

DSG-Info-Service

Juli 2014

Ausgabe Nr. 76

*Sehr geehrter DSG-Paket-Kunde!
Sehr geehrter Leser!*

Mit dem vorliegenden DSG-Info-Service wollen wir Sie über einige interessante Entwicklungen im europäischen und österreichischen Datenschutzrecht informieren. Zu allererst einige In-

formationen, wie es um die EU-Datenschutz-Grundverordnung (EU-DSG-VO) steht, anschließend das Ende der Vorratsdatenspeicherung. Last, but not least folgen einige Anmerkungen in Bezug auf das kürzlich vom EuGH ergangene Urteil in der Causa „Google“.

1. Wie steht es um die EU-Datenschutz-Grundverordnung?

Bekanntlich hat der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europaparlaments am 21. Oktober 2013 unter dem Vorsitz des deutschen Grün-Politikers Jan-Philipp Albrecht den „Entwurf zur Änderung der durch die EU-Kommission vorgelegten Datenschutz-Grundverordnung (KOM (2012)) 11, DSG-VO“ angenommen und die Aufnahme von Verhandlungen mit dem Rat der Europäischen Union gemäß Art. 70 beschlossen. Diesem Entwurf gingen intensive Verhandlungen voraus, so wurden allein zum Berichtsentwurf von MEP Jan-Philipp Albrecht mehrere tausend Änderungsanträge eingebracht. Insgesamt enthält der Entwurf ein Paket von 91 Kompromiss-Vorschlägen. Dieses Kompromiss-Paket wurde am 12. März 2014 vom Plenum des Europäischen Parlaments bestätigt (der angenommene Text befindet sich unter: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE&language=DE>).

Wir möchten anhand von zwei Beispielen exemplarisch aufzeigen, mit welcher „Qualität“ die Diskussionen geführt werden:

1. Als Beispiel, wie lange Diskussionen zum gleichen Ergebnis führen können (oder kennen Sie den Unterschied zwischen „expliziter“ und „ausdrücklicher“ Zustimmung? Wir jedenfalls nicht!):

Art. 4 (8), ursprünglicher Text:

*„Einwilligung der betroffenen Person“ jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte **explizite** Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.*

Art. 4 (8), derzeitiger Text:

*„Einwilligung der betroffenen Person“ jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte **ausdrückliche** Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.*

2. Als Beispiel, wie man auf Grund langer Diskussionen von einem Extrem in das andere fallen kann:

Art 35 (1): Ursprünglich sah der Entwurf die verpflichtende Bestellung eines Datenschutzbeauftragten durch Unternehmen vor, die 250 oder mehr Mitarbeiter beschäftigen. Diese Grenzziehung erfolgte analog der europäischen Unternehmensdefinition und hätte in Österreich von insgesamt rund 350.000 Unternehmen gerade einmal 1000 Unternehmen betroffen. Der geänderte Text sieht nunmehr die verpflichtende Bestellung eines Datenschutzbeauftragten für alle Unternehmen vor, die eine Datenanwendung betreiben, die sich auf mehr als 5000 Betroffene innerhalb eines Zeitraums von 12 aufeinander folgenden Monaten bezieht. Unter diese Regelung würde auch ein EPU fallen, das eine Adressdatei in dieser Größenordnung betreibt. Ob dieser Vorschlag praktikabel ist, muss stark bezweifelt werden.

Der Beschluss des Europäischen Parlaments vom 12. März 2014 allein reicht bekanntlich nicht aus. Erst wenn im sogenannten Trilog, sprich zwischen EU-Parlament, dem Rat (auch EU-Ministerrat genannt) und der Europäischen Kommission Einigung erzielt wird, kann die EU-DS-GVO verabschiedet werden.

Eine Einigung im EU-Ministerrat ist allerdings derzeit nicht absehbar, da die dort vertretenen Mitgliedsstaaten erhebliche unterschiedliche Sichtweisen haben. Vor allem Deutschland fürchtet um sein hohes Datenschutzniveau und will nicht akzeptieren, dass die DS-GVO auch für den öffentlichen Bereich gelten soll und nicht auf den privaten Bereich beschränkt wird. Weiters befürchtet Deutschland, dass die Rechtsstellung des in Deutschland derzeit schon verpflichtend zu bestellenden Datenschutzbeauftragten geschwächt wird. Auch sehen manche Datenschützer den derzeitigen Entwurf der DS-GVO bereits als veraltet an, da sie die neuen Herausforderungen wie z. B. Big Data oder das Internet der Dinge nicht entsprechend abbildet.

