Information Security Breaches & The Law

Type here and press enter t

- Home
- About »
- “Security Breaches” Library

The Safe Harbor Framework: not a “safe harbor” anymore for US companies? German expert body insists on stronger compliance stance

Posted by "Security Breaches" Administrator on 09/07/2010 · Leave a Comment

On April 29, 2010, the *Düsseldorfer Kreis,* an informal group of German data protection authorities, published a decision (in German only) that could have significant repercussions on U.S. companies importing personal data from organizations operating in the European Union.

Port de Carantec (Bretagne, France) - (c) 2009
Cédric Laurant

According to the German expert group, companies exporting personal data to the United States must no longer rely solely on the U.S. Safe Harbor self-certification list to deem that an organization indeed does provide an adequate level of personal data protection. We examine here the new requirements European and American companies are faced with when transferring personal data under the Safe Harbor Framework, in particular with respect to its Security Principle.

The E.U. Data Protection Directive

The European Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (“the Directive”) became effective on October

25, 1998. Its article 2(a) defines personal data as "*any information relating to an identified or identifiable natural person ('data subject').*"

Even though the Directive was enacted to ensure that personal data may flow easily between all European Union (E.U.) Member States, it also has an impact on countries outside the E.U. that wish to import personal data from a Member State. Indeed, the Directive imposes restrictions on transborder data flows, as its article 25 limits transfer of personal data only to third countries ensuring an "adequate level of protection."

The U.S. Safe Harbor Framework

The United States does not have a comprehensive data protection law, but rather has a myriad of federal and state privacy laws, supplemented by self-regulatory rules. The E.U. did not consider the U.S. as offering an adequate level of data privacy protection, so the U.S. had to find a way to ensure that the flow of personal data between the E.U. and the U.S. would not be interrupted, without having to implement a federal, all-inclusive, privacy law.

The U.S. Department of Commerce started negotiating in 1998 a Safe Harbor (S.H.) Framework with the E.U. Commission. The S.H. Framework consists mainly of seven privacy principles (1. Notice; 2. Choice; 3. Onward transfer restrictions; 4. Access; 5. Security; 6. Data integrity; and 7. Enforcement, as well as 15 "Frequently Asked Questions" (FAQ).

The European Commission finally recognized on July 26, 2000 that companies complying with the S.H. Framework would be considered as meeting the adequate standard of protection. (Decision 520/2000/EC)

Organizations participating in the S.H. are deemed to ensure an adequate level of data protection, and may thus import personal data from Member States' organizations. Adherence to the S.H. is entirely voluntary. An organization may adhere by filing a self-certification form. It must publish a privacy policy stating that it adheres to the S.H. Principles, and that it complies with them.

Organizations must reaffirm in writing every 12 months to the Department of Commerce their continuing adherence to the S.H. In compliance with FAQ 6, the Department of Commerce maintains a list of all self-certified organizations. However, the Department does not guarantee its accuracy, nor does it assess whether organizations on the list actually adhere to the S.H. Framework.

If a self-certified company no longer complies with the S.H. Framework, it must promptly notify the Department of Commerce. Failure to do so may be actionable as a misrepresentation under the False Statements Act (18 U.S.C § 1001). An organization may elect to withdraw, but nevertheless remains obligated to adhere to the S.H. Framework with respect to the personal information they imported while covered by it.

The European Commission, however, does not consider the self-certification program a great success. A Commission staff working document published in 2004 revealed that, by the end of 2003, only 400 companies had self-certified to the S.H. Even more troubling, the staff paper found that some self-certified companies did not comply with the requirement of having a visible privacy policy.

A study made in 2008 by Galexia, an independent privacy consulting firm, found that among the

1,597 organizations listed as members of the S.H. Framework, only 348 “meet even the most basic requirements of the S.H. Framework.”

This is where the *Düsseldorfer Kreis* decision becomes very relevant: it is the first decision coming from a Member State stating that relying on the S.H. list is not an acceptable way to assess whether the level of personal data protection offered by a data importer is adequate.

The *Düsseldorfer Kreis* decision

The *Düsseldorfer Kreis* stated that companies exporting personal data to the U.S. must be able to prove to the data protection authorities that they have indeed checked if the U.S. companies are respecting the S.H. Framework. In order to do so, they have to document their due diligence. (“*Diese Mindestprüfung müssen die exportierenden Unternehmen dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können”*).

If, after examining whether the U.S. company respects the S.H. Principles, the data exporter doubts that it respects the S.H. Framework, the *Düsseldorfer Kreis* “recommends” (“*empfehlen”*) using appropriate contractual clauses in agreements signed with this company. This is a way to satisfy the adequacy requirement which is authorized by article 26(2) of the Directive 95/46/EC.

German data exporters may also choose to adopt binding corporate rules (“B.C.R.”). (*“Sollten nach der Prüfung Zweifel an der Einhaltung der Safe Harbor-Kriterien durch das US-Unternehmen bestehen,empfehlen die Aufsichtsbehörden, der Verwendung von Standard-Vertragsklauseln oder bindenden Unternehmensrichtlinien zur Gewährleistung eines angemessenen Datenschutzniveaus beim Datenimporteur den Vorzug zu geben.”*)

If German companies were to find that a U.S. data importer does not comply with the S.H. Framework, they should (“*sollte*”) notify the German data protection commissioners of the situation.

The stake for data exporting companies is high, as failing to examine the lawfulness of data retrieval, at least by means of suitable random sampling procedures, if there is cause for such examination, is an administrative offence, pursuant to Section 10 (4) and Section 43 (1) 2 of the German Federal Data Protection Act (the *Bundesdatenschutzgesetz, or* BDSG), and is punishable by a fine of up to €50,000.

German organizations exporting personal data to the U.S. should therefore check if the U.S. data importer does indeed comply with the S.H. Framework. There are a few steps they should go through to comply with its Security Principle: from showing due diligence to using contractual clauses.

1. Due diligence

- **German companies should check if the S.H. self-certificate is still valid**

It is rather curious that the *Düsseldorfer Kreis* deemed it important to note that a S.H. self-certificate is no longer valid after seven years (*“Eine mehr als sieben Jahre zurückliegende Safe-Harbor-Zertifizierung ist nicht mehr gültig”).* We know that self-certifying organizations must reaffirm every year to the Department of Commerce their continuing compliance with the S.H. Framework. Does that mean that even if a self-certified organization reaffirms each year its continuing adherence to the S.H. Framework, and follows it, the self-certification nevertheless terminates automatically after

seven years?

- **German data exporters should ask self-certified companies how they actually comply with the S.H. Security Principle**

Organizations participating in the S.H. must comply with its seven Principles. In order to comply with its Security Principle, organizations must take reasonable precautions in order to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction.

A security principle needs to be implemented in a data security plan. According to a business guide issued by the U.S. Federal Trade Commission ("F.T.C.") in 2007, a sound data security plan is built on five key principles:

> *"1. Take stock. Know what personal information you have in your files and on your computers.*
>
> *2. Scale down. Keep only what you need for your business.*
>
> *3. Lock it. Protect the information that you keep.*
>
> *4. Pitch it. Properly dispose of what you no longer need.*
>
> *5. Plan ahead. Create a plan to respond to security incidents."*

German data exporters could use the five F.T.C. key security principles as a guideline.

However, the F.T.C. is not the only U.S. agency offering data security guidance to companies. For example, the U.S. Food and Drug Administration ("F.D.A.") published in 2007 several guidance documents, which include computer system security recommendations (the "Guidance for Industry: Importers and Filers: Food Security Preventive Measures Guidance" and the "Guidance for Industry: Computerized Systems Used in Clinical Investigations").

> *1. "restricting access to a company computer system to those with appropriate clearance (for example by using passwords or firewalls)*
> *2. eliminating computer access when a staff member no longer associated with the establishment*
> *3. establishing a system of traceability of computer transactions*
> *4. reviewing the adequacy of virus protection systems and procedures for backing up critical computer based data systems*
> *5. validating the computer security system"*

Security plan recommendations made by U.S. agencies provide for a useful guideline to E.U. data exporters against which to check the published privacy policies of data importers.

German companies should check whether the self-certified company actually complies with the Safe Harbor Security Principle by checking its privacy policy

Organizations participating in the S.H. must comply with the S.H.'s requirements and publicly declare

that they do so. So, reading the privacy policy of companies registered as participating in the S.H. should be the first step to take.

However, reading the privacy policy cannot alone constitute sufficient due diligence for data exporters, as privacy policies do not always clearly specify how they implement the S.H.’s Framework.

For example, Best Buy participates in the S.H. because it provides back office support for its European affiliates, and this involves the transfer and processing of customer and employee data. Its privacy policy reads:

> *Whether you are shopping online or in our stores, we use reasonable security measures to protect the confidentiality of personal information under our control and appropriately limit access to it. Best Buy cannot ensure or warrant the security of any information you transmit to us by e-mail, and you do so at your own risk.*

It seems that the personal data of customers are adequately protected. However, nothing is said about employee data. Whereas this information may be available internally, it is not available publicly, and thus would make the EU data exporter’s task of assessing whether the company complies with the S.H. more difficult. This missing information may come from the fact that Best Buy’s privacy policy applies to its website, and therefore only covers the privacy aspects of its visitors’ personal information, not of its employees. However, for a company that self-certified itself as complying with the S.H. not to disclose in its privacy policy how it actually protects all of the personal information it processes does not comply with the S.H. Framework requirements. (Cfr European Commission, Staff Working Document, “The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce”.)

Another self-certified SH company, RealNetworks, clearly states in its privacy policy how the company protects the security of personal information:

> *- “Use of secure connections using SSL to safeguard information when transmitted from your Web browser to RealNetworks;*
>
> *- Use of security controls to restrict access to databases housing personally identifying information;*
>
> *- Use of encryption for sensitive personal information, such as credit card numbers and user names;*
>
> *- Restrict employee access to databases containing personal information and impose confidentiality requirements upon employees who do; and*
>
> *- Bind subcontractors with contractual, technical and organizational measures to protect your personal information.”*

This policy details clearly all the security measures taken to protect the data, whereas the Best Buy policy merely stated that the company used “reasonable security measures” without enumerating

them.

If, after appropriate due diligence, the data exporter doubts that the data importer respects the S.H. Principles, the *Düsseldorfer Kreis* recommends the use of contractual clauses in agreements with this company.

2. Use of contractual clauses

- **German companies should use appropriate contractual clauses in their contract with U.S. data importers:**

An example of such contractual clauses can be found in the Commission decision of December 27, 2001.

That decision was repealed in 2010 by another Commission decision, which proposes new contractual clauses. Paragraph 12 of the 2010 decision states that “*standard contractual clauses should provide for the technical and organizational* ***security*** *measures to be applied by data processors established in a third country not providing adequate protection,* ***in order to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected***.” (our emphasis)

- **German companies should require that data importers comply with a security standard**

German companies could also add a contractual clause stating that the data importer must comply with industry security standards, such as the ISO 27000 international standard for information security.

Indeed, the Article 29 Working Party wrote in a 1997 Opinion that it considers that developing and adopting international privacy standards within the International Standard Organization (ISO) *“significantly contribute to the protection of fundamental rights and privacy on a world-wide basis.*”

- **German companies may elect to hire an independent third party auditing firm to review the data importer’s compliance with the S.H.**

German companies could also add a contractual clause stating that the contract will not be enforced unless the data importer is found to comply with the S.H. Principles by an independent auditing firm.

A stronger role for the F.T.C. in enforcing the Safe Harbor’s Security Principle?

The *Düsseldorfer Kreis* called for more involvement by the F.T.C., which could work more closely with the European DPAs on making sure that self-certified companies are indeed complying with the S.H. Framework.

Violating the S.H. Framework is considered an unfair or deceptive practice within the meaning of the Federal Trade Commission Act, and is thus actionable by the F.T.C. It should be noted however that the F.T.C. has jurisdiction over individuals and business entities, but does not have jurisdiction over banks and other financial institutions, nor does the F.T.C. have jurisdiction over common carriers, over which only the Department of Transportation has jurisdiction.

The F.T.C. is already enforcing breaches of security as violations of the F.T.C. Act. For example, in the *DSW* case, the F.T.C. issued a complaint against DSW, a shoe retailer, because it had failed to use reasonable and appropriate security measures to protect the personal information stored on its computer network. The F.T.C. entered into a consent decree with DSW, which ordered the retailer to establish a comprehensive information security program, the content and implementation of which must be fully documented in writing.

One could hope that, in the future, the F.T.C. will issue complaints against self-certified companies that violate their commitments to comply with the S.H. Framework’s Security Principle.

A stronger compliance stance, and not only for German companies

German data exporters must now assess carefully whether self-certified U.S. data importers are indeed complying with the Safe Harbor Framework. No enforcement agencies, whether from the E.U. or from the U.S., have enforced compliance with the Safe Harbor Framework, apart from the U.S. Federal Trade Commission in a August 2009 case (*FTC v. Javian Karnani*). However, enforcement of the Safe Harbor is not entirely self-regulatory, but has been described in a study analyzing in detail its implementation as “occupy[ing] the middle ground between a self-regulatory scheme and rules enforced by public authorities. As such, it may be viewed as a form for a “co-regulatory” scheme.

