Republik Österreich
Datenschutz behörde

NEWSLETTER 1/2017

Datenschutzgrundverordnung Kapitel III („Rechte der betroffenen Person“) - Überblick

Das III. Kapitel der DSGVO enthält Bestimmungen, die jene Rechte festlegen, die vom Betroffenen (der „betroffenen Person“) gegenüber einem Verantwortlichen (dem „für die Verarbeitung Verantwortlichen“, bisher: „Auftraggeber“) oder Auftragsverarbeiter (bisher: „Dienstleister“) geltend gemacht und in einem rechtsstaatlichen Verfahren auch durchgesetzt werden können. Auf die Einhaltung dieser Rechte besteht daher ein Anspruch bzw. ein subjektives Recht.

Die DSGVO enthält im Kapitel III jedoch auch einige Bestimmungen, bei denen dem Wortlaut nach nicht ganz klar ist, ob es sich wirklich um ein durchsetzbares Recht der betroffenen Person oder „nur“ um eine Pflicht des Verantwortlichen oder Auftragsverarbeiters handelt (bei deren Missachtung aber zukünftig von Seiten der jeweiligen Datenschutzbehörde bereits förmliche Verwarnungen oder Geldbußen drohen).

Die betroffene Person hat gemäß Art. 12 bis 14 DSGVO ein Recht auf transparente Informationen und Kommunikation, Verständlichkeit und eine klare, einfache Sprache. Auf Kinder und deren Bedürfnisse ist besonders Rücksicht zu nehmen. Datenschutzrechtliche Informationen sind im Zeitpunkt der Erhebung zu geben, wenn die Daten direkt bei der betroffenen Person erhoben werden (Art. 13 DSGVO), sonst anlässlich der ersten Verwendung (Mitteilung an den Betroffenen, Offenlegung der Daten gegenüber Dritten) und längstens innerhalb eines Monats nach „Erlangung“ der Daten (Art. 14 Abs. 3 lit a DSGVO).

Das Auskunftsrecht der betroffenen Person über eigene Daten (Art. 15 DSGVO) unterscheidet sich nicht grundlegend von dem nach § 26 DSG 2000 und Art. 12 RL 95/46/EG. Bei Übermittlungen kann weiterhin über „Empfänger oder Kategorien von Empfängern“ Auskunft erteilt werden, weiterhin besteht nur ein Recht auf Auskunft über die „verfügbaren Informationen“ zur Datenherkunft. Wichtige Ausweitungen dieses Betroffenenrechts betreffen das Recht auf Auskunft über Empfänger in Drittländern oder bei internationalen Organisationen und das Recht auf Auskunft über die geplante Speicherdauer. Vorgesehen ist weiters ein Recht auf Auskunft über die Möglichkeiten der Berichtigung und Löschung der Daten sowie der Einschränkung und des Widerspruchs sowie über das Bestehen eines Beschwerderechts bei der Datenschutzbehörde (hier handelt es sich inhaltlich wohl eher um Belehrungspflichten). Ausgeweitet wurde auch das Recht auf Auskunft über „die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen“ einer automatisierten Entscheidungsfindung sowie des Profiling gemäß Art. 4 Z 4 DSGVO. Die Auskunft muss in Form einer unentgeltlichen „Kopie“ der verarbeiteten Daten zur Verfügung gestellt werden, die Frist für die Auskunftserteilung wird deutlich von acht Wochen auf einen Monat verkürzt, kann aber zukünftig begründet um weitere zwei Monate verlängert werden (Art. 12 Abs. 3 DSGVO). Eine Ablehnung der Auskunftserteilung oder eine sonstige schriftliche Reaktion auf das Auskunftsverlangen muss jedenfalls innerhalb eines Monates erfolgen.

Das Recht auf Berichtigung von Daten (Art. 16 DSGVO) umfasst nunmehr auch das Recht, die Vervollständigung von Daten oder, vergleichbar § 27 Abs. 3 DSG 2000, die Speicherung einer ergänzenden Erklärung zu verlangen.

