Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 1. Übung vom 28.04.2010:

BDSG (1)

1.1 BDSG-Anforderungen an Auftragsdatenverarbeitungen

Aufgabe:

- Welche Anforderungen muss ein Outsourcing nach dem BDSG erfüllen, um als Auftragsdatenverarbeitung gelten zu können? Begründen Sie Ihre Antwort!

1.1 BDSG-Anforderungen an Auftragsdatenverarbeitungen (1)

Outsourcing = Aufgabenerledigung durch eine andere Stelle, wobei ein Auftragnehmer kein Dritter ist nach § 3 Abs. 8 Satz 3 BDSG)

Erheben, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag = Auftragsdatenverarbeitung mit folgenden Anforderungen (§§ = Begründung):

- Auftraggeber ist für die Einhaltung des Datenschutzes verantwortlich (§ 11 Abs. 1 BDSG)
- Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen (§ 11 Abs. 2 Satz 1 BDSG)
  - → Schutzmaßnahmen sind ausschlaggebendes Kriterium
  - → Auswahlprozess muss Sorgfaltspflicht genügen (Pflicht zur Übereinstimmung mit Gesetz, Gesellschaftsbeschlüssen & Vermeidung risikoreicher Geschäftsvorfälle)
  - → Folgen einer Auftragsarbeit müssen bewertet und als unkritisch eingestuft worden sein
- Der Auftrag muss schriftlich erteilt werden (§ 11 Abs. 2 Satz 2 BDSG)

1.1 BDSG-Anforderungen an Auftragsdatenverarbeitungen (2)

- Im Einzelnen müssen im Auftrag festgelegt werden:
  1. Gegenstand *(= was soll gemacht werden?)* & Dauer des Auftrags
  2. Umfang *(= Leistungskatalog)*, Art & Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten *(→ konkrete Bezeichnung des Verfahrens, das mittels Auftragsdatenverarbeitung durchgeführt werden soll)*, Art der Daten *(= präzise Einzelauflistung der Datenfelder im Unterschied zum Verfahrensverzeichnis, bei dem auch Datenkategorien ausreichen)* und Kreis der Betroffenen
  3. die nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen *(→ Prüfkatalog für Schutzniveau!)*
  4. Berichtigung, Löschung und Sperrung von Daten *(i.d.R. Aufgabe des Auftraggebers → Verpflichtung, dies nur auf Weisung des Auftraggebers zu tun)*
  5. die nach den §§ 5, 9, 43 Abs. 1 Nr. 2, 10 & 11, 43 Abs. 2 Nr. 1 bis 3, 43 Abs. 3 sowie 44 (und bei nicht-öffentlichen Stellen auch §§ 4f, 4g und 38) bestehenden Pflichten des Auftragnehmers zur Durchführung von Kontrollen

1.1 BDSG-Anforderungen an Auftragsdatenverarbeitungen (3)

- Im Einzelnen müssen im Auftrag festgelegt werden: (Forts.)
  6. etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen *(d.h., unter welchen Voraussetzungen darf der Auftragnehmer Subaufträge an andere Stellen vergeben)*
  7. Kontrollrechte des Auftraggebers und entsprechende Duldungs- und Mitwirkungspflichten des Auftragnehmers *(→ Auftragskontrolle nach Nr. 6 der Anlage zu § 9 BDSG näher zu beschreiben & einvernehmlich beschränkbar)*
  8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Vorschriften oder im Auftrag getroffenen Festlegungen *(zur permanenten Feststellung, ob der Auftrag den vertraglichen & gesetzlichen Anforderungen bei der Umsetzung genügt, und zur Absicherung einer sich ggf. aus § 42a BDSG ergebenden Informationspflicht sowie zur Vermeidung eines Schadensersatzes nach § 7 BDSG)*
  9. Umfang der (vorbehaltenen) Weisungsbefugnisse *(→ Weisungsrecht also einvernehmlich beschränkbar)*
  10. Rückgabe überlassener Datenträger und Datenlöschung nach Auftragsende

