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 2015 Ausgabe Nr. 81

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

Nachdem wir Sie mit unserem Juni-Newsletter (Nr. 78 – 80) ausführlich über den Status der DS-GVO informiert haben, dürfen wir Sie heute über das vom Gerichtshof der Europäischen Union (EuGH) am 6. Oktober 2015 gefällte Urteil in Bezug auf das Safe-Harbor-Abkommen informieren. Dies deshalb, weil dieses Urteil für alle Unternehmen, die Daten in die USA schicken bzw. ihre Kunden- und Mitarbeiterdaten amerikanischen Cloud-Anbietern anvertrauen, schwerwiegende Konsequenzen hat.

Weiters dürfen wir Sie über eine neue Standardanwendung informieren, und zwar die SA037 mit der Bezeichnung „Melde- und Kontrollsysteme zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung".

Last, but not least informieren wir Sie über die Empfehlung der DSB vom 1. Juli 2015, die bei vielen Unternehmen Handlungsbedarf auslösen sollte.

1. Das Ende des Safe-Harbor-Abkommens (Abkommen des „Sicheren Hafens")

Das Safe-Harbor-Abkommen (http://www.export.gov/safeharbor/eu/index.asp) war eine Entscheidung der Europäischen Kommission vom 26. Juli 2000 (E 2000/520/EG). Diese Entscheidung wurde deshalb notwendig, weil es die Datenschutzrichtlinie 95/46/EG grundsätzlich verbietet, personenbezogene Daten aus Mitgliedstaaten der EU in Staaten zu übertragen, deren Datenschutz kein dem EU-Recht vergleichbares Schutzniveau aufweist. Dazu zählen auch die USA, die keine umfassenden und durchgehenden gesetzlichen Regelungen auf dem Gebiet des Datenschutzes hat, die den EU-Standards entsprechen würden. Die USA kennen nämlich nur Regelungen für einzelne Teilbereiche, wie zB den „Children's Online Privacy Protection Act (COPPA)" oder den im Bereich der Krankenversicherung gültigen „Health Insurance Portability and Accountability Act (HIPAA)". Zum Teil gibt es Gesetze, die nur in einem einzigen Bundesstaat gelten, wie zB der „California Online Privacy Protection Act (CalOPPA)". Damit der Datenverkehr zwischen der EU und den USA funktioniert, wurde eben das Safe-Harbor-Abkommen beschlossen. Diese Vereinbarung sollte ein angemessenes Datenschutzniveau bei den US-amerikanischen Unternehmen sicherstellen, indem sich diese Unternehmen auf die im Abkommen definierten Grundsätze verpflichten. Diese Grundsätze lauten wie folgt:

1. *Informationspflicht*: Das Unternehmen muss Betroffene darüber unterrichten, welche Daten es für welche Zwecke er-

hebt und welche Rechte Betroffene haben.

2. *Wahlmöglichkeit*: Das Unternehmen muss Betroffenen die Möglichkeit geben, der Weitergabe ihrer Daten an Dritte oder der Nutzung für andere Zwecke zu widersprechen.
3. *Weitergabe*: Wenn ein Unternehmen Daten an Dritte weitergibt, muss es Betroffene darüber und über die unter 2. aufgeführte Wahlmöglichkeit informieren.
4. *Zugangsrecht*: Betroffene müssen die Möglichkeit haben, die über sie gespeicherten Daten einzusehen und sie ggfs. berichtigen, ergänzen oder löschen können.
5. *Sicherheit*: Das Unternehmen muss angemessene Sicherheitsvorkehrungen treffen, um die Daten vor unbefugtem Zugang, Zerstörung oder Missbrauch zu schützen.
6. *Datenintegrität*: Das Unternehmen muss sicherstellen, dass die von ihm erhobenen Daten korrekt, vollständig und zweckdienlich sind.
7. *Durchsetzung*: Das Unternehmen verpflichtet sich, Streitschlichtungsmechanismen beizutreten, so dass Betroffene ihre Beschwerden und Klagen untersuchen lassen können und im gegebenen Fall Schadensersatz erhalten.

Zuständig für die Entgegennahme und Verwaltung dieser Selbstzertifizierungen ist die Federal Trade Commission (FTC). Heute finden sich mehr als 5.400 Unternehmen aus den USA auf der sogenannten Safe-Harbor-Liste (https://safeharbor.export.gov/list.aspx).

