
COMPUTERWOCHE
VON IDG

Datenschutzabkommen verabschiedet

EU-US-Privacy Shield beerbt Safe Harbor

von Dr. Michael Rath, Simone Bach

Foto: jijomathaidesigners - shutterstock.com

Inhalt

Datenschutzabkommen verabschiedet

EU-US-Privacy Shield beerbt Safe Harbor

von Dr. Michael Rath, Simone Bach

Die Europäische Kommission hat das umstrittene EU-US-Privacy-Shield-Abkommen formell verabschiedet.

Trotz heftiger Kritik an der im Februar dieses Jahres bekannt gewordenen ersten Version einer Nachfolgeregelung für das im Oktober 2015 vom EuGH in der Sache Maximillian Schrems [1] v. Data Protection Commissioner (C-362/14) gekippte Safe-Harbor-Abkommen [2] wurde das sogenannte EU-US-Privacy Shield heute mit nur wenigen punktuellen Änderungen durch die Europäische Kommission formell verabschiedet. Zuvor hatten bereits am 8. Juli 2016 die EU-Mitgliedsstaaten in der sog. Art. 31 Gruppe mehrheitlich ihre Zustimmung zu der Nachfolgeregelung erteilt. Das Privacy Shield [3] kann zukünftig - vorbehaltlich der Anerkennung durch die nationalen Aufsichtsbehörden - zur Legitimation eines Datentransfers in die USA herangezogen werden.

EuGH hatte Safe-Harbor-Abkommen gekippt

Im Herbst 2015 hatte der EuGH das sogenannte Safe-Harbor-Abkommen [4], auf dessen Grundlage europäische Unternehmen personenbezogene Daten in die USA übermitteln durften, für ungültig erklärt, weil es keine hinreichende Garantie für den Schutz der übermittelten Daten - unter anderem vor unerlaubten Zugriffen durch US-Behörden - gewährleistete. Insbesondere habe es an einer Kontrolle und Durchsetzung der ausgehandelten Datenschutzstandards [5] gefehlt und betroffene Personen hätten keinerlei Möglichkeit gehabt, ihre Betroffenenrechte (Ansprüche auf Auskunft, Berichtigung und Löschung) in den USA durchzusetzen. Bereits im Februar 2016 hatte die Europäische Kommission einen ersten Entwurf einer Nachfolgeregelung für das Safe-Harbor-Abkommen veröffentlicht. Europäische Datenschützer sahen jedoch die oben genannten Kritikpunkte des EuGH hierin als nur unzureichend berücksichtigt; dementsprechend forderte auch etwa die sog. Art. 29 Gruppe umfangreiche Nachbesserungen [6].

Hohes Datenschutz-Niveau durch das neue Privacy Shield?

Nach Meinung der Europäischen Kommission vom 8. Juli 2016 [7] gewährleistet das neue EU-U.S. Privacy Shield ein hohes Datenschutzniveau zugunsten betroffener Personen sowie Rechtssicherheit für datenverarbeitende Unternehmen. Das Privacy Shield unterscheide sich fundamental von der Vorgängerregelung Safe Harbor, da es datenverarbeitenden Unternehmen in den USA klare und verbindliche Vorgaben zum Umgang mit den Daten auferlege und für deren Kontrolle und Durch-

1 http://www.computerwoche.de/a/eugh-prueft-datenschutz-regeln-fuer-facebook-und-co,3096285
2 http://www.computerwoche.de/a/ist-das-eu-us-privacy-shield-nur-bullshitbingo,3222900
3 http://www.computerwoche.de/a/ist-das-eu-us-privacy-shield-nur-bullshitbingo,3222900
4 http://www.computerwoche.de/a/anwender-wollen-gar-keine-deutsche-cloud,3216698
5 http://www.computerwoche.de/a/der-neue-eu-datenschutz-ab-2018-alles-wichtige,3226704
6 http://www.bvdw.org/mybvdw/media/download/art29gruppe-privacy-shield-en.pdf?file=3869
7 http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm

setzung sorge. Zudem habe die USA erstmalig schriftlich zugesagt, dass öffentliche Stellen, einschließlich Geheimdienste, nur unter bestimmten, engen Voraussetzungen auf personenbezogene Daten europäischer Bürger zugreifen dürfen und eine willkürliche Massenüberwachung ausgeschlossen sei.

