Zeitschrift für Datenrecht und Informationssicherheit

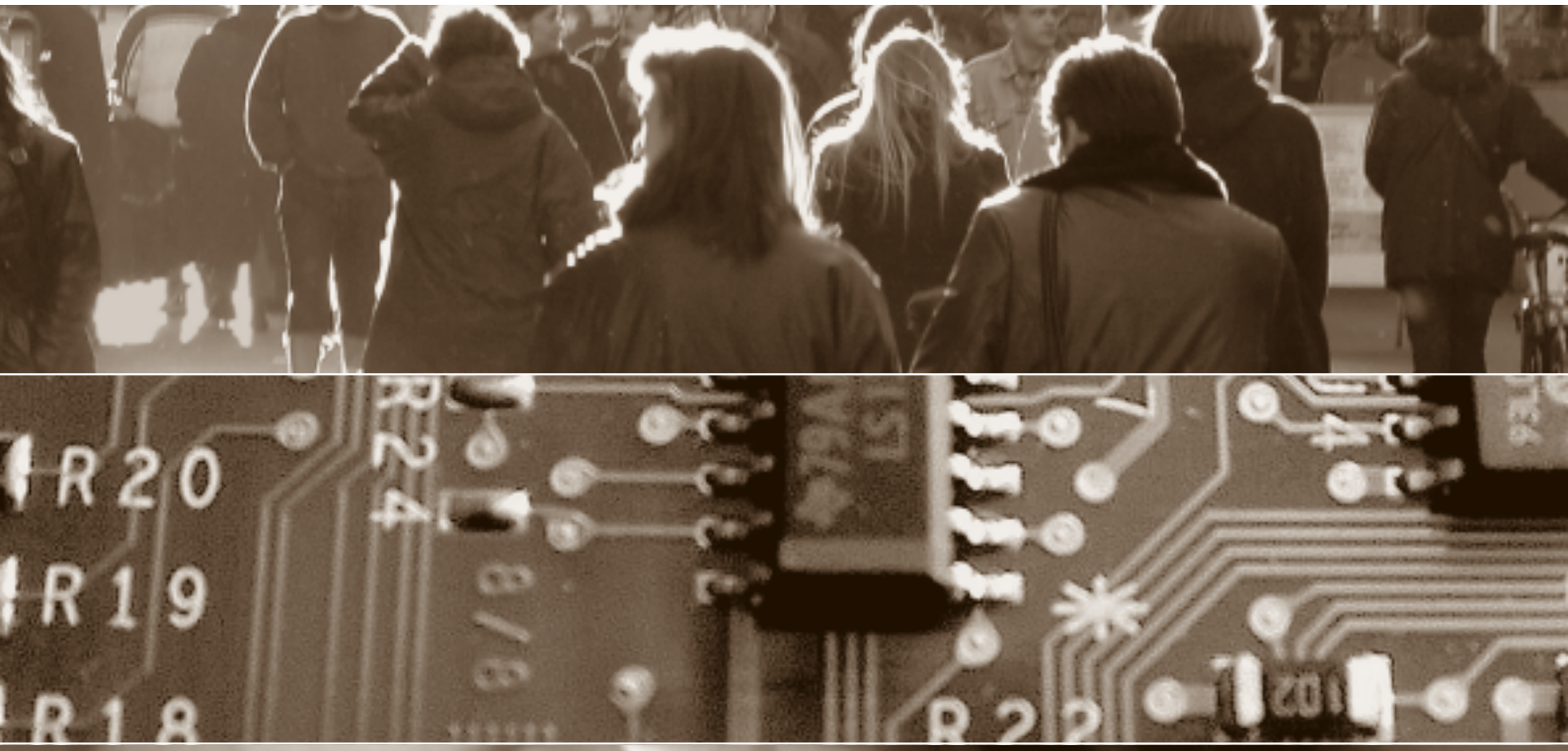
digma

www.digma.info 9. Jahrgang, Heft 4, Dezember 2009

Schwerpunkt:

Einwilligung

fokus: Einwilligung und ihre technische Umsetzung
report: Wunderheilmittel Videoüberwachung?
forum: Datenschutz ohne Grenzen



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

Schulthess §

inhalt

fokus

Schwerpunkt:
Einwilligung

Vertrauen muss man nicht lernen

Es ist viel von Vertrauen und Vertrauensverlust die Rede. Müssen wir (wieder) lernen zu vertrauen? Der stellvertretende Chefredaktor der Neuen Zürcher Zeitung meint nein, nicht vertrauen muss man lernen, sondern misstrauen. Das stimme hoffnungsvoll – stimmt!