1.1 BDSG-Anforderungen an Auftragsdatenverarbeitungen (4)

- 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)
- Durchgeführte Vertragsprüfungen, Audits und Auftragskontrollen sind zu dokumentieren (§ 11 Abs. 2 Satz 5 BDSG)
- Zweckbindung des Auftragnehmers, der die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen darf (§ 11 Abs. 3 BDSG), wobei er den Auftraggeber darauf hinzuweisen hat, wenn er der Meinung ist, dass eine Weisung gesetzlichen Auflagen zum Datenschutz widerspricht
- Auftragnehmer hat die bei der auftragsbezogenen Datenverarbeitung beschäftigen Personen auf das Datengeheimnis nach § 5 BDSG zu verpflichten (§ 11 Abs. 4 BDSG)
- Auftragnehmer hat die technischen und organisatorischen Maßnahmen nach § 9 BDSG zu treffen, die erforderlich sind (§ 11 Abs. 4 BDSG)

1.1 BDSG-Anforderungen an Auftragsdatenverarbeitungen (5)

- Auftragnehmer hat einen Datenschutzbeauftragten nach den Vorgaben aus § 4f BDSG mit den Aufgaben aus § 4g BDSG zu bestellen, sofern er personenbezogene Daten im Auftrag geschäftsmäßig erhebt, verarbeitet oder nutzt (§ 11 Abs. 4 Nr. 2 BDSG)
- Auftragnehmer hat sich der Kontrolle durch die Aufsichtsbehörde nach § 38 BDSG zu stellen, sofern er personenbezogene Daten im Auftrag geschäftsmäßig erhebt, verarbeitet oder nutzt (§ 11 Abs. 4 Nr. 2 BDSG)
- Eine Auftragsdatenverarbeitung liegt auch dann vor, 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 (§ 11 Abs. 5 BDSG)
  (→ dabei ist zu beachten, dass der Zugriff im Rahmen der regulären Tätigkeit der Prüfung oder Wartung üblicherweise erfolgt und nicht zufällig oder nur unter besonderen Ausnahmesituationen)

1.2 Voraussetzungen zur automatisierten DV

Aufgabe:

- Wann ist eine automatisierte Datenverarbeitung personenbezogene Daten bei einer GmbH zulässig? Gibt es hier Unterschiede in Abhängigkeit zur Art der personenbezogenen Daten? Begründen Sie Ihre Antwort!

Hinweis:

- *Automatisierte Datenverarbeitung = Erhebung, Verarbeitung oder Nutzung unter Einsatz einer Funktionseinheit zur Datenverarbeitung (DV-Anlage)*

1.2 Voraussetzungen zur automatisierten DV (1)

Abgrenzung:
GmbH = Kapitalgesellschaft = Gesellschaft des privaten Rechts
→ **nicht-öffentliche Stelle** nach § 2 Abs. 4 BDSG

Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur zulässig, soweit (nach § 4 Abs. 1 BDSG):

- das BDSG dies erlaubt oder anordnet,
- eine andere Rechtsvorschrift dies erlaubt oder anordnet,
- oder der Betroffene eingewilligt hat.

→ Verbot mit Erlaubnisvorbehalt!

1.2 Voraussetzungen zur automatisierten DV (2)

Gestattungsnormen für nicht-öffentliche Stellen:

- zur Erfüllung eigener Geschäftszwecke (§ 28 Abs. 1 BDSG), wenn
  - es erforderlich ist zur Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen bzw. rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen
  - es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und diesem keine schutzwürdigen Interessen des Betroffenen entgegenstehen (→ Abwägungserfordernis)
  - die Daten allgemein zugänglich sind
- für anderen Zweck unter Abwägung (§ 28 Abs. 2 BDSG)
- für Zwecke der Werbung oder des Adresshandels, soweit der Betroffene eingewilligt hat, wobei es für Werbungszwecke noch diverse Sondererlaubnisbestände gibt (§ 28 Abs. 3 BDSG), sofern der Betroffene der Werbung nicht widersprochen hat (nach § 28 Abs. 4 BDSG)

1.2 Voraussetzungen zur automatisierten DV (3)

Aber: Besondere Vorschriften für Umgang mit **besonderen Arten personenbezogener Daten** (gem. § 3 Abs. 9 BDSG = Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben)
→ **es gibt Unterschiede in Abhängigkeit zur Art der personenbezogenen Daten**:

- bei nicht-öffentlichen Stellen nach § 28 Abs. 6 BDSG zum Schutz lebenswichtiger Personeninteressen, bei vom Betroffenen offenkundig öffentlich gemachten Daten, zur Rechtsdurchsetzung unter Abwägung sowie zur wissenschaftlichen Forschung und nach § 28 Abs. 7 BDSG zur medizinischen DV

1.3 Einwilligungserklärung

Aufgabe:

- Welchen Anforderungen muss eine Einwilligung nach den Vorschriften des BDSG genügen? Begründen Sie Ihre Antwort! Nennen Sie zudem Fälle, wo es fragwürdig ist, ob diese Anforderungen wirklich erfüllt sind!