[Hinweis auf Bildergalerie: EU-Datenschutzreform 2016: Die wichtigsten Änderungen] gal1

Überwachung durch US-Geheimdienste weiterhin möglich

Ob die jetzt verabschiedete Version des Privacy Shields künftig ein angemessenes Schutzniveau in den USA gewährleisten kann, darf jedoch bezweifelt werden. Denn trotz punktueller Nachbesserungen dürfte der Mehrwert des Nachfolgeabkommens eher gering sein. Zwar entsprechen die ausgehandelten Standards europäischen Anforderungen an einen ausreichenden Datenschutz [8]. Auch ist eine stärkere Kontrolle der Einhaltung der Vorschriften und Sanktionierung von Verstößen vorgesehen. Jedoch ändert das neue Abkommen nichts an der geltenden Gesetzeslage in den USA, die Ermittlungsbehörden und Geheimdiensten umfangreiche Überwachungsbefugnisse [9] einräumt. Zudem sieht das Privacy Shield explizit Ausnahmen für die zwingende Befolgung der neuen Datenschutzstandards vor, nämlich unter anderem soweit ein Gesetz dies erlaubt oder die Missachtung der Grundsätze aus Gründen der nationalen Sicherheit, zum Zwecke der Rechtsdurchsetzung oder aus anderen öffentlichen Interessen erforderlich ist.

Da hilft es auch wenig, wenn die USA der Europäischen Kommission schriftlich zusagen, dass eine willkürliche Massenüberwachung europäischer Bürger zukünftig nicht mehr stattfinde, denn der Begriff der "Überwachung" wird durch europäische und US-amerikanische Stellen bereits grundlegend unterschiedlich definiert: Die USA halten eine "bulk collection [10]" von Daten für zulässig (auch wenn eine gezielte Datenerhebung in Bezug auf konkrete Einzelpersonen die Regel sein soll) und beschränken erst die eigentliche Auswertung der Daten.

Nach europäischem Datenschutzrecht unterliegen bereits die Erhebung und Speicherung der Daten dem strengen Erlaubnisvorbehalt und Zweckbindungsgrundsatz. Auf der Grundlage des Foreign Intelligence Surveillance Acts (FISA) [11] oder des National Security Letters [12] kann daher auch zukünftig eine umfangreiche Erhebung und Auswertung personenbezogener Daten europäischer Personen stattfinden.

[Hinweis auf Bildergalerie: Was Unternehmen zur EU-Datenschutzreform beachten müssen] gal2

Die Aufsichtsbehörden haben das letzte Wort

Zudem bleibt abzuwarten, wie die nationalen Aufsichtsbehörden auf das neue Abkommen reagieren werden. Der EuGH hatte in seinem Urteil explizit darauf hingewiesen, dass es originäre Aufgabe der Aufsichtsbehörden sei, die Einhaltung europäischen Datenschutzrechts [13] zu überwachen und zu

8 http://www.computerwoche.de/a/datenschutz-uebertreiben-wir-es-in-deutschland,3217898
9 http://www.computerwoche.de/a/privatsphaere-oder-sicherheit,3098203
10 http://edition.cnn.com/2015/11/28/us/nsa-ends-bulk-phone-surveillance/
11 https://de.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act
12 https://de.wikipedia.org/wiki/National_Security_Letter
13 http://www.computerwoche.de/a/datenschutz-nach-dem-brexit,3313019

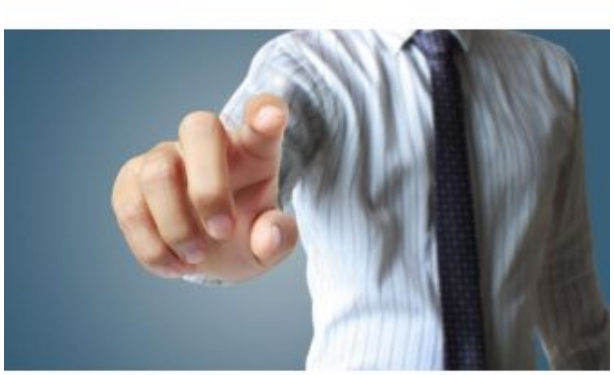
kontrollieren. Diese Kompetenz sei keineswegs durch eine Angemessenheitsentscheidung der Europäischen Kommission eingeschränkt. Demnach ist es also allen europäischen Aufsichtsbehörden zukünftig möglich, Datenübermittlungen in die USA auf der Grundlage des neuen EU-US-Privacy Shields zu untersagen. Darüber hinaus bleibt mit Spannung abzuwarten, wie der EuGH auf eine - wahrscheinliche - erneute Vorlage durch nationale Gerichte, die mit Klagen gegen Datenübermittlungen in die USA auf der Grundlage des EU-US-Privacy Shields befasst sind, reagieren wird. (fm)

