Secur-Data Betriebsberatungsges.m.b.H.
1010 Wien, Fischerstiege 9
Tel. +43 (1) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at

DSG-Info-Service

Oktober 2016 Ausgabe Nr. 85

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

Mit unserem Newsletter Nr. 84 aus Juli 2016 haben wir Sie über das aus Datenschutzsicht spektakuläre Urteil des Bundesgerichts in New York informiert, wonach die US-Regierung kein Recht hat, auf Daten von Microsoft-Kunden, die auf ausländischen Servern gespeichert sind, zuzugreifen. Falls jemand geglaubt hat, dass die US-Regierung dieses Urteil akzeptiert, hat er sich – wie Sie anschließend lesen können – kräftig geirrt.

Ein langerwartetes Urteil des EuGH, das die Frage beantwortet, ob es sich bei dynamischen IP-Adressen um personenbezogene Daten iSd RL 95/46/EG handelt, hat ebenfalls für einiges Aufsehen gesorgt.

Last, but not least, dürfen wir Sie noch in aller Kürze auf den bereits unter heftiger Kritik stehenden Entwurf des deutschen Bundesinnenministeriums zur Anpassung des BDSG an die DSGVO informieren.

1. Microsoft vs. US-Regierung – die nächste Runde

Die US-Regierung hat das zugunsten der Microsoft-Corporation gefällte Urteil – wie zu erwarten war – nicht akzeptiert und hat die Staatsanwaltschaft um eine erneute Anhörung aller aktiven Richter ersucht, die gegen die US-Regierung geurteilt haben. Mit dem Urteil vom 14. Juli 2016 hatte das in zweiter Instanz mit dem Fall betraute Berufungsgericht geurteilt, dass Microsoft aufgrund der nationalen Gesetzgebung in den USA nicht gezwungen werden könne, personenbezogene Daten seiner Kunden herauszugeben, die auf Servern außerhalb der USA – im gegenständlichen Fall auf einem Server in Irland – gespeichert sind. Das Gericht begründete das Urteil damit, dass diese Daten nicht der Anwendung des **„Stored Communication Act“** von 1986 unterliegen. Da eine exterritoriale Anwendung dieses Rechtsaktes seitens des US-Kongresses nicht vorgesehen war, ist dieser nur für Durchsuchungsbeschlüsse nach nationalem Recht relevant. Die nunmehrige Behauptung der Staatsanwaltschaft, dass es sich um ein Fehlurteil des Gerichts handle, weil die Daten zwar in Irland gespeichert sind, aber Microsoft von den USA aus zugreifen könne, erscheint mehr als abstrus. Entscheidet das Gericht wieder gegen die US-Regierung, so bleibt der Staatsanwaltschaft noch der Gang zum Supreme Court of the United States offen.

Folgt das Gericht jedoch dem Standpunkt der Staatsanwaltschaft, so würde dies bedeuten, dass die rechtstaatliche Autonomie eines europäischen Landes vollständig missachtet wird. Als Konsequenz könnte man nur zum Schluss kommen, dass US-Cloud-Anbieter von europäischen Nutzern nicht mehr eingesetzt werden dürfen.

Secur-Data Betriebsberatungsges.m.b.H.
1010 Wien, Fischerstiege 9
Tel. +43 (1) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at

2. EuGH-Urteil vom 19. Oktober 2016

Vorgeschichte (kurz): Der Kläger verlangte von der beklagten Bundesrepublik Deutschland die Unterlassung des Speicherns der ihm zugewiesenen dynamischen IP-Adressen über das Ende des jeweiligen Nutzungsvorgangs hinaus. Das Amtsgericht hatte die Klage abgewiesen. Auf die Berufung des Klägers hatte das Landgericht dem Kläger den Unterlassungsanspruch nur insoweit zuerkannt, als dieser das Speichern von IP-Adressen in Verbindung mit dem Zeitpunkt des jeweiligen Nutzungsvorgangs betrifft und der Kläger während dieses Nutzungsvorgangs seine Personalien angibt. Gegen dieses Urteil haben beide Parteien beim Bundesgerichtshof Berufung eingelegt. Der BGH hatte das Verfahren ausgesetzt und dem EuGH zwei Fragen zur Auslegung der EG-Datenschutzrichtlinie zur Vorabentscheidung vorgelegt. An dieser Stelle soll nur die erste Frage behandelt werden:

„Der Unterlassungsanspruch setzt voraus, dass es sich bei den dynamischen IP-Adressen für die verantwortlichen Stellen der Beklagten, die die Adressen speichern, um "personenbezogene Daten" handelt, die von dem durch die Richtlinie harmonisierten Datenschutzrecht geschützt werden. Das könnte in den Fällen, in denen der Kläger während eines Nutzungsvorgangs seine Personalien nicht angegeben hat, fraglich sein. Denn nach den getroffenen Feststellungen lagen den verantwortlichen Stellen keine Informationen vor, die eine Identifizierung des Klägers anhand der IP-Adressen ermöglicht hätten. Auch durfte der Zugangsanbieter des Klägers den verantwortlichen Stellen keine Auskunft über die Identität des Klägers erteilen.

*Der Bundesgerichtshof hat dem Europäischen Gerichtshof deshalb die Frage vorgelegt, ob Art. 2 Buchstabe a der EG-Datenschutz-Richtlinie*** dahin auszulegen ist, dass eine IP-Adresse, die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen schon dann ein personenbezogenes Datum darstellt, wenn lediglich ein Dritter über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt.“*

Das Urteil des EuGH[1] zur ersten Frage: Art. 2 lit. a der RL 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist dahingehend auszulegen, dass eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum iSd der genannten Bestimmung darstellt. Voraussetzung dafür ist, dass er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen. Dies wäre z.B. durch die Einschaltung der Strafverfolgungsbehörden nach einem Angriff auf den Online-Dienst möglich.

Damit ist die jahrelang andauernde Diskussion, ob es sich auch bei dynamischen IP-Adressen um personenbezogene Daten iSd RL 95/46/EG handeln kann, beendet.

[1] http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=de&mode=req&dir=&occ=first&part=1&cid=1070434

3. Erster Entwurf des deutschen Bundesministeriums des Innern (BMI) zur Anpassung des BDSG an die DSGVO

Am 7. September 2016 wurde der Volltext des Referentenentwurfs (Stand: 1. Ressortabstimmung vom 5. August 2016, 08:43)[2] geleaked. Der Entwurf eines Gesetzes zur Anpassung des deutschen Datenschutzrechts an die Datenschutz-Grundverordnung und zur Umsetzung der Richtlinie (EU) 2016/680[3] mit der Abkürzung EU-DSAnpUG-EU hat zu scharfer Kritik sowohl seitens der Bundesbeauftragten für den Datenschutz und die Informationssicherheit sowie anderen bekannten Datenschützern, darunter auch vom Ex-Bundesdatenschutzbeauftragten Peter Schaar, geführt.

Insgesamt umfasst der Entwurf eines Allgemeinen Bundesdatenschutzgesetzes (ABDSG) – als Artikelgesetz ausgeführt – acht Artikel, wobei die Artikel 3 bis 7 andere Gesetze wie zB das Gesetz über den militärischen Abschirmdienst (MADG) betreffen, deren Anpassungen noch offen sind. Artikel 2 umfasst die Anpassungen des Bundesverfassungsschutzgesetzes. Artikel 8 regelt die Inkraftsetzung des ABDSG sowie die gleichzeitige Außerkraftsetzung des BDSG.

Allgemein wird kritisiert, dass der gewählte Regelungsansatz, nämlich dass sowohl die DSGVO wie auch Richtlinie (EU) 2016/618 in einem gemeinsamen Gesetz geregelt werden sollen. Dieser Ansatz führe dazu, dass für viele Rechtsanwender bei vielen Vorschriften unklar ist, welche Texte nun für sie gelten. Darüber hinaus gewinne man den Eindruck, dass das BMI bestrebt ist, die Regelungsspielräume (Öffnungsklauseln) nicht zum Erhalt eines hohen Datenschutzniveaus, sondern eher zu dessen Absenkung auszunutzen.

Nach einer ersten Lektüre des Referentenentwurfs dürfen wir Ihnen beispielhaft einige wesentliche Bestimmungen zur Kenntnis bringen, die zeigen, dass das BMI noch einiges zu tun haben wird:

- Die Kontrollbefugnisse der Bundesdatenschutzbeauftragten (BfDI) sollen erheblich eingeschränkt werden, insb. gegenüber dem Verfassungsschutz und dem Bundesnachrichtendienst. Die BfDI soll sich bei Angelegenheiten, welche die Nachrichtendienste betreffen, auch nicht mehr an den Bundestag oder die parlamentarischen Kontrollgremien wenden dürfen. Darüber hinaus sind für diese Bereiche auch keine Sanktionsmöglichkeiten vorgesehen.
- Mit den Bestimmungen des § 6 ABDSG wird der Grundsatz der Zweckbindung aufgeweicht. Insgesamt werden 10 Ausnahmetatbestände aufgezählt, bei denen die Verarbeitung personenbezogener Daten zu einem anderen Zweck als den, für den sie erhoben wurden, erlaubt ist. Diese Ausnahmetatbestände weichen von den Bestimmungen des Art. 8 Abs. 4 DSGVO erheblich ab.
- § 10 ABDSG schränkt das Recht auf Löschung der personenbezogenen Daten des Betroffenen ein, wenn *„eine Löschung aufgrund der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem*

[2] https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/09/Entwurf-ABDSG-E-08.2016.pdf

[3] Richtlinie 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 http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1477654578458&uri=CELEX:32016L0680

Aufwand möglich ist. In diesem Fall tritt an die Stelle einer Löschung eine Einschränkung der Verarbeitung gem. Art. 18 DSGVO."

- § 14 ABDSG regelt die Benennung eines Beauftragten für den Datenschutz wie folgt:

  (1) Nach Maßgabe des Artikels 37 Absatz 1 der Verordnung (EU) 2016/679 und des Artikels 32 Absatz 1 der Richtlinie (EU) 2016/680 haben Verantwortliche und Auftragsverarbeiter Beauftragte für den Datenschutz zu bestellen. Das Gleiche gilt für Verantwortliche und Auftragsverarbeiter, soweit sie in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen.

  […]

  (5) Ist nach Absatz 1 eine Beauftragte oder ein Beauftragter für den Datenschutz zu bestellen, so ist die Kündigung des Arbeitsverhältnisses unzulässig, es sei denn, dass Tatsachen vorliegen, welche den Verantwortlichen zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach der Abberufung als Beauftragte oder Beauftragter für den Datenschutz ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass der Verantwortliche zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.

  Abs. 1 Satz 2 sieht vor, dass abweichend von den Bestimmungen des Art. 37 ein Datenschutzbeauftragter bestellt werden muss, wenn sich in der Regel mindestens 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen. Nach den Bestimmungen des Abs. 5 erhält der Datenschutzbeauftragte ein Jahr Kündigungsschutz nach Ablauf seiner Funktion.

- § 33 ABDSG regelt in ähnlicher Art und Weise den bereits in § 32 BDSG geregelten Beschäftigtendatenschutz wie folgt:

  (1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

  (2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten verarbeitet werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet oder für die Verarbeitung in einer solchen Datei erhoben werden.

  (3) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

  (4) Beschäftigte sind:

  1. *Arbeitnehmerinnen und Arbeitnehmer,*
  2. *zu ihrer Berufsbildung Beschäftigte,*
  3. *Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),*
  4. *in anerkannten Werkstätten für behinderte Menschen Beschäftigte,*
  5. *nach dem Jugendfreiwilligendienstegesetz Beschäftigte,*
  6. *Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,*

7. *Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,*
8. *Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.*

Damit scheint in Deutschland die Debatte um ein eigenes Gesetz zum Beschäftigtendatenschutz, dessen Entwurf 2013 in Erwartung der kommenden DSGVO auf Eis gelegt wurde, beendet zu sein.

- § 42 ABDSG:

  (1) Ordnungswidrig handelt, wer in Ausübung seiner Tätigkeit für den Verantwortlichen oder Auftragsverarbeiter vorsätzlich oder fahrlässig gegen Artikel 83 Absatz 4, 5 oder 6 der Verordnung (EU) 2016/679 verstößt. § 8 und §§ 10 bis 16 des Gesetzes über Ordnungswidrigkeiten finden Anwendung. Die Ordnungswidrigkeit kann im Fall des Satzes 1 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden.

  (2) Die nachfolgenden Vorschriften gelten für die Verhängung von Geldbußen nach der Verordnung (EU) 2016/679, für die Verhängung von Geldbußen gegen denjenigen, der nach Absatz 1 Satz 1 ordnungswidrig handelt sowie für die Verhängung von Geldbußen gegen denjenigen, der vorsätzlich oder fahrlässig entgegen § 40 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder entgegen § 40 Absatz 2 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.

  (3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt. Satz 1 gilt nicht für öffentliche Stellen, soweit die Verarbeitung im Rahmen einer Tätigkeit erfolgt, hinsichtlich derer die öffentliche Stelle mit anderen Verarbeitern im Wettbewerb steht.

  (4) Geldbußen können für im räumlichen Anwendungsbereich der Verordnung (EU) 2016/679 begangene Verstöße verhängt werden.

  (5) § 4 Absätze 1 bis 4 und §§ 6 und 7 des Gesetzes über Ordnungswidrigkeiten finden Anwendung.

  Da die Art. 83 und 84 DSGVO nur für

  - Unternehmen mit Sitz in der EU, und
  - Unternehmen, die personenbezogene Daten über in der EU ansässige Personen erheben, verarbeiten und nutzen, soweit diese Unternehmen ihre Tätigkeit auf die EU ausrichten,

  gelten, soll für natürliche Personen nur die in Abs. 1 festgelegte Geldbuße von bis zu EUR 300.000,00 zur Anwendung kommen.

  Damit ist klargestellt, dass die Bußgeldtatbestände des Art. 83 und 84 auch für natürliche Personen in Unternehmen (zB Vorstand einer AG, Geschäftsführer einer GmbH, Datenschutzbeauftragter) gelten, die gegen die Bestimmungen der DSGVO verstoßen haben, allerdings mit einer Obergrenze von EUR 300.000,00. Für die Unternehmen gelten dagegen die in der DSGVO festgelegten Bußgelder von bis zu EUR 20 Mio. oder 4 % des weltweiten Umsatzes.

Insgesamt kann die Kritik der deutschen Datenschützer wie folgt zusammengefasst werden:

- Gravierende Regelungslücken bei Polizei und Justiz
- Datenschutzverstöße bei Nachrichtendiensten bleiben in Zukunft sanktionslos
- Die Bundesdatenschutzbeauftragte darf sich nicht mehr an das Parlament wenden
- Aushöhlung des Zweckbindungsgrundsatzes
- Rechtliche Unklarheiten und Unsicherheiten

Die in den Medien verbreitete Kritik hat dazu geführt, dass das BMI die offizielle Versendung des ABDSG-Referentenentwurfes mittlerweile gestoppt hat.

Seitens des österreichischen BKA wurde ein erster Entwurf des Anpassungsgesetzes für Ende des Jahres 2016 angekündigt. Wir werden Sie über alle Entwicklungen in dieser Angelegenheit natürlich umgehend informieren. Bis dahin heißt es aber abwarten und hoffen.

••••