Auftragsdatenverarbeitung
Gängelung oder Chance für IT-Dienstleister?

SSW Schneider Schiffer Weihermüller
Rechtsanwalt Dominik Hausen
München, 16.5.2011

SSW SCHNEIDER SCHIFFER WEIHERMÜLLER
Rechtsanwälte Steuerberater Wirtschaftsprüfer

Gliederung:

Typische Situation beim Dienstleister

Auftragswas?

Ja, ich hoste bei mir Daten meiner Kunden.

Verstehe, dass mein Kunde nicht will, dass ich Unfug mit seinen Daten treibe.

Ich habe meine Server doch gegen alle bekannten Schwachstellen gesichert.

Auch eine Geheimhaltungs-vereinbarung habe ich schon unterzeichnet.

Was kann der Kunde jetzt noch von mir wollen?

SSW SCHNEIDER SCHIFFER WEIHERMÜLLER
Rechtsanwälte Steuerberater Wirtschaftsprüfer

Die Einhaltung von Datenschutzvorschriften…

Beispiel aus der Presse (1)

- BKK Gesundheit, zweitgrößte größte deutsche Betriebskrankenkasse (1,4 Millionen Versicherte)
- BKK erlaubt Mitarbeitern eines **externen Telefondienst-leisters** Zugriff auf Datensätze ihrer Mitglieder
- Zugriff vom Heimarbeitsplatz umfasste auch Gesundheitsdaten
- Mitarbeiter des Dienstleisters erpresst BKK Gesundheit
- Die Sprecherin der Kasse sagte, bei der Firma sei **keine Datenschutzprüfung** erfolgt.

Quelle: Meldung auf sueddeutsche.de vom 11.2.2010

Beispiel aus der Presse (2)

Was ist hier schief gelaufen?

- Mangelhafte Auswahl des Outsourcing-Dienstleisters
- Keine ausreichende Überwachung des Dienstleisters

Mögliche Konsequenzen für die Krankenkasse?

- Geldbuße bis zu 300.000 €
- Schadensersatzansprüche der Betroffenen

Mögliche Konsequenzen für den Dienstleister?

- Vorfall ist Dokumentation der datenschutzrechtlichen Unzuverlässigkeit
- Dienstleister darf von Auftraggeber nicht für die Verarbeitung personenbezogener Daten ausgewählt werden.

Die Einhaltung von Datenschutzvorschriften…

…eine hohe Hürde, die Kunde und Dienstleister gemeinsam nehmen müssen.

- Mit der Aufnahme einer einzelnen Klausel in den Vertrag ist es nicht getan!
- Mit der einmaligen Ausarbeitung einer Vereinbarung zum Datenschutz ist es ebenfalls nicht getan!

SSW SCHNEIDER SCHIFFER WEIHERMÜLLER
Rechtsanwälte Steuerberater Wirtschaftsprüfer

Begrifflichkeiten

Dienstleister

=

Auftragnehmer

=

Auftragsdaten-verarbeiter

Kunde

=

Auftraggeber

=

„Herr der Daten“

Auftragsdatenverarbeitung ist…

…wenn ein Dienstleister personenbezogene Daten ausschließlich nach Weisung seines Auftraggebers verarbeitet.

→ „Outsourcing“ der Datenverarbeitung

→ Auftragnehmer bloß „technisches Serviceunternehmen“

→ Aufgabe/Funktion verbleibt beim Auftraggeber

Auftragsdatenverarbeitung ist…

- Lohnabrechnung durch ein Dienstleistungszentrum
- Einscannen des schriftlichen Posteingangs durch einen Dienstleister
- Werbeadressenpflege und -ausdruck sowie Werbepostversand durch einen Lettershop
- Kontaktdatenerhebung durch ein Callcenter

Auftragsdatenverarbeitung ist aber auch...

- Auslagerung IT in **konzernangehöriges Unternehmen**.
  →Kein Konzernprivileg im Datenschutzrecht

- Fernzugriff von IT-Dienstleistern auf eigene IT-Infrastruktur zu **Wartung**szwecken

- **Aktenvernichtung**, Entsorgung von Datenträgern

Achtung: Regelungen über Auftragsdatenverarbeitung auch anwendbar, wenn Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, § 11 Abs. 5 BDSG.

Das Problem…

…fehlendes Problembewusstsein.

„Wir verarbeiten nicht die Daten, sondern die Bits."

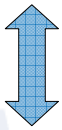
eco LocalTalk am 3.2.2011 zum Thema Cloud Computing

Michael Kranawetter
Chief Security Advisor Deutschland
Microsoft Deutschland GmbH

…also betrifft mich das Thema Datenschutz nicht.

Abgrenzung zwischen Datenschutz und Datensicherheit

Das **Datenschutzrecht** schützt natürliche Personen vor der Gefahr der Verletzung ihres Persönlichkeitsrechts.



Die **Datensicherheit** schützt IT-Systeme, also insbesondere Hardware, Software, Daten vor der Gefahr des Verlustes, der Zerstörung oder des Missbrauchs durch Unbefugte.

SSW SCHNEIDER SCHIFFER WEIHERMÜLLER
Rechtsanwälte Steuerberater Wirtschaftsprüfer

Vorteil der Auftragsdatenverarbeitung

Privilegierung

Keine gesonderte Erlaubnis für Datenverarbeitung durch Dienstleister notwendig.

Keine Einwilligung der Betroffenen in die Auslagerung notwendig.

Auftragsdatenverarbeitung hat zur Folge…

…dass Datenbewegungen zwischen Auftraggeber und Auftragnehmer keine Datenübermittlungen im Sinne des BDSG darstellen

…und damit einer **internen Nutzung gleichgestellt** sind.

Auftragsdatenverarbeitung liegt nicht vor, wenn…

…die Übertragung einer Aufgabe über eine datenverarbeitende Hilfsfunktion hinausgeht.