Das Abkommen war von Anfang an ein problematischer Kompromiss, und zwar durch das Fehlen einer unabhängigen Aufsichtsbehörde, die das datenschutzkonforme Verhalten der in dieser Liste eingetragenen Unternehmen überprüft. Die Angemessenheit des Datenschutzniveaus bei den zertifizierten US-amerikanischen Unternehmen wurde mehrmals in Frage gestellt, so zB durch die von der Galexia Pty Ltd. 2008 durchgeführten Studie mit der Bezeichnung „The US Safe Harbor – Fact or Fiction“. Diese Studie zeigte auf, dass ca. 1/3 der in dieser Liste eingetragenen Firmen entweder gar nicht mehr existierte bzw. ihre Zertifizierung nicht erneuert hatten. Die Studie führte 2010 zu einer Klarstellung des sogenannten Düsseldorfer Kreises (http://kurzelinks.de/ew5m), der feststellte, dass ein deutscher Datenexporteur der Behauptung des US-amerikanischen Datenimporteurs, der eine Safe-Harbor-Zertifizierung besitzt, nicht blind vertrauen darf, sondern dass er verpflichtet ist, sich vom Datenimporteur nachweisen zu lassen, dass seine Zertifizierung noch aktuell ist und dass das US-amerikanische Unternehmen seinen Informationspflichten gegenüber den Betroffenen nachkommt.

Durch die Snowden-Veröffentlichungen im Zusammenhang mit den Aktivitäten des US-Geheimdienstes NSA erhielt die Debatte um das Safe-Harbor-Abkommen eine völlig neue Dimension. Die EU-Kommission leitete bereits im Herbst 2013 Verhandlungen mit den USA über ein neues Safe-Harbor-Abkommen ein. Der für Sommer 2014 vorgesehene Abschluss der Verhandlungen wurde bis heute nicht erreicht. Wahrlich kein Ruhmesblatt für die EU-Kommission!

Der EuGH ist nunmehr am 6. Oktober 2015 der EU-Kommission zuvorgekommen, indem er das Safe-Harbor-Abkommen für ungültig erklärte. Ich erspare mir an dieser Stelle die Nacherzählung der in allen Medien ausgebreiteten Erfolgsgeschichte des österreichischen Juristen und Datenschutzaktivisten und gehe vor allem auf die Frage ein, was dieses Urteil für jene österreichischen Unternehmen bedeutet, die Datenverkehr mit US-amerikanischen Unternehmen haben. Denn die Entscheidung des EuGH hat weitreichende Konsequenzen insofern, dass österreichische Firmen, die ihre Daten an US-amerikanische Firmen übertragen, dies nicht mehr unter Inanspruchnahme des Safe-Harbor-Abkommens tun können. Es fehlt aufgrund dieser EuGH-Entscheidung die datenschutzrechtliche Rechtsgrundlage. Das Urteil des EuGH (http://kurzelinks.de/ekqw) besagt im We-

sentlichen, dass das Safe-Harbor-Abkommen aus dem Jahr 2000 nicht das angemessene Datenschutzniveau erfüllt und somit ungültig ist. Dies vor allem in Hinblick auf den Zugriff der US-Nachrichtendienste auf die personenbezogenen Daten. Es stellt weiter fest, dass selbst wenn die EU-Kommission dieses Abkommen unterzeichnet hat, die nationalen Datenschutzbehörden prüfen können, ob bei der Übermittlung der Daten einer Person in ein Drittland die in der Datenschutzrichtlinie 95/46/EG aufgestellten Anforderungen gewahrt werden. Das heißt, dass die EU-Kommission nicht das Recht hatte, die Befugnisse der nationalen Datenschutzbehörden zu beschränken. Der EuGH hält weiters fest, dass die US-amerikanischen Unternehmen ohne jede weitere Einschränkung verpflichtet sind, die im Safe-Harbor-Abkommen vorgesehenen Schutzregeln auszuhebeln, wenn sie in Widerstreit zu gesetzlichen Erkenntnissen stehen. Das Urteil hat nun zur Folge, dass die irische Datenschutzbehörde unter Bezugnahme auf Max Schrems prüfen und entscheiden muss, ob nach den Bestimmungen der Richtlinie 95/46/EG die Übermittlung der Daten der europäischen Nutzer von Facebook in die Vereinigten Staaten auszusetzen ist, weil dieses Land kein angemessenes Schutzniveau für personenbezogene Daten bietet. Die Antwort der irischen Datenschutzbehörde kann m.E. im Lichte dieses EuGH-Urteils nur ein **NEIN** sein!