However, U.S. public authorities have not been attentive to enforcing the regulations. Does the *Düsseldorfer Kreis* decision reflect a growing distrust of European data protection authorities towards the Safe Harbor Framework, or is it an isolated decision? Data exporters need to be mindful of future developments, and not only if they are German.

Marie-Andrée Weiss & Cédric Laurant

Reference documents:

- Düsseldorfer Kreis (informal group of German data protection authorities)’s decision (*Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich am 28./29. April 2010 in Hannover*), April 28-29, 2010 (in German only).

- U.S.-E.U. Safe Harbor Framework web site.

- European Commission, Staff Working Document, “The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce,” October 20, 2004 (SEC (2004) 1323).

- European Commission, “Model Contracts for the transfer of personal data to third countries”.

- Centre de Recherche Informatique et Droit, University of Namur (Jan Dhont, María Verónica Pérez Asinari and Prof. Dr. Yves Poullet), Prof. Dr. Joel R. Reidenberg (Fordham University School of Law, New York), and Dr. Lee A. Bygrave (Norwegian Research Centre for Computers and Law, University of Oslo), *Safe Harbour Decision Implementation Study* (written at the request of the

European Commission, Internal Market DG), Namur (Belgium), April 19 2004.

- Chris Connolly, “The US Safe Harbor – Fact or Fiction?, December 2008.

- United States Federal Trade Commission, *Protecting Personal Information, A Guide for Business*, 2007.

Filed under Comments, ENGLISH · Tagged with United States, European Union, Safe Harbor Framework, Düsseldorfer Kreis, Germany, EU Directive 95/46/EC, personal data, transborder data flows, Article 25 (EU DP Dir.), third countries, US Department of Commerce, US Federal Trade Commission, adequate level of data protection, privacy policy, Safe Harbor self-certified organizations, Safe Harbor self-certification, US False Statements Act, contractual clauses, adequacy requirement, Article 26(2) (EU DP Dir.), Binding corporate rules, data importer, European data protection authorities, German Federal Data Protection Act, Bundesdatenschutzgesetz, Safe Harbor Security Principle, loss, misuse, data security plan, data exporter, US Food and Drug Administration, due diligence, Best Buy, RealNetworks, European Commission, Article 29 Data Protection Working Party, personally identifying information, encryption, sensitive personal information, reasonable security measures, ISO 27000, information security, ISO, independent auditing firm, unfair and deceptive practice, US Department of Transportation, DSW, FTC v. Javian Karnani, self-regulation, co-regulation

Canada May Soon Have a Data Breach Law
Are ‘clouds’ located outside the European Union unlawful?

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <pre> <del datetime=""> <em> <i> <q`

cite=""> <strike>

Post Comment

Notify me of follow-up comments via email.

Send me site updates

- **Recent Posts**

  - Article 29 Data Protection Working Party reports on implementation of Data Retention Directive
  - Are ‘clouds’ located outside the European Union unlawful?
  - The Safe Harbor Framework: not a “safe harbor” anymore for US companies? German expert body insists on stronger compliance stance
  - Canada May Soon Have a Data Breach Law

- **Recent News on Security Breaches**

  - "Consumer View: Staying Safe from Cyber Snoops" (FCC, June 11, 2010) Recent news reports have focused attention on a growing concern: The ways in which wireless and WiFi networks can make consumers’ private data accessible. (…)
  - "Sécurité des données personnelles : les entreprises ne font pas face" (ITR News, 9 juin 2010) L’étude souligne le fait que, en dépit de ce que croient beaucoup d’entreprises, le fait de respecter la réglementation en vigueur ne suffit pas à assurer une protection efficace des données. En effet, alors que 70 % des sondés affirment (…)
  - "Twitter Settles Charges that it Failed to Protect Consumers’ Personal Information; Company Will Establish Independently Audited Information Security Program" (FTC, June 24, 2010) The FTC’s complaint against Twitter charges that serious lapses in the company’s data security allowed hackers to obtain unauthorized administrative control of Twitter, including access to non-public user information, tweets that consumers had (…)
  - "UK headed for data breach disclosure law within four years" (siliconcom, July 16, 2010) “According to lawyers at law firm Field Fisher Waterhouse, legislation requiring organisations to notify the relevant authorities as well as individuals affected in the event of a serious security breach will be introduced across Europe.”
  - "Survey: 87 per cent of UK businesses favour mandatory disclosure of data breaches" (Secure Business Intelligence, July 6, 2010) 87 per cent of organisations believe that data breaches should be revealed when sensitive data about the public is exposed. Revealed, but to whom?
  - "Putting a Private Detective in Your Laptop" (New York Times, June 16, 2010) “According to a study by the Ponemon Institute, 12,000 laptops are lost each week in American airports (…) You can keep an eye on your devices and not leave them visible and unattended, but they might best be protected with some software.”
  - "Credit Card Hackers Visit Hotels All Too Often" (New York Times, July 5, 2010) Hotels are a favorite target of hackers. A study released this year by data-security consulting company SpiderLabs found that “38 % of the credit card hacking cases last

year involved the hotel industry”.

