Neues im Datenschutz

Datenschutz-Grundverordnung, Vorratsdatenspeicherung, Datenschutz-Grundverordnung, „Recht auf Vergessen“: Im Datenschutzrecht hat sich in letzter Zeit viel getan.*

Der Vorschlag der Europäischen Kommission vom 25. Jänner 2012 für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) wurde nach Verhandlungen im Rat und im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE-Ausschuss) des Europäischen Parlaments von diesem nach zahlreichen Änderungen am 12. März 2014 in erster Lesung angenommen und dem Rat zugeleitet. Ein Beschluss des Rates steht noch aus.

Die Verordnung soll die Datenschutz-Richtlinie 95/46/EG ersetzen. Die Rechtsform der – unmittelbar anwendbaren – Verordnung wird gewählt, um in der Union das gleiche Maß an Datenschutz herzustellen.

Die Verordnung sieht von der Einführung einer generellen Meldepflicht für Datenverarbeitungen ab, überträgt den für die Verarbeitung Verantwortlichen dafür aber mehr Verantwortung. Vor der Verarbeitung ist eine Datenschutz-Folgenabschätzung (Art. 33) durchzuführen. Ergeben sich dabei Risiken, sind der Datenschutzbeauftragte oder die Aufsichtsbehörde zu Rate zu ziehen (Art. 34).

Datenschutzrechtsexpertin Eva Souhrada-Kirchmayer.

Ein Datenschutzbeauftragter ist unter anderem zu bestellen, wenn die Verarbeitung durch eine Behörde oder eine öffentliche Einrichtung erfolgt; wenn sich die Verarbeitung auf mehr als 5.000 betroffene Personen innerhalb von zwölf Monaten bezieht; wenn die Kerntätigkeit auf Überwachung gerichtet ist oder die Kernaktivitäten in der Verarbeitung von Ortungsdaten, sensiblen Daten oder umfangreicher Datenverwendungen von Arbeitnehmerdaten oder Daten von Kindern bestehen. Von allen für die Verarbeitung Verantwortlichen sind Dokumentationen vorzuhalten und regelmäßig zu aktualisieren (Art. 28).

Datenschutz soll auch von vornherein durch Technik und datenschutzfreundliche Voreinstellungen erfolgen (Art. 23; Data protection by design, by default). Voreinstellungen sollen standardmäßig dem Grundsatz der Datenminimierung und der Zweckbeschränkung entsprechen. Freiwillige Zertifizierungen können beantragt werden und zur Erteilung des „Europäischen Datenschutzsiegels“ (Art. 39) führen.

„Pseudonymisierte“ und „verschlüsselte“ Daten wie auch „Profiling“ werden definiert (Art. 4 Z 2a, 2b und 3a) und es werden Regelungen über das Profiling getroffen (Art. 20). Die „Besonderen Datenkategorien“ (Art. 9) werden gegenüber dem Vorschlag der Kommission um Daten über verwaltungsrechtliche Sanktionen und mutmaßliche Straftaten erweitert.

Eine „Einwilligung“ erfordert eine ohne jeden Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte ausdrückliche Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung. Der Widerruf muss so einfach wie die Erteilung der Einwilligung sein (Art. 4 Abs. 8; Art. 7). Ein Recht auf Vergessenwerden ist zwar nicht vorgesehen, doch das Recht auf Löschung wird detaillierter ausgeführt (Art. 17). Das Widerspruchsrecht (Art. 19) wird erleichtert.

Die Stellung der Datenschutzbehörden wird gestärkt. Sie erhalten Anordnungs- und Strafbefugnisse, wobei die Geldbußen bis zu 100 Millionen Euro oder im Fall eines Unternehmens bis zu fünf Prozent seines weltweiten Jahresumsatzes betragen können (Art. 79).

Das Prinzip des „One-Stop-Shops“ findet im Begriff der „federführenden Behörde“ seinen Ausdruck (Art. 54a). Zuständig ist die Datenschutzbehörde jenes Landes, in dem sich die Hauptniederlassung befindet.

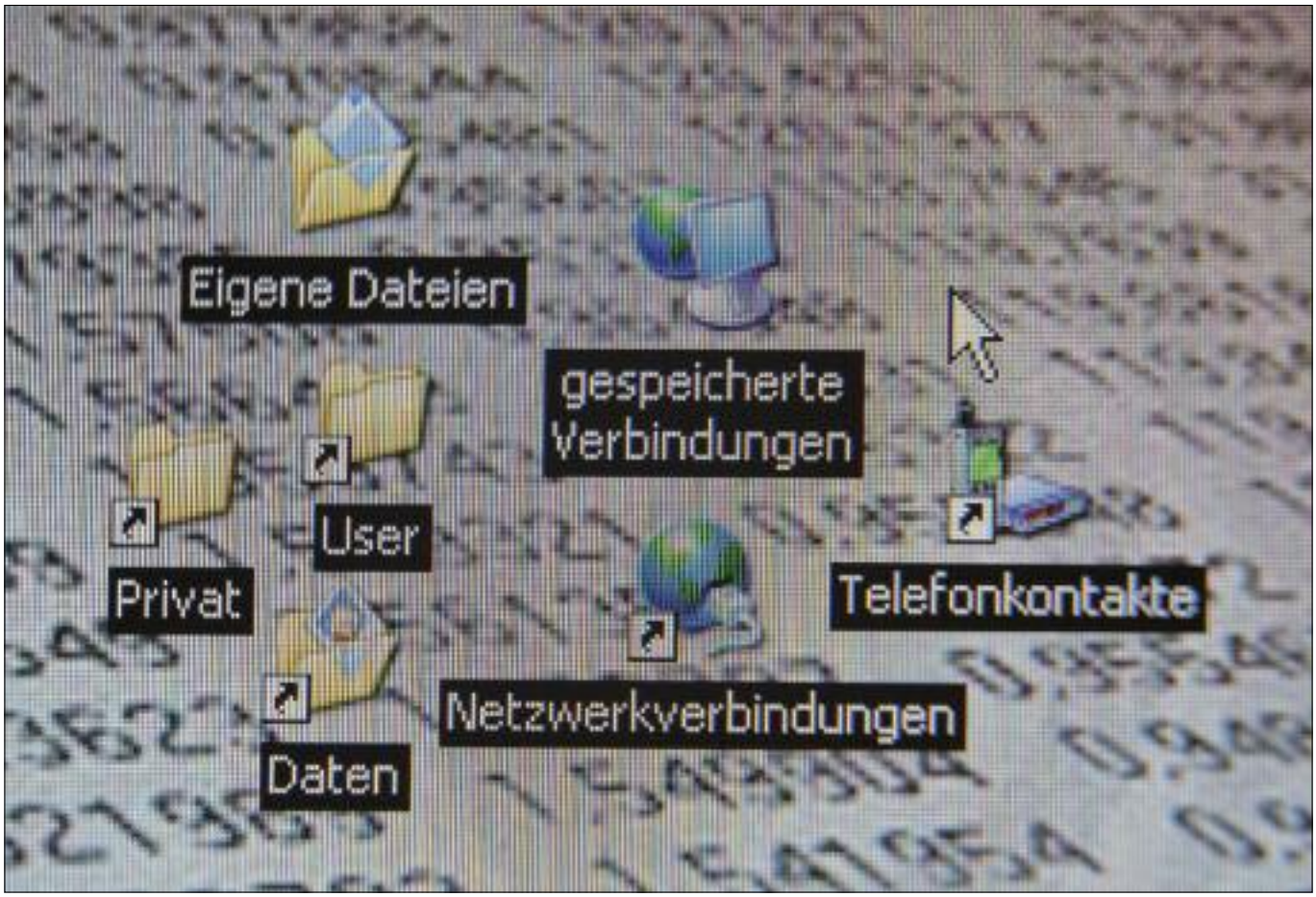
Europarats-Konvention. Das aus dem Jahr 1981 stammende Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Europaratskonvention Nr. 108 der European Treaty Series; BGBl 317/1988) ist das erste und einzige säulenübergreifende Datenschutz-Rechtsinstrument und insofern von Bedeutung, als es auch für Nicht-EU-Staaten des Europarats gilt. Die Konvention, die auch Drittstaaten zum Beitritt offen steht, haben 44 europäische Staaten ratifiziert. Als erster Drittstaat ist Uruguay beigetreten; der Beitritt Marokkos steht bevor.

Die Konvention sieht Mindeststandards vor; ein höheres Schutzniveau ist möglich. Es werden Grundsätze für die Verarbeitung von Daten festgelegt wie Rechtmäßigkeit, Treu und Glauben, Zweckbindung, Relevanz, sachliche Richtigkeit, Speicherung nur so lange, als es zur Zweckerfüllung notwendig ist (Art. 5). „Sensible“ Daten dürfen nur dann verarbeitet werden, wenn das innerstaatliche Recht Schutz gewährleistet (Art. 6). Rechte für die Betroffenen sind festgelegt (Art. 8), zulässige Ausnahmen und Einschränkungen (Art. 9), und es sind Sanktionen und Rechtsmittel vorgesehen (Art. 10). Es werden auch Regelungen über den grenzüberschreitenden Datenverkehr getroffen (Art. 12).

Vom Beratenden Ausschuss (Art. 18 bis 20), der ähnliche Funktionen wie die „Artikel-29-Gruppe“ der EU-Datenschutz-RL hat, wurde eine Überarbeitung

FOTO: KURT HICKISCH

** Der Beitrag beruht auf einem Vortrag von Dr. Eva Souhrada-Kirchmayer beim 8. Österreichischen IT-Rechtstag am 23. Mai 2014 in Wien. Eva Souhrada-Kirchmayer war bis zur Auflösung der Datenschutzkommission am 31. Dezember 2013 deren geschäftsführendes Mitglied und ist seither Richterin am Bundesverwaltungsgericht. Sie ist auch Datenschutzbeauftragte des Europarates.*



Die Vorratsdatenspeicherung wurde mit Erkenntnis des Verfassungserichtshofs am 27. Juni 2014 aufgehoben, weil sie dem Grundrecht auf Datenschutz und dem Art. 8 Menschenrechtskonvention (Recht auf Privat- und Familienleben) widerspricht.

FOTOS: JENS BUETTNER/DPA/PICTUREDESK.COM

der Konvention beschlossen, die nunmehr in einem zwischenstaatlichen Ad-hoc-Committee geprüft wird.

Bei dieser Modernisierung soll der Geltungsbereich der Konvention auf manuelle Dateien ausgeweitet werden. Datenverarbeitungen für persönlich-private Zwecke sollen ausgenommen werden. Die Möglichkeit, Vorbehalte zu machen, soll nicht mehr eingeräumt werden.

Der Katalog der besonders schützenswerten Daten wird überarbeitet und um genetische und biometrische Daten sowie Daten betreffend die Zugehörigkeit zu einer Gewerkschaft, strafbare Handlungen und strafrechtliche Verurteilungen ergänzt. Die „Data Breach Notification“ (Informationsverpflichtung bei Datenmissbrauch; vgl. § 24 Abs. 2a DSG 2000) wird nur für schwerwiegende Fälle vorgesehen. Normiert sind ein Widerspruchs- und Löschungsrecht, aber kein „Recht auf Vergessenwerden“.

Einschränkungen sollen dann möglich sein, wenn dies gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist zum Schutz der nationalen und der öffentlichen Sicherheit; zur Wahrung höherer wirtschaftlicher und finanzieller Interessen des Staates und zur Verhütung und Verfolgung von Straftaten; zum Schutz der betroffenen Person und der Rechte und Freiheiten Dritter. Die Pflichten der für die Verarbeitung Verantwortlichen werden festgelegt, wozu auch der durch Technik und durch Voreinstellungen herzustellende Datenschutz zählt.

Der freie Informationsaustausch zwischen den Vertragsparteien soll möglich sein, soweit sie ein hohes Datenschutzniveau gewährleisten können. Liegt dieses nicht vor, sind standardisierte oder im Einzelfall festzulegende Maßnahmen notwendig, damit ein Datentransfer zulässig ist. Die Überprüfung des Datenschutzniveaus in einem Mitgliedstaat wird dem Beratenden Ausschuss zukommen, der zum „Konventionskomitee“ wird.

Vorratsdatenspeicherung. Die „Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG“ (Vorratsdatenspeicherungs-RL) wurde vor allem nach den Terroranschlägen vom 11. September 2001 („9/11“) erarbeitet. Formell stellte sie eine Änderung der RL 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation; „ePrivacy-RL“) vom 12. Juli 2002 dar, deren Art. 15 Einschränkungen unter anderem im Interesse der Sicherheit des Staates und zur Verfolgung von Straftaten vorsieht.

Die Vorratsdatenspeicherungs-RL verpflichtete Provider, Verbindungsdaten (nicht Inhaltsdaten) öffentlicher Kommunikationsdienste in einem Rahmen von sechs Monaten bis zu zwei Jahren auf Vorrat zu speichern. Die Daten sollten zum Zweck der Ermittlung,

Feststellung und Verfolgung von schweren Straftaten zur Verfügung stehen. Der Regelung der Mitgliedstaaten blieb überlassen, was unter schweren Straftaten zu verstehen ist; ebenso, wer Zugriff auf die Daten haben sollte und an wen sie zulässigerweise übermittelt werden dürfen. Nach einem Vertragsverletzungsverfahren wurde in Österreich ein Entwurf zu einer der RL entsprechenden TKG-Novelle erarbeitet (§ 102a TKG idF BGBl I 2011/27). Novellen zur StPO und zum SPG folgten (BGBl I 2011/33).

In Österreich beim Verfassungsgerichtshof eingelangte Beschwerden (Anträge der Kärntner Landesregierung sowie von Privatpersonen auf Nichtigerklärung des § 102a TKG) wurden von diesem zur Vorabentscheidung dem EuGH vorgelegt („Österreichisches Verfahren", Rechtssache C-594/12).

Bei diesem war bereits das „Irische Verfahren" (Rs C-293/12) anhängig. Der EuGH stellte fest, dass die Daten Aufschluss darüber geben, wer mit wem wie oft und auf welchem Weg kommuniziert hat, wie lange die Kommunikation gedauert hat und an welchem Ort sie stattgefunden hat, sodass Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden, möglich sind, was einen Eingriff in das Recht auf Achtung des Privat- und Familienlebens nach Art. 7 der Grundrechte-Charta (GRC) darstellt.

Das Sammeln der Daten hat Auswirkungen auf die Nutzung der Kommunikationsmittel und indiziert einen Eingriff in das Recht auf Freiheit der Meinungsäußerung und der Informationsfreiheit (Art. 11 GRC). Ferner liegen Auswirkungen auf das Recht auf Datenschutz vor (Art. 8 GRC). Derartige Einschränkungen müssen nach Art. 52 GRC gesetzlich vorgesehen und erforderlich sein und den dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer entsprechen.

Österreichische Datenschutzbehörde.

Der Gerichtshof hat zwar anerkannt, dass der Wesensgehalt der Grundrechte nicht angetastet wird und die dem Gemeinwohl dienende Zielsetzung gegeben ist. Diese könne jedoch die Erforderlichkeit von Speicherungsmaßnahmen, wie sie die RL vorgesehen hat, nicht rechtfertigen. Fast die gesamte europäische Bevölkerung sei betroffen.

Beim Ziel der Bekämpfung schwerer Straftaten sei keine Differenzierung, Einschränkung oder Ausnahme erfolgt. Die Speicherung erfolge anlasslos, es gebe keine Einschränkung nach bestimmten Zeiträumen, geografischem Gebiet oder den Personenkreis, der in schwere Straftaten verwickelt sein könnte. Eine Regelung des Zugangs nationaler Behörden zu den Daten sei nicht erfolgt, die Nutzung nicht eingeschränkt. Zwischen den Datenkategorien seien keine Unterscheidungen gemacht worden. Die unwiderrufliche Vernichtung nach der Speicherung werde nicht angeordnet. Die Datenspeicherung sei nicht auf das Unionsgebiet beschränkt und es bestünden keine dem Art. 8 GRC entsprechenden Garantien dafür, dass die Daten vor Missbrauch geschützt seien. Der Unionsgesetzgeber habe beim Erlass der RL 2006/24 die Grenzen überschritten, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit im Hinblick auf die Art. 7, 8 und 52 Abs. 1 der Charta einhalten hätte müssen (Rn 69 des Urteils). Die RL wurde mit Urteil des EuGH vom 8. April 2014, das die beiden anhängigen Rechtssachen zusammengefasst hat, für ungültig erklärt.

Mit dem am 27. Juni 2014 verkündeten Erkenntnis des VfGH, G 47/2012 u. a., wurden die die Vorratsdatenspeicherung betreffenden Gesetzesstellen im TKG, der StPO und des SPG als dem Grundrecht auf Datenschutz und dem Art. 8 Menschenrechtskonvention (Recht auf Privat- und Familienleben) widersprechend aufgehoben; im Wesentlichen aus den bereits vom EuGH angestellten Erwägungen. Die Aufhebung ist mit dem Datum der Kundmachung (BGBl I 2014/44 vom 30. Juni 2014) in Kraft getreten.

Google. Zentraler Punkt im Urteil zum Verfahren C 131/12 des EuGH ist das „Recht auf Vergessen". Ein Spanier hatte bei der spanischen Datenschutzagentur eine Beschwerde gegen die Herausgeberin einer Tageszeitung sowie gegen *Google* Spain eingebracht. Er machte geltend, dass bei Eingabe seines Namens in die Suchmaschine *Google* Search Links zu zwei Seiten der Tageszeitung von Jänner und März 1998 angezeigt würden, in denen die Versteigerung seines Grundstücks wegen Schulden bei der Sozialversicherung angekündigt worden sei.

Google Spain und *Google Inc*. wurde von der Datenschutzbehörde aufgefordert, die betreffenden Daten aus dem Index zu entfernen. Dagegen haben die beiden Gesellschaften geklagt. Das damit befasste Gericht legte dem EuGH eine Reihe von Fragen zur Vorabentscheidung vor.

Der EuGH hat mit Urteil vom 13. Mai 2014 den Suchmaschinenbetreiber als „Verantwortlichen" für die vorgenommene Datenverarbeitung erkannt. Dieser sei unter bestimmten Voraussetzungen verpflichtet, von der Ergebnisliste, die bei einer mit dem Namen einer Person durchgeführten Suche angezeigt wird, Links zu von Dritten veröffentlichten Internetseiten mit Informationen über diese Person zu entfernen, selbst wenn die Veröffentlichung als solche rechtmäßig sei. Bei einer Namenssuche könnten strukturierte Informationen erhalten werden, die ein Profil der gesuchten Person ergeben würden. Ein solcher Eingriff könne nicht allein mit dem wirtschaftlichen Interesse des Suchmaschinenbetreibers gerechtfertigt werden. Ein Eingriff in die Grundrechte einer Person könne allerdings, etwa durch ihre Rolle im öffentlichen Leben („Public Figure"), durch das überwiegende Interesse der breiten Öffentlichkeit gerechtfertigt sein.

Kurt Hickisch