Konsens über alles – koste es, was es wolle?

Soll ein Einzelner in souveräner Willkür bewirken können, dass relevante Forschung unterbleibt und gesellschaftlicher Schaden entsteht, obwohl auf seiner Seite kein nachvollziehbares Interesse entgegensteht? Der Kriminologe hinterfragt den Grundsatz der Einwilligungsforschung mit Beispielen aus der Sozialforschung.

Einwilligung und ihre technische Umsetzung

Obwohl das Prinzip der Einwilligung ein tragendes Element des heutigen Datenschutzes ist, wurde nur wenig Fortschritt in seiner technischen Umsetzung gemacht. Die adäquate Behandlung der Einwilligung stellt eine gravierende praktische Herausforderung dar. Wie können Individuen in die Lage versetzt werden, ihre Einwilligung zum Gebrauch ihrer persönlichen Daten unmissverständlich auszudrücken und diese, wenn gewünscht, auch wieder zurückzuziehen? Auf der anderen Seite müssen Datenverarbeiter in der Lage sein festzustellen, ob für gewisse Informationen der Besitzer eingewilligt hat oder ob dafür eine Einwilligung benötigt wird.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Zustelladresse: Redaktion digma, per Adr. Datenschutzbeauftragter des Kantons Basel-Stadt, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, Fax +41 (0)61 201 16 41, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 99.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

Wunderheilmittel Videoüberwachung?

Videoüberwachung boomt. Zwar wird eine gesetzliche Grundlage verlangt – doch bloss formale Regelungen reichen nicht aus. Der Zweck muss im Mittelpunkt stehen, damit vorher die Verhältnismässigkeit beurteilt und hinterher die Wirksamkeit evaluiert werden kann.

Private Überwachung im öffentlichen Raum

Private können sich gegen Videoüberwachung durch andere Private nur auf dem zivilrechtlichen Weg zur Wehr setzen. Die Statuierung einer Bewilligungspflicht für gesteigerten Gemeingebrauch würde es den Behörden ermöglichen, Überwachungen, welche nicht mehr bestimmungsgemäss und gemeinverträglich sind, kontrolliert zuzulassen.

Datenschutz ohne Grenzen

Der Safe-Harbor-Beitrag in digma 2009.3 lädt zu einer vertieften Auseinandersetzung mit dem Thema der grenzüberschreitenden Datenbekanntgabe ein. Der Beitrag legt die wichtigsten Punkte dar, die bei der Überprüfung der Rechtmässigkeit einer solchen Datenbekanntgabe zu beachten sind.

report

forum

Follow-up: Safe Harbor

Datenschutz ohne Grenzen

lic. iur. Barbara Widmer LL.M./CIA, Doktorandin, Juristin beim Datenschutzbeauftragten des Kantons Basel-Stadt, Basel barbara.widmer@dsb.bs.ch

Dr. oec. Marc Frédéric Schäfer, lic. iur. HSG, Juristischer Mitarbeiter beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, Bern marc-frederic.schaefer@edoeb.admin.ch

«Das beste Mittel, Informationen zu erhalten, ist, Informationen zu geben.»[1]