Wie wirkt sich nun die EuGH-Entscheidung auf österreichische Unternehmen aus und welche Lösungsszenarien – soweit überhaupt im Augenblick absehbar – gibt es?

- Der Datentransfer aus Österreich in die USA steht künftig unter ausdrücklichem Genehmigungsvorbehalt. Eine generelle Weitergabe wie bisher unter dem Safe-Harbor-Abkommen ist nicht mehr möglich.
- Setzt das Unternehmen einen amerikanischen Dienstleister ein, so müsste versucht werden, alternative Dienstleister zu finden, die ihren Sitz und ihre Server in der EU haben.
- Eine wahrscheinlich wenig praktikable, aber trotzdem überlegenswerte Lösung ist die Einholung der Zustimmung zur Datenübermittlung bei den Betroffenen.
- Weiters wäre auch zu überprüfen, ob die in die USA zu übermittelnden Daten überhaupt personenbezogener Natur sein müssen, oder ob man nicht auch mit indirekt personenbezogenen, anonymisierten oder sicher verschlüsselten Daten das Auslangen finden könnte.
- Verwendet das Unternehmen SaaS-Dienste eines US-amerikanischen Anbieters, so wäre zu hinterfragen, ob dieser nicht auch innerhalb der EU Niederlassungen und Rechenzentren betreibt. So eröffnete SalesForce – einer der weltweit größten CRM-Anbieter – bereits 2014 ein Rechenzentrum in Großbritannien, ein weiteres steht in Deutschland knapp vor der Eröffnung. In diesem Fall müssten allerdings die zugehörigen Verträge angepasst werden.
- Als allerletzte Möglichkeit verbleibt der Gang zur DSB zwecks Einholung einer Genehmigung. Dabei muss allerdings nachgewiesen werden, dass sich der US-amerikanische Anbieter an die strengen Grundsätze der Richtlinie 95/46/EG hält.

Es bleibt zu hoffen, dass sich die europäischen Datenschutzbehörden um eine akkordierte und für die Unternehmen praktikable Lösung bemühen und somit den Unternehmen Rechtssicherheit geboten wird. Eine nichtakkordierte Vorgehensweise der einzelnen nationalen Datenschutzbehörden, die nunmehr die Datentransfers in die USA zu beurteilen haben, würde zu einem zersplitterten System führen und die durch die geplante DS-GVO angestrebte Vollharmonisierung des europäischen Datenschutzrechts konterkarieren.

2. Die neue Standardanwendung SA037 „Melde- und Kontrollsysteme zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung“

Mit BGBl. II 2015/278 vom 25. September 2015 wurde der Standard- und Musterverordnung 2004 (StMV 2004) eine neue Standardanwendung mit der Bezeichnung SA037 *Melde- und Kontrollsysteme zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung* hinzugefügt. Diese Datenanwendung betrifft alle Berufsgruppen/Institutionen, die nach folgenden Gesetzen bei Verdacht auf Geldwäsche verpflichtet sind, diesen an die beim BM für Inneres, Generaldirektion für die öffentliche Sicherheit, Bundeskriminalamt, Josef-Holaubek-Platz 1, 1090 Wien, angesiedelte Geldwäschemeldestelle zu melden:

- Bankwesengesetz
- Bilanzbuchhaltungsgesetz
- Börsegesetz 1989
- Finanzstrafgesetz
- Gewerbeordnung 1994
- Glückspielgesetz
- Körperschaftssteuergesetz 1988
- Notariatsordnung
- Rechtsanwaltsordnung
- Versicherungsaufsichtsgesetz
- Wertpapieraufsichtsgesetz 2007
- Wirtschaftstreuhandberufsgesetz
- Zahlungsdienstegesetz und
- Zollrechts-Durchführungsgesetz

Die SA037 lautet wie folgt:

SA037 Melde- und Kontrollsysteme zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung

Zweck der Datenanwendung:

Verarbeitung von Daten durch die gesetzlich verpflichteten Stellen und Übermittlung an die Geldwäschemeldestelle des Bundeskriminalamts (§ 4 Abs. 2 Z 1 und 2 des Bundeskriminalamt-Gesetzes (BKA-G), BGBl. I Nr. 22/2002) zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung sowie die Führung archivierter Textdokumente (wie zB Korrespondenz) in diesen Angelegenheiten.