…und damit eine eigenverantwortliche Wahrnehmung durch eine andere Stelle vorliegt.

…und somit eine sog. **Funktionsübertragung** vorliegt.

Auftragsdatenverarbeitung ist im Regelfall nicht…

- Personalverwaltung durch ein zentrales Konzernunternehmen
- Buchhaltung und Steuerberatung durch einen Steuerberater
- Kontoführung durch eine Bank
- Versicherungsbetreuung/-beratung durch einen selbständigen Handelsvertreter

und somit Funktionsübertragung

Zulässigkeit von Datenübermittlungen beurteilen sich nach allgemeinen Vorschriften des BDSG (§4 Abs. 1).

Im Falle der Auftragsdatenverarbeitung

Kunde ist

- datenschutzrechtlich verantwortliche Stelle für „seine“ Daten (z.B. Mitarbeiter- und Kundendaten)

Kunde haftet

- für nicht sorgfältige Auswahl und Überwachung von Dienstleistern

Kunde bleibt dies auch

- bei einer Auslagerung von Dienstleistungen an Dritte (Outsourcing)

Dienstleister

- hat ein Interesse, dem Kunden seine Zuverlässigkeit nachzuweisen, damit er den Auftrag erhält.

Erfüllen Kunde und Dienstleister nicht § 11 BDSG, sind beide datenschutzrechtlich verantwortlich.

Gliederung:

SSW SCHNEIDER SCHIFFER WEIHERMÜLLER
Rechtsanwälte Steuerberater Wirtschaftsprüfer

Schutzobjekt: Personenbezogene Daten (1)

Nach § 3 Abs.1 BDSG:

„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren [!] natürlichen Person (Betroffener).“

Alles was direkt oder indirekt in Verbindung mit einem Menschen steht.

- private Angaben
- **berufliche** und sonstige Informationen

→ personenbezogen > persönlich

Schutzobjekt: Personenbezogene Daten (2)

Auch im Business-Einsatz gibt es kaum Daten, die keinen Personenbezug aufweisen.

Denn es reicht schon aus, wenn ein Dritter den Personenbezug herstellen kann!

Grundsatz im Datenschutzrecht: Verbotsprinzip

Jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten, die nicht explizit erlaubt ist, ist verboten, vgl. § 4 Abs. 1 BDSG.

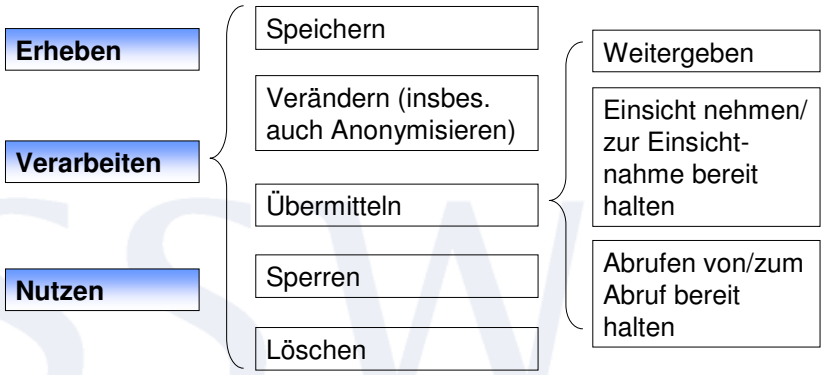
Grds. sind Datenübermittlungen an Dritte verboten!

Erlaubnis aufgrund:

- Gesetz
- Einwilligung des Betroffenen

Phasen des Umgangs mit personenbezogenen Daten (1)

Definition in § 3 Abs. 3 bis Abs. 6a BDSG:



Phasen des Umgangs mit personenbezogenen Daten (2)

Erheben

Verarbeiten

Nutzen

Die Begriffe werden im deutschen und europäischen Datenschutzrecht unterschiedlich verwendet und sollten bei Vertragsgestaltung ausdrücklich definiert werden, um Missverständnisse und eventuelle Regelungslücken zu vermeiden.

Europarechtlich (RL 95/46/EU) ist „Verarbeiten“ der **Oberbegriff** für jede Form der Erhebung, Verarbeitung und Nutzung.

Erlaubnis aufgrund Einwilligung des Betroffenen

Einwilligung kann grds. jede DV legitimieren. Voraussetzung:

+ informiert

+ konkret

+ freiwillig

Problem: Einholen Einwilligung unpraktikabel, da

- Grds. Schriftlichkeit
- Vielzahl Betroffener
- Hohe Hürden an wirksame Einwilligung
- Jederzeitige Widerruflichkeit
- Im Arbeitsverhältnis generell problematisch

Gesetzlich erlaubte Datenverarbeitung (DV)

Hauptanwendungsfall:
DV ist zur Begründung, Durchführung oder Beendigung eines Vertrages mit dem Betroffenen **erforderlich** (vgl. § 28 Abs. 1 S. 1 Nr. 1 BDSG).

Problem: Nicht „erforderlich“ bei Auslagerung von DV aus Gründen der

- Organisatorischen und finanziellen Entlastung
- Fehlenden Kompetenz für die Sicherstellung eines ordnungsgemäßen technischen Ablaufs

Konsequenzen fehlender Erlaubnis zur DV

Verstoß gegen formelles Datenschutzrecht:
Ordnungswidrigkeit mit Bußgeld bis zu 50.000 € (§ 43 Abs. 1, 3 BDSG)

Verstoß gegen materielles Datenschutzrecht:

- Ordnungswidrigkeit mit Bußgeld bis zu 300.000 € (§ 43 Abs. 2 BDSG)
- Bei Bereicherungs- oder Schädigungsabsicht bis zu 2 Jahre Freiheitsstrafe

„Selbstanzeigeverpflichtung“ bei Datenschutzpannen (§ 42a BDSG)

