Republik Österreich
Datenschutz behörde

NEWSLETTER 3/2016

Datenschutzgrundverordnung: Kapitel I und dazugehörige Erwägungsgründe

Dieser Artikel baut auf der letzten Ausgabe des Newsletters 2/2016 auf. In diesem Beitrag wird auf Kapitel I der Verordnung eingegangen:

Die Datenschutz-Grundverordnung heißt in ihrem vollen Wortlaut: „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG".

Dieses Kapitel hat 4 Artikel; die wesentlichsten Bestimmungen sind:

Einschränkend im Hinblick auf das DSG 2000 (nicht jedoch in Bezug auf die geltende Richtlinie), wonach sich jedermann - also auch juristische Personen - auf das Grundrecht auf Datenschutz berufen kann, sieht Art. 1 Absatz 1 der Datenschutz-Grundverordnung vor, dass nur natürliche Personen Schutz bei der Verarbeitung personenbezogener Daten genießen. Somit wird der Kreis der Betroffenen eingeschränkt.

Gemäß Art. 1 Abs. 3 darf der freie Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden. Erläuternd führt Erwägungsgrund 13 den Hintergrund dazu aus: Das reibungslose Funktionieren des Binnenmarktes mit einem gleichmäßigen Datenschutzniveau für natürliche Personen. Dementsprechend richtet sich die Datenschutz-Grundverordnung auch an Klein- und Kleinstunternehmen und soll für Rechtssicherheit und Transparenz sorgen.

Die Datenschutz-Grundverordnung ist eine sogenannte hinkende Verordnung. Der 8. Erwägungsgrund sieht vor, dass die Mitgliedsstaaten Teile dieser Verordnung in ihr nationales Recht aufnehmen können, um die Kohärenz zu wahren und um die Rechtsvorschriften verständlich zu machen. Normalerweise dürfen Verordnungen der EU nicht durch nationales Recht umgesetzt werden, da sie unmittelbar anwendbar sind.

Die Datenschutz-Grundverordnung gilt gemäß Artikel 2 für die (ganz oder teilweise) automatisierte Verarbeitung personenbezogener Daten. Ebenso gilt sie für nichtautomatisierte Verarbeitung in Form eines Dateisystems. Ausnahmen hievon sind z.B. die Datenverarbeitung für ausschließlich persönliche oder familiäre Tätigkeiten, die Aufdeckung oder Verfolgung von Straftaten, die Strafvollstreckung sowie die Gefahrenabwehr für die öffentliche Sicherheit.

Nicht minder wichtig ist auch der räumliche Anwendungsbereich der Datenschutz-Grundverordnung, wie auch einige Entscheidungen des EuGH zu diesem Thema zeigen (z.B. Rechtssache C 230/14 Weltimmo; Rs. C-131/12 Google Spain-Google). Hier kommt dem Begriff der Niederlassung eine ganz zentrale Bedeutung zu. Artikel 3 der Datenschutz-Grundverordnung knüpft an eine Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters an. Dabei spielt es keine Rolle, ob die Verarbeitung in der Union stattfindet. In diesem Zusammenhang erläutert der 22. Erwägungsgrund, dass eine Niederlassung die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung ist.

Ein Sonderfall des räumlichen Anwendungsbereiches wird in Satz 2 sowie im 23. Erwägungsgrund umschrieben: Hier wird folgende Konstellation beschrieben: Eine betroffene natürliche Person befindet sich in der Union, weder Verantwortlicher noch Auftragsverarbeiter befinden sich in der Union. Dennoch ist hier die Datenschutz-Grundverordnung anwendbar, wenn es um ein

offensichtlich beabsichtigtes Anbieten von entgeltlichen oder unentgeltlichen Waren oder Dienstleistungen geht. Der zweite Sonderfall in diesem Kontext betrifft die Verhaltensbeobachtung von Betroffenen. Dies liegt z.B. vor, wenn Internetaktivitäten nachvollzogen werden oder Profile der Nutzer erstellt werden (24. Erwägungsgrund).