Das Prinzip des vorgenannten Zitats dürfte, wenn auch auf den ersten Blick oft nicht erkennbar, für einen Grossteil der stattfindenden Datenbekanntgaben ausgeprägte Motivation sein. – Dies insbesondere in einer globalisierten Welt, wo Information und Wissen entscheidende Wettbewerbsvorteile bedeuten und wirtschafts- und sicherheitspolitisch von immenser Bedeutung sind. Vor diesem Hintergrund geht leicht vergessen, dass eine Bekanntgabe von Daten für die Betroffenen eine erhebliche Gefahr darstellen kann: Denn diesen wird dadurch die Kontrolle darüber, wer welche Informationen zu welchem Zweck über sie bearbeitet, weitgehend entzogen. Bei einer grenzüberschreitenden Bekanntgabe von Personendaten potenziert sich diese Gefahr insofern, als die Daten den territorialen Geltungsbereich der Gesetzgebung, unter welcher sie erhoben und bis anhin bearbeitet wurden, verlassen und in den territorialen Geltungsbereich einer neuen (unbekannten) Gesetzgebung gelangen. Umso wichtiger ist es, eine (grenzüberschreitende) Bekanntgabe von Personendaten sorgfältig auf ihre Rechtmässigkeit zu überprüfen. Nachfolgend sollen die wichtigsten in diesem Zusammenhang zu beachtenden Punkte aufgezeigt werden, wobei aus Gründen der praktischen Relevanz eine Fokussierung auf Art. 6 Abs. 1, Abs. 2 lit. a und g sowie Abs. 3 DSG[2] stattfindet – unter besonderer Berücksichtigung des Safe-Harbor-Abkommens zwischen der Schweiz und den USA[3].

Geltung und Grundsätze von Art. 6 DSG

Art. 6 DSG richtet sich aufgrund der Gesetzessystematik[4] sowohl an Bundesorgane[5] als auch an private Personen (natürliche und juristische[6] – Ausnahme Art. 2 Abs. 2 lit. e DSG) und kommt bei folgenden grenzüberschreitenden Sachverhalten zur Anwendung: wenn Bundesorgane oder private Personen Personendaten an

- öffentliche Organe aller Ebenen und/oder
- private natürliche und juristische Personen

im Ausland bekannt geben.

Keine Rolle im Anwendungsbereich von Art. 6 DSG spielen Anknüpfungskriterien wie Wohnsitz/Sitz oder Staatsangehörigkeit. In sachlicher Hinsicht umfasst Art. 6 DSG die grenzüberschreitende Bekanntgabe von Daten über natürliche und juristische Personen zu personenbezogenen Zwecken.

Art. 6 Abs. 1 DSG hält im Sinne eines Grundsatzes fest, dass Personendaten nur dann ins Ausland bekannt gegeben werden dürfen, wenn dadurch die Persönlichkeit der betroffenen Personen nicht schwerwiegend gefährdet wird, namentlich, weil eine Gesetzgebung mit angemessenem Schutz fehlt. Das DSG definiert die Begriffe Personendaten und Bekanntgeben (Art. 3 lit. a, c, d und f DSG), nicht aber, wann eine schwerwiegende Persönlichkeitsverletzung vorliegt und was unter einer Gesetzgebung mit angemessenem Schutz zu verstehen ist.

Daten können aus datenschutzrechtlicher Sicht (unabhängig, ob grenzüberschreitend oder nicht) in unterschiedlicher Form bekannt gegeben werden – so z.B. aktiv durch Transfer oder passiv durch Einsichtgewährung (in Papierform oder mittels Online-Zugriff auf Datensammlungen)[7]. Im Weiteren stellt auch ein Datenaustausch innerhalb derselben juristischen Person oder innerhalb einer Konzernstruktur eine datenschutzrechtlich relevante Bekanntgabe dar[8]. Ist die Datenbekanntgabe grenzüberschreitend, sind neben den allgemeinen, vom DSG für eine rechtmässige Bekanntgabe geforderten Vorgaben (Datenbearbeitung darf zu keiner widerrechtlichen Persönlichkeitsverletzung führen) die Vor-

aussetzungen von Art. 6 DSG zu beachten.