Rechtsgrundlagen der Anwendung sind insbesondere die folgenden Gesetze und Verordnungen sowie zwischenstaatliche Abkommen (in der geltenden Fassung):

Bankwesengesetz (BWG), BGBl. Nr. 532/1993, Börsegesetz 1989 (BörseG), BGBl. Nr. 555/1989, Wertpapieraufsichtsgesetz 2007 (WAG 2007), BGBl. I Nr. 60/2007, Versicherungsaufsichtsgesetz (VAG), BGBl. Nr. 569/1978, Gewerbeordnung 1994 (GewO 1994), BGBl. Nr. 194/1994, Körperschaftsteuergesetz 1988 (KStG 1988), BGBl. Nr. 401/1988, Glücksspielgesetz (GSpG), BGBl. Nr. 620/1989, Rechtsanwaltsordnung (RAO), RGBl. Nr. 96/1868, Notariatsordnung (NO), RGBl. Nr. 75/1871, Wirtschaftstreuhandberufsgesetz (WTBG), BGBl. I Nr. 58/1999, Bilanzbuchhaltungsgesetz 2014 (BiBuG 2014), BGBl. I Nr. 191/2013, Zahlungsdienstegesetz (ZaDiG), BGBl. I Nr. 66/2009, sowie das Zollrechts-Durchführungsgesetz (ZollR-DG), BGBl. Nr. 659/1994.

Höchstdauer der zulässigen Datenaufbewahrung:

Entsprechend den gesetzlichen Aufbewahrungsfristen.

Betroffene Personengruppen:	*Nr.:*	*Datenarten:*	*Empfängerkreise:*
Meldende Stellen:	*01*	*Bezeichnung*	*1*
	02	*Zeichen*	*1*
	03	*Kontaktdaten*	*1*
	04	*Ort und Datum der Meldung*	*1*
	05	*Betreff*	*1*
Verdächtige/überprüfte natürliche Personen:	*06*	*Name*	*1*
	07	*Geburtsdatum*	*1*

Betroffene Personengruppen:	*Nr.:*	*Datenarten:*	*Empfängerkreise:*
	08	*Geburtsort*	*1*
	09	*Wohnanschrift*	*1*
	10	*Staatsbürgerschaft*	*1*
	11	*Art des Ausweises*	*1*
	12	*Nummer des Ausweises*	*1*
	13	*Ausstellung des Ausweises (Behörde, Datum)*	*1*
	14	*Erreichbarkeit*	*1*
	15	*Bankverbindung/Kontounterlagen*	*1*
	16	*Einstufung als „Politically exposed Person(s)“ (PeP)*	*1*
	17	*Geschäft auf eigene/fremde Rechnung*	*1*
	18	*Grund der Meldung*	*1*
	19	*Rechtsgrundlage der Meldung*	*1*
	20	*Geschäftsfall/Transaktion (laufend, unmittelbar bevorstehend, bereits gelaufen)*	*1*
	21	*Art und Datum des Geschäftes/Transaktion*	*1*
	22	*Währung*	*1*
	23	*Betrag*	*1*
	24	*Aktueller Saldo*	*1*
	25	*Begründung/Sachverhalt*	*1*
	26	*Unterlagen*	*1*
Verdächtige/überprüfte juristische Personen oder Personengemeinschaften:	*27*	*Bezeichnung der juristischen Person oder Personengemeinschaft*	*1*
	28	*Registerdaten (zB Firmenbuch, Zentrales Vereinsregister)*	*1*
	29	*Sitz der juristischen Person oder Personengemeinschaft (Erklärung über Sitz der zentralen Verwaltung)*	*1*
	30	*Vertretungsbefugnis (geeignete Bescheinigungen)*	*1*
	31	*Identität des wirtschaftlichen Eigentümers*	*1*
	32	*Art des Ausweises*	*1*
	33	*Nummer des Ausweises*	*1*
	34	*Ausstellung des Ausweises (Behörde, Datum)*	*1*
	35	*Bankverbindung/Kontounterlagen*	*1*
	36	*Geschäft auf eigene/fremde Rechnung*	*1*
	37	*Grund der Meldung*	*1*
	38	*Rechtsgrundlage der Meldung*	*1*
	39	*Geschäftsfall/Transaktion (laufend, unmittelbar bevorstehend, bereits gelaufen)*	*1*
	40	*Art und Datum des Geschäftes/Transaktion*	*1*
	41	*Währung*	*1*
	42	*Betrag*	*1*
	43	*Aktueller Saldo*	*1*
	44	*Begründung/Sachverhalt*	*1*
	45	*Unterlagen*	*1*
Treugeber:	*46*	*Identität des Treugebers*	*1*
	47	*Schriftliche Erklärung des Treuhänders/Treuhandvertrag*	*1*
	48	*Bankverbindung/Kontounterlagen*	*1*

Empfängerkreis:

1 Geldwäschemeldestelle des Bundeskriminalamts (§ 4 Abs. 2 Z 1 und 2 BKA-G).

3. Empfehlung der Datenschutzbehörde – Aktualisierungspflicht DVR

Die Empfehlung der DSB vom 1. Juli 2015, DSB-D215.814/0003-DSB/2015 lautet wie folgt:

Aktualisierungspflicht DVR, VDS-Datenanwendungen sind zu streichen

Empfehlung der DSB vom 1. Juli 2015, DSB-D215.814/0003-DSB/2015

Anlässlich eines Kontrollverfahrens hat die DSB einem Unternehmen aus der Branche der Kommunikationsdienstleister folgende Empfehlungen erteilt:

1. Datenanwendungen (DAN), die ausschließlich die Durchführung der vom Verfassungsgerichtshof aufgehobenen Vorratsdatenspeicherung (VDS) zum Gegenstand hatten, wären nach dem 1. Juli 2014 unverzüglich durch Änderungsmeldung aus dem DVR zu streichen gewesen. Dass für die VDS eingeführte Software (Durchlaufstelle zu den Sicherheitsbehörden gemäß DSVO) noch verwendet wird, ist nicht entscheidend.

2. Die DVR-Eintragung muss aktuell gehalten werden, Änderungen der Firma (hier: aus einer Aktiengesellschaft wurde schon vor Jahren eine Ges.m.b.H.) sind unverzüglich zu melden.

Die DSB hielt allgemein fest, dass „das DVR jedermann ein wahrheitsgemäßes, der Realität der meldepflichtigen Datenverwendung durch einen datenschutzrechtlichen Auftraggeber bestmöglich angenähertes Bild bieten soll" und daher vom Auftraggeber regelmäßig zu prüfen und zu aktualisieren ist.

Diese Empfehlung ist innerhalb der gesetzten Dreitagesfrist umgesetzt worden.

Abschließend zu dieser Empfehlung ist darauf hinzuweisen, dass die DSB gem. § 22a DSG 2000 jederzeit die Erfüllung der Meldepflicht prüfen kann. Bei Verdacht der Nichterfüllung infolge der Mangelhaftigkeit oder Unterlassung einer Meldung kann ein Verfahren zur Berichtung des Datenverarbeitungsregisters durchgeführt werden.

Wird einem Verbesserungsauftrag nicht entsprochen, so kann die DSB mit Bescheid die Streichung der Meldung verfügen. Wird weiters einer Aufforderung zur Nachmeldung nicht Folge geleistet, so kann die DSB sogar den weiteren Betrieb der Datenanwendung untersagen und gleichzeitig eine Anzeige gem. § 52 Abs. 2 Z 1 DSG 2000 an die zuständige Behörde (Magistrat bzw. Bezirkshauptmannschaft) erstatten. Dieses Vergehen kann eine Verwaltungsstrafe in Höhe bis zu EUR 10.000 nach sich ziehen.

Da es sich bei DVR-Online um ein öffentliches Register handelt, in dem jeder sowohl den Registerauszug wie auch die einzelnen Datenanwendungen einsehen kann, empfiehlt sich schon aus Imagegründen eine entsprechende Aktualisierung des Meldebestandes.

••••