



Republik Österreich
Datenschutz
behörde

Grundsätzliches zu den Verhaltensregeln

Mag. Andreas Zavadił

Die Systematik der Datenschutz-Grundverordnung (DSGVO) folgt dem Konzept einer weitgehenden Selbstverantwortung und sieht mit der Schaffung von sektorspezifischen Verhaltensregeln („Codes of conduct“) gemäß Art. 40 DSGVO nunmehr eine Methode zur Selbstregulierung vor, um Klarstellungen im Zusammenhang mit der DSGVO und der Verarbeitung personenbezogener Daten innerhalb eines bestimmten Sektors zu erreichen. Verhaltensregeln stellen eine Art Leitlinie guter Datenschutzpraxis dar und können die datenschutzrechtliche Verhaltensweise von Verantwortlichen und Auftragsverarbeitern einer bestimmten Branche standardisieren. Die Ausarbeitung von Verhaltensregeln soll vor allem den besonderen Bedürfnissen von Kleinunternehmen sowie kleinen und mittleren Unternehmen dienen.

Seit dem 25. Mai 2018 hat die Datenschutzbehörde acht Anträge auf Genehmigung von Verhaltensregeln erhalten, wobei der Antrag der Internet Service Providers Austria (ISPA) inhaltlich bereits genehmigt wurde. Bei allen bisherigen Anträgen handelt es sich um solche, die eine inländische Verarbeitungstätigkeit von Verantwortlichen zum Regelungsgegenstand haben. Sofern Verhaltensregeln beantragt werden, die für mehrere Mitgliedstaaten – oder gar europaweit – Geltung haben sollen, ist zusätzlich der Europäische Datenschutzausschuss im Rahmen des Genehmigungsverfahrens zu befassen.

Ausgehend von den Anträgen zeichnet sich ab, dass der Frage der datenschutzrechtlichen Rollenverteilung unter Berücksichtigung datenschutzrechtlicher Materiengesetze, der Modalitäten und Ausübungen von Betroffenenrechten nach Kapitel III DSGVO sowie der Einhaltung der in der DSGVO verankerten Rechenschaftspflichten besondere Aufmerksamkeit gewidmet wird. Darüber hinaus ist auf Art. 40 Abs. 2 DSGVO zu verweisen, wonach demonstrativ weitere Aspekte genannt sind, die

im Rahmen von Verhaltensregeln präzisiert werden können. Dabei ist insbesondere an technische und organisatorische Maßnahmen nach Art. 32 DSGVO sowie an die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen nach Art. 46 Abs. 2 lit e DSGVO zu denken.

Die Unterwerfung unter Verhaltensregeln ist mit mehreren Wirkungen für Verantwortliche und Auftragsverarbeiter verbunden. So kann die Teilnahme an Verhaltensregeln als Indiz für die Einhaltung der in der DSGVO verankerten Rechenschaftspflichten herangezogen werden, können Verhaltensregeln „geeignete Garantien“ zur Datenübermittlung in ein Drittland oder an eine internationale Organisation darstellen und ist die Teilnahme an Verhaltensregeln bei einer etwaigen Geldbuße gebührend zu berücksichtigen.

Die obligatorische Überwachung von Verhaltensregeln ist ein wesentlicher Bestandteil des Konzepts der Selbstverantwortung. Vor diesem Hintergrund müssen im Rahmen von Verhaltensregeln geeignete Verfahren vorgesehen sein, die es der in Art. 41 Abs. 1 DSGVO genannten Überwachungsstelle („monitoring body“) ermöglichen, die regelmäßige Bewertung und Überprüfung der Einhaltung von Verhaltensregeln durchzuführen. Unter einer Überwachungsstelle ist eine private Stelle zu verstehen, die mit der Überwachung der Verhaltensregeln betraut wird und zu diesem Zweck von den Antragstellern ausgewählt wird. Allerdings setzt die Tätigkeit als Überwachungsstelle voraus, dass diese zu diesem Zweck von der Datenschutzbehörde akkreditiert wird, weshalb ein Antrag auf Akkreditierung als Überwachungsstelle notwendig ist.