Vorteil der Auftragsdatenverarbeitung

Auftragsdatenverarbeitung ist keine Gängelung des Auftraggebers

sondern

Chance

„Preis“ der Privilegierung: Enge vertragliche Vorgaben

Ziel der Regelungen zur Auftragsdatenverarbeitung:

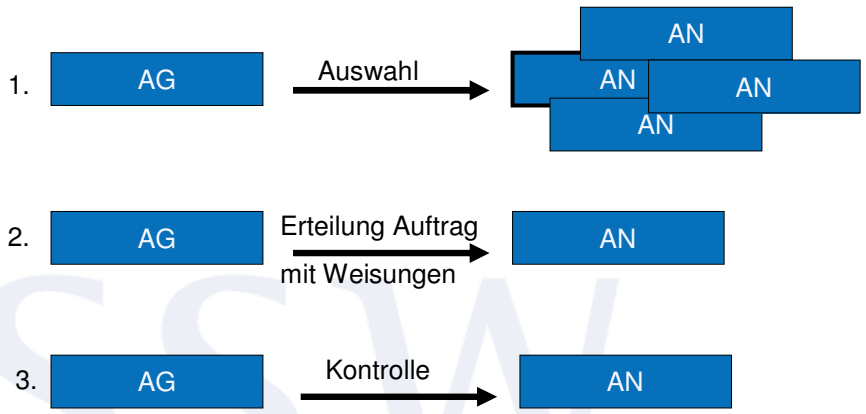
Keine Erhöhung der Gefährdung für Betroffene durch Fremdvergabe der Datenverarbeitung.

Gliederung:

Voraussetzungen des § 11 BDSG

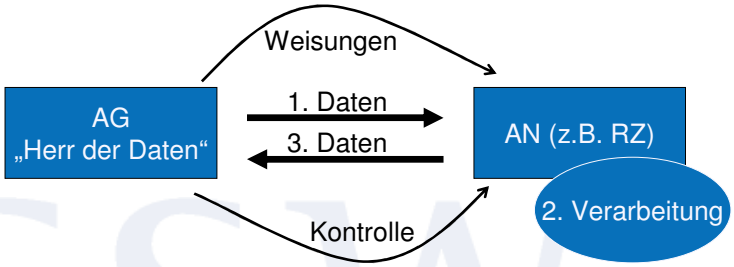
- Der Auftraggeber muss den Auftragnehmer unter Berücksichtigung der Eignung und der getroffenen technischen und organisatorischen Maßnahmen sorgfältig **auswählen**, § 11 Abs.2 S.1 BDSG.
- Der Auftragnehmer ist **schriftlich** zu beauftragen, § 11 Abs.2 S. 2 BDSG. (10-Punkte-Katalog)
- Der Auftraggeber muss dem Auftragnehmer **Weisungen** zur Verarbeitung und/oder Nutzung der Daten erteilen, § 11 Abs.3 S. 1 und § 11 Abs. 2 S.2 BDSG.
- Der Auftraggeber muss die Einhaltung der erteilten Weisungen **überprüfen**, § 11 Abs. 2 S.2 Nr. 9 BDSG.

Ablauf einer Auftragsdatenverarbeitung



Dokumentationspflichten beachten !

Schema Auftragsdatenverarbeitung, § 11 BDSG



1. Schritt: Auswahlentscheidung (1)

„Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen ***sorgfältig auszuwählen****.“* (§ 11 Abs. 2 Satz 1 BDSG)

„Der Auftraggeber hat sich ***vor Beginn der Datenverarbeitung*** *und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.“* (§ 11 Abs. 2 Satz 4 BDSG)

„Das Ergebnis ist zu ***dokumentieren****.“* (§ 11 Abs. 2 Satz 5 BDSG)

1. Schritt: Auswahlentscheidung (2)

Hürde für Dienstleister:

Beim Thema Datenschutz eine guten Eindruck beim Kunden hinterlassen.

Andernfalls: Gefahr, beim Bieterrennen auszuscheiden.

Hürde für Auftraggeber:

Ordnungsgemäße Auswahlentscheidung treffen und diese nachvollziehbar dokumentieren.

Andernfalls: Gefahr einer Geldbuße bis zu 50.000 € bei Verstoß gg. § 11 Abs. 2 Satz 4 BDSG, vgl. § 43 Abs. 1 Nr. 2b BDSG.

1. Schritt: Auswahlentscheidung (3)

Technische und organisatorische Maßnahmen nach § 9 BDSG u. Anlage

Zutrittskontrolle	→	Verh. Zutritt durch Unbefugte
Zugangskontrolle	→	Verh. Nutzung durch Unbefugte
Zugriffskontrolle	→	Regelung Zugriff der Berechtigten
Weitergabekontrolle	→	u.a. Sicherung des Transports
Eingabekontrolle	→	u.a. Nachvollziehbarkeit der DV
Auftragskontrolle	→	DV nur nach Weisung des AG
Verfügbarkeitskontrolle	→	Backup, jederzeitiger Zugriff
Trennungskontrolle	→	getrennte Verarbeitung unterschiedlicher Daten

Maßnahmen sind konkret sachverhaltsbezogen anzusprechen!

2. Schritt: Schriftliche Beauftragung, Festlegungen (1)

1. Gegenstand und Dauer des Auftrags
2. - Umfang, Art und Zweck der DV,
   - Art der Daten und
   - Kreis der Betroffenen
3. Technische und organisatorische Maßnahmen
4. Benachrichtigung, Löschung und Sperrung von Daten
5. Wahrung Datengeheimnis, Kontrolle Umsetzung und Einhaltung technischer und organisatorischer Maßnahmen durch Auftragnehmer selbst
6. Berechtigung zum Einsatz von Subunternehmern

SSW SCHNEIDER SCHIFFER WEIHERMÜLLER
Rechtsanwälte Steuerberater Wirtschaftsprüfer

2. Schritt: Schriftliche Beauftragung, Festlegungen (2)

7. die Kontrollrechte des Auftraggebers, Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. Pflicht des Auftragnehmers zur Mitteilung von Datenschutzverstößen und Verstößen gegen die im Auftrag getroffenen Festlegungen
9. Umfang der Weisungsbefugnisse des Auftraggebers gegenüber dem Auftragnehmer,
10. Rückgabe überlassener Datenträger an AG und Löschung beim AN gespeicherter Daten nach Beendigung des Auftrags

1. Gegenstand und Dauer des Auftrags

- **Gegenstand**: Lohnabrechnung, FiBu, Werbeaussendungen, Callcenter-Dienste, Kundenbefragungen im Auftrag, Internet-Providing, Betreuung IT-Systeme, Wartung/Fernwartung, Datenträgerentsorgung.

