Information Security Breaches & The Law

Type here and press ente

- About
- Post archives
- “Security Breaches” Library
- Authors
- Contact

Are ‘clouds’ located outside the European Union unlawful?

Posted by "Security Breaches" Administrator on July 16, 2010 · 2 Comments (Edit)

This is at least what Dr. Thilo Weichert argues. He is the head of the Independent Center for Privacy Protection of the State of Schleswig-Holstein (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, or “ULD”), and one of Germany’s top privacy experts. In a June 18, 2010 opinion, he wrote on the subject of cloud computing.

"Threatening Cloud" (New York, NY, 2010)
Photo: Marie-Andrée Weiss

According to him,

> *“The main issue in cloud computing rests with the integrity and the confidentiality of the data stored in the cloud.”*
>
> (“Das zentrale Problem des Cloud Computing besteht darin, die Integrität und Vertraulichkeit der Datenverarbeitung des Cloud-Nutzers zu gewährleisten.”)

He goes on by pointing out that

> *"A central aspect of every cloud service contract is the security of data processing. In order to eliminate data security breaches, one must maintain the system and take steps to troubleshoot it. It is thus important, if only for liability reasons, that responsibility for specific security measures be clearly assigned. This can be done by using Security Service Level Agreements ("SSLA") between the Cloud service provider and its client. SSLAs frequently have the character of general business conditions."*
>
> ("Ein zentraler Aspekt jedes Cloud-Vertrages ist die Sicherheit der Datenverarbeitung. Hierzu gehören Pflege- und Fehlerbeseitigungsmaßnahmen sowie Maßnahmen zur Abwehr von Angriffen und Störungen. Schon aus haftungsrechtlichen Gründen ist es von Bedeutung, dass die Verantwortlichkeit für spezifische Sicherheitsmaßnahmen eindeutig zugewiesen wird. Sicherheitszusagen können über Security-Service-Level-Agreements (SSLA) verabredet werden. Tatsächlich bleiben die Cloud-Anbieter bei ihren Garantien für Sicherheitsmaßnahmen „wolkig". SSLA haben regelmäßig den Charakter von allgemeinen Geschäftsbedingungen (AGB).")

However, storing data in a cloud located outside the EU raises specific legal compliance issues, as according to Dr. Weichert, such clouds are unlawful. There are, however, some ways to make sure that, even if a data controller stores data into a cloud located in a third country, he is still in compliance with German data protection law.

What is cloud computing?

There are three major cloud computing services: Software-as-a-Service ("SaaS"), Platform-as-a-Service ("PaaS"), and Infrastructure-as-a-Service ("IaaS"). Using cloud computing services allows companies to scale their system, bandwidth, and storage space as needed.

However, users of these services give up some control over their data, including personal data, which may be stored remotely in the cloud. This is why, as these cloud computing services are getting more and more popular, Dr. Weichert found it necessary to explain the data protection framework deriving from this new technology, after carefully reviewing the practices of private companies established in Germany and offering cloud computing services.

The opinion distinguishes between "private clouds" and "public clouds," but addresses both issues. In a private cloud, computers are linked in one network that is under the responsibility of one company. For instance, a very big company creates a private network, and then uses cloud services to provide applications which are only accessible on the cloud by the company's employees. In a public cloud, however, a company, such as Google or Yahoo, is providing cloud-computing services to clients which do not belong to the same entity. All of this data is stored on data centers and server farms, which may be in multiple locations, and multiple countries.

Data security in the Cloud

Dr. Weichert notes that a central aspect of storing data in the cloud is the security of this data. (*"Ein zentraler Aspekt jedes Cloud-Vertrages ist die Sicherheit der Datenverarbeitung"*.) Thus, it must be clearly stated who is in charge of data security by implementing a SSLA that clearly assigns who is responsible for which particular security measure. See here an example of service level agreement.

According to the German expert, the client is still the data controller, which is defined by Section 3 (8) of Germany's Federal Data Protection Act (*Bundesdatenschutzgesetz, or* BDSG), as "*any person or body storing personal data on his or its own behalf, or commissioning others to store them*."

> *“The client, as such, remains responsible for ensuring the confidentiality and the integrity of data.”* (“Der Auftraggeber bleibt für die Sicherstellung der Vertraulichkeit und Integrität der Daten verantwortlich.”)
>
> *“The cloud service provider should ideally be completely dependent upon the data security specifications of the data controller.”* (“Cloud- und Ressourcen-Anbieter erfüllen reine Hilfs- und Unterstützungsfunktionen und sind – idealtypisch – völlig von den Vorgaben der verantwortlichen Stelle abhängig.”)

Legal responsibilities of the data controllers storing data in the Cloud

It is especially important as users of cloud computing services remain responsible for complying with applicable data protection law. Pursuant to Section 11 of the BDSG, which regulates the commissioned processing or use of personal data,

> “*Where other bodies are commissioned to process or use personal data, responsibility for compliance with the provisions of this Act and with other data protection provisions shall rest with the principal.”*

Dr. Weichert’s opinion is that section 11 does apply, not only to data controllers when the data transfer is inside the European Union, but also when such transfer is outside the European Union. Dr. Weichert ‘s opinion reminds users of their responsibility: “[T]he customer remains responsible for ensuring the confidentiality and integrity of the data” (“*Der Auftraggeber bleibt für die Sicherstellung der Vertraulichkeit und Integrität der Daten verantwortlich*“) (at 6.1). He notes that **cloud computing clients are not able to fulfill their responsibilities if the cloud service provider does not provide them with information on how and where their data is stored.** By using cloud services the client will necessarily give up some of its control over the data. **In order to fulfill his responsibility as a data controller, there must a clear agreement between him and the cloud computing service provider. The client must therefore be certain that**

> ***“the technical and organizational measures, such as the contractor’s substantive data protection requirements in German law, are respected.”***
>
> (“Bei einer klassischen Auftragsdatenverarbeitung muss sich der Auftraggeber umfassend darüber vergewissern, dass die technisch-organisatorischen Maßnahmen wie die materiellen Vorgaben des Auftragnehmers beachtet warden.”)

This is only acceptable, according to Dr. Weichert’s opinion, in two ways:

> *1. “There is a binding commitment between the user and the cloud service provider, in which the cloud service provider commits itself to respect the data protection law.*
> *2. The responsibility to monitor if these obligations are respected is transferred to an independent and competent agency. In doing so, cloud service providers would have to submit themselves to external audits, or obtain some certifications.”*
>
> (“Diese Entledigung von Kontrollen und Weisungen können nur durch zwei Vorgehensweisen akzeptiert werden: 1. die verbindliche Zusage des Auftragnehmers in Form einer umfassenden Selbstbindung und 2. die Übertragung der Kontrolle, ob diese Pflichten beachtet werden, an eine unabhängige und kompetente Stelle. Dies kann in der Form erfolgen, dass sich sämtliche Anbieter bestimmten externen Audits oder Zertifizierungen unterwerfen.”)

So, according to Dr. Weichert, data controllers, when processing transfers of data outside the European Union, also have to comply with section 11 of the BDSG.

Cloud located in third countries

Also, since a cloud computing service may have servers based in a country which is neither the cloud provider's country nor the client's country, the law of this country would apply to the data. One of the major security problems of a cloud computing system is that data may be then legally accessed by third parties. However, Dr. Weichert notes that there are technical ways that may be used to protect the data if it is accessed by a third party, such as encryption, use of pseudonyms, or anonymization.

Dr. Weichert goes on by affirming that,

> *"When cloud service providers located outside the European Union are part of a transfer of data, such a data transmission would be fundamentally illegal because it would be lacking the legitimacy given by data protection laws."*
>
> ("Werden Stellen außerhalb der Europäischen Union mit einbezogen, so sind Clouds wegen der damit zwangsläufig erfolgenden Datenübermittlung, für die es keine datenschutzgesetzliche Legitimation gibt, grundsätzlich unzulässig.")

How to ensure that third country cloud providers provide an adequate level of data protection?

A way to provide that legitimacy is to ensure that there is an "adequate level of protection" for the data transmitted, pursuant to § 4b Abs. 2, 3 BDSG, which is the transposition in German law of article 25 of the 95/46/EC Directive, which limits transfer of personal data to third countries ensuring an "adequate level of protection."

Dr. Weichert continues by explaining that

> *"Some countries, Switzerland, Canada, and Argentina, have indeed been deemed by the EU Commission as meeting this adequate level of protection standard. However, ascertaining the adequacy of the level of data protection in a country outside the European Union does not automatically give a company located in that country the right to be considered an agent of the data controller pursuant to section 11 of the BDSG."*
>
> ("Dies wurde für bestimmte Staaten durch die EU-Kommission festgestellt (…) für die Schweiz, Kanada oder Argentinien. Die Feststellung der Angemessenheit des Datenschutzniveaus in einem außereuropäischen Staat hat jedoch nicht zur Folge, dass Stellen dort rechtlich als Auftragnehmer gemäß § 11 BDSG behandelt werden können.")

As data processing in a cloud system from countries outside the EU does not comply with section 28 of the BDSG, which requires that a data transfer be necessary to fulfill a contract, such systems are "inadmissible" ("*unzulässig*").

Therefore, a data exporter must use, in order to satisfy the adequacy requirement, specific standard contractual clauses for all contracts with a cloud service company located outside the EU, as authorized by article 26(2) of the Directive 95/46/EC.

However,

> *"The mere fact that a company is self-certified to the Safe Harbor Framework is never enough to attain an appropriate level of protection pursuant to EU standards."*
>
> ("Allein die Selbstzertifizierung von US-Unternehmen zu Safe Harbor genügt in keinem Fall, um ein den EU-Standards entsprechendes Datenschutzniveau zu erreichen.")

In order to prove that they ensure an appropriate level of protection, cloud providers located in third countries may obtain a certification, such as the SAS-70 Type II audit. However, obtaining such certification only partly satisfies German legal requirements.

Instead of using standard contractual clauses, cloud providers may also be bound by corporate rules (Binding Corporate Rules, or "BCRs"). BCRs are legally binding internal rules governing how a company protects the privacy of data transferred internationally within the company. In order to be effective, BCRs must be approved by the Data Protection Authority ("DPA") of the country of which the company is a citizen. The European Union Article 29 Working Party has published in June 2008 a Working Document "Setting up a framework for the structure of Binding Corporate Rules," which provides a checklist that companies may follow when implementing their BCRs.

Conclusion

Although Dr. Weichert is a renowned data privacy expert in Germany, and the data protection authority for the German Federal State of Schleswig-Holstein, whether his opinion will have an influence beyond the border of that State is yet to be determined. This opinion is not legally binding, and thus German companies will not have to defer to it, by having to adapt their cloud computing practices. However, as Dr. Weichert's expertise is well recognized, such a forcefully written opinion may influence other German DPAs. It may influence other European Unions DPAs as well, and we may see similar opinions being published in the future.

As we reported earlier in this blog, a recent decision by the *Düsseldorfer Kreis,* an informal group of German data protection authorities, similarly decided that the mere fact of being on the Safe Harbor list is not sufficient to deem that a company provides an adequate level of personal data protection. The German expert body also advocated the use of binding corporate rules when exporting data to a third country.

The relationship between data privacy and cloud computing is also a growing topic of interest in the United States. In this report, privacy advocates call for reforming current privacy protection laws, and for stronger business privacy protection practices.

Are certifications the best way to ensure an adequate level of protection? The European Privacy Seal, for example, is a project funded by the EU Commission that certifies that an IT-based service complies with European data protection regulations.

It will be interesting to find out which solution will predominate in the future to ensure that adequate data safety measures are being established by third country cloud providers: regulations, business practices, or certifications?

Marie-Andrée Weiss & Cédric Laurant

6

Possibly related posts: (automatically generated)

- **The Safe Harbor Framework: not a “safe harbor” anymore for US companies…**
- **Will France adopt a law requiring the notification of security breaches?**
- The US cares for data protection
- European Commission Consultation on the Privacy Directive

Filed under Comments, Cédric Laurant, English, Europe, European Union, Marie-Andrée Weiss, Outlines · Tagged with United States, Safe Harbor Framework, Düsseldorfer Kreis, Germany, EU Directive 95/46/EC, personal data, adequate level of data protection, Safe Harbor self-certification, Binding corporate rules, German Federal Data Protection Act, Bundesdatenschutzgesetz, European Commission, encryption, cloud computing, Datenschutzzentrum, data security, Security Service Level Agreement, data controller, BDSG, SAS 70, European Privacy Seal, EuroPriSe, data processing security, SaaS, PaaS, IaaS, Article 29 Working Party, State of Schleswig-Holstein, Dr. Thilo Weichert, confidentiality, integrity, cloud service contract, liability, private cloud, public cloud, Google, Yahoo, cloud service provider, external audit, third country, third party, pseudonym, anonymization, data protection law, Switzerland, Argentina, Article 26 (EU DP Dir.), standard contractual clauses, Data Protection Authority

← The Safe Harbor Framework: not a “safe harbor” anymore for US companies? German expert body insists on stronger compliance stance
Article 29 Data Protection Working Party reports on implementation of Data Retention Directive →
Like
Be the first to like this post.

Comments

2 Responses to “Are ‘clouds’ located outside the European Union unlawful?”

Trackbacks

Check out what others are saying...

1. *Are ‘clouds’ located outside the European Union unlawful? | Digital Asset Management* says:
   July 23, 2010 at 9:27 am (Edit)

   [...] Are ‘clouds’ located outside the European Union unlawful? « Information Security Breaches &…. [...]

   Reply
2.  *New Blog: “Information Security Breaches & The Law” « Cedric's Privacy Blog* says:
   August 7, 2010 at 11:15 pm (Edit)

   [...] Are ‘clouds’ located outside the European Union unlawful? (July 16, 2010): A central aspect of every cloud service contract is the security of data processing. It is therefore

important, if only for liability reasons, that responsibility for specific security measures be clearly assigned. This can be done by using security service level agreements between the cloud service provider and its client that clearly assign who is responsible for which particular security measure. Storing data in a cloud located outside the EU raises specific legal compliance issues. According to some experts, such clouds are even unlawful. There are, however, some ways to make sure that, even if a data controller stores data into a cloud located in a third country, he is still in compliance with German data protection law. A data exporter must use, in order to satisfy the adequate level of data protection requirement, specific standard contractual clauses for all contracts with a cloud service company located outside the EU. Binding corporate rules are the alternative solution, though only for private clouds. [...]

Reply

Leave a Reply

Logged in as marieandreeweiss. Log out?

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> <strong>`

Post Comment

Notify me of follow-up comments via email.

Notify me of site updates

- **Read this website in your language!**

  --> Click here to translate

- **Recent Posts**

  - Will France adopt a law requiring the notification of security breaches?
  - La France va-t-elle se doter d’une loi rendant obligatoire les notifications des violations de sécurité ?
  - 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

- **Recent News on Security Breaches**

  - "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?
  - "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. (…)
  - Verizon & U.S. Secret Service "2010 Data Breach Investigations Report" (PR Newswire, July 27, 2010) This report “has found that breaches of electronic records last year involved more insider threats, greater use of social engineering and the continued strong involvement of organized criminal groups.” It also “noted that the overall number of breaches in
  - The average SMB spends about USD 51,000 a year to protect information, according to a new report (Marketwire, June 21, 2010) “The survey found that small and mid-sized businesses (with 10 to 499 employees) are now making protecting their information their highest IT priority, as opposed to 15 months ago when a high percentage had failed to enact even the most basic safeguards.”

- **Tag Cloud**

adequate level of data protection Article 29 Data Protection Working Party Binding corporate rules Bundesdatenschutzgesetz C-29 California Office of Privacy Protection California Security Breach Notification Act cloud computing Commission nationale de l’informatique et des libertés confidentiality contractual clauses damage to reputation data breach notification statute data controller data

security Düsseldorfer Kreis encryption EU Directive 95/46/EC European Commission European data protection authorities external audit Facebook France German Federal Data Protection Act Germany identity theft integrity material breach personal data PIPEDA preemption Privacy Commissioner of Canada reputation Safe Harbor Framework Safe Harbor self-certification security breach security breach disclosure security breach notification self-regulation sensitive information sensitive personal information significant harm social networking sites TJX United States

- **Tweets (last 10)**
  - Will France adopt a law requiring the notification of #security_breaches? New blog posting http://bit.ly/cyZcC2 #in - tweeted 2 weeks ago
  - "La France va-t-elle se doter d’1 loi rendant obligatoire les notifications des violations de sécur.?" New blog posting http://bit.ly/9DJS36 - tweeted 2 weeks ago
  - List of recent surveys and reports on security breaches: http://bit.ly/9VamhE - tweeted 3 weeks ago
  - ArcSight & Ponemon Institute: release of "1st Annual Cost of Cyber Crime Study" http://bit.ly/d1Us8e - tweeted 3 weeks 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 month ago
  - "Are ‘clouds’ located outside the European Union unlawful?" New blog posting. http://bit.ly/djUNCy #in - tweeted 1 month ago
  - "The Safe Harbor Framework: not a 'safe harbor' anymore for US Companies?" New blog posting. http://lnkd.in/ShwMWj - tweeted 1 month ago
  - "The Safe Harbor Framework: not a "Safe Harbor" anymore for US Companies?" New blog posting: http://wp.me/pW5Fc-1D - tweeted 1 month 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

- **Blog Authors**
  - 

  - 

- **Disclaimer & Comments Policy**
  - Disclaimer & Comments Policy
- **Meta**
  - Site Admin
  - Log out
  - Entries RSS
  - Comments RSS
  - WordPress.com
- **Authors' upcoming talks & conferences on information security & legal issues**
  - 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)
  - Cédric Laurant: "El uso de las redes sociales en el ámbito laboral: consideraciones jurídicas, seguridad de la información y medidas prácticas" Congreso Internacional de Derecho y Tecnología (International Congress on Law & Technology): “Nueva Convergencia, Nuevos Desafíos” – Universidad Blas Pascal (Córdoba, Argentina – Oct. 14-15, 2010)
- **Archives by date**
  - August 2010 (2)
  - July 2010 (3)
  - June 2010 (1)
- **Subscribe to this blog by e-mail**

  Click to subscribe to this blog and receive notifications of new posts by e-mail.

  Sign me up!
-

- **Counters**

Information Security Breaches & The Law · Privacy, data protection and information systems security issues

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