Bildergalerien im Artikel:

gal1EU-Datenschutzreform 2016: Die wichtigsten Änderungen

Ein Gesetz für alle
EU-weit gelten die gleichen Datenschutzregeln. Das bedeutet auch eine gestiegene Verantwortung und Haftung für alle, die persönliche Daten verarbeiten.
Foto: Yvonne Bogdanski - Fotolia.com

"Recht auf Vergessen"
Wollen Nutzer ihre Daten nicht weiter verarbeitet sehen, werden diese gelöscht - vorausgesetzt, es spricht aus juristischer Sicht nichts dagegen.
Foto: Anson/Fotolia.com



"Opt-in" statt "Opt-out"
Sollen persönliche Daten verabeitet werden, müssen Nutzer aktiv zustimmen (und nicht aktiv widersprechen wie bisher).
Foto: violetkaipa - Fotolia.com

Recht auf Transparenz
Nutzer haben ein Recht auf Transparenz - sie dürfen erfahren, welche Daten über sie gesammelt und wie diese verarbeitet werden.
Foto: Kritchanut - www.shutterstock.com

Zugang und Portabilität
Der Zugang zu den bei Dritten über einen selbst gespeicherten Daten soll einfacher möglich sein. Zudem ist die Dartenportabilität zu gewährleisten - also sicherzustellen, dass persönliche Informationen leichter von einem Dienstanbieter zu einem anderen übertragen werden können.
Foto: Doc Rabe Media, Fotolia.com

Schnellere Meldung
Tritt ein Datenverlust auf, müssen Unternehmen und Organisationen im Regelfall binnen 24 Stunden, mindestens aber so schnell wie möglich ihrer behördlichen Meldepflicht nachkommen.
Foto: kantver/Fotolia

Weniger Behördenchaos
Unternehmen müssen sich nur noch mit einer einzigen Aufsichtsbehörde auseinandersetzen - und zwar dort, wo sie ihren Hauptsitz haben.
Foto: Firma V - Fotolia.com

Grenzübergreifend
Privatanwender dürfen jeden Fall von Datenmissbrauch an ihre nationale Aufsichtsbehörde melden - selbst dann, wenn die betroffenen Daten im Ausland verarbeitet wurden.
Foto: R. Schramm - Fotolia.com

Erweiterter Geltungsbereich
Die EU-Richtlinie gilt auch für Unternehmen, die keinen Sitz in der EU haben, sobald sie Waren oder Dienstleistungen in der EU anbieten oder auch nur Online-Marktforschung unter EU-Bürgern betreiben.
Foto: WavebreakMediaMicro - Fotolia.com

Höhere Bußgelder
Verstößt ein Unternehmen gegen die Datenschutzbestimmungen, droht ein Bußgeld in Höhe von bis zu vier Prozent des Jahresumsatzes.
Foto: rangizzz - Fotolia.com

Bürokratieabbau
Administrative Umstände wie Meldepflichten für Unternehmen, die persönliche Daten verarbeiten, entfallen.
Foto: Jochen Binikowski - Fotolia.com

Erst ab 16
Die rechtswirksame Anmeldung bei Internetnetservices wie Facebook oder Instagr.am soll Jugendlichen im Regelfall erst ab 16 Jahren möglich sein - weil sie erst ab diesem Lebensalter eine gültige Einwilligung in die Verarbeitung ihrer persönlichen Daten geben können. Nationale Gesetze sollen laut Datenschutzverordnung hier aber Ausnahmen möglich machen.
Foto: Sergey Novikov - www.shutterstock.com

Stärkung der nationalen Aufsichtsbehörden
Nationale Datenschutzbehörden werden in ihren Kompetenzen gestärkt, so dass sie die neuen EU-Regeln besser umsetzen können. Unter anderem dürfen sie einzelnen Unternehmen verbieten, Daten zu verarbeiten. können bestimmte Datenflüsse stoppen und Bußgelder gegen Unternehmen verhängen, die bis zu zwei Prozent der jeweiligen weltweiten Jahreseinkünfte betragen. Darüber hinaus dürfen sie Gerichtsverfahren in Datenschutzfragen anstrengen.

