

Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 1. Übung im SoSe 2007:
BDSG (1)

1.1 Voraussetzungen zur automatisierten DV (1)

Anmerkung: Automatisierte Datenverarbeitung = Erhebung, Verarbeitung oder Nutzung unter Einsatz von DV-Anlagen (also einer Funktionseinheit zur Datenverarbeitung)

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!

1.1 Voraussetzungen zur automatisierten DV (2)

Gestattungsnormen bei **öffentlichen Stellen des Bundes**:

- nur zulässig, wenn die Kenntnis personenbezogener Daten zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist (§ 13 Abs. 1 BDSG)
- darüber hinaus besteht (i.d.R.) eine Zweckbindung beim Speichern, Verändern oder Nutzen personenbezogener Daten (§ 14 Abs. 1 BDSG)
- unter Zweckänderung nur in ausgewiesenen Fällen, darunter insbesondere das Vorliegen einer Rechtsvorschrift, eine Betroffenen Einwilligung, das Betroffeneninteresse, allgemeine Zugänglichkeit der Daten, zur öffentlichen Sicherheit und zur Verfolgung von Straftaten/Ordnungswidrigkeiten oder zur wissenschaftlichen Forschung (§ 14 Abs. 2 BDSG)

1.1 Voraussetzungen zur automatisierten DV (3)

Gestattungsnormen bei **nicht-öffentlichen Stellen**:

- zur Erfüllung eigener Geschäftszwecke (§ 28 Abs. 1 BDSG), wenn
 - es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient
 - es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und diesem keine schutzwürdigen Interessen des Betroffenen entgegenstehen
 - die Daten allgemein zugänglich sind
- für anderen Zweck unter Abwägung (§ 28 Abs. 2 BDSG)
- zur Übermittlung oder Nutzung für anderen Zweck gemäß Katalog aus § 28 Abs. 3 BDSG: Wahrung berechtigter Interessen, Gefahrenabwehr, Strafverfolgung, Werbung bei Listenprivileg unter Abwägung oder zur wissenschaftlichen Forschung

1.1 Voraussetzungen zur automatisierten DV (4)

Aber: Besondere Vorschriften bei **besonderen Arten personenbezogener Daten** (gem. § 3 Abs. 9 BDSG):

- bei öffentlichen Stellen des Bundes nach § 13 Abs. 2 BDSG wichtiges öffentliches Interesse erforderlich, zum Schutz lebenswichtiger Personeninteressen, bei vom Betroffenen offenkundig öffentlich gemachten Daten, zur Abwehr erheblicher Gefahren/Gemeinwohlbelange, zur medizinischen DV, zur wissenschaftlichen Forschung unter Abwägung sowie im Krisenfall
- 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

1.2 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)

1.2 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

1.2 Einwilligungserklärung (3)

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.

1.3 Übermittlung vs Nutzung (1)

Übermittlung:

- Transfer an oder Kenntnisnahme bzw. Abruf durch **Dritten**, also außerhalb der verantwortlichen Stelle (§ 3 Abs. 4 Nr. 3 BDSG i.V.m. § 3 Abs. 8 Satz 2 BDSG)

Nutzung:

- Kenntnisnahme oder Verwendung (ohne Veränderung, Speicherung oder Übermittlung), also z.B. Auswertung, innerhalb der gleichen verantwortlichen Stelle (§ 3 Abs. 5 BDSG)

1.3 Übermittlung vs Nutzung (2)

Übermittlung:

- Datenweitergabe an verbundene, aber eigenständige Unternehmen (§ 3 Abs. 4 BDSG i.V.m. § 3 Abs. 7 und 8 BDSG)
- Auftragsdatenverarbeitung außerhalb der EU (§ 11 BDSG i.V.m. § 3 Abs. 8 Satz 3 BDSG)

Nutzung:

- Auskunftserteilung an Betroffenen (§§ 19 und 34 BDSG i.V.m. § 3 Abs. 8 Satz 3 BDSG)
- Transfer an Auftragnehmer innerhalb EU (§ 11 BDSG i.V.m. § 3 Abs. 8 Satz 3 BDSG)

1.3 Übermittlung vs Nutzung (3)

Übermittlung:

→ **Verfügungsgewalt**
über weitergegebene
Daten liegt bei **neuer**
verantwortlicher Stelle!

Nutzung:

→ **Verfügungsgewalt**
über weitergegebene
Daten liegt weiterhin bei
alter verantwortlicher
Stelle!

1.4 Prüfkriterien zum Datenschutzniveau

- Unternehmen = nicht-öffentliche Stelle
- Zulässigkeitsüberprüfung der Datenverarbeitung
(Rechtsvorschrift oder Einwilligungserklärung)
[§ 4 Abs. 1 BDSG]
- Überprüfung der technischen und organisatorischen
Maßnahmen [§ 9 BDSG samt Anlage]
- Einhaltung der Datensparsamkeit [§ 3a BDSG]
- Gewährleistung der Betroffenenrechte [§§ 33 – 35 BDSG i.V.m.
§ 6 BDSG]
- Bestellung eines Datenschutzbeauftragten [§ 4f BDSG]
- Audit von Datenschutzkonzept & technischen Einrichtungen
[§ 9a BDSG] – *Hinweis: Ausführungsgesetz fehlt noch!*