Die Fiktion einer schwerwiegenden Persönlichkeitsverletzung ist aufgrund der Formulierung von Art. 6 Abs. 1 DSG von Gesetzes wegen dann gegeben, wenn die Bekanntgabe von Daten in ein Land ohne eine Gesetzgebung mit angemessenem Schutz erfolgt. Gleiches gilt, wenn ein Land zwar über eine Gesetzgebung mit angemessenem Schutz verfügt, diese in der Praxis jedoch nicht umbzw. durchsetzt[9].

Einen angemessenen Schutz weist eine Gesetzgebung dann auf, wenn sie den Anforderungen der Europaratskonvention 108[10] (ERK 108) entspricht. Diese bezweckt im privaten und öffentlichen Sektor die Verstärkung des Rechtsschutzes des Einzelnen bei der automatischen Verarbeitung von Personendaten (vgl. Art. 1 ERK 108). Sie soll einerseits in allen Mitgliedstaaten ein Minimum an Persönlichkeitsschutz und eine gewisse Harmonisierung der Schutzsysteme sicherstellen sowie andererseits den internationalen Datenverkehr dahingehend gewährleisten, als keine Vertragspartei den Informationstransfer an eine andere Vertragspartei, deren Gesetzgebung den Mindestschutz gemäss ERK 108 erfüllt, untersagen darf[11]. Beitreten können der ERK 108 Mitgliedstaaten des Europarats und damit auch nicht EU-Mitgliedstaaten. Für die Schweiz ist die ERK 108 am 1. Februar 1998 in Kraft getreten.

Gemäss Art. 7 VDSG[12] veröffentlicht der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) eine Liste der Staaten[13], deren Gesetzgebung einen angemessenen Schutz gewährleistet. Allerdings erfüllt eine Grosszahl der Gesetzgebungen der in dieser Liste aufgeführten Staaten die Anforderungen gemäss ERK 108 nur in Bezug auf die Bekanntgabe von Daten über natürliche Personen. Bei einer Bekanntgabe von Daten über juristische Personen kann nur dann von einem entsprechenden Schutz ausgegangen werden, wenn dies in der genannten Liste ausdrücklich vermerkt ist – so z.B. im Fall von Italien, Liechtenstein, Luxemburg, Österreich oder eingeschränkt im Fall von Dänemark und Argentinien. Jedoch kann eine Datenbekanntgabe ins Ausland, wie die folgenden Ausführungen zeigen werden, unter bestimmten Voraussetzungen auch dann zulässig sein, wenn Art 6 Abs. 1 DSG nicht erfüllt ist.

Garantien nach Art. 6 Abs. 2 DSG

Das DSG sieht in Art. 6 Abs. 2 eine Reihe von Fällen und Massnahmen vor, aufgrund welcher ein Datentransfer ins Ausland trotz fehlender Gesetzgebung mit angemessenem Schutz zulässig ist: Dies sind im Speziellen

- die Vereinbarung von hinreichenden Garantien, insbesondere durch Vertrag, die einen angemessenen Schutz im Ausland gewährleisten (Art. 6 Abs. 2 lit. a DSG), und
- bei einer Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, das Vorhandensein von so genannten Corporate Binding Rules, die einen angemessenen Schutz gewährleisten (Art. 6 Abs. 2 lit. g DSG).

Bei den genannten Garantien kommt es nicht auf die Form der Klauseln, sondern lediglich auf deren Inhalt an. Sie müssen insbesondere einen ausreichenden Schutz aufgrund einer Vereinbarung gewährleisten[14]. In diesem Rahmen erwähnt die Botschaft zur Änderung des DSG das «Safe Harbor Privacy Framework» der EU als ein Regelwerk, welches für einen Datentransfer ins Ausland hinreichende Garantien gewährleistet[15]. In der bisherigen Praxis hat der EDÖB anerkannt, dass ein Unternehmen einen angemessenen Datenschutz gemäss Art. 6 Abs. 2 DSG gewährleistet, wenn das US-Unternehmen gegenüber dem EDÖB erklärt hat, die Grundsätze des EU Safe Harbor Frameworks[16] auch für Personendaten, die aus der Schweiz übermittelt werden, anzuwenden[17]. Andere vom EDÖB anerkannte Musterverträge sind die Standardvertragsklauseln der EU[18], der Mustervertrag des Europarates für die Sicherstellung eines angemessenen Datenschutzes im Rahmen des grenzüberschreitenden Datenverkehrs[19] sowie der Mustervertrag des EDÖB für das Outsourcing von Datenbearbeitungen ins Ausland[20]. Dem Datenexporteur steht es allerdings frei, eigene Vereinbarungen mit dem