Da die geltende Datenschutzrichtlinie 95/46/EG, umgesetzt durch das DSG 2000, die Basis für die Datenschutz-Grundverordnung ist, werden in der Folge jene Begriffsbestimmungen (Artikel 4) genannt, die von besonderem Interesse sind, vor allem, weil diese bis dato nicht normiert waren.

Beim „Profiling" geht es um personenbezogene Daten, die verwendet werden, um bestimmte persönliche Aspekte wie Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel zu analysieren oder vorherzusagen.

„Pseudonymisierung" ist die Verarbeitung personenbezogener Daten in der Weise, dass ohne Hinzuziehung zusätzlicher Informationen Daten nicht mehr spezifischen Personen zugeordnet werden können. Diese Zusatzinformationen bedürfen gesonderter Aufbewahrung und unterliegen technischen und organisatorischen Maßnahmen. Eine etwaige Identifizierung wäre mit entsprechenden Kosten und Zeitaufwand verbunden.

Die Begriffe des „Auftraggebers" und des „Dienstleisters" werden durch die Bezeichnungen „Verantwortlicher" und „Auftragsverarbeiter" ersetzt.

Eine Neuerung stellt die Definition genetischer (genetische Eigenschaften mit eindeutiger Information über die Physiologie oder Gesundheit, ebenso biologische Proben) und biometrischer Daten (z.B. Gesichtsbilder, daktyloskopische Daten- Fingerabdruck) dar.

Im Fokus

Empfehlungen an Krankenanstalten

Dr. Matthias Schmidl

Die DSB führt seit 2014 jährliche Schwerpunktverfahren durch, in welchen Auftraggeber eines bestimmten Sektors einer vertieften Prüfung unterzogen werden. 2014 wurde der Sektor der Kreditauskunfteien näher untersucht, im Rahmen des Schwerpunktverfahrens 2015 wurden fünf Krankenanstaltenträger überprüft. Die Überprüfungen beginnen in der Regel mit der Versendung eines Fragebogens, in welchem der Auftraggeber ersucht wird, zu allgemeinen und sektorspezifischen datenschutzrechtlichen Fragen Stellung zu nehmen. Auch die DVR-Meldungen des Auftraggebers werden dabei überprüft. Die DSB führt bei diesen Verfahren auch Einschauen durch.

Ziel der Schwerpunktverfahren ist es, auf allfällige Missstände hinzuweisen und die Auftraggeber aufzufordern, den rechtmäßigen Zustand herzustellen.

Der Fokus der Prüfung 2015 lag auf Patientenverwaltungssystemen und wie die darin gespeicherten sensiblen Daten vor unberechtigten Zugriffen geschützt werden.

Die Überprüfung der fünf Krankenanstaltenträger wurde im Mai 2016 abgeschlossen und es wurden fünf Empfehlungen ausgesprochen, die im RIS abrufbar sind. Dabei ging die DSB aber auch auf jene Punkte ein, die als besonders positiv hervorzuheben waren und als „best practice" angesehen werden können.

Die Empfehlungen behandeln vor allem den Umstand, dass bei den meisten Krankenanstaltenträgern die Daten ehemaliger Bediensteter zeitlich unbefristet in Datenverarbeitungssystemen gespeichert bleiben. Es wird zwar der Zugang dieser Mitarbeiter deaktiviert, nicht jedoch deren Profil.

In einer Empfehlung wird einem Krankenanstaltenträger empfohlen, Routineprüfungen hinsichtlich der Zugriffe auf Patientendaten einzuführen (Logfile-Auswertungen).

Ein anderer Krankenanstaltenträger führte eine verdeckte Videoüberwachung zur Hintanhaltung von Medikamentenschwund durch, was von der DSB als rechtswidrig beurteilt wurde. Ebenso als rechtwidrig wurde die Überwachung eines Behandlungsraumes durch einen anderen Krankenanstaltenträger bewertet.

In Summe hat die Schwerpunktprüfung jedoch ergeben, dass alle Krankenanstaltenträger sich der Notwendigkeit der Einhaltung datenschutzrechtlicher Vorschriften bewusst sind und auch effektive Methoden zum Schutz von Patientendaten entwickelt haben.

Ausgewählte Entscheidungen der DSB

Auskunftsersuchen an Dienstleister

Im Bescheid vom 12.05.2016, GZ DSB-D122.515/0004-DSB/2016, war die DSB zum erst zweiten Mal mit einer Vorgangsweise nach § 26 Abs. 10 DSG 2000 befasst. In diesem Fall wurde das Auskunftsbegehren offenkundig an den Dienstleister gerichtet. Dieser setzte den Auskunftswerber zwar darüber in Kenntnis lediglich Dienstleister zu sein und gab auch die Kontaktdaten des Auftraggebers bekannt. Eine Weiterleitung des Auskunftsbegehrens an den Auftraggeber – wie von § 26 Abs. 10 DSG 2000 verlangt – erfolgte jedoch nicht. Die DSB entschied daher, dass eine Verletzung im Recht auf Auskunft vorlag.

Beauskunftung Standortdaten durch Telekommunikationsanbieter

Bescheid der Datenschutzbehörde vom 15. April 2016 zu Zl. DSB-D122.418/0002-DSB/2016

Die Datenschutzbehörde hatte in diesem Fall zu prüfen, ob die Verweigerung der Auskunft von Standortda-

ten durch den Anbieter mobiler Kommunikationsdienste gegenüber dem Teilnehmer (also dem Vertragsinhaber) zu Recht erfolgte oder Auskunft zu erteilen gewesen wäre.

Die Beschwerdeführerin ist Vertragspartnerin für zwei mobile Rufnummern bei einem österreichischen Anbieter mobiler Kommunikationsdienste und richtete ein Auskunftsverlangen betreffend der Standortdaten beider Rufnummern – eingeschränkt auf einen zweiwöchigen Zeitraum im Vormonat - an den Mobilfunkanbieter.

Der Mobilfunkanbieter verweigerte die Auskunft mit der Begründung, dass Standortdaten ausschließlich im Zuge polizeilicher Ermittlungen oder auf richterliche Anordnungen bzw. an den Betreiber von Notrufdiensten, wenn ein Notfall dadurch abgewehrt werden könne, übermittelt werden dürften.

Die Datenschutzbehörde wies die Beschwerde als unbegründet ab und begründete ihre Entscheidung folgendermaßen:

Die Verfassungsbestimmung des § 1 Abs. 3 Z 1 DSG 2000 beschränkt das Auskunftsrecht ihrem Wortlaut nach darauf, dass jedermann ein Auskunftsrecht hinsichtlich der ihn betreffenden personenbezogenen Daten hat.

§ 26 Abs. 1 DSG 2000 präzisiert das verfassungsgesetzlich gewährleistete Recht auf Auskunft auf die zu dieser Person oder Personengemeinschaft verarbeiteten Daten, vorausgesetzt, dass dies schriftlich (oder mit Zustimmung des Auftraggebers auch mündlich) verlangt und die Identität in geeigneter Form nachgewiesen wird.

Beide Bestimmungen zielen nach Auffassung der Datenschutzbehörde sowohl ihrem Wortlaut nach, als auch in ihrer intentionalen Zweckbestimmung darauf ab, dass das (verfassungsgesetzlich gewährleistete) Auskunftsrecht ausschließlich auf personenbezogene Daten des Auskunftswerbers als Betroffenen beschränkt ist.

Ein Telekommunikationsdiensteanbieter kann nicht feststellen, ob ein Teilnehmer (Vertragsinhaber) der tatsächliche Nutzer der einem Endgerät zugeordneten Rufnummer und der damit angefallenen Standortdaten war.

Der Teilnehmer (Vertragsinhaber) ist nämlich tatsächlich häufig eben gerade nicht der tatsächliche Nutzer, dessen Aufenthaltsort (und Wechsel von Aufenthaltsorten) in den betriebstechnischen Standortdaten abgebildet ist.

Denkbar ist, dass Teilnehmer (Vertragsinhaber) und Nutzer des mobilen Endgerätes auseinanderfallen, etwa wenn der Vertragsinhaber ein Elternteil und der Nutzer das Kind ohne eigenes Erwerbseinkommen ist.

Eine Beauskunftung des Teilnehmers hinsichtlich der Standortdaten jener Rufnummern, für die er Vertragspartner ist – so wie ihn die Beschwerdeführerin betreffend der beiden Rufnummern geltend macht –, hätte zur Folge, dass der Vertragsinhaber Auskunft zu (Bewegungs) Daten erhält, die unter Umständen nicht seine Person betreffen und ihm die Feststellung und Kontrolle ermöglichen, wo sich das Endgerät (und damit in der Regel ein Nutzer) zu einem bestimmten Zeitpunkt befand.

Die Datenschutzbehörde gelangte aufgrund dieser Erwägungen zum Schluss, dass der mobile Kommunikationsdiensteanbieter das Auskunftsverlangen zu Recht verweigert hatte, da letztlich eine Feststellung, ob die auskunftsgegenständlichen Standortdaten zweier Rufnummern (ausschließlich) den Vertragsinhaber oder auch andere Nutzer betreffen, nicht feststellbar sind.

Die Entscheidung ist nicht rechtskräftig.

Überlassungen an Cloud-Dienstleister

Die Datenschutzbehörde stellt Genehmigungen für die Weitergabe von personenbezogenen Daten in das Ausland aus (§ 13 DSG 2000). In letzter Zeit sind Überlassungen an Cloud-Dienstleister im Ausland häufiger geworden. Diese Unternehmen bieten ihren Kunden Speicherkapazität für deren Daten auf Cloud-Servern zur Verfügung, die oft von Sub-Dienstleistern betrieben werden. Es handelt sich dabei um eine Überlassung an Dienstleister (§ 4 Z 5 und 11 DSG 2000).

Die Genehmigung wird derzeit mit der Auflage erteilt, dass das in den Standardvertragsklauseln zugesicherte Sicherheitsniveau der abgeschlossenen Standardvertragsklauseln und anderer einschlägiger Verträge eingehalten werden muss. Falls erkennbar ist, dass der Dienstleister oder seine Sub-Dienstleister allgemein nicht in der Lage sind, die Sicherheit ihrer Cloud-Technologie zu gewährleisten, muss das Dienstleistungsverhältnis gelöst werden. Die Auflage greift auch dann, wenn die dem Dienstleister anvertrauten Daten nicht unmittelbar gefährdet sind, aber die eingesetzte Cloud Technologie sich an anderer Stelle als grundsätzlich unsicher erweist. Als Nachweis der Unzuverlässigkeit gelten insb. Urteile zuständiger Gerichte, eine negative Bewertung durch die Artikel 29-Datenschutzgruppe oder andere namhafte Datenschutz- und Datensicherheitsorganisationen oder Entzug oder Verweigerung von Zertifizierungen wie ISO/IEC 27018:2014 (Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors).

Ausgewählte Entscheidungen der Gerichte

Schlussantrag d. Generalanwalts in der Rechtssache C-582/14 (Breyer)

(Urteil ausständig)

Zusammenfassung/Sachverhalt:

Im Ausgangsverfahren wird darüber gestritten, ob dynamische IP-Adressen personenbezogene Daten im Sinne von Art. 2 lit.a der Richtlinie 95/46/EG sind. Zur Beantwortung dieser Frage muss zunächst geklärt werden,

welche Bedeutung dabei dem Umstand zukommt, dass die für die Identifizierung des Nutzers erforderlichen zusätzlichen Daten sich nicht im Besitz des Inhabers der Internetseite, sondern im Besitz eines Dritten (konkret des Internetzugangsanbieters) befinden.

Auffassung des Generalanwalts laut Schlussantrag:

In Verbindung mit anderen Daten ermöglicht die dynamische IP-Adresse eine „indirekte" Identifizierung des Nutzers. Nach Auffassung des Generalanwalts ist bei systematischer Auslegung davon auszugehen, dass nur ein bestimmter Dritter (nicht schlechthin irgendwer) gemeint sein kann. Im gegenständlichen Fall ist der Dritte jedoch kein hypothetischer, unbekannter und unerreichbarer Dritter, sondern einer der Hauptakteure im Geflecht des Internets, von dem man mit Sicherheit weiß, dass er im Besitz der Daten ist, die der Diensteanbieter braucht, um einen Nutzer zu identifizieren. Der Internetzugangsanbieter ist typischerweise jener Dritte an den sich der Diensteanbieter im Anlassfall „am vernünftigsten" wenden würde.

Der Generalanwalt schlägt letztlich vor auf die Vorlagefragen wie folgt zu antworten:

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:

- Lohn- und Sozialdumping-Bekämpfungsgesetz; Arbeitsvertragsrechts-Anpassungsgesetz, Arbeitskräfteüberlassungsgesetz u.a., Änderung
- Bauarbeiter-Urlaubs- und Abfertigungsgesetz, Bauarbeiter-Schlechtwetterentschädigungsgesetz u.a., Änderung
- Schulrechtspaket 2016
- SFT-Vollzugsgesetz; Finanzmarktaufsichtsbehördengesetz, Investmentfondsgesetz 2011 u.a., Änderung
- Börsegesetz 1989, Änderung
- Präventions-Novelle 2016
- Gedenkstättengesetz
- Strafprozessordnung 1975, Staatsanwaltschaftsgesetz, Änderung

Weblink:

- Parlament aktiv: alle Stellungnahmen

DVR-Online Tipps und Tricks

Auftraggeber-Erstmeldung im DVR-Online:

Bevor Sie eine Meldung durchführen, überprüfen Sie unter Verwendung der „DVR-Recherche", ob bereits eine Eintragung im DVR besteht. Eine Erstmeldung im DVR-Online besteht aus den „Angaben zum Auftraggeber"(Seiten 1-4) und der Meldung mindestens einer Datenanwendung, die mit dem Button „Angaben zur Datenanwendung" (weitere 8 Seiten) angeschlossen wird. Erst nach dem Befüllen aller Pflichtfelder beider Online-Formulare und dem Betätigen des Buttons „Versenden" ist die Meldung im Datenverarbeitungsregister eingelangt. Diese Meldung wird entweder automatisch registriert oder einem Sachbearbeiter zur Bearbeitung weitergeleitet. Beim Betätigen des Buttons „Drucken" wird ein Dokument mit Signatur zum Ausdrucken erzeugt, dieses Dokument gilt jedoch nicht als Meldung.

Weblinks:

- DVR: Anleitung
- USP: Antworten auf häufige Fragen – Wie kann ich mein Unternehmen am USP registrieren?
- Handy-Signatur
- Finanz-Online

Teens & Kids

„S t r e a m i n g"- Datenfluss in der Grauzone

Darunter ist das Abspielen von Videos, Musik oder Filmen aus dem Internet zu verstehen, ohne dass die jeweilige Datei vollständig auf den Computer heruntergeladen wird.

Nähere Informationen und Tipps dazu auf http://www.rataufdraht.at/themenubersicht/handy-internet/streaming-18802

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: http://www.dsb.gv.at/impressum.