1.5 BDSG & Schutzziele des Datenschutzes (1)

Schutz vor Missbrauch

- § 4 Abs. 1 BDSG (Zulässigkeitsprüfung)
- § 4 Abs. 2 BDSG (Primärerhebung beim Betroffenen)
- § 4d Abs. 5 BDSG (Vorabkontrolle)
- § 4g Abs. 1 Nr. 1 BDSG (Überwachungsaufgabe Datenschutzbeauftragter)
- § 6b Abs. 2 BDSG (Hinweis auf Videoüberwachung)
- § 6c Abs. 2 BDSG (Unentgeltliches Chiplesegerät)
- § 13 Abs. 1 BDSG (Erforderlichkeitsprüfung)
- § 14 Abs. 1 BDSG (zweckgebundene Erforderlichkeitsprüfung)
- § 19 Abs. 1 BDSG (Auskunftsrecht)

1.5 BDSG & Schutzziele des Datenschutzes (2)

Schutz vor Missbrauch (Forts.)

- § 19a Abs. 1 BDSG (Benachrichtigungspflicht)
- § 21 BDSG (BfDI-Anrufung)
- § 24 Abs. 1 BDSG (BfDI-Aufgaben)
- § 28 Abs. 1 BDSG (Zulässigkeitsprüfung für eigene Geschäftszwecke & Zweckfestlegung)
- § 31 BDSG (besondere Zweckbindung)
- § 33 Abs. 1 BDSG (Benachrichtigungspflicht)
- § 34 Abs. 1 BDSG (Auskunftsrecht)
- § 39 Abs. 1 BDSG (Zweckbindung Berufs-/ Amtsgeheimnis)
- Nr. 3 zur Anlage von § 9 BDSG (Zugriffskontrolle)
- Nr. 4 zur Anlage von § 9 BDSG (Weitergabekontrolle)

1.5 BDSG & Schutzziele des Datenschutzes (3)

Schutz vor falschen Wirklichkeitsmodellen

- § 4d Abs. 5 BDSG (Vorabkontrolle)
- § 6a BDSG (keine automatisierte Einzelentscheidung)

1.5 BDSG & Schutzziele des Datenschutzes (4)

Schutz der informationellen Gewaltenteilung

- § 3a BDSG (Datenvermeidung)
- § 4d Abs. 5 BDSG (Vorabkontrolle)
- § 5 BDSG (Datengeheimnis)
- § 6b Abs. 1 BDSG (Zulässige Videoüberwachung)
- § 10 Abs. 1 und 2 BDSG (automatisierte Abrufverfahren)
- § 13 Abs. 1 BDSG (Erforderlichkeitsprüfung)
- § 14 Abs. 1 BDSG (zweckgebundene Erforderlichkeitsprüfung)
- § 15 BDSG (Übermittlungsbefugnis zwischen öffentlichen Stellen)
- § 20 Abs. 2 BDSG (Löschungspflicht)

1.5 BDSG & Schutzziele des Datenschutzes (5)

Schutz der informationellen Gewaltenteilung (Forts.)

- § 28 Abs. 1 BDSG (Zulässigkeitsprüfung für eigene Geschäftszwecke & Zweckfestlegung)
- § 35 Abs. 2 BDSG (Löschungspflicht)
- § 38 Abs. 1 BDSG (Aufsichtsbehörde)
- Nr. 3 zur Anlage von § 9 BDSG (Zugriffskontrolle)
- Nr. 8 zur Anlage von § 9 BDSG (Datentrennung)

1.5 BDSG & Schutzziele des Datenschutzes (6)

Schutz vor dem Kontextproblem

- § 3a BDSG (Datenvermeidung)
- § 4d Abs. 5 BDSG (Vorabkontrolle)
- § 6a BDSG (keine automatisierte Einzelentscheidung)
- § 20 Abs. 1 BDSG (Berichtigungspflicht)
- § 20 Abs. 2 BDSG (Löschungspflicht)
- § 35 Abs. 1 BDSG (Berichtigungspflicht)
- § 35 Abs. 2 BDSG (Löschungspflicht)

1.5 BDSG & Schutzziele des Datenschutzes (7)

Schutz vor verletzlichen DV-Systemen

- § 6a BDSG (keine automatisierte Einzelentscheidung)
- § 7 BDSG (Schadensersatz)
- § 8 Abs. 1 BDSG (öffentlicher Schadensersatz)
- § 10 Abs. 1 und 2 BDSG (automatisierte Abrufverfahren)
- § 20 Abs. 1 BDSG (Berichtigungspflicht)
- § 20 Abs. 2 BDSG (Löschungspflicht)
- § 35 Abs. 1 BDSG (Berichtigungspflicht)
- § 35 Abs. 2 BDSG (Löschungspflicht)
- § 43 BDSG (Ordnungswidrigkeit)
- § 44 BDSG (Straftaten)

1.5 BDSG & Schutzziele des Datenschutzes (8)

Schutz vor verletzlichen DV-Systemen (Forts.)

- Nr. 5 zur Anlage von § 9 BDSG (Eingabekontrolle)
- Nr. 6 zur Anlage von § 9 BDSG (Auftragskontrolle)
- Nr. 7 zur Anlage von § 9 BDSG (Verfügbarkeitskontrolle)