Kurz&bündig

Zur Datenübermittlung ins Ausland muss der Datenexporteur neben den allgemeinen Datenschutzgrundsätzen für einen angemessenen Schutz der Daten im Ausland sorgen. Ein solcher kann erreicht werden, wenn das Empfängerland über ein angemessenes Datenschutzniveau verfügt oder der Datenexporteur mit dem Datenempfänger entsprechende Garantien vereinbart hat. Das Safe Harbor Framework zeigt, wie auf staatsvertraglicher Ebene ein angemessenes Schutzniveau erreicht werden kann.

Empfänger zu treffen, die einen angemessenen, mit dem DSG konformen Datenschutz gewährleisten. Er muss allerdings den EDÖB hierüber informieren.

Informationspflicht nach Art. 6 Abs. 3 DSG

Die Informationspflicht nach Art. 6 Abs. 3 DSG erlaubt es dem EDÖB, die bei einer grenzüberschreitenden Datenbekanntgabe getroffenen Schutzmassnahmen auf ihre Angemessenheit zu überprüfen[21]. Sie gilt sowohl für Bundesorgane als auch für private Personen[22]. In sachlicher Hinsicht kommt sie nur in den Fällen von Art. 6 Abs. 2 lit. a und g DSG zur Anwendung und gilt nur für die Bekanntgabe von Datensammlungen, nicht jedoch Einzelübermittlungen wie z.B. E-Mail oder Briefe[23]. Die Informationspflicht ist grundsätzlich vor der Datenbekanntgabe ins Ausland zu erfüllen. Ist dies nicht möglich, hat sie unmittelbar danach zu erfolgen (Art. 6 Abs. 1 VDSG).

Der Umfang der Informationspflicht hängt davon ab, ob die Datenübermittlung gestützt auf Musterverträge bzw. Standardvertragsklauseln, die vom EDÖB erstellt oder anerkannt sind[24], erfolgt. Ist dies der Fall, muss lediglich in allgemeiner Form über deren Verwendung informiert werden (vgl. Art. 6 Abs. 3 VDSG) und eine Prüfung im Sinn von Art. 6 Abs. 5 VDSG entfällt.

Wird die Informationspflicht vorsätzlich verletzt, werden private Personen (nicht jedoch Bundesorgane) mit Haft oder Busse bestraft (Art. 34 Abs. 2 lit. a DSG). Häufiger als eine vorsätzliche dürfte allerdings eine fahrlässige Verletzung der Informationspflicht sein, so z.B. wenn sich eine private Person ihrer diesbezüglichen Pflicht nicht bewusst ist oder diese im Einzelfall vergisst.

Das US-Swiss Safe Harbor Framework

Das US-Swiss Safe Harbor Framework[25] (Framework) trat am 16. Februar 2009 in Kraft