- Ponemon Institute: First Annual Cost of Cyber Crime Study (ArcSight, July 26, 2010) “The purpose of this benchmark study is twofold. First, we wanted to quantify the economic impact of a cyber attack. Second, we believed a better understanding of the cost of cyber crime will assist organizations in determining the appropriate amount (…
- Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees (FTC, July 27, 2010) “The FTC began its investigation following news reports about Rite Aid pharmacies using open dumpsters to discard trash that contained consumers’ personal information such as pharmacy labels and job applications. (…)”

- **Tag Cloud**

adequate level of data protection Article 29 Data Protection Working Party Binding corporate rules Bundesdatenschutzgesetz C-29 Canada cloud computing confidentiality contractual clauses damage to reputation data breach notification statute data security Düsseldorfer Kreis encryption EU Directive 95/46/EC European Commission European data protection authorities European Union external audit Facebook German Federal Data Protection Act Germany identity theft integrity material breach online reputation personal data PIPEDA preemption Privacy Commissioner of Canada profile building companies reputation Safe Harbor Framework Safe Harbor self-certification search engines security breach security breach disclosure security breach notification self-regulation sensitive information sensitive personal information significant harm social networking sites TJX United States

- **Blog Authors**

- 

- **Disclaimer & Comments Policy**
  - Disclaimer & Comments Policy

- **Authors' upcoming talks & conferences on information security & legal issues**
  - Cédric Laurant: "Seminario internacional: seguridad de la informacion, cibercriminalidad y propiedad intelectual" (international seminar on information security, cybercriminality and intellectual property) IUSTIC & Universidad Pontificia Bolivariana (Medellin, Colombia – Aug. 3-12, 2010)
  - Cédric Laurant: II Congresso Crimes Eletrônicos e formas de proteção (2nd Congress on Cybercrimes and Protection Measures) Federação do Comércio do Estado de São Paulo (Sao Paulo Chamber of Commerce), Sao Paulo, Brazil – Sept. 27-28, 2010
  - Cédric Laurant: "Legal Developments and Relevant Court Decisions in Latin America" High Technology Crime Investigation Association (HTCIA) International Conference (Atlanta, GA-USA – Sept. 20-22, 2010)

- **Tweets (last 10)**
  - List of recent surveys and reports on security breaches: http://bit.ly/9VamhE - tweeted 22 hours ago
  - ArcSight & Ponemon Institute: release of "1st Annual Cost of Cyber Crime Study" http://bit.ly/d1Us8e - tweeted 22 hours ago
  - Article 29 Data Protection Working Party reports on implementation of Data Retention Directive. New blog posting at http://bit.ly/aOG3cY #in - tweeted 1 week ago
  - "Are ‘clouds’ located outside the European Union unlawful?" New blog posting. http://bit.ly/djUNCy #in - tweeted 1 week ago
  - "The Safe Harbor Framework: not a 'safe harbor' anymore for US Companies?" New blog posting. http://lnkd.in/ShwMWj - tweeted 2 weeks ago
  - "The Safe Harbor Framework: not a "Safe Harbor" anymore for US Companies?" New blog posting: http://wp.me/pW5Fc-1D - tweeted 2 weeks ago
  - FTC's proposed consent agreement with #Twitter: company misrepresented its security measures. http://bit.ly/cF8LNk - tweeted 1 month ago
  - Your "private" tweets are... public! #Twitter prone to security breaches, FTC says in consent agrmt. Com'ts requested. http://bit.ly/axKpnV - tweeted 1 month ago
  - FTC's 1st case agst social netwkg website: #Twitter failed to safeguard users' PII despite promises in privacy policy http://bit.ly/ajUG9J - tweeted 1 month ago
  - Backing up data is one thing, encrypting the backups another, but restoring the encrypted data, even more complex. http://bit.ly/bGgQt2 - tweeted 1 month ago

- **Subscribe to this blog by e-mail**

  Enter your e-mail address here to subscribe to this blog and receive notifications of new posts by e-mail.

  Sign me up!

-

- **Counters**

- 

Information Security Breaches & The Law ·

Blog at WordPress.com. Theme: Structure by Organic Themes.