Mit welchem Datum nun die DS-GVO in Kraft treten wird, steht in den Sternen. Bekanntlich spielen auf EU-Ebene nicht nur sachliche Erwägungen eine Rolle, siehe z. B. die Streitereien um die Besetzung des Kommissionspräsidenten. Aus Brüssel ist zu hören, dass man die Verabschiedung einer EU-DSG-VO für das erste oder spätestens zweite Halbjahr 2015 für denkbar hält. Bei einer üblicherweise zweijährigen Umsetzungsfrist wäre also mit dem Inkrafttreten mit Beginn 2018 zu rechnen.

2. Das Ende der Vorratsdatenspeicherung

Mit der Entscheidung des Europäischen Gerichtshofes (EuGH) vom 8. April 2014 wurde die umstrittene Richtlinie über die Vorratspeicherung von Daten 2006/24/EG vom 15. März 2006 für nichtig erklärt. Der Anlass zur Klage ging primär von Österreich aus. Die Richtlinie verpflichtete bekanntlich Provider – unter ausdrücklicher Ausnahme von Inhaltsdaten – zur Speicherung von Verkehrs- und Standort-Daten und deren Herausgabe an die national zuständigen Behörden.

Der EuGH sieht in erster Linie einen Verstoß gegen das Grundrecht auf Achtung des Privatlebens (Art. 8 EMRK), weil aus den Verkehrsdaten Rückschlüsse auf deren Inhalt gezogen

werden können. Weiters weist der EuGH darauf hin, dass die Definition der schweren Straftaten nicht entsprechend differenziert ist und darüber hinaus die Speicherdauer – zwischen 6 und 24 Monate – zu lange sei.

Nachdem der EuGH die Richtlinie aufgehoben hatte, hat auch der österreichische Verfassungsgerichtshof (VfGH) mit Urteil vom 27. Juni 2014 das Gesetz zur Vorratsdatenspeicherung als verfassungswidrig erklärt. Der VfGH begründet das Urteil in seiner Presseinformation vom 27. Juni 2014 wie folgt:

Gesetze zur Vorratsdatenspeicherung in Österreich verfassungswidrig

Bestimmungen widersprechen dem Datenschutz und dem Recht auf Privatsphäre

Die Gesetze zur Vorratsdatenspeicherung in Österreich sind verfassungswidrig. Sie widersprechen dem Grundrecht auf Datenschutz sowie dem Artikel 8 der Europäischen Menschenrechtskonvention („Recht auf Privat- und Familienleben“).

Eine Frist zur Reparatur wird nicht gewährt. Die Aufhebung tritt mit Kundmachung der Aufhebung, die unverzüglich durch den Bundeskanzler zu erfolgen hat, in Kraft.

Die Verfassungsrichterinnen und Verfassungsrichter begründen ihre Entscheidung – knapp zusammengefasst – wie folgt:

- Ein so gravierender Eingriff in die Grundrechte, wie er durch die Vorratsdatenspeicherung erfolgt, muss so gestaltet sein, dass er mit dem Datenschutzgesetz und der Menschenrechtskonvention im Einklang steht.
- Ob ein solcher Eingriff verfassungsrechtlich zulässig ist, hängt davon ab, wie die Bedingungen für die Speicherung solcher Daten, die Anforderungen an deren Löschung sowie die Sicherungen beim Zugriff auf diese Daten geregelt sind. Die angefochtenen Bestimmungen des Telekommunikationsgesetzes, der Strafprozessordnung und des Sicherheitspolizeigesetzes erfüllen diese Anforderungen nicht.
- Es fehlen nämlich zahlreiche präzise gesetzliche Sicherheitsvorkehrungen, etwa, was die genaue Ausgestaltung der Speicherverpflichtung, die Voraussetzungen für die Zugriffe auf diese Daten oder die Verpflichtung der Löschung dieser Daten, betrifft.
- Die „Streubreite“ der Vorratsdatenspeicherung übertrifft die bisher in der Rechtsprechung des Verfassungsgerichtshofes zu beurteilenden Eingriffe in das Grundrecht auf Datenschutz, und zwar sowohl hinsichtlich des betroffe-

nen Personenkreises – nahezu die gesamte Bevölkerung ist davon betroffen – als auch der Art der betroffenen Daten, sowie der Modalität der Datenverwendung.

