ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Sommerakademie 2011

„Optimierte Verantwortungslosigkeit“

Infobörse 9

Wenn andere Daten verarbeiten – von A(uftragsdatenverarbeitung) bis Z(ertifizierung)

Referenten: ***Henry Krasemann (ULD)***
Dr. Thomas Probst (ULD)
Heiko Behrendt (ULD)

Moderation: ***Henry Krasemann (ULD)***

Wenn andere Daten verarbeiten - von A(uftragsdatenverarbeitung) bis Z(ertifizierung)

Sommerakademie 2011
Workshop 9

Heiko Behrendt
Henry Krasemann
Dr. Thomas Probst

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Rechtliche Grundlagen

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Sieben Goldene Regeln des Datenschutzes

- Rechtmäßigkeit
  - Gesetz, Einwilligung, Vertrag, Dienst- oder Betriebsvereinbarung
- Einwilligung
  - Informiert und freiwillig
- Zweckbindung
  - Verwendung nur für Erhebungszweck
- Erforderlichkeit
  - Verarbeitung nur soweit für Erhebungszweck erforderlich
- Transparenz
  - Unterrichtung über Verwendung
- Datensicherheit
  - Organisatorische und technische Vorkehrungen
- Kontrolle
  - Interner / externer Datenbeschutzbeauftragter, Audit

Verantwortlichkeit

- Verantwortlich
  - wer personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt
  - wer andere im Wege der Auftragsdatenverarbeitung für sich tätig werden lässt
- Auftragsdatenverarbeitung
  - Datenverarbeitung nach Weisung des Auftraggebers
  - „Verlängerter Arm“ des Auftraggebers
    - Beispiel: DV im Rechenzentrum
  - Gegenteil: Übermittlung an einen Dritten / Funktionsübertragung

§ 11 BDSG (§ 17 LDSG)

Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

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.

ULD www.datenschutzzentrum.de

§ 11 BDSG (§ 17 LDSG)

- Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

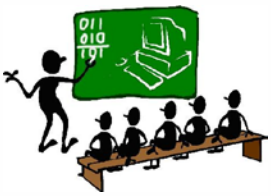
- Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

- Gilt entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 203 StGB

- Keine Auftragsdatenverarbeitung möglich, wenn Verletzung von Privatgeheimnissen
- Gilt für Geheimnisträger wie: Anwälte, Ärzte, Psychologen, Eheberater, Beratungsstellen, Versicherungen, Steuerberater

- Problembereiche: Aktenvernichtung, EDV-Wartung etc.



Auftragsdatenverarbeitung

Probleme der Praxis

Schwachstellen

- Der Umfang, der Zweck und die Nutzung der in Auftrag gegebenen Datenverarbeitung ist nicht konkret festgelegt.
- Der Vertrag über die Auftragsdatenverarbeitung ist lückenhaft und enthält nicht ausreichende Regelungen über die beim Auftragnehmer zu treffenden organisatorischen und technischen Maßnahmen.
- Die beim Auftragnehmer umgesetzten technischen und organisatorischen Maßnahmen sind unzureichend und entsprechen nicht den Anforderungen des Bundes- bzw. Landesdatenschutzgesetzes.

Schwachstellen

- Die vom Auftragnehmer beauftragten Unterauftragnehmer sind dem Auftraggeber nicht bekannt.
- Der Auftraggeber verfügt beim Auftragnehmer über keine Kontrollrechte.
- Eine vom Auftraggeber durchzuführende Kontrolle beim Auftragnehmer ist nicht durchgeführt worden.

Ist nur einer der genannten Punkte nicht erfüllt, werden die datenschutzrechtlichen Anforderungen nicht hinreichend beachtet.