Fussnoten

1 Niccolò Machiavelli (1469–1527).
2 Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1.
3 Vgl. Fn. 25.
4 Art. 6 findet sich im 2. Abschnitt unter «Allgemeine Datenschutzbestimmungen».
5 Definition in Art. 3 lit. h DSG.
6 Vgl. Anwendungsbereich gemäss Art. 2 Abs. 1 DSG.
7 Botschaft DSG, BBl 1988 II 447.
8 David Rosenthal/Yvonne Jöhri, Handkommentar zum DSG, Art. 3 Bst. f DSG, Rz 75, Zürich/Basel/Genf 2008; vgl. für die grenzüberschreitende Datenbekanntgabe Art. 6 Abs. 2 lit. g DSG.
9 Botschaft Änderung DSG, BBl 2003 2128.
10 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SR 0.235.1.
11 Botschaft Änderung DSG, BBl 2003 2113.
12 Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (VDSG), SR 235.11.
13 Zu finden unter: <http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de>; Ausgabe vom 15. Mai 2008.
14 Rosenthal/Jöhri (Fn. 8), Art. 6 Abs. 2 Bst. a DSG, Rz. 38.
15 BBl 2003 2129.
16 <http://www.export.gov/safeharbor/>.
17 Rosenthal/Jöhri (Fn. 8), Art. 6 Abs. 2 Bst. a DSG, Rz. 49.
18 <http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_de.htm>.
19 <http://www.coe.int/t/f/affaires_juridiques/coop%E9ration_juridique/protection_des_donn%E9es/documents/rapports_et_%E9tudes_des_comit%E9s_de_protection_des_donn%E9es/WContratType_1992.asp#TopOfPage>.
20 <http://www.edoeb.admin.ch/dienstleistungen/00587/00966/00968/index. html?lang=de>.
21 Botschaft Änderung DSG, BBl 2003 2130.
22 Art. 6 VDSG befindet sich im 1. Kapitel unter «Bearbeiten von Personendaten durch private Personen». Für Bundesorgane verweist Art. 19 VDSG auf Art. 6 VDSG.
23 Botschaft Änderung DSG, BBl 2003 2130.
24 Vgl. Links in Fn. 16, 18, 19, 20.
25 Briefwechsel vom 1. und 9. Dezember 2008 zwischen der Schweiz und den Vereinigten Staaten von Amerika über die Schaffung eines Datenschutzrahmenwerkes zur Übermittlung von personenbezogenen Daten in die Vereinigten Staaten von Amerika (US-Swiss Safe Harbor Framework; SR 0.235.233.6. <http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de>.
26 Safe-Harbor-Dokumente (vollständiger Briefwechsel zwischen den USA und der Schweiz); <http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de&download=M3wBPgDB/8uIl6Du36WenojQ1NTTjaXZnqWfVpzLhmfhnapmmc7Zi6rZnqCkkIN1e3d+bKbXrZ6lhuDZz8mMps2gpKfo)>.
27 Oliver (2002), Safe Harbor: An Alternative Regulatory Model in R. Pedler (Ed.), European Union Lobbying (pp. 13–34). New York: Palgrave.
28 Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung, SR 0.235.11.
29 <http://www.ftc.gov/ogc/FTC_Act_IncorporatingUS_SAFE_WEB_Act.pdf>.
30 Safe Harbor Dokumente; 2.
31 Safe Harbor Dokumente; 2.
32 Dies war deshalb möglich, weil die FTC bereits heute aufgrund unlauterer Wettbewerbshandlungen gegen Firmen vorgehen kann. Eine Unternehmung in den USA, die erklärt, den Schweizerischen Datenschutz einzuhalten und hierdurch Wettbewerbsvorteile hat, allerdings tatsächlich keinen ausreichenden Datenschutz gewährleistet, begeht auch ohne Safe Harbor eine Verletzung von Section 5 FTCA. Im Rahmen des Frameworks wird lediglich ein standardisierter Rahmen geschaffen und die FTC und das DOT verpflichten sich, Verstösse in diesem Rahmen prioritär zu behandeln.
33 Rosenthal/Jöhri (Fn. 8), Art. 6 Abs. 2 Bst. a DSG, Rz. 49.
34 <https://www.export.gov/safeharbor>.
35 <https://www.export.gov/safehrbr/swisslist.aspx>.

Alle URLs letztmals kontrolliert am 17.11.2009.

und ist für die Schweiz das erste staatsvertragliche Abkommen seiner Art. Ihm gilt deshalb nachfolgend besonderes Augenmerk:

Das Framework attestiert den USA sektoriell für die gemäss diesem zertifizierten Firmen ein angemessenes Datenschutzniveau in Sinne von Art. 6 Abs. 1 DSG[26]. Es schlägt dabei die Brücke zwischen den unterschiedlichen Rechtssystemen, wie dies Botschafter David Aaron treffend feststellt: «The Europeans are seeking to develop a comprehensive system of regulation that covers every eventuality. The US cares about privacy protection but […] prefers a system of specific laws targeted to prevent specific abuses. Furthermore, private sector self-regulation, backed up by the Federal Trade Commission [and the implied thread of potential legal redress] is a major component of the US system[27].»