Das Recht auf Löschung von Daten (Art. 17 DSGVO) setzt logisch voraus, dass der rechtmäßige Zweck ihrer Verarbeitung fehlt oder weggefallen ist. Letzteres ist insbesondere dann der Fall, wenn die betroffene Person eine Einwilligung widerrufen oder berechtigt Widerspruch (Art. 21 DSGVO) gegen die weitere Daten-

verarbeitung eingelegt hat, oder wenn die Zustimmung der Eltern („Träger der elterlichen Verantwortung“) zur Nutzung von Online-Diensten („Diensten der Informationsgesellschaft“) durch ein Kind fehlt. Das vielzitierte „Recht auf Vergessenwerden“ (Klammerausdruck zur Überschrift vor Art. 17 DSGVO) findet insoweit im Text der Rechtsvorschrift Ausdruck, als gemäß Art. 17 Abs. 2 DSGVO bei einer Veröffentlichung von Daten der Verantwortliche auf Verlangen der betroffenen Person nicht nur selbst Löschen sondern auch „unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art,“ ergreifen muss, um weitere Verantwortliche (insbesondere wohl Suchmaschinenbetreiber) zu informieren, dass ein Betroffener die Löschung aller Links und „Kopien oder Replikationen“ verlangt hat. Ausnahmen vom Löschungsrecht bestehen zum Schutz des Rechts auf freie Meinungsäußerung und Information, bei Bestehen einer rechtlichen Verpflichtung zur Verarbeitung, bei Verarbeitung zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, und bei Verarbeitung für Zwecke des öffentlichen Gesundheitswesens oder für Archiv-, Forschungs- oder Statistikzwecke.

Ein völlig neues, von der DSGVO geschaffenes Recht ist das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO). Wird es ausgeübt, dann dürfen die jeweiligen Daten nur mehr gespeichert und, außer die betroffene Person gibt ihre Einwilligung, nur zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses verarbeitet werden. Eine solche Einschränkung der Verarbeitung ist möglich, wenn a) die Richtigkeit der Daten bestritten wird für die Dauer der Überprüfung, b) an Stelle der Ausübung des Löschungsrechts (bei Vorliegen der Voraussetzungen einer Löschung), c) wenn die betroffene Person ihre Daten selbst zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt (hier handelt es sich faktisch um eine Löschungssperre) und d) im Fall eines Widerspruchs für die Dauer des Verfahrens zur Prüfung, ob dieser zu Recht erhoben worden ist.

Gemäß Art. 19 DSGVO muss jeder Verantwortliche allen Empfängern, denen Daten offengelegt worden sind, von jeder Berichtigung, Löschung oder Einschränkung der Verarbeitung Mitteilung machen, es sei denn, dies wäre unmöglich oder mit unverhältnismäßigem Aufwand verbunden. Die betroffene Person hat ein Recht, auf Verlangen über diese Empfänger informiert zu werden.

Ebenfalls neu ist das in Art. 20 DSGVO festgelegte Recht der betroffenen Person auf Datenübertragbarkeit. Es ist auf die freiwillige Verarbeitung von Daten, die die betroffene Person „bereitgestellt hat“, mittels „automatisierter Verfahren“ beschränkt. Die betroffene Person kann verlangen, dass ihre Daten „in einem strukturierten, gängigen und maschinenlesbaren Format“ möglichst direkt nach ihrer Anweisung von einem Verantwortlichen zum nächsten übermittelt oder ihr übergeben werden.

Betreffend das Widerspruchsrecht sieht Art. 21 DSGVO eine differenzierte Regelung nach dem Verarbeitungszweck vor. Ein berechtigter Widerspruch beseitigt in Fällen, in denen die betroffene Person nicht ihre Einwilligung gegeben hat, die Grundlage für die Rechtmäßigkeit der Datenverarbeitung. Bei Datenverarbeitung für den Zweck der Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt ist das Widerspruchsrecht nur begrenzt möglich. Die betroffene Person muss jedenfalls das Vorliegen einer „besonderen Situation“ glaubhaft machen. Gelingt ihr dies, so tritt eine Beweislastumkehr ein. In diesem Fall muss der Verantwortliche entweder zwingende schutzwürdige Gründe nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen (etwa eine gesetzliche Grundlage), oder nachweisen, dass die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Erfolgt die Datenverarbeitung allgemein lediglich auf Grundlage einer Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO), so muss der Verantwortliche das Überwiegen der Gründe nachweisen, die für die weitere Verarbeitung der Daten sprechen.

Besonders geregelt (Art. 21 Abs. 2 und 3 DSGVO) ist die Datenverarbeitung für den Zweck der Direktwerbung und damit verbundenes Profiling. Hier ist ein Widerspruch jederzeit und auch ohne Begründung möglich. Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft (Online-Diensten) muss ein Widerspruch auch „mittels automatisierter Verfahren“ möglich sein.

Einen weiteren Spezialfall bildet der Widerspruch gegen eine Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken (Art. 21 Abs. 6 DSGVO). In diesem Fall ist das Widerspruchsrecht nur begrenzt ausübbar (Interessenabwägung).

In allen Fällen eines Widerspruchs ist die betroffene Person innerhalb der allgemeinen Fristen (Art. 12 Abs. 3 DSGVO) über die getroffenen Maßnahmen (Anerkennung oder Ablehnung) zu informieren.

Art. 22 DSGVO enthält die Regelung betreffend automatisierte Einzelentscheidungen und Profiling (Art. 4 Z 4 DSGVO). Zur Bewertung einer Person durch Profiling wird in Zukunft wohl auch Datenverarbeitung für Marketing- und Werbezwecke gehören (z.B. Marketingklassifikationen). Art. 22 Abs. 1 DSGVO erklärt Entscheidungen, die der betroffenen Person gegenüber rechtliche Wirkungen entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen, und die ausschließlich auf einer automatisierten Verarbeitung, Profiling eingeschlossen, beruhen, für

grundsätzlich unzulässig. Es gibt allerdings drei Hauptausnahmen: a) die automatisierte Einzelfallentscheidung ist für den Abschluss oder die Erfüllung eines Vertrags erforderlich, b) die automatisierte Einzelfallentscheidung, Profiling ausdrücklich eingeschlossen, ist aufgrund von Rechtsvorschriften zulässig oder c) eine ausdrückliche Einwilligung der betroffenen Person liegt vor. In den Fällen a) und c) kommt der betroffenen Person das Recht zu, das Eingreifen einer Person (also eines Menschen an Stelle einer Maschine) zu verlangen, ihren Standpunkt darzulegen und die auf automatisierter Grundlage getroffene Entscheidung anzufechten. Automatisierte Einzelentscheidungen und Profiling ausschließlich auf Grundlage besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO, sensible Daten) sind nur unter besonders strengen Voraussetzungen zulässig.

Jeder Verstoß gegen die Betroffenenrechte kann mit sehr hohen Geldbußen (bis zu 20 Millionen Euro oder 4 % des weltweit erzielten Jahresumsatzes bei Unternehmen, Art. 83 Abs. 5 lit b DSGVO) geahndet werden.

Im Fokus

Whistleblowing-Hotlines

Mag. Georg Lechner

Whistleblowing-Hotlines, auch bekannt als Hinweisgebersysteme oder Compliance-Hotlines sind innerhalb von Konzernen seit Jahren Maßnahmen zur Korruptionsbekämpfung. Das grundsätzliche Konzept ist einfach: Die Konzernleitung richtet einen speziellen Kommunikationsweg für Mitarbeiter ein, mit dem Hinweise auf interne Missbräuche (Korruption, Verstöße gegen Buchführungsvorschriften und Steuerhinterziehung, illegale Praktiken im Zusammenhang mit Banken wie Geldwäsche und Bankenbetrug sowie Fälschung von Finanzunterlagen und Insiderhandel) direkt der Konzernspitze übermittelt werden können. Diese Systeme umgehen bewusst die „normale“ Hierarchie und sollen insbesondere dazu dienen, Korruption in der Führungsebene des eigenen Unternehmens oder an anderer höherer Stelle aufzudecken.