Feststellung der Eignung

- Anforderungskatalog oder Checkliste erstellen
- Schutzbedarf der Daten festlegen
- Sicherheitsnachweis anfordern
- Abweichungen ggf. vor Ort klären
- Datenschutzrechtliche Bewertung durchführen
- Über Eignung entscheiden

Vor-Ort Kontrolle

- Überprüfung der im Vertrag festgelegten Regelungen
- Analyse der Organisationsstrukturen, insbesondere des IT-Sicherheitsmanagements und der Datenkommunikations-prozesse
- Soll-Ist-Abgleich der festgelegten technischen und organisatorischen Maßnahmen
- Korrekturmaßnahmen bei festgestellten Mängeln festlegen
- Erstellung eines Berichts und ggf. Nachkontrolle

Wichtige Vertragsinhalte

- Abgrenzung der Auftragsdatenverarbeitung
- Beschreibung der Datenkommunikationsprozesse
- Sicherheitsmanagement und Sicherheitsvorfallmanagement
- Sicherheitsmaßnahmenkatalog
- Unterauftragsverhältnisse
- Kontrollbefugnis

Zertifizierung als Lösung?

Zertifizierung

- Zertifizierung = Teil einer **Konformitätsbewertung** durch **unabhängige Dritte**
- Konformität: Einhaltung von Anforderungen oder Normen
- hier: Konformitätsbewertung= Auditierung + Zertifizierung
- Auditierung: Sachverhalt ermitteln und bewerten
- Zertifizierung: Bestätigung der Konformität

Datenschutz/Datensicherheits-Zertifizierung

- Zertifizierung = Teil einer Konformitätsbewertung durch **unabhängige Dritte** (z. B. BSI, ULD, TÜV, ...)
- Konformität: Einhaltung von Anforderungen oder Normen (z. B. LDSG, BDSG, IT-Grundschutz, ISO 27001, ...)
- Auditierung: Sachverhalt ermitteln und bewerten (durch Sachverständige, Auditoren, [ULD-Mitarbeiter], ...)
- Zertifizierung: Bestätigung der Konformität (ISO 27001 [auf Basis von IT-Grundschutz], Datenschutz-Gütesiegel, Datenschutz-Audit, EuroPriSe, ...)

Kann eine Zertifizierung bei ADV helfen?

- kein Automatismus!
- Einflussfaktoren:
  - WAS wurde geprüft und zertifiziert? (Gegenstand)?
  - WOGEGEN wurde geprüft (Norm, Gesetz, eigene Kriterien)?
  - WER hat geprüft und zertifiziert?

- zu prüfen:
  - Welche Teile/welcher Umfang des Auftragsgegenstandes / der Dienstleistung wurden geprüft und zertifiziert?
  - Wieweit decken sich die Anforderungen des Auftraggebers mit den Prüfkriterien?
  - Ist die Zertifizierungsstelle vertrauenswürdig?

Wem kann eine Zertifizierung helfen?

- Wem soll sie helfen: Auftragnehmer (AN) oder Auftraggeber (AG)?
- Auftraggeber:
  - direkt: bekommt Leistungs**nachweis** des AN
  - indirekt:
    - Dokumentation mit Fokus auf Datenschutz und Datensicherheit bei AN vorhanden
    - Audit/Kontrollfähigkeit dürfte vorhanden sein
- Auftragnehmer:
  - dokumentierte Darstellung der eigenen Leistungen
  - Drittparteien**nachweis** der eigenen Leistungen

Diskussion: Kann eine Zertifizierung eigene Kontrollen des Auftraggebers ersetzen?

Einige Argumente:

- Vollständiger Ersatz oft nicht möglich, da Anforderungen des AG und Prüf-/Zertifizierungskriterien sich nicht decken (IT-Sicherheit ≠ Datenschutz)
- Know-How-Unterschiede zwischen AG und Auditoren/Zertifzierungsstelle? In beide Richtungen?
- Drittmeinung / Blick von außen hilfreich?
- Größenunterschied zwischen Auftraggeber und Auftragnehmer als Einflussfaktor?

Diskussion / Fragen