Republik Österreich
Datenschutz behörde

NEWSLETTER 3/2017

DATENSCHUTZ-GRUNDVERORDNUNG KAPITEL V („ÜBERMITTLUNGEN PERSONENBEZOGENER DATEN AN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN") - ÜBERBLICK

Das geltende Datenschutzgesetz 2000 regelt die Weitergabe von Daten in das Ausland („Internationaler Datenverkehr" oder „Datenexport") in §§ 12 und 13 DSG 2000. Die Anträge für Genehmigungen haben in den letzten Jahren stark zugenommen. Waren es im Jahr 2014 noch 79 Anträge, so stieg die Anzahl im Jahr 2015 auf 128 und im Jahr 2016 auf 312.

Die Datenschutz-Grundverordnung (DSGVO) regelt diesen Bereich neu. Viele der bekannten rechtlichen Instrumente zum Schutz der Rechte der Betroffenen beim Empfänger finden ihren Platz in der DSGVO, und einige Neue kommen dazu. Es soll künftig nur noch wenige oder fast gar keine Fälle geben, in denen eine Genehmigung der Datenschutzbehörde erforderlich ist.

Die Datenschutz-Grundverordnung regelt den Datenexport in den Art. 44-50 (Kapitel V). Weiters sind die Erwägungsgründe 101-116, 153, 168 und 169 von Bedeutung. Wie die gesamte DSGVO beziehen sich die Bestimmungen auf natürliche Personen. Die Bestimmungen des Kapitels V kennen aber auch die Weitergabe an internationale Organisationen.

Artikel 44 ordnet an, dass das von der DSGVO gewährleistete Schutzniveau für natürliche Personen auch bei der Weiterübermittlung von Daten gewährleistet sein muss. Dies gilt auch bei Weiterübermittlung personenbezogener Daten durch das betreffende Drittland an ein anderes Drittland.

Artikel 45 normiert den genehmigungsfreien Datenexport in Länder (oder an internationale Organisationen) mit angemessenem Schutzniveau. Die Entscheidung, wann dies vorliegt trifft die Kommission. Zu den Anforderungen gehört auch die Existenz und wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden. Es gibt ein Verfahren zur Aberkennung und sogar ein Schnellverfahren für hinreichend begründete Fälle äußerster Dringlichkeit. Die Regelung kann eine ganzes Land, ein Gebiet oder spezifische Sektoren betreffen. Die bestehende Liste der Länder mit angemessenem Schutzniveau, in die auch jetzt schon gemäß § 12 Abs. 2 DSG 2000 genehmigungsfrei weitergegeben werden darf, ist kurz (siehe Datenschutzangemessenheits-Verordnung (DSAV), BGBl. II Nr. 521/1999 idgF.). Die bestehende Liste bleibt gültig. Für den Fall der Aberkennung des Schutzniveaus können die anderen Instrumente verwendet werden.

Artikel 46 regelt die Weitergabe ohne Genehmigung mit Hilfe geeigneter Garantien. Das erste Instrument sind Verträge zwischen Absender und Empfänger, die ein angemessenes Datenschutzniveau bei Empfänger garantieren sollen (Artikel 46 Abs. 2 lit. c). Die Vertragstexte (die Standarddatenschutzklauseln) werden von der

Kommission nach einem Prüfverfahren erlassen. Diese Verträge gab es schon bisher in Form der Standardvertragsklauseln. Die Standardvertragsklauseln waren das gebräuchlichste Instrument für den internationalen Datenverkehr.

Dazu kommen die verbindlichen internen Datenschutzvorschriften, die Binding Corporate Rules (BCR), die in Artikel 46 Abs. 2 lit. b und Artikel 47 geregelt sind. BCR sind eine Art „konzerneigenes Datenschutzgesetz", das für alle Töchter verpflichtend ist. BCR sind bereits jetzt in Verwendung. Sie sind nicht leicht zu erstellen (und daher bis dato selten anzutreffen), aber sehr nützlich weil sie Vertragsabschlüsse (vor allem Bündel von Verträgen mit vielen Empfängern) ersparen.

Neben diesen bereits bekannten Instrumenten gibt es auch neue Möglichkeiten: Öffentliche Stellen können mit rechtlich bindenden und durchsetzbaren Dokumen-

ten arbeiten (Artikel 46 Abs. 2 lit. a). Verhaltensregeln gemäß Artikel 40 (Artikel 46 Abs. 2 lit. e) und Zertifizierungsmechanismen gemäß Artikel 42 (Artikel 46 Abs. 2 lit. f) kommen ebenfalls in Frage. Bei Verhaltensregeln und Zertifizierungs-mechanismen müssen jedenfalls rechtsverbindliche und durchsetzbare Verpflichtungen des Empfängers bestehen, die den Betroffenen schützen.

