaten fallen. Ausnahmen der Benachrichtigungspflicht gemäß Art. 34 Abs. 3 DSGVO lagen nicht vor. Dieser Bescheid ist rechtskräftig.

Kein Recht auf Löschung von Beiträgen aus Diskussionsforen eines Online-Zeitungsartikels

Im Bescheid vom 13. August 2018 zur GZ: DSB-D123.077/0003-DSB/2018 hatte sich die Datenschutzbehörde mit der Frage zu beschäftigten, ob ein Recht auf Löschung von Beiträgen einer betroffenen Person besteht, die diese im Rahmen eines Diskussionsforums unterhalb eines Online-Zeitungsartikels gepostet hat. Zweifelsfrei war, dass der Online-Artikel als solches unter das in § 9 Abs. 1 DSG normierte Medienprivileg fällt. Mit Bezug auf die Judikatur des EuGH wurde ausgesprochen, dass – um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen – Begriffe wie Journalismus weit ausgelegt werden müssen. Vor diesem Hintergrund muss das Privileg nach § 9 Abs. 1 DSG nach unionsrechtlichem Verständnis betrachtet werden und kann auch „Bürgerjournalismus“ umfassen (wie etwa Internet-Diskussionsforen). Insbesondere war zu berücksichtigen, dass gegenständlich mit den Beiträgen der betroffenen Person auch Beiträge anderer Benutzer (in Form von Antworten oder „Diskussionsbäumen“) verkettet waren. Die Beschwerde war daher im Ergebnis abzuweisen. Dieser Bescheid ist rechtskräftig.

Keine freiwillige Einwilligung zur Verwendung eines „GPS-Trackers“ in Firmenfahrzeugen

Im Rahmen eines amtswegigen Prüfverfahrens wurde im Bescheid vom 8. August 2018 zur GZ: DSB-D213.658/0002-DSB/2018 festgehalten, dass die Einwilligung der Arbeitnehmer zur Nutzung eines GPS-Systems für firmeneigene Fahrzeuge nicht freiwillig erfolgt. Im gegenständlichen Fall wurde ein „GPS-Tracker“ in Firmenfahrzeugen installiert und die Einwilligung der Arbeitnehmer bzw. Fahrer als Erlaubnistatbestand zur Verarbeitung herangezogen. Der Verantwortliche führte dabei Schutz bzw. Sicherheit des Firmeneigentums, Erleichterung der monatlichen Abrechnung mit der Leasingfirma, Routenplanung und -optimierung sowie einen Versicherungsbonus ins Treffen, übersah dabei jedoch, dass diese Faktoren zwar im Rahmen einer Beurteilung von berechtigten Interessen iSv Art. 6 Abs. 1 lit f berücksichtigt werden können, jedoch nicht im Rahmen der Beurteilung der Freiwilligkeit einer Einwilligung. Hinzu kam, dass die GPS-Daten 93 Tage gespeichert wurden und somit objektiv ein Leistungsprofil des Arbeitnehmers erstellt werden konnte, wie schnell bzw. pünktlich dieser Fahrten erledigt. Ein klar erkennbarer Vorteil durch dieses GPS-System war für den Arbeitnehmer nicht ersichtlich, weshalb dem Verantwortlichen im Ergebnis aufgetragen wurde, die Verarbeitung (Nutzung des GPS-Systems für firmeneigene Fahrzeuge) in Einklang mit der Datenschutz-Grundverordnung zu bringen, da die Einwilligung im vorliegenden Fall mangels Freiwilligkeit nicht als Erlaubnistatbestand herangezogen werden kann. Dieser Bescheid ist nicht rechtskräftig.

DSGVO-konforme, vorformulierte Einwilligungserklärungen

Im Bescheid vom 31. Juli 2018, GZ: DSB-D213.642/0002-DSB/2018, hatte sich die Datenschutzbehörde im Zuge eines amtswegigen Prüfverfahrens mit der DSGVO-konformen Ausgestaltung vorformulierter Einwilligungserklärungen zu befassen. Verfahrenseinleitender Gegenstand war der Textabschnitt eines Mitgliederanmeldeformulars, in welchem die datenschutzrechtliche Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO zu Marketingzwecken eingeholt wurde. Hierbei hielt die Datenschutzbehörde drei wesentliche Punkte fest:
Zum einen erfolgt die Einwilligung nur dann freiwillig, wenn die betroffene Person frei entscheiden kann, ob und in welcher Form sie der Datenverarbeitung zustimmt. Der suggerierte Eindruck, lediglich bestimmen zu können durch welches Medium (Post, elektronischen Übermittlungsweg oder Telefon) Marketing-Zusendungen erhalten werden, widerspricht daher einerseits dem Kriterium der Freiwilligkeit als auch jenem der Verständlichkeit, welche für eine DSGVO-konforme Einwilligung nach Art. 7 iVm Art. 4 Z 11 DSGVO jedoch essenziell sind.
Zum anderen entspricht auch die Platzierung der Einwilligungserklärung direkt über der Unterschrift, welche die Anmeldung zur Mitgliedschaft bestätigt, nicht den genannten Kriterien, da durch einen solchen Aufbau der irrige Eindruck erweckt wird, die Einwilligung zu einer Datenverarbeitung für Marketingzwecke sei für die Anmeldung zur Mitgliedschaft erforderlich.
Obendrein ist auch die Darstellung der Einwilligungserklärung in einem unmittelbaren textlichen Zusammenhang mit der Widerrufsmöglichkeit nicht DSGVO-konform, weil für die betroffene Person hierdurch der fälschliche Anschein entsteht, der Datenverarbeitung vorerst jedenfalls zustimmen zu müssen und diese erst durch späteren Widerruf unterbinden zu können (nicht zulässige „opt-out“-Lösung). Dieser Bescheid ist rechtskräftig.