Dabei kommt regelmäßig ein externer Dienstleister zum Einsatz, der die Technik für die Hotline zur Verfügung stellt (eine Website oder eine Telefonnummer mit Callcenter).

Zur rechtlichen Darstellung im Detail bieten wir Informationen auf unserer Website: https://www.dsb.gv.at/hinweisgebersystem.

Hinweisgebersysteme waren noch vor einigen Jahren „exotische“ Datenanwendungen in US-Konzernen (ein amerikanisches Gesetz, der Sarbanes-Oxley-Act aus dem Jahr 2002, ist eine der Rechtsgrundlagen). Mittlerweile sind sie auch in europäischen Unternehmen üblich.

Die datenschutzrechtlichen Voraussetzungen für den Betrieb einer Whistleblowing-Hotline sind eine Meldung beim Datenverarbeitungsregister und – falls erforderlich – eine Genehmigung für den internationalen Datenverkehr. Viele der Übermittlungen (an Konzernmütter) und Überlassungen (an die Dienstleister) gehen und gingen in die USA. In diesem Bereich sind Regelungen zum genehmigungsfreien Datenexport von großer Bedeutung.

Nach dem Fall der „Safe Harbor“-Regelung am 6. Oktober 2015, die den genehmigungsfreien Datentransfer in die USA bis dahin für jene Unternehmen gestattete, die sich dem Reglement unterworfen hatten, kam es zu einem Anstieg von Anträgen auf internationalen Datenverkehr (§ 13 DSG 2000) bei der Datenschutzbehörde. Mittlerweile existiert das EU-US Privacy Shield, und viele der Empfänger in den USA sind wieder von der Genehmigungspflicht ausgenommen, da sie sich der Selbstzertifizierung unterworfen haben. Die Dienstleister für Whistleblowing-Hotlines bemühen sich, rasch das Privileg des genehmigungsfreien Datenverkehrs in Anspruch nehmen zu können. Leider wird in den Konzernen nicht immer kommuniziert, dass ein Empfänger in den USA die neue Regelung des EU-US Privacy Shields in Anspruch nehmen kann. Ein Blick auf die Liste der Mitglieder des EU-US Privacy Shields ist daher sinnvoll, bevor ein Antrag auf Genehmigung gemäß § 13 DSG 2000 gestellt wird.

Der Meldung beim Datenverarbeitungsregister muss der Ethikkodex des Konzerns angeschlossen werden, mit dem das System eingeführt wird. Die meisten Konzerne erlassen anlässlich der Einführung ihrer Whistleblowing-Hotline einen solchen Kodex, der regelt, welche Verstöße gemeldet werden sollen und müssen. Manche verfügen bereits über ein derartiges Regelwerk, das nur um neue Regeln ergänzt wird. Die Meldung und das sonstige Vorbringen sollten dem Inhalt des Kodex entsprechen, insbesondere beim Katalog der Verstöße. Es ist auch wichtig, darauf zu achten, wie die Pflicht zur Meldung gestaltet ist (also z.B. welcher Wissensstand bereits als Mitwisserschaft geahndet werden soll). Dabei können sich Grauzonen ergeben, die im Verfahren möglicherweise als Mängel angesehen und verbessert werden müssen.

Darüber hinaus verlangt die Datenschutzbehörde eine Betriebsvereinbarung (oder die Zustimmung gemäß § 10 AVRAG).

Ausgewählte Entscheidungen der DSB

Empfehlung an WK Tirol

Im Zuge eines amtswegig geführten Verfahrens nach § 30 DSG 2000 ist hervorgekommen, dass die Wirtschaftskammer Tirol – zum Zweck der Erwirkung von Sperren des Arbeitslosengeldes – ihre Mitglieder mittels eines Newsletters zur Namhaftmachung von arbeitsunwilligen Arbeitslosen auffordert.