- Das Grundrecht auf Datenschutz, so der Verfassungsgerichtshof, ist in einer demokratischen Gesellschaft auf die Ermöglichung und Sicherung vertraulicher Kommunikation zwischen den Menschen gerichtet. Der Einzelne und seine freie Persönlichkeitsentfaltung sind nicht nur auf die öffentliche Kommunikation in der Gemeinschaft angewiesen; die Freiheit als Anspruch des Individuums und als Zustand einer Gesellschaft wird bestimmt von der Qualität der Informationsbeziehungen.
- Dem Verfassungsgerichtshof ist bewusst, dass neue Kommunikationstechnologien auch neue Herausforderungen für die Kriminalitätsbekämpfung, die ein öffentliches Interesse darstellt, bedeuten. Dies hat der Verfassungsgerichtshof stets berücksichtigt.
- Die Erweiterung der technischen Möglichkeiten führen aber auch dazu, dass den Gefahren, die diese Erweiterung für die Freiheit des Menschen in sich birgt, in einer dieser Bedrohung adäquaten Weise entgegengetreten werden muss.
- Regelungen wie eine Vorratsdatenspeicherung können zwar zur Bekämpfung schwerer Kriminalität zulässig sein, aber nur, wenn sie im Einklang mit dem Datenschutz und der Menschenrechtskonvention stehen. Die angefochtenen Bestimmungen über die Vorratsdatenspeicherung im Telekommunikationsgesetz, in der Strafprozessordnung und im Sicherheitspolizeigesetz bilden in ihrem Zusammenhang einen unverhältnismäßigen Eingriff und damit eine Verletzung des Grundrechts auf Datenschutz. Die Frage, wie eine verfassungskonforme Regelung aussehen könnte, stellt sich für den Verfassungsgerichtshof jetzt nicht.

3. EuGH verurteilt Google

Der EuGH hat mit Urteil vom 13. Mai 2014 (<http://curia.europa.eu/juris/liste.jsf?language=de&num=C-131/12>) festgestellt, dass der Betreiber einer Internetsuchmaschine bei personenbezogenen Daten, die auf von Dritten veröffentlichten Internetseiten erscheinen, für die von ihm vorgenommene Verarbeitung verantwortlich ist. Google hat inzwischen reagiert und ein Online-Antragsformular für die Löschung datenschutzwidriger Inhalte zur Verfügung gestellt. Dem Urteil lag das Verfahren eines spanischen Bürgers zu Grunde, der sich gegen Google Spain und Google Inc. mit der Begründung wandte, dass der bei Eingabe seines Namens erscheinende Bericht über finanzielle Schwierigkeiten aus dem Jahr 1998 einen Verstoß gegen datenschutzrechtliche Vorgaben darstelle. Er forderte daher die Löschung dieses Berichts.

Die Reaktionen auf dieses Urteil sind gemischt: Eine Gruppe sieht das im Entwurf der EU-DS-GVO vorgesehene „Recht auf Vergessen“ bereits vorweg genommen, andere Gruppen sehen Probleme in Bezug auf die faktische Abkehr vom bisher gültigen Sitzlandprinzip, wie es die Richtlinie 95/46/EG in Art. 4 vorsieht. Weiters wird befürchtet, dass der Aufbau einer parallelen „Sperr-Datenbank“ notwendig wird, wo die beanstandeten Inhalte gespeichert werden. Außerdem führt nach Meinung vieler Kritiker das Urteil des EuGH zu einem Konflikt zwischen datenschutzrechtlichen Vorgaben einerseits und dem Anspruch auf freien und globalen Zugang zu Information andererseits.

Jedenfalls wird spannend, wie sich dieses Urteil auf die weiteren Diskussionen in Zusammenhang mit der EU-DS-GVO auswirken wird.

••••

Unser nächstes Seminar „**Datenschutz im modernen Unternehmen – Vom Gesetzestext bis zur unternehmenskonformen Umsetzung**“ findet am 17. November 2014 statt.

Es referiert der Mitautor des Standardwerkes zum österreichischen DSG:
Prof. KommR Hans-Jürgen Pollirer.

Anmeldung unter www.secur-data.at oder telefonisch unter (01) 533 42 07-0.



Im Jänner 2014 neu erschienen ist die zweite Auflage der **handlichen Ausgabe zum Datenschutzrecht**.

Das Handbuch enthält bereits die neuesten Änderungen im österreichischen Datenschutzrecht wie insbesondere

- Verwaltungsgerichtsbarkeits-Novelle 2012
- DSG-Novelle 2013
- DSG-Novelle 2014

Neuerungen wie die Zusammensetzung und Bestellung der durch die DSG-Novelle 2014 geschaffenen Datenschutzbehörde sowie die Schaffung des Bundesverwaltungsgerichts als neue Berufungsinstanz durch die Verwaltungsgerichtsbarkeits-Novelle 2012 werden ebenfalls behandelt.

Die Möglichkeit zur Direktbestellung finden Sie unter www.manz.at