

Datenschutzgrundverordnung Kapitel II („Grundsätze“) - Überblick

Das II. Kapitel der DSGVO enthält Bestimmungen zu den „Grundsätzen für die Verarbeitung personenbezogener Daten“ zur „Rechtmäßigkeit der Verarbeitung“, ausführliche Regelungen wie eine „Einwilligung“ gestaltet sein sollte, sowie Regelungen zur Verarbeitung „besonderer Kategorien von Daten“.

Die Grundsätze der „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“, der grundsätzlichen „Zweckbindung“, der „Datenminimierung“, der „Richtigkeit“, der „Speicherbegrenzung“ sind – wenn auch in der DSGVO etwas modifiziert – ähnlich wie in der Richtlinie 95/46/EG geregelt (vgl. Art 6 RL 95/46/EG, „Grundsätze in Bezug auf die Qualität der Daten“).

Ebenso weist die „Rechtmäßigkeit der Verarbeitung“ in Artikel 6 DSGVO ähnliche Regelungen auf, wie sie aus Art 7 RL 95/46/EG („Zulässigkeit der Verarbeitung von Daten“) bekannt sind.

Neu ist, dass eine Verarbeitung personenbezogener Daten nun auch für einen anderen Zweck möglich ist, als für jenen, für den sie ursprünglich erhoben wurde und zwar dann, wenn ursprünglicher und neuer Zweck miteinander vereinbar sind. Art. 6 Abs. 4 DSGVO legt dabei die Kriterien fest, nach denen eine Prüfung der Vereinbarkeit durch den Verantwortlichen erfolgen soll:

Hierzu zählen u. a. die Verbindung zwischen den Zwecken (ursprünglicher und geänderter Zweck), der Gesamtkontext, in dem die Daten erhoben wurden, die Art der personenbezogenen Daten, mögliche Konsequenzen der zweckändernden Verarbeitung für den Betroffenen oder das Vorhandensein von angemessenen Sicherheitsmaßnahmen wie eine Pseudonymisierung oder Verschlüsselung. Beachtenswert erscheint, dass die DSGVO im Zusammenhang mit dem Prüfkriterium „Gesamtkontext“ aber auch bei einer Verarbeitung zur Wahr-

nehmung des berechtigten Interesses des Verantwortlichen in den Erwägungsgründen 47 und 50 von den „vernünftigen Erwartungen der betroffenen Person“ spricht. Die Erwartbarkeit bzw. Absehbarkeit für die betroffene Person spielt also sowohl bei der Verarbeitung zur Wahrnehmung eines berechtigten Interesses des Verantwortlichen, als auch bei der Weiterverarbeitung zu einem anderen Zweck eine Rolle.

Einen besonderen Fokus legt die DSGVO in Art. 7 und Art. 8 auf die Einwilligung des Betroffenen, wobei Artikel 7 die Bedingungen für eine Einwilligung allgemein regelt, und Artikel 8 spezielle Bestimmungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft enthält.

Eine Einwilligung gemäß Artikel 7 muss klar unterscheidbar von anderen Erklärungen (Zustimmungen, Vertragsklauseln), in verständlich und leicht zugänglicher Form, in einfacher und klarer Sprache und freiwillig erteilt werden. Zahlreiche Erwägungsgründe der DSGVO nehmen auf das Thema „Einwilligung“ Bezug, wobei im Erwägungsgrund 42 ausdrücklich die RL 93/13/EWG (RL über missbräuchliche Klauseln in Verbraucherverträgen) erwähnt wird. Wie mit „Einwilligungen“ vor Inkrafttreten der DSGVO im Lichte von Erwägungsgrund 171 zu verfahren sein wird, wird von der Rechtsprechung noch zu klären sein.