(Quelle: Forrester Research)
Foto: Martin Fally - Fotolia.com

gal2Was Unternehmen zur EU-Datenschutzreform beachten müssen

Was Unternehmen zur EU-Datenschutzreform beachten müssen
Es ist wohl nur noch eine Frage von Wochen und Monaten, bis die neue EU-Datenschutzverordnung in Kraft tritt. Was bedeutet das für die Unternehmen? Was müssen sie wissen? Marco Schmid, Country Manager DACH beim Webhoster Rackspace, gibt Tipps.
Foto: Maksim Kabakou - shutterstock.com

Einwilligung
Unternehmen müssen sicherstellen, dass sie über eine unmissverständliche Einwilligung zur Verarbeitung personenbezogener Daten verfügen, sowohl von Kunden als auch von Mitarbeitern. Von dieser Neuerung sind vor allem Firmen im Consumer-Bereich betroffen, die alle Daten aus ihren Kunden-Datenbanken löschen müssen, für die kein Einverständnis vorliegt. So ist es beispielsweise nicht zulässig, die Daten von Frau Mustermann, die vor zehn Jahren Socken für ihren Mann gekauft hat, weiterhin zu speichern. Marketingabteilungen müssen zukünftig in der Lage sein, Anfragen von Kunden zu berücksichtigen, die um die Löschung ihrer persönlichen Daten bitten oder wollen, dass ihre Daten nicht weiter genutzt werden.
Foto: Robert Kneschke - Fotolia.com

"Recht auf Vergessen"
Die meisten Unternehmen konzentrieren sich erfolgreich darauf, Daten zu sammeln – aber die wenigsten darauf, sie auch wieder aus ihren Systemen zu löschen. Dies wird eine Herausforderung für viele Firmen, sobald Googles „Recht auf Vergessen“ zum Tragen kommt. Eventuell ist die Anonymisierung von Daten eine Alternative für Unternehmen, die es sich leisten können.
Foto: Lightspring - shutterstock.com

Technische und organisatorische Maßnahmen
Ein weiterer wichtiger Aspekt ist die Sicherheit der IT-Systeme vor ungewollten Zugriffen. Setzen Unternehmen geeignete Kontrollen ein, um Kunden- und Personaldaten zu schützen – und das solange es erforderlich ist und ohne dass die Gefahr eines unbeabsichtigten Verlusts entsteht? Ist überhaupt bekannt, warum solche Daten gespeichert werden – geschieht es einfach nur wegen der legitimen Absicht, sie weiter zu verarbeiten? Indem Unternehmen diese Fragen beantworten, bereiten sie sich technisch und organisatorisch auf die Einführung der neuen Datenschutz-Verordnung vor.
Foto: alphaspirit - shutterstock.com

Anzeige bei Verstößen
Unternehmen, die Daten verarbeiten, sind dazu verpflichtet, Verstöße gegen die Datensicherheit den zuständigen Datenschutz-Behörden und den Betroffenen innerhalb von 72 Stunden zu melden, wenn der Verstoß zu hohen Risiken führt. Daher müssen Unternehmen zuverlässige Reaktionsprozesse zum Incident Management etablieren, mit denen sie dieser Verpflichtung nachkommen können.
Foto: vector illustration - shutterstock.com

Umsetzung und Strafen
Wenn ein Unternehmen aus irgendeinem Grund gegen die Datenschutz-Verordnung verstößt, kann die zuständige Behörde eine Strafe von bis zu einer Million Euro oder zwei Prozent des jährlichen Umsatzes fordern.
Foto: Suzanne Tucker - shutterstock.com

12.07.2016