Die näheren Voraussetzungen dieser Akkreditierung werden im Rahmen einer Akkreditierungs-Verordnung durch die Datenschutzbehörde kundgemacht. Der ent-

sprechende Entwurf zu dieser Akkreditierungs-Verordnung befindet sich bereits in Begutachtung. Ein Antrag auf die inhaltliche Genehmigung von Verhaltensregeln kann zwischenzeitig trotzdem gestellt werden, allerdings wird eine allfällige Genehmigung jedenfalls unter der aufschiebenden Bedingung erteilt, dass die gewählte Überwachungsstelle in weiterer Folge auch akkreditiert wird. Die Datenschutzbehörde genehmigt Verhaltensregeln mit Bescheid und veröffentlicht diese auf ihrer Homepage sowie im Rechtsinformationssystem (RIS).

Eine Hilfestellung zur Ausarbeitung von Verhaltensregeln bieten die Leitlinien des Europäischen Datenschutzausschusses, die sich derzeit in öffentlicher Konsultation befinden ([Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679](#)). Darüber hinaus hat die Datenschutzbehörde ein Informationsblatt zum Thema Verhaltensregeln veröffentlicht, welches ebenfalls als Leitfaden zur Ausarbeitung von Verhaltensregeln herangezogen werden kann (<https://www.dsb.gv.at/genehmigung-von-verhaltensregeln>).



Im Fokus

One-Stop-Shop-Verfahren¹

Mag. Christina Schwaiger

Ein knappes Jahr nach In-Geltung-Treten der DSGVO kann ein erstes Resümee über die grenzüberschreitende Zusammenarbeit im datenschutzrechtlichen Kontext gezogen werden: Das durch die DSGVO etablierte One-Stop-Shop-Verfahren macht den täglichen Austausch von Informationen zwischen den einzelnen nationalen Aufsichtsbehörden erforderlich. Dabei verwenden diese eine eigene Kommunikationsplattform, nämlich das Binnenmarktsystem IMI (Internal Market Information System), welches entsprechend den Erfordernissen von Kapitel VII DSGVO angepasst wurde, indem es mit den dafür notwendigen Workflows ausgestattet wurde.

Voraussetzung für die Anwendung des One-Stop-Shop-Verfahrens ist das Vorliegen eines grenzüberschreitenden Sachverhalts gemäß Art. 4 Z 23 DSGVO. Bevor allerdings der Fall im Register des Binnenmarktsystems IMI eingetragen werden kann, ist als Vorfrage nach der Zuständigkeit der Aufsichtsbehörden gemäß Art. 56 DSGVO zu fragen. Im Zuge dieses Prozesses werden im ersten Schritt federführende sowie betroffene Aufsichtsbehörden identifiziert. In weiterer Folge

wird von der federführenden Behörde der Eintrag im sogenannten Fallregister („case register“) betreffend den grenzüberschreitenden Sachverhalt vorgenommen. Bei diesem Fallregister handelt es sich um eine zentrale Datenbank, von der aus neben dem One-Stop-Shop-Verfahren auch die Prozesse für die gegenseitige Amtshilfe sowie gemeinsame Maßnahmen der Aufsichtsbehörden gestartet werden können. Seit 25. Mai 2018 wurden in diesem Zusammenhang 732 Prozesse im IMI gestartet, um die zuständigen Aufsichtsbehörden gemäß Art. 56 DSGVO zu identifizieren, von denen bereits in 414 Fällen die federführende Aufsichtsbehörde abschließend festgestellt werden konnte. Insgesamt kamen die Eingaben aus 24 EWR-Staaten, wobei 26 von 28 Aufsichtsbehörden bisher als federführende Behörde vorgeschlagen wurden. Im Zuge dieser Verfahren wurde bis dato kein Streitbeilegungsmechanismus gemäß Art. 65 DSGVO ausgelöst.

Nach erfolgtem Eintrag im Fallregister leitet die zuständige federführende Behörde das Ermittlungsverfahren nach den nationalen Verfahrensvorschriften und hält die betroffenen Aufsichtsbehörden über das IMI-System entsprechend den Erfordernissen von Art. 60 DSGVO auf dem Laufenden. Seit dem 25. Mai 2018 wurden dabei insgesamt 76 Fälle mit grenzüberschreitender Komponente im Rahmen des One-Stop-Shop-Verfahrens im IMI-System eingetragen. In 4 von diesen Fällen ist die Österreichische Datenschutzbehörde als federführende Behörde zuständig.

Nachdem das Ermittlungsverfahren abgeschlossen wurde, ist es Aufgabe der federführenden Behörde einen Beschlussentwurf über das IMI-System vorzulegen. Sofern keine der betroffenen Behörden einen begründeten Einspruch erhebt, gilt die jeweilige Entscheidung der federführenden nationalen Aufsichtsbehörde als final. Ist eine betroffene Behörde jedoch nicht mit dem vorgeschlagenen Beschlussentwurf der federführenden Behörde einverstanden und erhebt deshalb einen Einspruch, kann dieser entweder im nächsten Schritt von der federführenden Behörde im überarbeitenden Beschlussentwurf berücksichtigt werden oder aber der Fall wird dem Europäischen Datenschutzausschuss im Wege des Streitbeilegungsmechanismus gem. Art. 65 DSGVO vorgelegt. Bisher liegen 29 Beschlussentwürfe, 1 neuerlich überarbeiteter Beschlussentwurf und 6 finale Entscheidungen im Rahmen des One-Stop-Shop-Verfahrens vor. Darüber hinaus sind derzeit 40 Fälle anzuführen, die sich in der Vorstufe zum Beschlussentwurf befinden, in denen also die federführende Behörde den betroffenen Behörden bereits maßgebliche Informationen zum Fall zur Verfügung gestellt hat.

Abschließend ist darauf hinzuweisen, dass die relativ geringe Anzahl der bisher vorliegenden finalen Entscheidungen bzw. vorgelegten Beschlussentwürfe

¹ Die im gegenständlichen Beitrag angeführten Statistiken beziehen sich auf Stand Anfang März 2019.

zu einem Großteil auf die Unterschiede in den jeweiligen nationalen Verfahrensvorschriften, welche für das Ermittlungsverfahren gelten, zurückzuführen ist. Außerdem nimmt ein fundiertes grenzüberschreitendes Ermittlungsverfahren stets eine gewisse Zeit in Anspruch, sodass zeitnahe vermehrt mit Beschlusssentwürfen bzw. finalen Entscheidungen im Zuge des One-Stop-Shop-Verfahrens zu rechnen ist.

Ausgewählte Entscheidungen der DSB

■ Keine Rechtsgrundlage für intelligente Wasserzähler

Im Bescheid vom 22. November 2018, GZ: DSB-D122.956/0007-DSB/2018, hatte sich die Datenschutzbehörde mit der Zulässigkeit eines intelligenten Wasserzählers zu befassen, der kontinuierlich Wasserdurchfluss und Wassertemperatur erfasste und diese Daten täglich in Form von Mindest-, Mittel- und Höchstwerten für einen längeren Zeitraum speicherte. Der Beschwerdeführer machte sein Recht auf Geheimhaltung geltend und führte unter anderem aus, dass für den Verbau von intelligenten Funkwasserzählern weder eine sachliche Rechtfertigung noch eine Rechtsgrundlage vorliegt und der Beschwerdegegner daher einen solchen Wasserzähler, nicht zuletzt trotz ausdrücklichem Widerspruch des Beschwerdeführers, unrechtmäßig verbaut hätte. Der Beschwerdegegner stützte sich hingegen bei dem Erfassen und Verwalten von Zählerdaten auf die Rechtsgrundlagen des Art. 6 Abs. 1 lit. b, e und f DSGVO. Die Datenschutzbehörde gab der Beschwerde statt und hielt fest, dass Eingriffe durch den Beschwerdegegner gemäß § 1 Abs. 2 DSG stets einer gesetzlichen Grundlage bedürfen, da dieser als Körperschaft öffentlichen Rechts konstituiert ist und daher als staatliche Behörde nach leg. cit. qualifiziert wird. Eine Berufung auf die Rechtmäßigkeit der Verarbeitung aufgrund von Art. 6 Abs. 1 lit. b und f DSGVO ist somit nicht zulässig. Weder das Maß- und Eichgesetz, die Trinkwasserverordnung oder das Wasserrechtsgesetz 1959 sehen jedoch eine entsprechende gesetzliche Grundlage für den Einsatz von intelligenten Wasserzählern vor, wie dies etwa für den Elektrizitätssektor im Elektrizitätswirtschafts- und organisationsgesetz 2010 geregelt ist. Der Einbau und Betrieb des intelligenten Wasserzählers durch den Beschwerdegegner stellt daher einen unzulässigen Eingriff dar und verstößt gegen das Recht des Beschwerdeführers auf Geheimhaltung nach § 1 DSG. Der Bescheid ist nicht rechtskräftig.

■ Entfernung des Personenbezugs („Anonymisierung“) als Mittel zur Löschung

Im Rahmen des Beschwerdeverfahrens zur GZ: DSB-D123.270/0009-DSB/2018 hatte sich die Datenschutzbe-

hörde mit Bescheid vom 5. Dezember 2018 mit der Frage zu befassen, welche Mittel zur Löschung eingesetzt werden können. Der Beschwerdeführer hatte die Löschung sämtlicher Daten begehrt. Die Beschwerdegegnerin entsprach dem Löschbegehren jedoch in der Form, dass sie die Daten des Beschwerdeführers teils faktisch durch Entfernung in ihrem System gelöscht hat, teils hat sie jedoch bloß den Personenbezug zum Beschwerdeführer entfernt (also den Datenbestand des Beschwerdeführers „anonymisiert“). Der Beschwerdeführer brachte im Zuge seiner Beschwerde an die Datenschutzbehörde vor, dass das Primat der faktischen Löschung gelte und er daher in seinem Recht auf Löschung verletzt sei.

Die Datenschutzbehörde hat festgehalten, dass dem Verantwortlichen hinsichtlich der Mittel – also der vorgenommenen Art und Weise, wie eine Löschung durchgeführt wird – ein Auswahlermessen zusteht. Da die DSGVO auf Daten ohne Personenbezug keine Anwendung findet, ist die Entfernung des Personenbezugs (also die „Anonymisierung“) grundsätzlich ein mögliches Mittel, um einem Löschbegehren zu entsprechen. Dabei gilt jedoch ein strenger Maßstab, wonach sichergestellt sein muss, dass weder der Verantwortliche selbst, noch ein Dritter ohne unverhältnismäßigen Aufwand den Personenbezug wiederherstellen kann.

Die Beschwerdegegnerin hat im gegenständlichen Fall durch mehrfache Screenshots von ihrem System belegt, dass der Personenbezug entfernt wurde. Darüber hinaus hat die Beschwerdegegnerin den Prozess der Entfernung des Personenbezugs ausreichend und nachvollziehbar dargelegt. Die Beschwerde wurde daher im Ergebnis abgewiesen.

■ Minderjährigkeit im datenschutzrechtlichen Verfahren

Im Zurückweisungsbescheid vom 11. Februar 2019, GZ: DSB-D123.463/0005-DSB/2018 hatte sich die Datenschutzbehörde aufgrund der Minderjährigkeit des Beschwerdeführers mit dessen Prozessfähigkeit im datenschutzrechtlichen Verfahren auseinander zu setzen. Die Datenschutzbehörde kam zu dem Schluss, dass der Beschwerdeführer zwar aufgrund seines Alters beschränkt prozessfähig (§ 170 Abs. 2 ABGB) ist; diese Prozessfähigkeit aber auf Verfahren, die sich auf die diesem zur freien Verfügung überlassenen Sachen beziehen oder Einkommen aus eigenem Erwerb betreffen - dh. auf vermögensrechtliche Angelegenheiten - beschränkt ist. Die Prozessfähigkeit zur Führung eines datenschutzrechtlichen Verfahrens vor der Datenschutzbehörde kommt dem Beschwerdeführer jedoch nicht zu. In der Sache wurde die Beschwerdeführung zwar nachträglich durch den obsorgeberechtigten Vater genehmigt; der an den Beschwerdeführer zu Händen seines Vaters gerichteten Mangelbehebungsauftrag wurde jedoch nur vom Be-

schwerdeführer selbst beantwortet. Da der minderjährige Beschwerdeführer nicht prozessfähig ist und damit eigene Willenserklärungen gegenüber der Behörde keine Rechtsfolgen auslösen, wurde dem Mangelbehebungsauftrag der Datenschutzbehörde nicht entsprochen, weshalb die Beschwerde gemäß § 13 Abs. 3 AVG zurückzuweisen war.

Ausgewählte Entscheidungen der Gerichte

■ Schlussanträge des Generalanwalts zu C-40/17 (Fashion-ID) vom 19.12.2018¹

Fashion ID ist ein Onlinehändler für Mode-Artikel, auf dessen Webseite ein Plugin von Facebook („Gefällt mir“-Button) eingebunden ist. Besucht ein Nutzer diese Webseite, so werden Informationen über die IP Adresse dieses Nutzers und der Browser-String an Facebook übermittelt, unabhängig davon, ob der Nutzer den „Gefällt mir“-Button anklickt oder ein Facebook-Konto hat. Auch Cookies werden von Facebook auf dem Gerät des Nutzers installiert. Dagegen hatte ein deutscher Verbraucherschutzverband Unterlassungsklage erhoben. Das Oberlandesgericht Düsseldorf hatte ein Vorabentscheidungsersuchen an den EuGH gerichtet.

Der Generalanwalt schlägt dem EuGH in seinen Schlussanträgen vom 19. Dezember 2018 im Wesentlichen vor, dass jener, der ein von einem Dritten bereitgestelltes Plugin in seine Webseite eingebunden hat (das die Erhebung und Übermittlung personenbezogener Nutzerdaten veranlasst), als ein für die Verarbeitung Verantwortlicher im Sinne von Art. 2 lit. d der Richtlinie 95/46 anzusehen sei. Die (gemeinsame) Verantwortlichkeit sei jedoch auf jene Verarbeitungsvorgänge beschränkt, für die er tatsächlich einen Beitrag zur Entscheidung über die Mittel und Zwecke der Verarbeitung der personenbezogenen Daten leiste. Auch in der Haftungsfrage äußert sich der Generalanwalt dahingehend einschränkend, dass die Haftung des Beklagten auf die Phase der Datenverarbeitung beschränkt sein müsse, an der er tatsächlich beteiligt sei, und sie nicht auf etwaige nachfolgende Phasen der Datenverarbeitung erstreckt werden dürfe, wenn diese außerhalb der Einflussphäre und uU auch ohne Kenntnis der Beklagten erfolgt seien.

Weiters vertritt der Generalanwalt die Meinung, dass die nach Art. 7 lit. a der Richtlinie 95/46 einzuholende Einwilligung der betroffenen Person gegenüber dem Webseiten-Betreiber zu erklären sei, der die Dritthalte in seine Webseite eingebunden hat. Die Einwilligung der betroffenen Person und die Informationen im Sinne von Art. 10 müssten bereitgestellt werden, bevor die Erhebung und die Übermittlung der Daten erfolgt sei.

1 <http://curia.europa.eu/juris/celex.jsf?celex=62017C-00040&lang1=en&type=TEXT&ancre=>

Interessant ist, dass der Generalanwalt in diesem Fall eine gemeinsamen Verarbeitung auch dann als gegeben erachtet, wenn keine Parametrierung durch den Webseiten-Betreiber erfolgt (wie dies im Verfahren zum Betreiber einer Facebook - Fanpage (C-216/16) der Fall war), sondern die Einbindung eines Plug-In ausreichend erscheint.

Gesetzesbegutachtung – Stellungnahmen

Die DSB hat zu folgenden Gesetzesvorhaben eine Stellungnahme abgegeben:

- Wehrrechtsänderungsgesetz 2019
- Verordnung des Bundesministers für Bildung, Wissenschaft und Forschung, mit der die Hochschülerinnen- und Hochschülerschaftswahlordnung 2014 – HSWO 2014 geändert wird

Weblink:

- [Parlament aktiv: alle Stellungnahmen](#)

News

Folgende neue Mitarbeiterinnen nahmen ihre Tätigkeit in der DSB auf:

Frau **Christa Muck** war im Bundesministerium für Inneres in der Abteilung für Budget und Controlling tätig und unterstützt nun die DSB in den Bereichen Budget und Personal.

Frau **Astrid Koschitz** kommt vom Bundesverwaltungsgericht, Abteilung Qualitätsmanagement, und unterstützt nun das Team des Sekretariats.

Hinweis neue Kontaktdaten:

Wir sind übersiedelt! Die DSB ist nach 1030 Wien, Barichgasse 40-42, übersiedelt. Die E-Mailadressen und die Telefonnummern sind gleich geblieben.

Impressum:

Medieninhaber, Herausgeber und Redaktion: Österreichische Datenschutzbehörde (DSB), Barichgasse 40-42, 1030 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>.