Gemäß Art. 8 DSGVO kann eine Einwilligung in Bezug auf Dienste der Informationsgesellschaft („information society services“) durch einen Minderjährigen selbst erteilt werden, soweit er das 16. Lebensjahr vollendet hat; die Mitgliedsstaaten können durch Gesetz eine niedrigere Altersgrenze vorsehen, die aber das dreizehnte Lebensjahr nicht unterschreiten darf. Ausdrücklich legt Art. 8 Abs. 3 fest, dass dadurch Vorschriften der Mitglieds-

staaten hinsichtlich Gültigkeit und Rechtsfolgen unberührt bleiben.

Hinsichtlich des Begriffes „Dienst der Informationsgesellschaft“ verweist die DSGVO in ihren Begriffsbestimmungen auf Art 1 Abs. 1 lit. b der RL (EU) 2015/1535 (RL über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft).

Ein „Dienst der Informationsgesellschaft“ ist demnach jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung, wobei Anhang I der RL (EU) 2015/1535 eine Beispielliste von Diensten enthält, die nicht unter den Begriff „Dienst der Informationsgesellschaft“ fallen.

Bei unter 16-jährigen (oder einer niedrigeren Altersstufe, wenn ein Mitgliedsstaat dies im nationalen Recht regelt) ist eine Verarbeitung jedenfalls nur rechtmäßig, sofern und soweit ein vertretungsbefugter Elternteil die Einwilligung für den Minderjährigen erteilt hat oder die Einwilligung mit dessen Zustimmung erteilt wurde, wobei der Verantwortliche unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen zu übernehmen hat, um sich zu vergewissern, dass die Einwilligung durch den vertretungsbefugten Elternteil oder zumindest mit dessen Zustimmung erteilt wurde.

Die Verarbeitung „sensibler Daten“ – wie in der RL 95/46/EG „besondere Kategorien personenbezogener Daten“ genannt - erfährt in Art. 9 DSGVO eine Erweiterung dahingehend, dass genetische oder biometrische Daten zur eindeutigen Identifizierung von Personen hinzukommen.

Allerdings können die Mitgliedsstaaten zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

Die Verarbeitung von Kategorien besonderer Daten bleibt – wie bisher – grundsätzlich untersagt, soweit nicht eine der Ausnahmen des Art. 9 Abs. 2 DSGVO zur Anwendung kommt. Die Ausnahmen sind weitgehend aus Art. 8 der RL 95/46/EG bekannt.



Im Fokus

Neugestaltung der Website der Datenschutzbehörde

Mag. Georg Lechner

Die Website der Datenschutzbehörde besteht seit 2001. Sie übersiedelte 2004 auf die Domain dsk.gv.at der damals zuständigen Datenschutzkommission, wurde 2008 umgebaut und übersiedelte 2014 erneut, diesmal auf die Domain dsb.gv.at der Datenschutzbehörde. Mit 1. September 2016 fand die größte Verän-

derung bisher statt: Die Website wurde inhaltlich neu gestaltet und auf eine neue technische Basis gestellt.

Die offensichtlichste Änderung ist die Zusammenführung der bisher nebeneinander geführten Unter-Websites des Datenverarbeitungsregisters, der Stammzahlenregisterbehörde und der Seite für alle weiteren Kompetenzen der Datenschutzbehörde. Die entsprechenden Inhalte sind besser vernetzt. Sie finden ab jetzt auf jeder Seite am rechten Rand Verbindungen zu DVR-Online, der Web-Applikation des Datenverarbeitungsregisters, zur Stammzahlenregisterbehörde und zum Vollmachtenservice, mit dem Sie eine Vertretungsbefugnis auf Ihre Bürgerkarte eintragen lassen können. Das Datenschutzgesetz und die Formulare sind ab sofort auch von jeder Seite aus zugänglich. Am linken Rand finden Sie die Artikel zu den Aufgabengebieten der Datenschutzbehörde. Die Dokumente finden Sie auf einer Seite zusammengefasst. Es gibt eine wesentliche technische Neuerung beim Umgang mit PDF-Dokumenten und externen Seiten. Bei der alten Seite wurden diese in einem neuen Fenster (oder einem neuen Reiter) geöffnet. Bei der neuen Webseite öffnen sich neue Seiten im selben Fenster, und der Besucher kann mit der „Zurück“-Schaltfläche im Browser auch wieder zur vorigen Seite zurückkehren. Die PDF-Dokumente erscheinen im Browser wie normale Artikel auf der Website, und auch von dort kann man mit einem einfachen Klick auf die „Zurück“-Schaltfläche zur vorigen Seite zurückkehren. Die Navigation auf der Seite ist dadurch userfreundlicher und übersichtlicher, weil sich nicht ständig neue Fenster öffnen.

Ausgewählte Entscheidungen der DSB

■ Auskunftserteilung durch Online-Zugang

Im Bescheid vom 15.06.2016, GZ DSB-D122.471/0007-DSB/2016, war die DSB erstmals mit einer behaupteten Verletzung im Recht auf Auskunft durch einen Suchmaschinenbetreiber konfrontiert.

Der Beschwerdeführer behauptete eine Verletzung im Recht auf Auskunft, weil ihm der Suchmaschinenbetreiber lediglich auf einen Online-Zugang zu seinen Daten verwiesen habe, in diesem Zugang aber nicht alle über ihn verarbeiteten Daten erfasst sind. Darüber hinaus habe er Anspruch auf eine schriftliche Auskunft (d.h. in Papierform), weshalb eine Online-Auskunft unzulässig sei.

Mit dem verfahrensabschließenden Bescheid wurde der Beschwerde teilweise stattgegeben und teilweise abgewiesen. Die DSB erblickte eine Verletzung im Recht auf Auskunft darin, dass der Online-Zugang nur einen Teil der über den Beschwerdeführer verarbeiteten Daten erfasse, nicht jedoch sämtliche Daten. Darüber hinaus

sei keine Auskunft zur genauen Herkunft und zu genauen Übermittlungsempfängern sowie herangezogenen Dienstleistern erteilt worden.

Hingegen hegte die DSB keine Bedenken, dass die Auskunft in Form eines Online-Zuganges – und nicht in Papierform – erteilt wird.

Beide Verfahrensparteien erhoben Beschwerde an das Bundesverwaltungsgericht.

■ Personenbezogene Aktenzahl

Im Verfahren GZ: DSB-D122.454/0006-DSB/2016, musste die DSB über die Frage entscheiden, ob die Verwendung des Geburtsdatums zur Bildung einer personenbezogenen Aktenzahl (Grundzahl für Verfahren zur Gewährung von Leistungen der Mindestsicherung im Land Salzburg) zulässig ist. Diese Frage wurde verneint und ein dadurch erfolgter Eingriff einer Bezirksverwaltungsbehörde in das Geheimhaltungsrecht des Beschwerdeführers festgestellt. Entscheidend dafür waren das Fehlen einer ausdrücklichen gesetzlichen Ermächtigung und der fehlende Nachweis, dass es sich bei der Verwendung des Geburtsdatums zur Bildung einer Aktenzahl um eine wesentliche Voraussetzung für die Wahrnehmung einer der Bezirksverwaltungsbehörde gesetzlich übertragenen Aufgabe handelt (§ 8 Abs. 3 Z 1 DSG 2000). Ob diese Form der Bildung einer Aktenzahl in irgendeiner Weise (etwa von einem hierarchisch übergeordneten Betreiber oder technisch durch den Softwarehersteller) vorgegeben war, ist für die Frage der datenschutzrechtlichen Verantwortung nicht entscheidend. Diese Datenverwendung widerspricht dem in § 6 Z 3 DSG 2000 (in Umsetzung von Art 6 Abs. 1 lit c) der EU-Datenschutzrichtlinie 95/46/EG) festgelegten Grundsatz der Datensparsamkeit (Wesentlichkeit der Datenverwendung für den verfolgten Zweck) und dem Grundsatz des gelindesten Mittels gemäß § 7 Abs. 3 DSG 2000. Der Beschwerde wurde daher (in einem Teilbescheid und nur gegenüber der Bezirksverwaltungsbehörde) Folge gegeben. Der Bescheid ist nicht rechtskräftig, da die Bezirksverwaltungsbehörde dagegen am 31. August 2016 (Amts-) Beschwerde an das Bundesverwaltungsgericht erhoben hat.

Ausgewählte Entscheidungen der Gerichte

■ Erkenntnis des Verwaltungsgerichtshofes

Mit Erkenntnis vom 4. Juli 2016, Zl. Ra 2016/04/0014, gab der Verwaltungsgerichtshof einer a.o. Revision der DSB statt und behob den angefochtenen Beschluss des Bundesverwaltungsgerichtes. Das Erkenntnis enthält einige grundsätzliche Aussagen zum Recht auf Auskunft.

Die DSB hat Revision erhoben, weil ihrer Ansicht nach das Bundesverwaltungsgericht zu Unrecht davon ausgegangen war, dass eine Meldebestätigung einen geeigneten Identitätsnachweis nach § 26 Abs. 1 DSG 2000 dar-

stellt. Darüber hinaus fehlte nach Meinung der DSB eine höchstgerichtliche Rechtsprechung zur Frage, ob einem von einem Rechtsanwalt für seinen Mandaten gestelltes Auskunftsbegehren an einen Auftraggeber des privaten Bereiches eine Sondervollmacht beizulegen ist.

In dem Erkenntnis führte der Verwaltungsgerichtshof aus, dass eine Meldebestätigung nach § 19 MeldeG kein geeigneter Identitätsnachweis ist. Ein Identitätsnachweis ist ein solcher, der dem Nachweis der Identität dient (was bei einer Meldebestätigung nicht der Fall ist).

Gegenüber Auftraggebern des privaten Bereiches reicht außerdem eine Berufung auf die anwaltliche Bevollmächtigung nicht aus. Ein Auftraggeber kann hier zusätzlich den urkundlichen Nachweis der Bevollmächtigung verlangen.

Da das DSG 2000 aber bei Auskunftsbegehren auch eine Abweichung von der Schriftform vorsieht, ist auch die „geeignete Form“ des Identitätsnachweises nicht in jedem Fall formstrenge zu sehen. Entscheidend bleibt, dass es dem Auftraggeber verlässlich ermöglicht wird, die Identität des Auskunftswerbers mit der Person zu überprüfen, deren Daten Gegenstand der Auskunft sein sollen.

■ Schlussanträge beim EuGH

In den verbundenen Rechtssachen C-203/15 und C-698/15 legte der Generalanwalt am 19. Juli 2016 seine Schlussanträge vor. In beiden Rechtssachen geht es um die Vereinbarkeit von nationalen Regelungen zur Vorratsdatenspeicherung mit dem Unionsrecht.

Der Generalanwalt führt dazu aus, dass eine Vorratsdatenspeicherung nicht per se mit dem Unionsrecht unvereinbar ist, jedoch bestimmte Kautelen zu beachten sind. Ob diese Voraussetzungen vorliegen, ist von den Gerichten des Ausgangsverfahrens zu prüfen.

In den Schlussanträgen vom 8. September 2016 in der Rechtssache Gutachten 1/15 geht es um die Vereinbarkeit des Entwurfes eines Abkommens zwischen Kanada und der EU über die Übermittlung und Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) u.a. mit Art. 7 EU-GRC (Recht auf Datenschutz). Der Generalanwalt kommt zum Schluss, dass das Abkommen in seiner derzeitigen Form teilweise dem Unionsrecht – so auch Art. 7 EU-GRC – widerspricht und folglich nicht abgeschlossen werden kann.

DVR-Online Tipps und Tricks

Identifizierung im DVR-Online

Es gibt drei Möglichkeiten, um sich im DVR-Online zu identifizieren:

- Bei der Lokalen Bürgerkartenumgebung (BKU) müssen auf dem PC des Benutzers ein Kartenlese-

gerät und eine Software für die lokale BKU installiert werden. Sobald die Karte in den Kartenleser gesteckt und die Anmeldung in DVR-Online gestartet wird, wickelt die lokale BKU die Identifikation des Benutzers mit oder ohne Vertretung ab.

- Bei der Online-BKU muss auf dem PC ein Kartenlesegerät installiert werden. Dabei wird auch die Rechtsanwaltseigenschaft auf der Karte berücksichtigt. Im Internetbrowser wird ein Programm in Java (automatisch) vom Server geladen und ausgeführt. Aus Sicherheitsgründen lassen einige Browser das Laden von Java nicht zu, in diesem Fall muss die lokale BKU benutzt werden.
- Die Mobile BKU ist ohne Installation von Lesegerät und Software möglich, man benötigt lediglich ein Handy und eine Handysignatur. Diese Methode ist für Rechtsanwälte/Notare nicht möglich, da bei der Handysignatur nur die Personendaten gespeichert sind, und keine Daten der juristischen Person.

Unter <http://www.buergerkarte.at/downloads-karte.html> gibt es weitere Informationen, Werkzeuge und Downloads, zur Installation der lokalen BKU. Auf dieser Seite kann auch die Funktion der Bürgerkarte getestet werden.

Gesetzesbegutachtung – Stellungnahmen

Die DSB hat zu folgenden Gesetzesvorhaben eine Stellungnahme abgegeben:

- Ärztegesetz, Änderung
- Sicherheitspolizeigesetz, Änderung
- Finanzmarkt-Geldwäschegesetz u.a

Weblink:

- [Parlament aktiv: alle Stellungnahmen](#)

Teens & Kids

„Pokémon Go“

Virtuelle Jäger und Sammler - Einfallstor für Datendiebstahl

-Sicherheitstipps-

Original-App installieren. Apps von Drittanbietern sind oft mit Schadsoftware verseucht – Pokémon Go daher nur aus dem offiziellen App-Shop herunterladen.

App-Berechtigungen beachten. Wer Pokémon Go spielen möchte, muss der App umfassende Berechtigungen gewähren (z.B. Zugriff auf die

Handykamera, den genauen Standort und die Netzwerkverbindung). Die GPS-basierte Standortbestimmung ist für die Nutzung zwingend notwendig – die App muss schließlich wissen, ob sich Spieler/innen gerade in der Nähe von Pokémon oder besonderen Orten wie Arenen oder PokéStops aufhalten.

Tipp: Zu Spielbeginn nicht mit einem bestehenden Google-Account einloggen, sondern ein eigenes Konto im „Pokémon Trainer Club“ erstellen. Auf diese Weise ist Pokémon Go nicht an das Google-Konto gebunden und es kann kein Datenaustausch stattfinden.

Sammlung von Daten bewusst machen. Durch die permanente GPS-Ortung während des Spiels sammelt die App umfassende Nutzungsdaten der einzelnen Spieler/innen. Laut Nutzungsbedingungen behält sich die App auch vor, personenbezogene Informationen aus Sicherheitsgründen nach eigenem Ermessen weiterzugeben. Eine (personalisierte) Werbung bei Pokémon Go könnte geplant sein. Wer mit diesen Bedingungen nicht einverstanden ist, kann nur eines tun: auf Pokémon Go verzichten.

Screenshots mit Bedacht posten. Erfolgreiche Spieler/innen teilen gerne ihre Erfolge bei Pokémon Go per Screenshot in Sozialen Netzwerken. Aber Vorsicht: Sämtliche Pokémon-Grafiken – also sowohl die kleinen Monster selbst als auch Spielgegenstände wie Pokébälle oder Teamabzeichen – sind urheberrechtlich geschützt und dürfen streng genommen nicht einfach so weiterverbreitet werden. Wer Screenshots postet sollte auch darauf achten, dass im Hintergrund keine unbeteiligten Passant/innen zu sehen sind. Oft verraten solche Aufnahmen auch den eigenen Standort – daher besser vor dem Posten überprüfen, für wen der Beitrag sichtbar ist!

Diese und weitere Sicherheitstipps auf <https://www.saferinternet.at>

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 Mediengesetz); die gesetzlich gebotenen Angaben sind über folgenden Link abrufbar: <https://www.dsb.gv.at/web/daten-schutzbehörde/impressum-copyright>