Outsourcing und Tracking in einer vernetzten Welt

Infobörse 2

Referent: Dr. Sven Polenz, ULD
Moderation: Harald Zwingelberg, ULD

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Übersicht

1. Outsourcing im innereuropäischen Kontext

1.1 Auftragsdatenverarbeitung öffentlicher / nichtöffentlicher Stellen

Beispiele

- Nutzung fremder Rechnerkapazitäten
- Tätigkeit von Druck- und Kuvertierzentren
- Hosting-Dienste für Webseitenbetreiber
- Tätigkeit von Callcentern
- Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen

ULD www.datenschutzzentrum.de

1. Outsourcing im innereuropäischen Kontext

1.1 Auftragsdatenverarbeitung öffentlicher / nichtöffentlicher Stellen

- Anforderungen nach § 11 Bundesdatenschutzgesetz -

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

1. Outsourcing im innereuropäischen Kontext

1.1 Auftragsdatenverarbeitung öffentlicher / nichtöffentlicher Stellen

- **Exkurs: Cloud Computing**

Die verantwortliche Stelle hat die **Rechtmäßigkeit der gesamten Datenverarbeitung** zu gewährleisten, insbesondere muss sie ihren **Löschpflichten** nachkommen (§ 35 Abs. 2 BDSG/§ 28 Abs. 2 LDSG), unrichtige Daten **berichtigen** (§ 35 Abs. 1 BDSG/§ 28 Abs. 1 LDSG), für eine **Sperrung** von Daten sorgen (§ 35 Abs. 3 BDSG/§ 28 Abs. 3 LDSG) und dem Betroffenen (§ 3 Abs. 1 BDSG/§ 2 Abs. 1 LDSG) u. a. **Auskünfte über die zu seiner Person gespeicherten Daten**, auch soweit sie sich auf die Herkunft dieser Daten beziehen, erteilen (§ 34 Abs. 1 BDSG/§ 27 Abs. 1 LDSG).

ULD www.datenschutzzentrum.de

1. Outsourcing im innereuropäischen Kontext

1.1 Auftragsdatenverarbeitung öffentlicher / nichtöffentlicher Stellen

§ 17 Landesdatenschutzgesetz Schleswig-Holstein (LDSG)

- Weisungsgebundene Verarbeitung
- Sicherstellung technisch-organisatorischer Anforderungen (§§ 5, 6 LDSG)
- Schriftliche Festlegung zur Zulässigkeit von Unteraufträgen

1. Outsourcing im innereuropäischen Kontext

1.2 Technisch-organisatorische Anforderungen

- **Nichtöffentlicher Bereich:** (§ 9 BDSG i.V.m. der Anlage zum BDSG: Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Getrennte Datenhaltung´)

- **Öffentlicher Bereich:** insbesondere Anforderungen nach der DSVO-Scheswig-Holstein; *Allgemeine Anforderungen* (§ 5 LDSG): Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nicht-Verkettbarkeit, Intervenierbarkeit; *Besondere Anforderungen* (§ 6 LDSG): Berechtigungskonzept, Protokollierung von Zugriffen, Verschlüsselung von Datenbeständen, Protokollierungskonzept, Aufbewahrung von Protokolldaten

ULD www.datenschutzzentrum.de

1. Outsourcing im innereuropäischen Kontext

1.3 Maßnahmen der europäischen Nachrichtendienste

- Government Communications Headquarters (GCHQ – britischer Nachrichten- und Sicherheitsdienst) und die Direction Générale de la Sécurité Extérieure (DGSE – französischer Nachrichtendienst) sollen umfassend und ohne Rechtsgrundlage auf personenbezogene Daten von EU-Bürgern, d.h. Verbindungs- wie Inhaltsdaten (Telefon- und Internetverbindungsdaten sowie E-Mails, SMS, Chats), zugreifen. Quelle: Lehnartz, Meldung vom 05.07.2013, „Franzosen spionieren auch mit“, http://www.welt.de/print/die_welt/politik/article117740966/Franzosen-spionieren-auch-mit.html

- Entsprechende Maßnahmen würden gegen europäisches Datenschutzrecht verstoßen.

2. Outsourcing im außereuropäischen Kontext

2.1 Datenverarbeitung durch US-Behörden

- Federal Bureau of Investigation (FBI), National Security Agency (NSA), Central Intelligence Agency (CIA)

- US-Behörden sind auf der Grundlage von US-amerikanischem Recht ermächtigt, auf personenbezogene Daten in Europa zuzugreifen (z.B. der Patriot Act, der Foreign Intelligence Surveillance Act, der Electronic Privacy Act, der Stored Communications Privacy Act).

ULD www.datenschutzzentrum.de

2. Outsourcing im außereuropäischen Kontext

2.1 Datenverarbeitung durch US-Behörden

Studie des Instituts für Informationsrecht der Universität Amsterdam (Schröder/Haag, Studie zu staatlichen Zugriffen beim Cloud Computing, ZD-Aktuell 2012, 03132 – beck online; Vgl. Van Hoboken/Arnbak/Van Eijk, Studie des Instituts für Informationstechnik der Universität Amsterdam, „Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act“), abrufbar unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2181534)

2. Outsourcing im außereuropäischen Kontext

2.2 Zukunft des Safe-Harbor-Abkommens

►B

ENTSCHEIDUNG DER KOMMISSION

vom 26. Juli 2000

gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA

(Bekannt gegeben unter Aktenzeichen K(2000) 2441)

(Text von Bedeutung für den EWR)

(2000/520/EG)

(ABl. L 215 vom 25.8.2000, S. 7)

Berichtigt durch:

►C1 Berichtigung, ABl. L 115 vom 25.4.2001, S. 14 (2000/520/EG)

2. Outsourcing im außereuropäischen Kontext

2.2 Zukunft des Safe-Harbor-Abkommens

Sitzung des Düsseldorfer Kreises am 28./29. April 2010 in Hannover

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover (überarbeitete Fassung vom 23.8.2010)

Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen

2. Outsourcing im außereuropäischen Kontext

2.2 Zukunft des Safe-Harbor-Abkommens

EUROPEAN COMMISSION

MEMO

Brussels, 19 July 2013

Informal Justice Council in Vilnius

At the informal Justice Council in Vilnius today, Vice President Reding made the following remarks:

On data Protection

"Today's Council meeting sent a powerful signal to citizens. All EU institutions agree that we have to join forces in order to have a strong European data protection law for our continent.