Artikel 46 Abs. 3 bietet die Möglichkeit, mit individuell angefertigten Verträgen sowie Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen zu arbeiten. Dies erfordert aber eine Genehmigung durch die zuständige Aufsichtsbehörde.

Artikel 47 behandelt die Formulierung von Binding Corporate Rules. Bisher konnten BCR nur für Konzerne geschaffen werden. In Zukunft soll dies auch für Gruppen von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, möglich sein.

Artikel 49 enthält einige Sonderfälle wie den Einsatz von Einwilligungen, Erfüllung von Verträgen, Verteidigung von Rechtsansprüchen und im lebenswichtigen Interesse des Betroffenen, wenn dieser keine Einwilligung geben kann.

Gemäß Artikel 48 darf in Urteilen aus Drittländern die Offenlegung von Daten nur gefordert werden, wenn es dazu Abkommen gibt. Artikel 50 regelt die internationale Zusammenarbeit.

Die Datenschutz-Grundverordnung macht vieles einfacher und unbürokratischer, bringt aber auch mehr Verantwortung für die für die Datenanwendung Verantwortlichen. Diese müssen in Zukunft die eigenen Datenbanken und Zwecke für Übermittlungen besser kennen und selbst entscheiden, wie sie den internationalen Datenverkehr organisieren wollen. Wie bisher muss immer darauf geachtet werden, dass alle Verarbeitungsvorgänge zuerst im Inland zulässig sind, bevor ein Datenexport erwogen wird.

Im Fokus

Datenschutzverletzungen - Meldepflichten

Mag. Michael Suda

Mit der Datenschutz-Grundverordnung (DSGVO) kommen auch in Österreich neue, bisher ungekannte Meldepflichten auf datenschutzrechtlich Verantwortliche zu. Diese werden in der Praxis vor allem Unternehmen betreffen. Gelten werden sie aber für jeden, auf dessen Datenverarbeitung die DSGVO Anwendung findet. Also z.B. auch für gemeinnützige Organisationen und Gebietskörperschaften wie Länder und Gemeinden.

Verantwortliche werden durch die DSGVO verpflichtet, Meldungen von Verletzungen des Schutzes personenbezogener Daten (Englisch: Data Breach Notifications) an die Aufsichtsbehörde zu erstatten (Art. 33 DSGVO) und gegebenenfalls Betroffene von der Verletzung zu verständigen (Art. 34 DSGVO).

Ein Verantwortlicher hat eine Meldung im Falle einer Verletzung des Schutzes personenbezogener Daten an die Datenschutzbehörde zu erstatten, wenn dadurch ein Risiko für die Rechte und Freiheiten der Betroffenen besteht; dies unverzüglich und möglichst binnen 72 Stunden nachdem ihm die Verletzung bekannt wurde. Darüber hinaus sind die notwendigen Informationen (Beschreibung der Verletzung, Anzahl der Betroffenen bzw. der Datensätze, Maßnahmen, wahrscheinliche Folgen, Dokumentation, etc.) der Datenschutzbehörde zu übermitteln.

Ein Verantwortlicher hat Betroffene über die von ihm verursachten Datenschutzverletzungen zu benachrichtigen, wenn ein hohes Risiko für Rechte und Freiheiten der Betroffenen besteht; dies ohne ungebührliche Verzögerung. Ausnahmen sind möglich, z.B. bei geeigneten technischen und organisatorischen Sicherheitsvorkehrungen, etwa bei Verschlüsselung. Oder wenn der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht. Weiters wenn die Verständigung mit unverhältnismäßigem Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche, vergleichbar wirksame Maßnahme zu erfolgen.

Unter welchen genauen Bedingungen eine Datenschutzverletzung zu melden ist, wird in hohem Maße von der Auslegung von Begriffen wie „hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen“ (Art. 34 Abs. 1 DSGVO) abhängen. Wertvolle Hinweise dazu können dabei die laufend veröffentlichten vorläufigen Leitlinien (Guidelines, auf Englisch verfügbar) der Artikel-29-Gruppe geben: Article 29 Working Party.

Wie die Meldepflicht nach Art. 33 DSGVO in der Praxis umgesetzt wird, ob es etwa ein spezielles, technisch besonders gesichertes Mittel zur Erstattung der Meldungen geben wird (etwa ein Meldeportal, Onlineformular oder eine besondere Website), ist noch Gegenstand näherer Planungen. Die Datenschutzbehörde wird dabei auf ihre Erfahrungen mit der Meldepflicht von Datenschutzverletzungen im Bereich der elektronischen Kommunikation zurückgreifen (Archivseite: Meldepflicht Datenschutzverletzungen elektronische Kommunikation).

Das Unterlassen einer Meldung oder der Verständigung der Betroffenen kann zukünftig nach Art. 83 Abs. 4 lit. a) DSGVO mit Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs bestraft werden.

Ausgewählte Entscheidungen der DSB

Auskunft über Standortdaten an den Vertragsinhaber

In der Entscheidung, GZ DSB-D122.616/0006-DSB/2016, setzt sich die Datenschutzbehörde mit der Frage auseinander, ob ein Vertragsinhaber bei seinem Mobilfunkanbieter Standortdaten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers angeben, im Rahmen des Auskunftsrechts erfragen darf. Da die Standortdaten als betriebstechnisch notwendige Daten zum „Routing" innerhalb des Kommunikationsnetzes – also letztlich im Rahmen der Diensteerbringung (z.B. Telefonieren, SMS) bei mobilen Endgeräten – erforderlich sind, kann die Entstehung dieser Standortdaten vom Nutzer nicht verhindert/beendet oder ausgeschaltet werden, wie dies etwa bei einigen Apps, die über die GPS-Funktion des Smartphone eine Standortverfolgung ermöglichen, der Fall ist. Der Beschwerdeführer legte eine eidesstättige Erklärung vor, in der er darlegte Eigentümer und einzig Verfügungsbefugter für Gerät und Vertrag zu sein.

Der Mobilfunkanbieter verweigerte dem Vertragsinhaber die Daten zu beauskunften. Dies wurde damit begründet, dass aufgrund des Telekommunikationsgesetzes (TKG 2003), als spezialgesetzliche Norm, Standortdaten ausschließlich im Zuge polizeilicher Ermittlungen oder richterlicher Anordnungen bzw. den Betreibern von Notrufdiensten, wenn ein Notfall dadurch abgewehrt werden kann, übermittelt werden dürften.

Die Datenschutzbehörde folgte im Ergebnis dem Mobilfunkanbieter und sprach aus, dass die Einschränkung des Auskunftsrechts durch die Rechtsprechung des OGH gedeckt ist, wonach aufgrund des TKG 2003 dem Betroffenen nur ein auf Erhalt eines Einzelentgeltnachweises eingeschränktes Recht, über gespeicherte Verkehrsdaten Auskunft zu erhalten, einzuräumen ist. Im konkreten Fall war somit der Einschränkung der Auskunftserteilung im Rahmen der spezialgesetzlichen Bestimmung des TKG 2003 der Vorzug gegenüber dem in § 26 Abs. 1 DSG 2000 festgelegten allgemeinen Recht auf Auskunft des Beschwerdeführers zu geben.

Auskunft über Mitarbeiter des Auftraggebers?

Im Bescheid vom 07.04.2017, GZ: DSB-D122.671/0007-DSB/2017, hatte die DSB die Frage zu beurteilen, ob das Auskunftsrecht auch die Benennung konkreter Mitarbeiter eines Auftraggebers umfasst. Die Beschwerdeführerin hatte eine allgemeine Auskunft darüber verlangt, welche Mitarbeiter des Auftraggebers ihre Daten in einem bestimmten Zeitraum abgefragt hatten. Unter Verweis auf die Rechtsprechung der Datenschutzkommission hielt die Datenschutzbehörde zunächst fest, dass das Auskunftsrecht nur Übermittlungsvorgänge an neue Auftraggeber umfasst, nicht aber einzelne Datenverarbeitungen von Mitarbeitern des Auftraggebers. Die Namen von Mitarbeitern des Auftraggebers sind auch nicht „zur Person des Auskunftswerbers verarbeitete Daten" oder „verfügbare Informationen über ihre Herkunft", weshalb diese auch nicht von § 26 DSG 2000 umfasst sind. Darüber hinaus soll das Auskunftsrecht dem Auskunftswerber helfen, sein Recht auf Geheimhaltung und sein Recht auf Löschung zu sichern. Diese Rechte richten sich jedoch gegen den jeweiligen Auftraggeber und nicht gegen den jeweiligen Mitarbeiter. Die Datenschutzbehörde erkannte allerdings auch, dass die Benennung konkreter Mitarbeiter eines Auftraggebers dann vom Auskunftsrecht umfasst ist, wenn der Betroffene hinreichend konkrete Hinweise hat, dass er von einem Mitarbeiter des Auftraggebers in seinen datenschutzrechtlichen Rechten verletzt worden ist. Der Auskunftswerber muss dies aber bereits im Auskunftsbegehren klar zum Ausdruck bringen, damit der Auftraggeber abwägen kann, ob das Recht des Betroffenen auf Auskunft oder das Recht des Mitarbeiters auf Geheimhaltung höher zu bewerten ist. Da die Beschwerdeführerin im gegenständlichen Fall keinen konkreten Verdacht äußerte, wurde die Beschwerde abgewiesen.