Ausgewählte Entscheidungen der Gerichte

Urteil des EuGH vom 10.07.2018, C-25/17, Zeugen Jehovas

In diesem Vorabentscheidungsverfahren hatte der EuGH zu beurteilen, ob die Verkündungstätigkeit von Tür zu Tür einer Religionsgemeinschaft unter die Datenschutzrichtlinie (DSRL) fällt oder als „Tätigkeit für ausschließlich persönliche oder familiäre“ Zwecke zu werten ist und somit nicht unter die DSRL fällt. Der EuGH hat diese Frage dahingehend beantwortet, dass eine solche Tätigkeit unter die DSRL fällt und diese daher zu beachten ist.

Weiters war die Frage zu klären, ob die handschriftlichen Aufzeichnungen, die von den verkündenden Mitgliedern im Zuge der Verkündungstätigkeit von Tür zu Tür gemacht werden, eine „Datei“ im Sinne der DSRL sind. Der EuGH geht hier von einem weiten Dateibegriff aus und verlangt nur, dass die Daten nach bestimmten Kriterien, die eine leichte Wiederauffindbarkeit der Daten gewährleisten, strukturiert sein müssen. Um unter diesen Begriff zu fallen, muss eine solche Datensammlung nicht aus spezifischen Kartotheken oder Verzeichnissen oder anderen der Recherche dienenden Ordnungssystemen bestehen.

Zuletzt war strittig, wer im Falle einer Verkündungstätigkeit von Tür zu Tür als Verantwortlicher der Datenverarbeitung anzusehen ist – das verkündende Mitglied oder die dahinterstehende Religionsgemeinschaft. Der EuGH hat ausgesprochen, dass aufgrund der Umstände des Ausgangsverfahrens eine gemeinsame Datenverarbeitung vorliegt und dass verkündende Mitglieder und die Religionsgemeinschaft als gemeinsam Verantwortliche zu werten sind. Dafür ist es nicht erforderlich, dass die Religionsgemeinschaft Zugriff auf diese Daten hat oder ihren Mitgliedern nachweislich schriftliche Anleitungen oder Anweisungen zu diesen Datenverarbeitungen gegeben hat.

Das Urteil erging zwar noch zur DSRL, ist jedoch für die DSGVO von Relevanz, weil die wesentlichen Definitionen in der DSRL und in der DSGVO nicht voneinander abweichen.

Gesetzesbegutachtung – Stellungnahmen

Die DSB hat zu folgenden Gesetzesvorhaben eine Stellungnahme abgegeben:

- Entwurf eines Gesetzes, mit dem die Bauordnung für Wien, das Wiener Kleingartengesetz 1996, das Wiener Garagengesetz 2008, das Wasserversorgungsgesetz und das Wiener Wohnbauförderungs- und Wohnhaussanierungsgesetz – WWFSG 1989 geändert werden (Bauordnungsnovelle 2018)
- Entwurf einer Verordnung des Bundesministers für Inneres gemäß § 2 Abs. 5 PNR-G
- Entwurf eines Bundesgesetzes, mit dem das Telekommunikationsgesetz 2003, das Funkanlagen-Marktüberwachungs-Gesetz und das Funker–Zeugnisgesetz geändert werden soll
- Entwurf eines Gesetzes über die Anpassung der Burgenländischen Landesrechtsordnung an die Datenschutz-Grundverordnung im Agrarwesen
- Verordnung, mit der die Eignungsprüfungsverordnung-Inneres geändert wird

Weblink:

- Parlament aktiv: alle Stellungnahmen

News

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

Herr **Mag. Thomas Hofmann** absolvierte vor dem Studium der Rechtswissenschaften die Höhere technische Bundeslehr- und Versuchsanstalt Graz-Gösting (Wirtschaftsingenieur Betriebsinformatik), war Studienassistent im Bereich Datenschutzrecht an der Karl-Franzens-Universität Graz und arbeitet derzeit als Jurist in den Bereichen nationales und internationales Verfahren sowie Stammzahlenregister.

Frau **Mag. Clarissa Lechner**, MA war nach Absolvierung der Gerichtspraxis vier Jahre lang als juristische Mitarbeiterin am Verwaltungsgerichtshof tätig und unterstützt nun das Team der Juristinnen und Juristen in nationalen und internationalen Verfahren.

Impressum:
Medieninhaber, Herausgeber und Redaktion: Österreichische Datenschutzbehörde (DSB), Wickenburggasse 8, 1080 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

Informationen der DSB gem. Art. 13 und 14 DSGVO sind abrufbar unter: https://www.dsb.gv.at/datenschutz