Das Framework ist bis auf einige technische Anpassungen an das DSG mit dem US-EU Safe Harbor Framework identisch und enthält die wesentlichen Anforderungen an eine ausreichende Datenschutzgesetzgebung im Sinne der ERK 108 und deren Zusatzprotokoll vom 8. November 2001[28]. Um die vom Zusatzprotokoll geforderte unabhängige Datenschutzbehörde in den USA zu kreieren und ein angemessenes Datenschutzniveau zu etablieren, wurde auf die wettbewerbsrechtlichen Regelungen des Federal Trade Commission Acts[29] (FTCA) zurückgegriffen. Im Rahmen der Registrierung erklären die Unternehmen gegenüber der Öffentlichkeit, dass sie die Safe Harbor Principles einhalten, wodurch sie einen Wettbewerbsvorteil erhalten. Verstösst eine zertifizierte Unternehmung im Anschluss gegen die Safe Harbor Principles, kann sie in den USA gemäss Section 5 des FTCA aufgrund unlauteren Wettbewerbs von der Federal Trade Commission (FTC) oder vom Department of Transportation (DOT) sanktioniert werden[30]. Aus diesem Grund können sich nur diejenigen Unternehmen in den USA unter dem Framework selbst zertifizieren, die unter die Jurisdiktion der FTC oder des DOT fallen[31]. Auf diese Weise konnten die USA ohne Anpassung ihrer nationalen Gesetzgebung einen rechtlichen Rahmen schaffen, innerhalb welchem ein angemessenes Datenschutzniveau erreicht wird[32]. Im Kern stellt das Framework eine weitreichende Selbstregulierung der zertifizierten Unternehmen dar, welche allerdings in den USA auf dem Rechtsweg einklagbar ist.

Das Framework besteht aus insgesamt fünf Dokumenten (Annex I-V). In den Principles (Annex I) werden die Mindeststandards für die Datenbearbeiter in den USA festgelegt. Die FAQ (Annex II) dienen als Erläuterungen und Auslegungshilfen der Principles. Der Safe Harbor Enforcement Overview (Annex III) gibt einen Überblick über die Jurisdiktion der FTC und des DOT in der relevanten Materie. Annex IV erläutert die Jurisdiktion in den USA betreffend Schadenersatzforderungen im Bereich von Datenschutzverletzungen, gesetzlichen Bewilligungen und Unternehmenszusammenschlüssen unter US-Recht. Im Annex V werden die FTC und das DOT als rechtliche Instanzen in den USA festgelegt, die zu Untersuchungen bei Verstössen gegen das Framework ermächtigt sind.

In den Principles (Annex I) sind die Mindeststandards für die Bearbeitung der aus der Schweiz transferierten Daten festgelegt[33]. Gemäss dem Grundsatz «NOTICE» müssen Personen über den Zweck der Datenbearbeitung informiert werden. Zudem muss gemäss dem Grundsatz «CHOICE» (FAQ 12) den Betroffenen ein Widerspruchsrecht (opt-out) eingeräumt werden, wenn Personendaten an Dritte weitergegeben oder zu einem anderen Zweck als dem bei der Erhebung angegebenen verwendet werden. Für besonders schützenswerte Personendaten wird ein Opt-in verlangt. Der Grundsatz «ONWARD TRANSFER» regelt die Datenweitergabe an Dritte, welche nur zulässig ist,

- wenn die Grundsätze «NOTICE» und «CHOICE» eingehalten werden oder
- der Datenempfänger entweder dem Framework oder dem DSG bzw. einer Gesetzgebung untersteht, die einen angemessenen Schutz gewährleistet, oder
- entsprechende Garantien vereinbart wurden.