  Tipp: Beschreibung muss für Datenschutzbehörde verständlich sein.

- **Dauer**: einmalig, befristet, unbefristet mit Kündigungsmöglichkeit,

2. Umfang des Auftrags, Daten, Betroffene (1)

- **Umfang, Art und Zweck der Datenverarbeitung**:
  - Welche Leistungen sind im Einzelnen zu erbringen ? Bezug auf Leistungsverzeichnis, Pflichtenheft?
  - Auftragsdatenverarbeitung nur mi Inland, auch im EU/EWR-Bereich oder auch in Drittstaaten?
  - Welche Leistungsphasen sollen außer Haus gegeben werden?
  - Vorübergehende oder dauernde Speicherung von Daten beim DL?
  - Welche Menge an Daten, Datensätzen, Datenträgern?
  - Nur Verwendung von Telefondaten oder E-Mail-Adressen mit nachweisbarem Opt-in

2. Umfang des Auftrags, Daten, Betroffene (2)

- **Art der Daten**: Personaldaten, Vertragsdaten, Werbedaten, Werbewidersprüche, Befragungsergebnisse, Gesundheitsdaten, Nutzungsdaten aus Telemedien- oder Telekommunikationsdiensten, DV-Protokolldaten.

- **Kreis der Betroffenen**: Mitarbeiter, Stellenbewerber, Kunden, Interessenten, Lieferanten, Werbekontakte, Besucher/Gäste, Passanten, Systemnutzer

3. Technische und organisatorische Maßnahmen

- Beispiele für Themen:
  - Festlegung Transportwege und -verfahren für die Daten mit den dabei zu treffenden Sicherheitsmaßnahmen
  - Technische Vorsorgemaßnahmen zur Ausfallsicherheit (Ersatz-RZ, Notfalleinrichtungen)
  - Verfahrensweise zur Trennung der Daten verschiedener Auftraggeber
  - Festlegungen zu Protokollierungen der Verarbeitungen beim Dienstleister
  - Festlegungen zur Aufbewahrung von zu entsorgenden Datenträgern und der Sicherheitsstufe für die Löschung/Vernichtung.
  - Regelungen zum Schutz vor Datenunterschlagung (USB-Sticks)

4. Berichtigung, Löschung, Sperrung von Daten

- Mitwirkung des DL bei Anträgen von Betroffenen an den Auftraggeber nach § 35 BDSG.
- Führung von Werbesperrlisten für den Auftraggeber
- Sperrung oder Löschung von Daten nach abgrenzbaren Datenverarbeitungsschritten, sichere Löschverfahren
- Löschfristen für die Daten bei Videoüberwachung, für Nutzungsdaten beim Internetprovider.

5. Pflichten des Auftragnehmers, insb. Kontrollen (1)

- Relevante Pflichten nach § 11 Abs. 4 BDSG:
  - Datengeheimnis, § 5 BDSG
  - Datensicherheit, § 9 BDSG
  - Beauftragter für den Datenschutz, §§ 4f, 4g BDSG

5. Pflichten des Auftragnehmers, insb. Kontrollen (2)

- Beispiele:
  - ➢Verpflichtung der Beschäftigten auf das Datengeheimnis einschließlich entsprechender Belehrung
  - ➢Bestellung eines Datenschutzbeauftragten beim Dienstleister
  - ➢Mitteilung von Name und Kontaktdaten des Datenschutzbeauftr.
  - ➢Eigene Kontrollmaßnahmen des DL zur Einhaltung des Datenschutzes und der Datensicherheit, Erstellung von Prüfberichten
  - ➢Kontrolle der Arbeitsergebnisse durch den DL
  - ➢Kontrollen des DL bei eingesetzten Subunternehmen

SSW SCHNEIDER SCHIFFER WEIHERMÜLLER
Rechtsanwälte Steuerberater Wirtschaftsprüfer

6. Subunternehmerverhältnisse

- Möglichkeiten:
  - ➢ Verbot von Subunternehmerverhältnissen
  - ➢ Zulässig nach vorheriger Genehmigung durch den Auftraggeber
  - ➢ Genehmigung muss sich auf konkreten Subunternehmer beziehen, Benennung im Vertrag.
- Festlegung, ob Subunternehmer aus dem Inland, dem EU-/EWR-Raum oder einem Drittstaat
- Einsatz von Subunternehmern für welche Zwecke, in welchem Umfang
- Zulässigkeit von Sub-Subunternehmerverhältnissen

Wichtig: Notwendige Nebenleistungen von Externen beim Dienstleister, (z.B. Telekommunikationsleistungen) sind keine DV durch Subunternehm.

7. Kontrollrechte des Auftraggebers

- Umfang der Kontrollrechte (mit bzw. ohne Vorankündigung)
- Duldungs- und Mitwirkungspflichten des Dienstleisters
- Kontrollen beim Dienstleister (und ggf. Sub.) vor Ort
- Wer führt welche Kontrollen von Seiten des Auftraggebers aus und wer wirkt beim Dienstleister mit (Ansprechpartner).
- Einsichtsrechte des Auftraggebers in
  - DV-Protokolle
  - Berichte der Revision, des Datenschutzbeauftragten
  - in vom Dienstleister veranlasste externe Audits
- Mitlesen am Kontrollbildschirm bei Fernwartung
- Kontrolle des Opt-in bei Werbemaßnahmen
- Zutrittsrechte in Privatwohnungen bei Tele-/Heimarbeit.