Eine gesetzliche Berechtigung zur Überprüfung des Vorliegens der Voraussetzungen des Anspruches auf Arbeitslosengeld und damit verbunden zur Ermittlung von personenbezogenen Daten arbeitsunwilliger Arbeitsloser kommt jedoch ausschließlich der regionalen Geschäftsstelle des Arbeitsmarktservice, und nicht der Wirtschaftskammer Tirol zu.

Die Datenschutzbehörde hat daher mit Empfehlung vom 16. November 2016, GZ.: DSB-D213.480/0004-DSB/2016, ausgesprochen, dass die zum Zweck der Erwirkung einer Sperre des Arbeitslosengeldes erfolgte Ermittlung von personenbezogenen Daten arbeitsunwilliger Arbeitsloser (Name) zukünftig unterbleiben möge.

Ausgewählte Entscheidungen der Gerichte

„Dash-Cams" – Revision an VwGH

Wie im Newsletter 3/2015 bereits berichtet, wurde der Bescheid der DSB im Bereich Dash-Cams vom Bundesverwaltungsgericht (BVwG) inhaltlich bestätigt. Der Auftraggeber hat gegen dieses Urteil die ordentliche Revision an den Verwaltungsgerichtshof (VwGH) erhoben.

Mittels Erkenntnis vom 12. September 2016 (Ro 2015/04/0011-7) wurde die Revision als unbegründet abgewiesen. Der VwGH ändert dabei jedoch die zu demselben Ergebnis führende Begründung der Vorinstanzen (DSB und BVwG) dahingehend, dass das gegenständliche System nicht als gelindestes Mittel im Sinne des § 7 Abs. 3 DSG 2000 anzusehen ist (Rz 33). Es liegt somit erstmals höchstgerichtliche Rechtsprechung zur Unzulässigkeit von Dash-Cams vor.

Urteil in der Rs C-582/14 (Breyer)

Das Verfahren wurde inklusive Schlussanträge des Generalanwalts im Newsletter 3/2016 der Datenschutzbehörde behandelt. Mit seinem Urteil vom 19. Oktober 2016 folgt der EuGH vollinhaltlich der Empfehlung des Generalanwalts.

Die wesentliche Aussage: Gemäß Art. 2 Buchst. a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist eine dynamische IP-Adresse, über die ein Nutzer die Internetseite eines Telemedienanbieters aufgerufen hat, für Letzteren ein „personenbezogenes Datum", soweit ein Internetzugangsanbieter über weitere zusätzliche Daten verfügt, die in Verbindung mit der dynamischen IP-Adresse die Identifizierung des Nutzers ermöglichen.

Gesetzesbegutachtung – Stellungnahmen

Die DSB hat zu folgenden Gesetzesvorhaben eine Stellungnahme abgegeben:

- Gewerbeordnung, Änderung
- Deregulierungsgesetz 2017 - Teil BMF/BMJ/BMFJ
- Innovationsstiftungsgesetz – ISG; Einkommensteuergesetz, Körperschaftsteuergesetz, Änderung
- Dereglierungsgesetz 2017 – Bundeskanzleramt
- Referenzwerte-Vollzugsgesetz

Weblink:

- Parlament aktiv: alle Stellungnahmen

Hinweise zur DSGVO:

Die vom Plenum der Art. 29-Gruppe verabschiedeten Richtlinien (Guidelines) zu den Themen

- Datenübertragbarkeit
- Datenschutzbeauftragter
- Federführende Aufsichtsbehörde

sind unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 in Englisch abrufbar.

Die Mitarbeiterinnen und Mitarbeiter der DSB wünschen Ihnen ein gesundes, friedvolles und erfolgreiches Jahr 2017!

Stellvertretend für Alle:

Dr. Andrea Jelinek und Dr. Matthias Schmidl

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