Empfehlung der Datenschutzbehörde vom 21.03.2017, GZ DSB-D215.937/0003-DSB/2017

Der Empfehlung liegt folgender Sachverhalt zugrunde:

Im Zuge einer Wahl zu einer gesetzgebenden Körperschaft reicherte eine politische Partei die Daten aus der Wählerevidenz mit Telefonnummern der Y*** AG an und verschickte am Wahltag eine SMS mit dem Inhalt: „Heute ist Wahltag in Wien! Nütze deine Stimme und entscheide in welche Richtung Wien in Zukunft gehen soll. [Name eines Kandidaten der A***-Partei]".

Die Y*** AG teilte im Verfahren vor der Datenschutzbehörde mit, dass mit der Partei vertraglich vereinbart worden war, dass die Telefonnummern ausschließlich zum Zweck der Marktforschung eingesetzt werden dürfen; eine Erlaubnis für die Nutzung der Telefonnummern zu Marketingzwecken bestand demgegenüber nicht. Da aus Sicht der Datenschutzbehörde die SMS als Werbung zu qualifizieren war, sprach sie unter Verweis auf § 6 und 7 DSG 2000 die Empfehlung aus, dass die Aussendung von Wahlwerbe-SMS mit der durch die Y*** AG bereitgestellten Telefonnummern künftig zu unterbleiben hat.

Gesetzesbegutachtung – Stellungnahmen

Die DSB hat zu folgenden Gesetzesvorhaben eine Stellungnahme abgegeben:

- Bundesgesetz, mit dem das Insolvenz-Entgeltsicherungsgesetz geändert wird
- Sozialversicherungs-Zuordnungsgesetz
- Gesetzespaket zur MiFID II-Umsetzung
- Bundesgesetz, mit dem das Bilanzbuchhaltungsgesetz 2014 geändert wird
- Wirtschaftstreuhandberufsgesetz 2017
- Bundes-Sportförderungsgesetz 2017 u.a.
- Novelle der Kommunikations-Erhebungs-Verordnung
- Wirtschaftliche Eigentümer Registergesetz
- Änderung des Suchtmittelgesetzes
- Änderung der Suchtgiftverordnung
- Datenschutz-Anpassungsgesetz 2018

Weblink:

- Parlament aktiv: alle Stellungnahmen

DVR-Online Tipps und Tricks

Datenanwendung Videoüberwachung - folgende zusätzliche Informationen sind bei der Meldung gem. Datenschutzgesetz im DVR-Online anzugeben:

Ort:

Welche konkreten Räumlichkeiten/Objekte sollen videoüberwacht werden? Wo befinden sich diese (Anschrift) und welche Bereiche werden innerhalb der Objekte überwacht (z.B. Verkaufsraum, Foyer, Garage etc.). Befinden sich Arbeitsplätze in den überwachten Bereichen?

Verhältnismäßigkeit:

Sehen Sie die Verhältnismäßigkeit des Grundrechtseingriffs durch die Videoüberwachung aufgrund besonderer Ereignisse in der Vergangenheit als gegeben an (erfolgte Straftaten, Vorfallsstatistik, Schadenshöhe), oder gehen Sie allgemein von einer besonderen Gefährdung der zu überwachenden Örtlichkeiten aus (z.B. Bank, Museum, Juwelier)?

Weiters sollte angegeben werden, ob andere gelindere Mittel (etwa der vermehrte Einsatz von Sicherheitspersonal, die Installation einer Alarmanlage, eines Zugangskontrollsystems oder eine Livebild-Kamera) nicht ebenso den beabsichtigten Zweck erfüllen können. Existiert eine Vereinbarung mit den von der Videoüberwachung betroffenen Personen (z.B. mit den Mitarbeitern)?

Systemablauf:

Wird digital oder analog aufgezeichnet?

Erfolgt eine verschlüsselte Speicherung?

Sollen neben Bild- auch Tondaten erfasst werden?

Wird permanent aufgezeichnet oder erst bei Auslösen eines Bewegungsmelders?

Soll die Anlage rund um die Uhr in Betrieb sein, oder nur in der Nacht bzw. außerhalb der Büro-/Öffnungszeiten?

Sind die Kamerapositionen fix oder auch schwenkbar?

Wie lange werden Videodaten gespeichert bevor sie gelöscht bzw. automatisch überschrieben werden (Bei einer längeren Speicherdauer als 72 Stunden ist eine Begründung notwendig.)?

Erfolgt eine Auswertung/Sichtung tatsächlich nur im Anlassfall?

Wer ist berechtigt, das Bildmaterial auszuwerten?

Wie wird sichergestellt, dass keine unbefugten Dritten Zugriff auf die Videoüberwachungsanlage und das aufgezeichnete Bildmaterial nehmen können?

Bitte beantworten Sie die Fragen in einem Begleitschreiben im DVR-Online, das Sie als Beilage auf der Seite 7/8 der Meldung der Datenanwendung übertragen.

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