1.3 Einwilligungserklärung (1)

Anforderungen an eine Einwilligungserklärung:

- Einwilligung nur wirksam, wenn aufgrund **freier Entscheidung** des Betroffenen erfolgt (§ 4a Abs. 1 Satz 1 BDSG)
- **Verwendungszweck** ist anzugeben (§ 4a Abs. 1 Satz 2 BDSG)
- **Schriftform** i.d.R. erforderlich (§ 4a Abs. 1 Satz 3 BDSG)
- Einwilligung muss **gut erkennbar** sein (§ 4a Abs. 1 Satz 4 BDSG)
- Bei **besonderen Arten personenbezogener Daten** muss dies **ausdrücklich erklärt** werden (§ 4a Abs. 3 BDSG)

1.3 Einwilligungserklärung (2)

Fragwürdige Einwilligungserklärungen:

- Kopplung der Einwilligung an andere Leistungen
- Belohnung der Einwilligung durch Geschenke oder Vergünstigungen
- Einwilligung in unbestimmte Zwecke
- Einwilligung in beliebige Zweckänderungen
- Einwilligung in Verzicht auf Betroffenenrechte
- Einwilligung ohne Aufklärung über Folgen
- Einwilligung in umfassende AGBs ohne Abänderbarkeit
- Einwilligung in beliebige Weiterübermittlung
- Einwilligung in umfangreiche Erhebungen bei Bewerbungen bzw. Beschäftigungs-/Dienstantritt

1.4 Einwilligungserklärungsmuster

Aufgabe:

- Formulieren Sie eine Einwilligungserklärung, die alle Anforderungen nach dem BDSG erfüllt, anhand eines frei gewählten Beispiels!

1.4 Einwilligungserklärungsmuster

Muster einer Einwilligungserklärung:

Hiermit willige ich ein, dass die unten aufgeführten personenbezogenen Daten von der <Bezeichnung der verantwortlichen Stelle> zum Zweck der <Zweck> erhoben, verarbeitet und genutzt werden dürfen. Ich wurde darüber informiert, dass ich diese Einwilligung jederzeit ohne Nachteile widerrufen kann. Von der <Bezeichnung der verantwortlichen Stelle> wurde mir versichert, dass meine datenschutzrechtlichen Belange ohne Einschränkung gewährleistet werden und keine Übermittlung meiner Daten an Dritte erfolgt.

1.5 Prüfkriterien zum Daten-schutzniveau: Unternehmen

Aufgabe:

- Anhand welcher Prüfkriterien, basierend auf den Bestimmungen aus dem BDSG, kann man das Datenschutzniveau eines Unternehmens beurteilen? Begründen Sie Ihre Antwort unter Angabe der Rechtsquellen!

1.5 Prüfkriterien zum Daten-schutzniveau: Unternehmen (1)

- Unternehmen = nicht-öffentliche Stelle

→ Vorhandensein und Angabentiefe eines Verfahrensverzeich-nisses [§ 4g Abs. 2 BDSG]

→ Hinweis zur Rechtsgrundlage für die jeweilige Datenverarbei-tung (Rechtsvorschrift oder Einwilligungserklärung) [§ 4 Abs. 1 BDSG]

→ Vorliegen einer informierten Einwilligungserklärung [§ 4a BDSG]

→ Umsetzung der Betroffenenrechte [§§ 33 – 35 BDSG i.V.m. § 6 BDSG]

→ ggf. Bestellung eines Datenschutzbeauftragten [§ 4f BDSG]

→ Veröffentlichtes Ergebnis eines Datenschutzaudits [§ 9a BDSG] – *Hinweis: Ausführungsgesetz fehlt noch!*

1.5 Prüfkriterien zum Daten-schutzniveau: Unternehmen (2)

- → Meldung/Bericht der Aufsichtsbehörde über festgestellte Datenschutzverstöße [§ 38 Abs. 1 BDSG]
- → Überprüfung der technischen und organisatorischen Maßnahmen (z.B. durch Dritte im Rahmen eines Datenschutz-Audits) [§ 9 BDSG samt Anlage]
- → Einhaltung der Datensparsamkeit [§ 3a BDSG]
- → Mitteilung oder Veröffentlichung zu einer nachgewiesenen unrechtmäßigen Kenntniserlangung von Daten durch Dritte [§ 42a BDSG]