8. Benachrichtigungspflicht des Dienstleisters bei Verstößen gegen Datenschutz und Festlegungen

- Neu: wg. Pflicht des Auftraggebers nach § 42a BDSG (Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten)
- Festlegungen: Welche Art, welcher Grad von Verstößen ist mitzuteilen (Fehlversendungen, verlorene Datenträger, unterschlagene Daten, Zugangs-/Passwortoffenlegungen)
- Nicht nur Verstöße des Dienstleisters und seiner Beschäftigten, sondern auch rechtswidrige Handlungen Dritter (z.B. Subunternehmer, Hacker, Einbrecher).

9. Umfang Weisungsbefugnisse des Auftraggebers

- Einzelweisungen zur Auftragserledigung
- Einzelanweisungen zu zusätzlichen Sicherheitsmaßnahmen
- Anweisungen zum Vorgehen bei Datenschutzverstößen
- Weisungen zur Gestaltung und Beendigung von Subunternehmerverhältnissen
- Wer erteilt die Weisungen seitens des Auftraggebers und an welchen Mitarbeiter sind die Weisungen beim Dienstleister zu richten
- In welcher Form erfolgen Weisungen

10. Datenrückgabe

- Was ist wann wie zurückzugeben.
- Wie soll „zurückgegeben“ werden: Echte Rückgabe oder Rückgabe durch Löschung/Vernichtung von Datenträgern

2. Schritt: Schriftliche Beauftragung, Festlegungen (3)

Hürde für Dienstleister:

-Erreichen einer ausgewogenen Regelung hinsichtlich

- der zu ergreifenden technischen und organisatorischen Maßnahmen
- der Ausgestaltung der Weisungs- und Kontrollrechte des Kunden

-evtl. durch Einbringen eigener Regelungsvorschläge in die Vertragsverhandlungen.

2. Schritt: Schriftliche Beauftragung, Festlegungen (4)

Hürde für Auftraggeber:

Vermeiden einer fehlerhaften Auftragserteilung: Katalog von 10 Punkten sind zwangsweise schriftlich zu regeln!

Ordnungsgemäße Dokumentation der Einhaltung der IT-Sicherheitsmaßnahmen durch den Dienstleister.

Andernfalls: Gefahr einer Geldbuße bis zu 50.000 € bei Verstoß gg. § 11 Abs. 2 Satz 2 BDSG, vgl. § 43 Abs. 1 Nr. 2b BDSG.

3. Schritt: Kontrolle der Datenverarbeitung (1)

„Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann **regelmäßig** *von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen."* (§ 11 Abs. 2 Satz 4 BDSG)

„Das Ergebnis ist zu dokumentieren." (§ 11 Abs. 2 Satz 5 BDSG)

3. Schritt: Kontrolle der Datenverarbeitung (2)

Pflicht zu Vor-Ort-Kontrollen?

Gesetzestext als auch Gesetzesbegründung verlangen diese nicht verpflichtend.

Ausreichend kann sein:

- Vom Dienstleister vorgelegtes schlüssiges Datensicherheitskonzept
- Ein durchgeführtes externes Audit

3. Schritt: Kontrolle der Datenverarbeitung (3)

Kontrollhäufigkeit ?

Je nach Sachverhalt Fristen zwischen 1 und 3 Jahren angemessen.

Abhängig von mehreren Faktoren:

- Berichterstattung in den Medien zu Datenschutzverletzungen
- Eigene und fremde Erfahrungen mit dem Dienstleister bzw. Branche

Berichte über Datenschutzvorfälle (1)

27.04.2011 08.37 « Vorige | Nächste »

Angriff auf Playstation Network: Persönliche Daten von Millionen Kunden gestohlen

vorlesen / MP3-Download

Rund eine Woche, nachdem Sony sein Playstation Network und den Video- und Musikservice Qriocity abgeschaltet hat, gab der Elektronikkonzern am Dienstagabend in seinem offiziellen Playstation-Blog eine Erklärung zu dem Vorfall ab. Hatte Sony bislang zuvor lediglich von einem "externen Eingriff" gesprochen, teilte das Unternehmen nun mit, dass man davon ausgehe, dass sich zwischen dem 17. und 19. April 2011 eine "unbefugte Person" Zugriff auf die persönlichen Daten der Nutzer der genannten Netzwerke verschaffen konnte – darunter auf deren Namen, Anschrift und Geburtsdatum sowie Log-in und Passwort. Darüber hinaus könne es laut Sony möglich sein, dass auch die Profilangaben inklusive Kaufhistorie und Rechnungsanschrift sowie die Sicherheitsfragen zum Passwort widerrechtlich abgerufen wurden.

Berichte über Datenschutzverletzungen (2)

28.04.2011 16:30 « Vorige | Nächste »

Wolkenbruch bei Amazon: Datenverlust in der Cloud

vorlesen / MP3-Download

Die Panne des Cloud-Service Amazon EC2 hat schwerwiegende Folgen. Beim Crash des Angebots vergangene Woche ging eine unbekannte Anzahl an Daten unwiederbringlich verloren. Das geht aus einer von Amazon an betroffene Kunden verschickten Mail hervor, welche das US-Magazin Business Insider veröffentlichte. Amazon räumt darin ein, Versuche zur manuellen Wiederherstellung der Kundendaten seien gescheitert.

Nach wie vor hat sich das Unternehmen aus Seattle nicht dazu geäußert, wie es zum mehrstündigen Ausfall der Serverwolke kommen konnte. "Die Cloud, auf die Sie sich verlassen können" (Produktbeschreibung) war bislang nicht zuletzt in der US-Technologieszene äußerst beliebt; zahlreiche viel besuchte Internetdienste wie Foursquare, Quora und Reddit waren von der Störung betroffen und mehrere Stunden lang [illegible].