Unter dem Grundsatz «SECURITY» wird die zu gewährleistende Datensicherheit festgelegt. Im Grundsatz «DATA INTEGRITY» sind das Verhältnismässigkeits-, das Zweckmässigkeits- und das Datenrichtigkeitsprinzip verankert. Durch den Grundsatz «ACCESS» (präzisiert in FAQ 8) haben die Betroffenen die Möglichkeit, ein Auskunfts-, Berichtigungs- und Löschungsrecht geltend zu machen. Der Grundsatz «ENFORCEMENT» sieht bei Streitigkeiten bezüglich der Datenbearbeitung Klagemöglichkeiten vor, welche in FAQ 11 näher präzisiert werden. Das Framework sieht bei Streitigkeiten für die Betroffenen grundsätzlich einen dreistufigen Beschwerdeweg vor: In einem ersten Schritt wird eine Einigung mit dem Datenbearbeiter angestrebt – misslingt eine solche, steht den Betroffenen in einem zweiten Schritt ein vom Datenbearbeiter bei der Zertifizierung benannter «independent dispute resolution body» zur Verfügung, an welchen sie

sich wenden können. In schwerwiegenden Fällen kann in einem dritten Schritt die FTC angerufen werden, welche bei Verstössen gegen das Framework und Section 5 FTCA Ermittlungen durchführen kann.

Um vom Framework Gebrauch machen zu können, müssen sich US-Unternehmen auf der Webseite des Department of Commerce (DOC) registrieren[34]. Das Zertifizierungsverfahren ist abgeschlossen, sobald die Unternehmung in die Safe Harbor List aufgenommen wurde[35]. Per 3. November 2009 hatten sich bereits über 300 US-Unternehmen selbstzertifiziert.

Für Schweizer Unternehmen und Behörden (Bund und Kantone) wird der Datenaustausch mit zertifizierten US-Unternehmen dahingehend erleichtert, als diese durch die Zertifizierung in den Anwendungsbereich von Art. 6 Abs. 1 DSG fallen und somit die Aushandlung von individuellen Garantien entfällt. Allerdings werden vom Framework nur Daten über natürliche Personen erfasst. Zertifizierte Unternehmen können sich jedoch mittels Erklärung an den EDÖB verpflichten, das Framework auch für Daten über juristische Personen einzuhalten.

Fazit

Die Schweizer Datenschutzgesetzgebung weist die Besonderheit auf, dass sie ihre Datenschutzgrundsätze quasi ins Ausland exportiert und Drittländer auffordert, sich ihrem Datenschutzniveau anzupassen (Art. 6 Abs. 1 DSG). Der Schweizer Gesetzgeber stellt allerdings lediglich die Schutzfunktion in den Vordergrund, was – je nach Land und Situation – zu kreativen (vertraglichen) Lösungen, wie z.B. dem Safe Harbor Framework, führen kann; dieses verbindet die kontinentaleuropäische paternalistische Staatsidee (Staat verwirklicht Allgemeinwohl) mit dem US-Rechtssystem, wonach der Gesellschaft der Vorrang vor der einschränkenden Staatsgewalt eingeräumt wird. ■

agenda

17. DFN-Workshop
«Sicherheit in vernetzten Systemen»
9./10. Februar 2010, Hamburg/D
http://www.dfn-cert.de/veranstaltungen/workshop.html

InfoSociety Days 2010
Education Forum, eGovernment Forum, eHealth Forum
8.–12. März 2010, Bern
http://www.infosocietydays.ch

Eurocrypt 2010
International Association for Cryptologic Research (IACR)
30. Mai–3. Juni 2010, Nizza, F
http://crypto.rd.francetelecom.com/events/eurocrypt2010/

Swiss IT Academy @Community36
Unabhängige Schweizer IT-Konferenz
6./7. Mai 2010, Zürich
http://www.swissitacademy.ch

15th Symposium on Privacy and Security
Stiftung für Datenschutz und Informationssicherheit
31. August 2010, ETH Zürich
http://www.privacy-security.ch/

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 123.00** (inkl. Versandkosten)

Name Vorname

Firma

Strasse

PLZ Ort Land

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §