Datenschutz auf neuer Basis

Europarechtlichen Regelungen waren Schwerpunkte des datenschutzrechtlichen Teils beim 10. Österreichischen IT-Rechtstag am 28. und 29. April 2016 in Wien.

Am 4. Mai 2016 wurden im Amtsblatt der Europäischen Union die Datenschutz-Grundverordnung[1] sowie die Richtlinie für Justiz und Inneres[2] verlautbart. Die – in innerstaatliches Recht noch umzusetzende – Richtlinie ist am Tag nach ihrer Veröffentlichung in Kraft getreten. Ihre Umsetzung hat bis 6. Mai 2018 zu erfolgen. Die – unmittelbar anwendbare – Verordnung ist am 20. Tag nach ihrer Veröffentlichung, somit am 24. Mai 2016, in Kraft getreten und gilt ab 25. Mai 2018 (Art. 99 DSGVO). Mit diesem Tag wird die RL 95/46/EG (Datenschutz-RL) aufgehoben (Art. 94).

Über den Diskussionsverlauf, der zu diesen beiden Rechtsakten geführt hat, berichtete Mag. Natalie Fercher, LL.M., vom Bundeskanzleramt, die an der Ausarbeitung der Formulierungen mitgewirkt hatte. Der Standpunkt Österreichs, dass gegenüber dem durch das DSG 2000 gewährleisteten Datenschutzniveau keine Verschlechterung beim Schutz personenbezogener Daten für die Betroffenen eintreten dürfe, konnte laut Fercher in Teilbereichen nicht zur Gänze umgesetzt werden. Beispielsweise konnte das Grundproblem, dass etwa in sozialen Medien in Grundrechte anderer eingegriffen werden kann, nicht zufriedenstellend gelöst werden.

Eva Souhrada-Kirchmayer, Richterin am Bundesverwaltungsgericht.

Stephan Winklbauer, Experte für IT-Recht und Immobilienrecht.

Nach Art. 6 Abs. 1 lit. f ist die Datenverarbeitung nur rechtmäßig zur Wahrung berechtigter Interessen des Verantwortlichen (Auftraggeber nach der Diktion des DSG). Ein „Überwiegen" dieser Interessen gegenüber den Geheimhaltungsinteressen Betroffener, wie in § 8 DSG, wird nicht mehr vorausgesetzt. Sollen personenbezogene Daten, die zu anderen Zwecken erhoben wurden, verarbeitet werden, hat der hierfür Verantwortliche die Vereinbarkeit mit dem ursprünglichen Zweck zu prüfen (Art. 6 Abs. 4). Das kann über den ursprünglich Verantwortlichen hinaus zu einer Kette von Verarbeitungen führen.

Art. 23 gibt, aus übergeordneten Interessen, der Union oder den Mitgliedstaaten Möglichkeiten der Beschränkung nicht nur der Art. 12 bis 22, sondern sogar von Grundsätzen nach Art. 5 (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Verhältnismäßigkeit).

Probleme dürfte auch aufwerfen, dass parallel zur (verwaltungsrechtlichen) Beschwerdemöglichkeit vor den Datenschutzkontrollbehörden der Gerichtsweg beschritten werden kann. Bei mehreren Aufsichtsbehörden ist die für die Hauptniederlassung zuständige Behörde die federführende („One-Stop-Shop"; Art. 60).

Bei der Richtlinie liegen Problemgebiete im Anwendungsbereich und in der Abgrenzung zur Grundverordnung. In einzelnen Punkten, etwa bei den Dokumentations- und Protokollierungspflichten, wird das Schutzniveau abgesenkt.

DSGVO. Rechtsanwalt Dr. Rainer Knyrim hob hervor, dass, in Anbetracht des hohen Strafrahmens, durch die DSGVO der Datenschutz bewusst auf die höchste Management-Ebene gehoben wird, wie bereits bei anderen Compliance-Themen, etwa Wettbewerbsrecht oder Korruptionsbekämpfung. Immerhin können von den Aufsichtsbehörden Geldbußen bis zu 20 Millionen Euro oder im Fall eines Unternehmens bis zu vier Prozent seines weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden, je nachdem, welcher der Beträge höher ist (Art. 83). Demgegenüber ist der Strafrahmen des DSG 2000 mit 25.000 Euro begrenzt.

Das Ersuchen um eine schriftliche Einwilligung in eine Datenverarbeitung muss in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von anderen Sachverhalten klar zu unterscheiden ist (Art. 7 Abs. 2). Untätigkeit des Betroffenen, vorab angeklickte Checkboxen oder ein „Verstecken" der Erklärung in AGBs vermögen keine gültige Einwilligung zu bewirken. Bei Kindern und Jugendlichen unter 16 Jahren ist die Zustimmung der Eltern nötig, wobei diese Altersgrenze durch die Mitgliedstaaten bis auf das vollendete 13. Lebensjahr herabgesetzt werden darf (Art. 8 Abs. 1).

Datenschutz ist auch durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu gewährleisten (Erwägungsgrund 78; Art. 25). Dazu gehört die Pseudonymisierung von Daten. Pseudonymisierte Daten (Art. 4 Z 5) sind keine eigene Kategorie mehr.

Die Informationspflichten des Verantwortlichen gegenüber der betroffenen Person

FOTOS: KURT HICKISCH

---

[1] *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 (CELEX-Nummer: 32016R0679)*

[2] *Richtlinie EU 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (CELEX-Nummer: 32016L0680)*

bei der Erhebung personenbezogener Daten sind umfangreich geregelt (Art. 13) und umfassen Informationen über das Auskunfts-, Widerrufs- und Beschwerderecht (Abs. 2) und über die beabsichtigte Weiterverarbeitung zu anderen Zwecken (Abs. 3). Ähnlich umfangreich sind die bei einem Verlangen nach Auskunft zu übermittelnden Daten (Art. 14).

Neu ist das „Recht auf Vergessenwerden" (Recht auf Löschung, Art. 17), wobei den Verantwortlichen, sofern die betreffenden Daten öffentlich gemacht wurden, die Verpflichtung trifft, Dritte, die diese Daten verarbeiten, von dem Löschungsbegehren zu informieren (Abs. 2). Diese Mitteilungspflicht betrifft auch jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung (Art. 19).

An die Stelle der DVR-Meldungen wird mit fast gleichem Inhalt das „Verzeichnis von Verarbeitungstätigkeiten" (Art. 30) treten, das von jedem Verantwortlichen zu führen ist. Ausgenommen sind unter gewissen Voraussetzungen Unternehmen oder Einrichtungen, die nicht mehr als 250 Mitarbeiter beschäftigen (Abs. 5).

Meldungen von Verletzungen des Schutzes personenbezogener Daten („Data loss") sind vom Verantwortlichen innerhalb von 72 Stunden der Aufsichtsbehörde anzuzeigen (Art. 33). Die Betroffenen sind unverzüglich von der Verletzung zu verständigen, sofern die Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten anderer Personen zur Folge hat und dies nicht behoben werden konnte. Wäre die persönliche Verständigung mit einem unverhältnismäßigen Aufwand verbunden, hat eine öffentliche Bekanntmachung zu erfolgen (Art. 34).

IT-Rechtstag: Rainer Knyrim, Natalie Fercher, Andrea Jelinek, Clemens Appl.

Wenn die Verwendung neuer Technologien voraussichtlich ein hohes Risiko für die schutzwürdigen Geheimhaltungsinteressen natürlicher Personen zur Folge hat, ist vom Verantwortlichen eine Datenschutz-Folgenabschätzung durchzuführen (Art. 35.) Sollte sich aus dieser ergeben, dass die Verarbeitung ein hohes Risiko zur Folge hätte, hat er die Aufsichtsbehörde zu konsultieren (Art. 36).

Art. 37 schreibt vor, dass Behörden oder öffentliche Stellen jedenfalls einen Datenschutzbeauftragten zu bestellen haben. Unternehmen, gleichgültig, ob diese Verantwortlicher (Auftraggeber) oder Auftragsverarbeiter (Dienstleister) sind, trifft diese Verpflichtung unabhängig von ihrer Größe dann, wenn die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, die auf Grund von Umfang, Art oder Zweck eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder diese Kerntätigkeit in der umfangreichen Verarbeitung sensibler oder strafrechtlich relevanter Daten besteht.

Der Datenschutzbeauftragte hat Fachwissen auf dem Gebiet des Datenschutzrechtes und der Datenschutzpraxis aufzuweisen. Er ist bei der Erfüllung seiner Aufgaben weisungsfrei und darf wegen der Erfüllung dieser Aufgaben nicht abberufen oder benachteiligt werden. Er berichtet unmittelbar der höchsten Managementebene (Art. 38 Abs. 3). Ihm sind die erforderlichen Ressourcen zur Verfügung zu stellen. Der Datenschutzbeauftragte kann auch andere Aufgaben und Pflichten wahrnehmen, doch darf kein Interessenskonflikt entstehen. Die Aufgaben des Datenschutzbeauftragten können auch durch Externe auf Grund eines Dienstleistungsvertrages erfüllt werden.

Safe Harbor. Dr. Andrea Jelinek, Leiterin der seit 1. Jänner 2014 bestehenden Datenschutzbehörde *(www.dsb.gv.at),* zeichnete die Entwicklung der auf Art. 25 Abs. 6 der Datenschutz-RL 95/46/EG gestützten Safe-Harbor-Entscheidung der Kommission (Nr. 2000/-520/EG) nach. US-Unternehmen konnten sich selbst zertifizieren und der Safe-Harbor-Regelung unterwerfen. Mit diesen in einer Liste aufscheinenden Unternehmen war in der Folge ein genehmigungsfreier Datenverkehr zwischen Auftraggebern des privaten Bereichs in der EU und in den USA zulässig.

Die Enthüllungen von Edward Snowden im Juni 2013 führten ab Ende 2013 zu Verhandlungen der Kommission mit Vertretern der US-Administration sowie zu einem Brief der Artikel-29-Gruppe an Kommissarin Viviane Reding im April 2014. Die nach Art. 29 der Datenschutz-RL gebildete, auch als Working Party (WP) bezeichnete Gruppe, die die Kommission in datenschutzrechtlichen Belangen berät, setzt sich zusammen aus den Leitern der unabhängigen Datenschutzbehörden der EU-Mitgliedstaaten, dem Europäischen Datenschutzbeauftragten und einem Vertreter der Kommission. Ab Geltung der DSGVO werden diese Agenden vom Datenschutz-Ausschuss nach den Art. 68 ff übernommen.

Mit Urteil des EuGH vom 6. Oktober 2015, Rs C-362/14, wurde die Safe-Harbor-Entscheidung mit sofortiger Wirkung für ungültig erklärt. Ein gleichwertiges Datenschutzniveau sei nicht (mehr) gegeben. Die Kommission habe keine Feststellungen zum Vorliegen wirksamer Überwachungs- und Kontrollmechanismen in den USA getroffen, keine Feststellungen zur Begrenzung staatlicher Eingriffe in private Daten und zu wirksamen gerichtlichen Rechtsbehelfen. Das US-Recht kenne keine Zweckbegrenzung für behördlich ermittelte Daten. Dadurch und durch den generellen Zugriff auf den Inhalt elektronischer Kommunikation werde der Wesensgehalt des Grundrechts auf Datenschutz verletzt.

In der Folge ist jeglicher Datentransfer in die USA auf der Grundlage von Safe Har-

FOTO: KURT HICKISCH

bor unzulässig. Für solche Datentransfers ist eine Genehmigung durch die österreichische Datenschutzbehörde erforderlich.

Am 29. Februar 2016 veröffentlichte die Kommission den Entwurf einer Adäquanzentscheidung zum „EU-US-Privacy Shield". Dieser Beschlussentwurf basiert auf Verhandlungen und schriftlichen Zusicherungen der amerikanischen Partner (Federal Trade Commission, Departments of Commerce, Trade, Justice und andere Institutionen). Die Kommission gab am gleichen Tag bekannt, dass die Garantien für die Datenübermittlung den Datenschutzstandards der EU entsprechen. Dies sei durch strenge Auflagen, klare Schutzvorkehrungen, Rechtsbehelfe für EU-Bürger in den USA und gemeinsame jährliche Überprüfungen gewährleistet.

Die Artikel-29-Gruppe nahm am 13. April 2016 dazu Stellung, schlug Verbesserungen im Bereich der privaten Unternehmen, der nationalen Sicherheit und der Ermittlungen im Dienste der Strafrechtspflege vor und äußerte kritische Bemerkungen und Bedenken.

Judikatur. Über Rechtsmittel gegen Entscheidungen der Datenschutzbehörde entscheidet ein Senat des Bundesverwaltungsgerichtes, der sich aus einem Berufsrichter und zwei fachkundigen Laienrichtern zusammensetzt. Dr. Eva Souhrada-Kirchmayer als Richterin in diesem Senat und Datenschutzbeauftragte des Europarates, zeigte an Beispielen aus der Judikatur des Bundesverwaltungsgerichtes auf, wie vielfältig sich datenschutzrechtliche Probleme in der Praxis ergeben. Es ging um Mitteilungen an Medien über Hausdurchsuchungen (W214 200964-1/41E), Weitergabe von strafrechtsrelevanten Daten an eine Zeitung (W214 2009971-1/52E), die Verwendung eines polizeilichen Vernehmungsprotokolls (W214 2106278-1/22E), die Weitergabe von Gesundheitsdaten im Rahmen der Anzeigeerstattung (W214 2106365-1/17E), den Identitätsnachweis beim Auskunftsrecht (W 214 2108081-1/9E), das Auskunftsrecht bei Verlassenschaft (W214 2113213-1/10E), die Transparenz von Landwirtschaftsförderungen (W224 2113499-1/4E), bis zur Aquakultur-Seuchenverordnung (W214 2016573-1/11E). Der EuGH hatte sich, über Safe Harbor hinaus, richtungweisend mit datenschutzrechtlichen Fragen aus Rumänien (Übermittlung von Einkommensdaten von der Finanz an die Krankenkassen; C-201/14) und aus Ungarn (Weltimmo; C-230/14) zu befassen.

Sonja Dürager, Expertin für IT-Recht, Urheberrecht und Datenschutzrecht.

Walter Blocher, Experte für Wirtschafts-, Unternehmens- und Informationsrecht.

Eng mit datenschutzrechtlichen Fragen verbunden ist die im Elektronische-Gesundheitsakte-Gesetz (ELGA-G; Art. 1 GesundheitstelematikGesetz 2012 – GTelG 2012, BGBl I 2012/111) geregelte Elektronische Gesundheitsakte ELGA. Über die umfassenden Datensicherheitsmaßnahmen berichtete Mag. Theresa Philippi von der ELGA-GmbH. Individualanträge, das ELGA-Gesetz in seiner Gesamtheit als verfassungswidrig aufzuheben, wurden vom VfGH mit Erkenntnis vom 2.3.2015, G 140/2014-15, G 159/2014-12, zurückgewiesen. Seit Dezember 2015 sind die ELGA-Bereiche Wien und Steiermark „live". In diesen Bundesländern gibt es ELGA-Ombudsstellen.

Datenverwertung. Primärdaten wie Identifikationsdaten können mit aggregierten oder recherchierten Daten angereichert, verknüpft und ausgewertet werden und letztlich durch Berechnung von Zusatzinformationen, durch Daten aus Webshops und Social Media zu einer neuen aufbereiteten Form (z. B. Kundenprofil) führen. Über die Frage, wem diese Daten gehören und wer sie nutzen darf, referierte Rechtsanwältin Dr. Sonja Dürager. Der Sachbegriff des § 285 ABGB erfasst auch unkörperliche Sachen. Eigentum (§ 354 ABGB) betrifft nur körperliche Sachen. § 126a StGB (Datenbeschädigung) stellt auf die Verfügungsmacht dessen ab, der die Daten geschaffen hat (Skripturakt). Für sich gesehen, sind Daten keine schöpferische Leistung nach dem UrhG, sondern bloße Information. Auch bei einer Datenbank, die zufolge der Auswahl und/oder die Anordnung des Stoffs eine eigentümliche geistige Schöpfung sein kann, sind nur Aufbau und Struktur geschützt, nicht die Daten als einzelne Elemente. Sofern die Entnahme von Daten nicht die Wesentlichkeit der Datenbank erreicht, ist sie zulässig. Allerdings können Website-Betreiber in ihren Nutzungsbedingungen das Auslesen von Daten vertraglich verbieten (EuGH 15.1.2015, C-30/14, Ryanair vs. PR Aviation). Gegen Webcrawling (automatisches Analysieren von Websites) können technische Maßnahmen ergriffen werden, auch gegen Screen-Scraping (gezieltes Extrahieren). Bei Verletzung von schutzwürdigen Geheimhaltungsinteressen besteht Schadenersatzanspruch nach § 33 DSG iVm § 1311 ABGB. Persönlichkeitsrechte sind durch § 16 ABGB geschützt. Bei kommerzieller Verwertung von Persönlichkeitsrechten („geldwerter Bekanntheitsgrad") durch andere steht dem Betroffenen ein Bereicherungsanspruch nach § 1041 ABGB zu.

Rechtsanwalt Dr. Stephan Winklbauer empfahl, bei Cloud-Services die Nutzungsbedingungen genau zu lesen und zu analysieren. Die Ankündigungen halten vielfach nicht das, was sie versprechen („unbegrenzter Speicherplatz", „unbegrenzt Musik", „Daten immer griffbereit"). Zumeist unterliegen die Verträge US-amerikanischem Recht, mit Gerichtsstand in den USA.

Als Zukunftsvision stellte Univ.-Prof. Dr. Walter Blocher, Universität Kassel, Smart Contracts vor. Verträge werden statt bei einem Notar im Internet abgelegt. Vertragsklauseln sind entweder selbst ausführbar und/oder selbst durchsetzbar. Das System baut auf der von Bitcoin und Ethereum verwendeten Block-Chain-Technologie auf.

Kurt Hickisch

Fotos: Kurt Hickisch