Berichte über Datenschutzvorfälle (3)

News-Meldung vom 28.04.2011 15:44 « Vorige | Nächste »

Tomtom entschuldigt sich wegen Datenweitergabe für Radarfallen

vorlesen / MP3-Download

Tomtom, einer der größten Navigationsgerätehersteller, hat seine gespeicherten Verkehrsdaten an die niederländische Regierung verkauft und ist nun über deren Nutzung wenig begeistert. Die Regierung hat die erworbenen Daten nämlich nicht, wie von Tomtom angenommen, zur Verbesserung des Straßennetzes verwendet, sondern um Temposünder zur Kasse zu bitten. Der Firmenchef von Tomtom, Harold Goddijn, entschuldigt sich nun öffentlich für diesen Vorfall.

Berichte über Datenschutzvorfälle (4)

28.04.2011 19:47 « Vorige | Nächste »

Datenpanne: Unesco entblößt Bewerber im Netz

vorlesen / MP3-Download

Die UN-Organisation für Bildung, Wissenschaft und Kultur (Unesco) hat über Jahre hinweg Bewerbungsunterlagen für jeden einsehbar ins Internet gestellt. Die Dokumente enthielten nach Recherchen von Spiegel Online Informationen über den Bildungsweg, die bisherigen Arbeitgeber und zum Teil auch Angaben über Jahresgehälter. Betroffen waren zwei Datenbanken, eine mit Bewerbungen um Praktikumsplätze, die andere für reguläre Posten innerhalb der Organisation. "Ja, es gab ein echtes Problem", bestätigte eine Unesco-Sprecherin am Donnerstagabend gegenüber dpa in Paris. Die Sicherheitslücken seien nach ihren Informationen aber mittlerweile geschlossen.

Laut dem Bericht von Spiegel Online waren Zehn-, womöglich Hunderttausende Bewerbungsunterlagen frei im Internet abrufbar – inklusive Anschreiben und Adressen. Aus den Bewerbungen erfahre man zum Beispiel exakt, wie viel ein leitender Mitarbeiter im diplomatischen Dienst Pakistans verdiene (einen sechsstelligen Dollar-Betrag) und welche Angestellten der Weltbank zur Unesco wechseln wollen. Die Bewerber kämen aus aller Welt. Unter ihnen seien Diplomaten und Wissenschaftler. "Die Unesco und ich, das könnte eine Liebesgeschichte werden", zitiert Spiegel Online aus dem Anschreiben einer Bewerberin. Die stichprobenweise eingesehenen Bewerbungen stammten aus den Jahren 2006 bis 2011.

Berichte über Datenschutzvorfälle (5)

15.05.2011 14:09 « Vorige | Nächste »

US-Behörde soll sich mit Dropbox beschäftigen

vorlesen / MP3-Download

Der IT-Blogger Christopher Soghoian hat sich laut dem Magazin *Wired* bei der US-amerikanischen Handelsbehörde Federal Trade Commision (FTC) über den populären Anbieter von Internet-Speicherplatz Dropbox beschwert (PDF-Datei). Seiner Meinung nach setzt das Unternehmen die Verschlüsselung für die von Benutzern abgespeicherten Daten nicht bestmöglich ein. Deshalb sollen Dropbox-Mitarbeiter die Kundendateien einsehen können. Bislang hat Dropbox aber damit geworben, dass dem Unternehmen anvertraute Daten in manchen Fällen sicherer seinen als auf dem eigenen Computer.

Dropbox behauptet auf seiner Website jetzt nicht mehr wie ursprünglich, dass "niemand" die abgespeicherten Daten einsehen kann; das Unternehmen spricht jetzt nur noch von "anderen Dropbox-Benutzern". Das schürt die Spekulationen, dass

Berichte über Datenschutzvorfälle (6)

15.05.2011 14:25 « Vorige | Nächste »

BSI verärgert Ärzte

vorlesen / MP3-Download

Eine Verfügung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sorgt für Verärgerung unter Ärzten und Krankenhausbetreibern. Laut der Verfügung, die heise online vorliegt, dürfen die Kartenlesegeräte für die elektronische Gesundheitskarte (eGK) nur in einer kontrollierten Einsatzumgebung aufgestellt werden, in der sie nicht länger als 30 Minuten unbeaufsichtigt sind. Lesegeräte, über die ein Arzt mit der qualifizierten elektronischen Signatur des Heilberufeausweises seine Unterschrift etwa für Arztbriefe abgibt, dürfen nur so installiert sein, dass sie unter der "dauerhaften [illegible] Kontrolle" des Arztes stehen.

Berichte über Datenschutzvorfälle (7)

28.04.2011 14:15 « Vorige | Nächste »

Google gibt Einblicke in Rechenzentrum

vorlesen / MP3-Download

Mit Hilfe einer Videotour durch eines seiner Rechenzentren versucht der Internetdienstleister Google, Vertrauen in Datendienste in der "Cloud" zu wecken. Angefangen von der Pförtnerkontrolle bis hin zur Vernichtung von nicht mehr dienlichen Festplatten in einem mehrstufigen Prozess zeigt das Unternehmen sieben Minuten lang Einblicke in das Rechenzentrum Moncks Corner im US-Bundesstaat South Carolina, die normalerweise dem Publikum nicht gewährt werden. Dort werden unter anderem Daten von Kunden verarbeitet, die Googles Online-Software wie Textverarbeitung und Tabellenkalkulation nutzen.