Without the France-German motor, it cannot work.

It is good to see that the French and German ministers have reaffirmed, in a joint declaration, that we need a high level of data protection for European citizens, which strikes the right balance between freedom and security.

It is also good to see that they have both committed to quickly adopting the reform of Europe's data protection rules that the Commission put on the table in January 2012.

PRISM has been a wake-up call. The data protection reform is Europe's answer."

On Safe Harbour

"The Safe Harbour agreement may not be so safe after all.

It could be a loophole for data transfers because it allows data transfers from EU to US companies – although US data protection standards are lower than our European ones.

I have informed ministers that the Commission is working on a solid assessment of the Safe Harbour Agreement which we will present before the end of the year."

2. Outsourcing im außereuropäischen Kontext

2.3 Datenschutz und Datensicherheit durch Standardvertragsklauseln?

- Beispiel: Standardvertragsklauseln 2010/87/EU -

BESCHLUSS DER KOMMISSION

vom 5. Februar 2010

über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates

(Bekannt gegeben unter Aktenzeichen K(2010) 593)

(Text von Bedeutung für den EWR)

(2010/87/EU)

2. Outsourcing im außereuropäischen Kontext

2.3 Datenschutz und Datensicherheit durch Standardvertragsklauseln?

- Beispiel: Standardvertragsklauseln 2010/87/EU -

Klausel 5: Garantie des Datenimporteurs, dass er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen

Berechtigungen des Datenexporteurs bei Verstößen:

- **Aussetzung der Datenübermittlung / Rücktritt vom Vertrag**

2. Outsourcing im außereuropäischen Kontext

2.3 Datenschutz und Datensicherheit durch Standardvertragsklauseln?

- Beispiel: Standardvertragsklauseln 2010/87/EU -

Klausel 4d):

d) die Sicherheitsmaßnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligem Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung geschützt sind;

2. Outsourcing im außereuropäischen Kontext

2.3 Datenschutz und Datensicherheit durch Standardvertragsklauseln?

- Beispiel: Standardvertragsklauseln 2010/87/EU -

Art. 4 des Beschlusses der Kommission v. 5. Februar 2010 (2010/87/EU) i.V.m. Art. 13 der Richtlinie 95/46/EG:
Verbieten / Aussetzen der Datenübermittlung in Drittland durch Aufsichtsbehörde?

Artikel 4

(1) Unbeschadet ihrer Befugnisse, tätig zu werden, um die Einhaltung nationaler Vorschriften gemäß den Kapiteln II, III, V und VI der Richtlinie 95/46/EG zu gewährleisten, können die zuständigen Kontrollstellen in den Mitgliedstaaten ihre Befugnisse ausüben und zum Schutz von Privatpersonen bei der Verarbeitung ihrer personenbezogenen Daten die Datenübermittlung in Drittländer verbieten oder aussetzen, wenn

a) feststeht, dass der Datenimporteur oder Unterauftragsverarbeiter nach den für ihn geltenden Rechtsvorschriften Anforderungen unterliegt, die ihn zwingen, vom anwendbaren Datenschutzrecht in einem Maß abzuweichen, das über die Beschränkungen hinausgeht, die im Sinne von Artikel 13 der Richtlinie 95/46/EG für eine demokratische Gesellschaft erforderlich sind, und dass sich diese Anforderungen wahrscheinlich sehr nachteilig auf die Garantien auswirken würden, die das anwendbare Datenschutzrecht und die Standardvertragsklauseln bieten,

3. Datensicherheit <-> Tracking?

3.1 Verschlüsselung

- Transportverschlüsselung
- Verschlüsselung von Inhalten
- Notwendigkeit der Entschlüsselung für Datenverarbeitung

3. Datensicherheit <-> Tracking?

3.2 Protokollierung

- Protokolldaten müssen darüber Auskunft geben können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.
- Protokolldaten dürfen nicht nachträglich verändert werden können und nur Berechtigten zugänglich sein.
- Die Nutzung administrativer Rechte muss zu einem Protokolleintrag führen.
- Protokolldaten müssen Auskunft geben zu: Zeitpunkt einer Tätigkeit/eines Ereignisses, Bezeichnung von Tätigkeit/Ereignis, mit Tätigkeit/Ereignis befasste Person bzw. Systemkomponente, Zweck der Tätigkeit
- Aufbewahrungsdauer von Protokollen muss definiert werden.

3. Datensicherheit <-> Tracking?

3.3 Mandantenfähigkeit

- Abgeschlossener Datenhaltungs- und Verarbeitungskontext einer Daten verarbeitenden Stelle = „Mandant“
- Ziel: getrennte Datenverarbeitung mehrerer Mandanten (verschiedene gesetzliche Vorgaben, unterschiedliche Fachverfahren, verschiedene Verfahrenszwecke)
- Verarbeitungsfunktionen und Konfigurationseinstellungen sind für jeden Mandanten eigenständig festlegbar.

Fragen?