Google folgt damit – in kleinerem Rahmen – dem Vorbild des Social Network Facebook, das vor drei Wochen für sein Open Compute Project das Rechenzentrum in Prineville im US-Bundesstaat Oregon vorgestellt hat. Dabei hat Facebook unter anderem technische Spezifikationen für Mainboards und Server-Netzteile, Gehäuse und Schränke sowie Daten und Typen der Transformatoren für den Anschluss ans [illegible]

3. Schritt: Kontrolle der Datenverarbeitung (4)

Hürde für Dienstleister:

Senkung der Kontrollhäufigkeit durch schlüssiges Sicherheitskonzept

Kostentragung von Audits, Kontrollen des Auftraggebers durch den Auftraggeber

Hürde für Auftraggeber:

Ordnungsgemäße Dokumentation der Einhaltung der IT-Sicherheitsmaßnahmen durch den Dienstleister.

Andernfalls: Gefahr einer Geldbuße bis zu 50.000 €, vgl. § 43 Abs. 1 Nr. 2b BDSG.

Gliederung:

Praxishinweise für Dienstleister: Datenschutz als Wettbewerbsvorteil

Proaktive Ansprache des Themas Datenschutz bei Vertragsverhandlungen

- Bewusstsein des Kunden für die Problematik vorhanden?
- Hinweis auf Pflicht zur Berücksichtigung von Datenschutzaspekten bei der Auswahl des Dienstleisters?
- Ggf. Hinweis auf Konsequenzen der Nichtbeachtung des Themas
- Vorlage Aufstellung über standardmäßig vom Dienstleister ergriffene technische und organisatorische Maßnahmen?

SSW SCHNEIDER SCHIFFER WEIHERMÜLLER
Rechtsanwälte Steuerberater Wirtschaftsprüfer

Praxishinweise für Dienstleister Initiative ergreifen durch eigenen Entwurf eines ADV

Entwurf eines Vertragsmusters für eine Auftragsdatenverarbeitung

- Ausfüllen mit Gegenstand und Dauer des Auftrags
- Arbeit mit Lückentext bzw. Ankreuzmöglichkeit dort wo Kunde Input liefern muss
- Ausfüllhilfen für technische und organisatorische Maßnahmen
- Festlegung von Ansprechpartnern (vorzugsweise betriebliche Datenschutzbeauftragte)

Mustertext: Art der Daten

„Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: _____“

oder

„Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezoger Daten sind folgende Datenarten / -kategorien (Aufzählung / Beschreibung der Datenkategorien)

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)“

Mustertext: Zutrittskontrolle
(z.B. zur Überprüfung der Eignung des Auftragnehmers)

„Zutrittskontrolle

☐ Es sind **keine** Maßnahmen zur Zutrittskontrolle erforderlich, weil _____

☐ Es existieren **keine** Maßnahmen zur Zutrittskontrolle.

☐ Es existieren folgende Maßnahmen zur Zutrittskontrolle:
1) _____
2) _____
3) _____

Ggf. separates Zusatzblatt verwenden.“

Mustertext: Ausfüllhilfe Zutrittskontrolle (1)

Zutrittskontrolle

Ziel der Zutrittskontrolle ist es, dass Unbefugten der Zutritt zu solchen Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogener Daten verarbeitet oder genutzt werden.

Vorgehensweise:

1. Festlegung von Sicherheitsbereichen
2. Absicherung der Zugangswege
3. Festlegung von Zutrittsberechtigungen für
   - Mitarbeiter der Firma
   - Firmenfremde (Wartungspersonal, Besucher, usw.)
   - Legitimation der Zutrittsberechtigten
   - Kontrolle des Zutritts

Mustertext: Ausfüllhilfe Zutrittskontrolle (2)

Beispiele für Maßnahmen zur Zutrittskontrolle

- Festlegung befugter Personen
- Betrieb einer elektronischen Zutrittskontrolle
- Beauftragung eines Werkschutzdienstes mit einer Zutrittskontrolle
- Ausgabe von Zutrittsberechtigungsausweisen
- Vorhandensein von Regelungen für Firmenfremde
- Durchführung von Anwesenheitsaufzeichnungen
- Ausgabe von Besucherausweisen
- Sicherung durch Alarmanlage und/oder Werkschutz außerhalb der Arbeitszeit

Mustertext: Ausfüllhilfe Weitergabekontrolle (1)

Ziel der Weitergabekontrolle

ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

SSW SCHNEIDER SCHIFFER WEIHERMÜLLER
Rechtsanwälte Steuerberater Wirtschaftsprüfer

Mustertext: Ausfüllhilfe Weitergabekontrolle (2)

Vorgehensweise

1. Festlegung der Stellen, an die durch die Einrichtungen zur Datenübertragung Daten übermittelt werden können
2. Dokumentation, dass eine Feststellung von "Dritten" möglich ist
3. Festlegung der zur Übermittlung bzw. zum Transport Befugten
4. Festlegung von Bereichen, in denen sich Datenträger befinden dürfen
5. Festlegung von Personen festgelegt, die aus diesen Bereichen befugt Datenträger entfernen dürfen
6. Kontrolle des Entfernens von Datenträgern
7. Absicherung von Bereichen, in denen sich Datenträger befinden
8. Legitimation der zum Transport berechtigten Personen
9. Festlegung der Wege und Verfahren des Transportes
10. Absicherung der Übermittlungen bzw. des Transportes

Mustertext: Ausfüllhilfe Weitergabekontrolle (2)

Beispiele für Maßnahmen zur Übermittlungskontrolle

- Vorhandensein von Dokumentationen der Abruf- und Übermittlungsprogramme,
- Durchführung von Protokollierungen jeder Übermittlung oder einer repräsentativen Auswahl
- Vorhandensein von Verpackungs- und Versandvorschriften (Versand in verschlossenen Behältnissen)
- Durchführung einer Verschlüsselung
- Feststellung zur Übermittlung befugter Personen
- Ausgabe von Datenträgern nur an autorisierte Personen
- Erstellung einer differenzierten Datenträgerverwaltung
- Lagerung von Datenträger in Sicherheitsbereichen

...

3 Mythen der Auftragsdatenverarbeitung

- Auftragsdatenverarbeitung ist nur ein schwer verdaulicher Begriff ohne große praktische Bedeutung

  → Technische Wartung erfordert grds. eine entspr. Vereinb.

- Datenschutz kostet nur Geld, ein „Return of Investment“ ist nicht ersichtlich.

  → Datenschutz wird immer mehr zum Wettbewerbsvorteil

- Datenschutz schützt „nur“ meine Kunden

  → ... und das Ansehen Ihres Unternehmens in der Öffentlichkeit

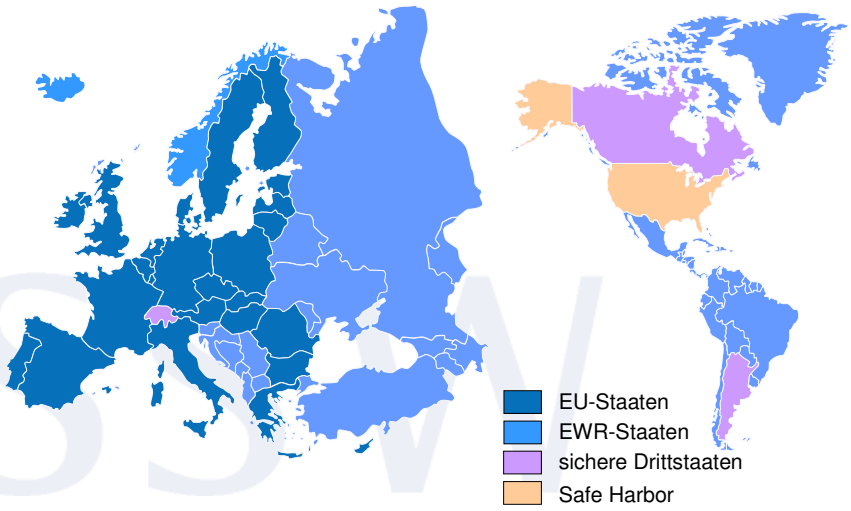
Gliederung:

SSW SCHNEIDER SCHIFFER WEIHERMÜLLER
Rechtsanwälte Steuerberater Wirtschaftsprüfer

Internationale Auftragsdatenverarbeitung

- Beschränkung der Privilegierung auf EU/EWR-Staaten sowie
- auf Staaten, die ein angemessenes Datenschutzniveau gewährleisten können
  - positive Feststellung durch die EU notwendig
  - nur wenige Staaten haben sich bislang darum bemüht
- Einbezug der USA über Safe-Harbor-Abkommen
- Datenübermittlungen an andere als die o.g. Staaten nur bei Abschluss von sog. EU-Standardvertragsklauseln (von der EU-Kommission gestellte Vertragsvorgaben beim Einsatz eines Auftragsdatenverarbeiters in einem so genannten Drittland).

Grenzen einer Auftragsdatenverarbeitung



Safe-Harbor

Anforderungen der Datenschutzbehörden an Auftraggeber (Beschluss des Düsseldorfer Kreises vom 28./29.4.2010):

Nachweis der Safe-Harbor-Zertifizierung und Beachtung der Safe-Harbor-Grundsätze erforderlich (Verlassen auf Behauptung des US-Unternehmens nicht ausreichend):

- Datum der Zertifizierung der Datenimporteure (nicht älter als 7 Jahre)
- Einhaltung der Pflicht zur Information der Betroffenen (Notice-Verfahren: Zweck der DV, Weitergabe Daten an Dritte, Recht auf Auskunft, Berichtigung und Löschung)

Datenexporteure in Deutschland müssen diese Mindestprüfung dokumentieren und auf Nachfrage den Aufsichtsbehörden nachweisen.

Links (1)

- Bayerisches Landesamt für Datenschutzaufsicht

  Erläuterung zu § 11 BDSG, abrufbar unter:

  www.regierung.mittelfranken.bayern.de/aufg_abt/abt1/baylda_daten/auftragsdatenverarbeitung1010.pdf

- Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

  Muster zur Auftragsdatenverarbeitung nach § 11 BDSG (Anpassung an konkreten Auftrag notwendig!), abrufbar in englisch und deutsch unter :

  https://www.gdd.de/nachrichten/news/neues-gdd-muster-zur-auftragsdatenverarbeitung-gemas-a7-11-bdsg

- BITKOM

  Mustervertragsanlage zur Auftragsdatenverarbeitung mit englischer Übersetzungshilfe (Anpassung an konkreten Auftrag notwendig!):

  www.bitkom.org/de/publikationen/38336_45940.aspx

Links (2)

- Zentralarchiv für Tätigkeitsberichte des Bundes- und der Landesdatenschutzbeauftragten und der Aufsichtsbehörden für den Datenschutz (ZafTDA)

  Tätigkeitsberichte, Behördenkompass
  www.th-mittelhessen.de/zaftda/

- Ebenfalls hilfreich:

  Stellungnahmen/Musterverträge/Leitlinien der Datenschutzbehörden

  (z.B. ULD Schleswig-Holstein www.datenschutzzentrum.de, www.datenschutz.de, www.datenschutz-berlin.de, www.duesseldorfer-kreis.de, auf EU-Ebene: Website der Artikel 29 Gruppe http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm)

- Fachzeitschriften:

  zum IT-Recht: CR, ITRB, K&R, MMR
  speziell zum Datenschutz: DuD, RDV

Vielen Dank für Ihre Aufmerksamkeit.

Noch Fragen?

Rechtsanwalt

Dominik Hausen

Beethovenstraße 6
80336 München

dominik.hausen@ssw-muc.de

JUVE Handbuch Wirtschaftskanzleien 2010/2011 über SSW:

„Eine der führenden IT-Boutiquen, die unangefochten auf Augenhöhe mit internationalen Kanzleien agiert und von Mandanten hoch gelobt wird."

IT-Rechts-Team: