UKD Universitätsklinikum Düsseldorf

GKD Gesellschaft für klinische Dienstleistungen Düsseldorf mbH

Ambient Assisted Living: Relevante Aspekte des Datenschutzes

HAUS NOTRUF

Zu meiner Person

- Ausbildung
  - Studium Informatik
    (FH-Dortmund)
  - Studium Humanmedizin
    (Uni Düsseldorf / Uni Witten/Herdecke)
  - Studium Jura
    (Fern-Uni Hagen)
  - Zusatzausbildung Datenschutzbeauftragter
    (Ulmer Akademie für Datenschutz und IT-Sicherheit)
  - Zusatzausbildung Datenschutz-Auditor
    (TüV Rheinland)
  - Zusatzausbildung Medizin-Produkte-Integrator
    (VDE Prüf- und Zertifizierungsinstitut)
- Berufserfahrung
  - 12 Jahre klinische Erfahrung
  - 20 Jahre IT im Krankenhäusern
  - 18 Jahre Datenschutz im Gesundheitswesen
- Mitarbeit in Verbänden
  - GMDS
  - Berufsverband Medizinischer Informatiker e.V. (BVMI)
  - Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)
  - Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)
  - HL7 Deutschland e.V.
  - Fachverband Biomedizinische Technik e.V. (fbmt)

AAL-Szenarien

- Szenario 1: Erleichterung im Haushalt
- Szenario 2: Notfallhilfe von Verwandten/Freunden
- Szenario 3: Notfallhilfe durch einen kommerziellen Dienste-Anbieter
- Szenario 4: Fernbetreuung durch eine telemedizinische ärztliche / nichtärztliche Einrichtung
- Szenario 5: Wohnen im Pflegeheim mit telemedizinischer Betreuung durch den Hausarzt
- Szenario 6: Unterstützung bei der Wahrnehmung von Freizeitaktivitäten
- Szenario 7: Zugriff von Dritten auf AAL-Daten
  - Strafverfolgungsbehörden
  - Versicherungen
  - Forschungseinrichtung
  - …

AAL-Szenarien

- Szenario 1: Erleichterung im Haushalt

In allen Szenarien spielt der

Datenschutz

eine Rolle

  - Versicherungen
  - Forschungseinrichtung
  - …

UKD Universitätsklinikum Düsseldorf

GKD Gesellschaft für klinische Dienstleistungen Düsseldorf mbH

Grundlage des Datenschutzes

Artikel 1 Grundgesetz

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.

(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Artikel 2 Grundgesetz

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

Grundlage des Datenschutzes

Andere Artikel des Grundgesetzes sind nachrangig.

D.h. beispielsweise

Art. 5 Meinungsfreiheit, Freiheit Lehre und Forschung

Art. 10 Briefgeheimnis

sind bzgl. Art. 1 und Art. 2 GG nachrangig.

„Volkszählungsurteil“ des BVerfG. von 1983

„Recht auf informationelle Selbstbestimmung“
(BVerfGE 65, 1 – Volkszählung, http://www.servat.unibe.ch/dfr/bv065001.html)

1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfaßt.
   Das Grundrecht gewährleistet insoweit die **Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen**.

2. Einschränkungen dieses Rechts auf **"informationelle Selbstbestimmung"** sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

30 Jahre Infomationelle Selbstbestimmung: Happy Birthday !

Datenschutzrecht im Rechtssystem

- EU
  - Europäische Grundrechte-Charta
  - Datenschutz-Richtlinie
    Wirkung über Umsetzung in deutsche Gesetze
  - Datenschutz-Verordnung
    (derzeit im Entwurf, sie würde unmittelbar gelten und deutsches Recht ersetzen)
- Bundesdatenschutzgesetz (BDSG)
  - Privatpersonen
  - Privatwirtschaft
  - Bundesbehörden
- Kirchliche Datenschutzgesetze
  - Einrichtungen der evang. und kath. Kirche
- Landesdatenschutzgesetze
  - öffentliche Verwaltung in Land und Kommunen
- Spezialgesetze
  (Vorrang vor allg. Gesetzen)
  - TeleMedienGesetz
  - TeleKommunikationsGesetz
  - Gesundheitsdatenschutz
  - Hochschulgesetz
  - SGB, AO, Polizeigesetz, Passgesetz, Personalausweisgesetz, Aufenthaltsgesetz, LandesMeldeGesetz, Landesverwaltungsgsetz, …

- Rechtmäßigkeit der Datenverarbeitung
  - Gesetzliche Grundlagen
  - Einwilligung
- Grundsatz der Zweckbindung
- Grundsatz der Erforderlichkeit
- Grundsatz der Datenvermeidung und Datensparsamkeit
- Grundsatz der Transparenz
- Grundsatz der klaren Verantwortlichkeiten
- Grundsatz der Kontrolle
- Grundsatz der Gewährleistung der Betroffenenrechte
  - Verbot der Profilbildung
  - Verbot der Datensammlung auf Vorrat
  - Verbot der automatisierten Einzelentscheidung
- Nutzung pseudonymisierter oder anonymisierter Daten
- Verpflichtung zum Schutz der Daten

Goldene Regeln des Datenschutzes*

1. Einwilligung: Eine Einwilligung ist nur dann wirksam, wenn der Betroffene ausreichend informiert worden ist und seine Einwilligung freiwillig erteilt hat.
2. Zweckbindungsprinzip: Personen bezogene Daten dürfen nur für den explizierten Zweck verwendet werden.
3. Rechtmäßigkeit: Jede Datenverarbeitung mit Personenbezug bedarf einer rechtlichen Grundlage, entweder als Gesetz, Vertrag oder als betriebliche Regelung.
4. Erforderlichkeit und Datensparsamkeit: Die Datenverarbeitung ist auf den für den Erhebungszweck notwendigen Umfang zu begrenzen, insbesondere im Hinblick auf Menge und Art der verarbeiteten Daten. Sie umfasst auch Löschung von Teildaten, sobald diese nicht mehr benötigt werden.
5. Transparenz und Betroffenenrechte: Erhebung und Verarbeitung personenbezogener Daten muss gegenüber Betroffenen transparent sein. Dies schließt Auskunfts-, Berichtigungs-, Sperrungs- und Löschungsrechte ein.
6. Datensicherheit: Datenschutz ist nur dann gewährleistet, wenn personenbezogene Daten sicher verarbeitet werden.
7. Kontrolle: Die Datenverarbeitung muss einer internen und externen Kontrolle unterliegen.

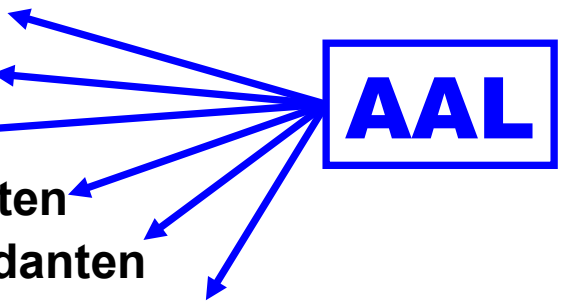
* Bizer J. (2007) Sieben Goldene Regeln des Datenschutzes. DuD 31(5): 350-356

Was ist Datenschutz?

1. Datenschutz ≠ Schutz der Daten
2. Datenschutz = Schutz der Freiheit einer Person, selbst zu entscheiden, was mit ihren/seinen Daten geschieht

Datenschutz = Personenschutz

- Die Person soll selbst entscheiden, was mit ihren Daten geschieht
- Datenschutz ist überall dort vorhanden, wo eine ***asymmetrische Machtbeziehung*** zwischen Personen und Organisationen existiert:
  - Öffentliche Verwaltung und **Bürger**
  - Private Unternehmen und **Kunden**
  - Arbeitgeber und **Arbeitnehmer**
  - Praxen, Krankenhäuser und **Patienten**
  - Institute, Gemeinschaften und **Mandanten**
  - Wissenschaftsorganisationen und **Forschungsobjekte** (wenn diese Menschen darstellen)
  - Verein und Mitglieder
  - Schule und Schüler
  - …



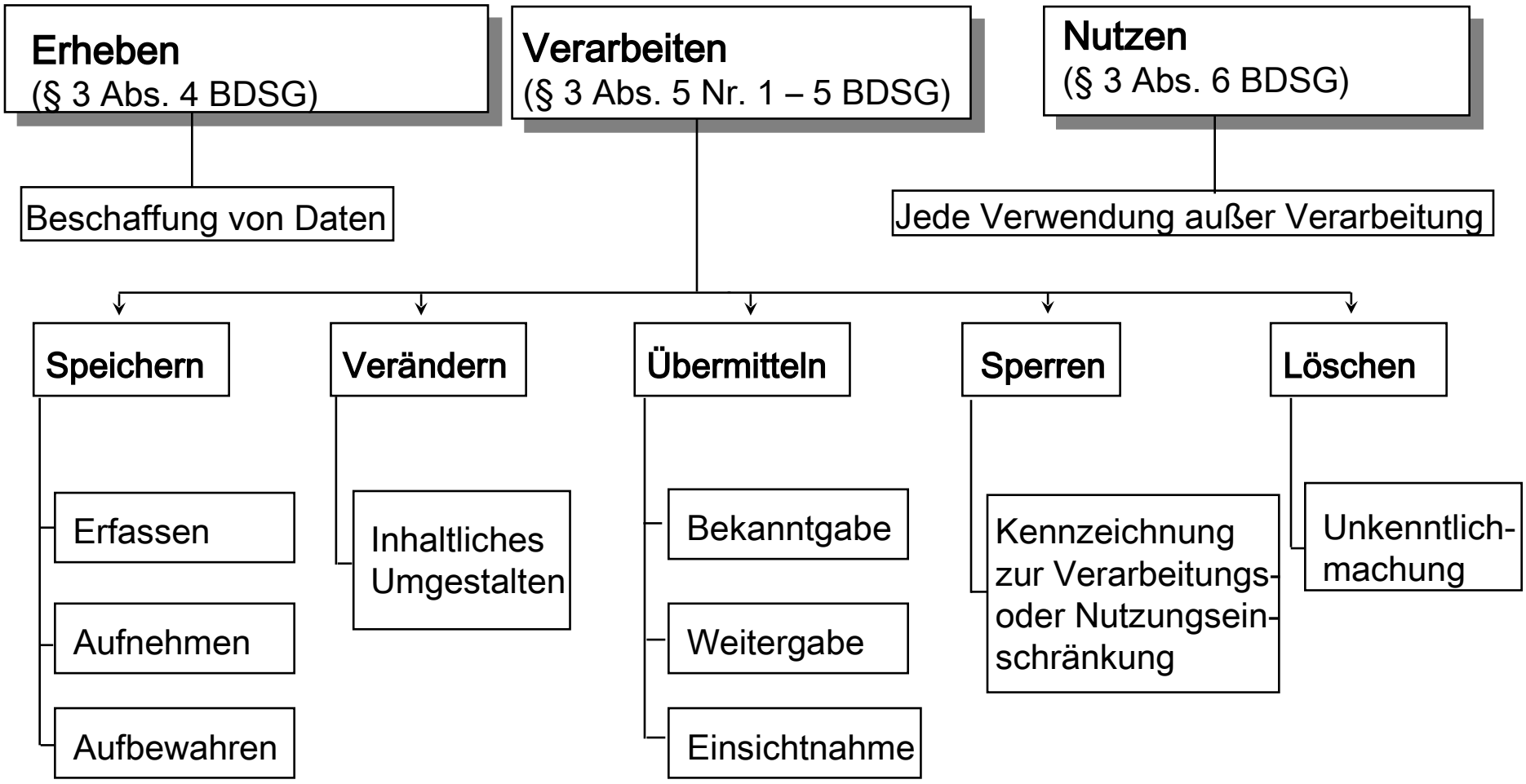
AAL und Datenschutz

- Rechtsgrundlagen fehlen weitgehend
  + Einwilligungserklärung („Vertrag“) notwendig
- AAL-Systeme erzeugen Gesundheitsdaten
  + Hoher Schutzbedarf der Daten
- Hoher Schutzbedarf erfordert entsprechende Anforderung an der Umsetzung der technisch-organisatorischen Maßnahmen

Technische und organisatorische Maßnahmen („TOMs“)

1. **Zutrittskontrolle**
   (Bsp.: Verschlossene Türen)
2. **Zugangskontrolle**
   (Bsp.: Computer mit Passwortschutz)
3. **Zugriffskontrolle**
   (Bsp.: Zugriff auf Daten nur gemäß Berechtigungskonzept)
4. **Weitergabekontrolle**
   (Bsp.: Logmechanismen bei elektr. Datentransport)
5. **Eingabekontrolle**
   (Bsp: Eingabe personenbezogener Daten nur durch autorisiertes Personal)
6. **Auftragskontrolle**
   (Bsp.: Verarbeitung nur gemäß erteiltem Auftrag)
7. **Verfügbarkeitskontrolle**
   (Bsp.: Schutz gegen zufällige Zerstörung oder Verlust durch Backup)
8. **Gebot der Datentrennung**
   (Bsp.: zu unterschiedlichen Zwecken erhobene Daten werden getrennt verarbeitet)

Begriffsbestimmungen



Apropos „Begriffsbestimmungen“…

- Automatisierte Verarbeitung:= Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen
- Speichern:= Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger
- Verändern:= inhaltliche Umgestalten gespeicherter personenbezogener Daten
- Übermitteln:= Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritte
  a. Weitergabe der Daten an einen Dritten,
  b. Dritter bekommt Daten zur Einsicht,
  c. Dritter sieht zum Abruf bereitgehaltene Daten ein oder
  d. Dritter ruft zum Abruf bereitgehaltene Daten ab
- Sperren:= Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken
- Löschen:= Unkenntlichmachung gespeicherter personenbezogener Daten

Akteure

- Betroffener (als Patient, Klient, Kunde, Nutzer, Mensch, ...)
- Vertragspartner
- Datenschutzrechtliche Dritte
  - Privater Dritter
    - Nachbar,
    - Vermieter,
    - Familienangehöriger
    - …
  - Vertraglicher Dritter
    - IT-Infrastruktur-Anbieter
    - Medizinische und sonstige Hilfsanbieter
    - Mitarbeitende von IT- und Hilfsanbieter
    - Öffentliche Verwaltung
    - ...
  - Allgemeinheit als Dritter
    - Forschende
    - Interessengruppen
    - Öffentlichkeit
    - ...

AAL-Szenarien

- Szenario 1: Erleichterung im Haushalt
- Szenario 2: Notfallhilfe von Verwandten/Freunden
- Szenario 3: Notfallhilfe durch einen kommerziellen Dienste-Anbieter
- Szenario 4: Fernbetreuung durch eine telemedizinische ärztliche / nicht-ärztliche Einrichtung
- Szenario 5: Wohnen im Pflegeheim mit telemedizinischer Betreuung durch den Hausarzt
- Szenario 6: Unterstützung bei der Wahrnehmung von Freizeitaktivitäten
- Szenario 7: Zugriff von Dritten auf AAL-Daten
  - Strafverfolgungsbehörden
  - Versicherungen
  - Forschungseinrichtung
  - …

AAL-Szenarien

- Szenario 1: Erleichterung im Haushalt

In allen Szenarien gibt es
- Betroffene
- Vertragspartner und
- Dritte,
also alle Akteure spielen eine Rolle.

  - Versicherungen
  - Forschungseinrichtung
  - …

Verantwortlichkeiten definieren

- Wer hat Einflussmöglichkeiten auf das AAL-System?
- Wer hat die Datenhoheit über die erhobenen Daten?
  - Nutzer?
  - Hersteller des AAL-Systems?
  - Betreiber des AAL-Systems?
  - „Paten“ (Verwandter/Freund/Arzt/Institution)?
  - …
- Grundlage der Tätigkeiten ist
  - gesetzlicher
  - vertraglicher
  - gewillkürter

  Art?

Gesetzliche Grundlage

- Gesetz oder Einverständniserklärung
- Bei Verwendung externer Unterstützung
  - Auftragsdatenverarbeitung?
  - Funktionsübertragung

Grundsatz Einwilligung (§ 4a BDSG)

- Einwilligung ist freiwillig (§ 4a Abs. 1 Satz 1)
- Einwilligung bedarf der Schriftform (§ 4a Abs. 1 Satz 3)
- Es ist hinzuweisen auf (§ 4a Abs. 1 Satz 2):
  - Zweck der Speicherung
  - ggf. der Übermittlung
  - auf Folgen der Verweigerung (bei Verlangen)
  - Löschung, Widerrufsmöglichkeit, Geltungsdauer der Einwilligung
  - Soweit nicht offensichtlich:
    - verantwortliche Stelle
    - Erhobene Daten

Grundsatz Einwilligung (§ 4a BDSG)

- Einwilligung ist freiwillig (§ 4a Abs. 1 Satz 1)
- Einwilligung bedarf der Schriftform (§ 4a Abs. 1 Satz 3)
- Es ist hinzuweisen auf (§ 4a Abs. 1 Satz 2):

Cave: Die Verarbeitung ist grundsätzlich nur erlaubt,

- **für den Zweck zu dem eingewilligt wurde**
- **für den Zweck der gesetzlich bestimmt ist.**

  - verantwortliche Stelle
  - Erhobene Daten

Auftragsverarbeitung vs. Funktionsübertragung

Eine Funktionsübertragung ist nach der herrschenden Meinung anzunehmen, wenn

- der Auftragsdatenverarbeiter eigene Entscheidungsbefugnisse hinsichtlich des „Wie“ der Datenverarbeitung und der Auswahl der Daten hat,
- neben der Übertragung der Datenverarbeitung eine Übertragung der zugrunde liegenden Aufgabe auf den Dienstleister erfolgt,
- der Auftragsdatenverarbeiter für die Zulässigkeit der Verarbeitung der Daten verantwortlich ist,
- dem Auftragsdatenverarbeiter Rechte zur Nutzung an den Daten für eigene Zwecke überlassen sind und er ein eigenes Interesse an der Datenverwendung hat

Funktionsübertragung

Wenn ein Zugriff auf personenbezogene Daten möglich ist, ist eine Funktionsübertragung grundsätzlich nicht zulässig, außer:

- Der Betroffene willigt ein
- Ein Gesetz schreibt es vor

Auftragsverarbeitung: Vertragsgestaltung (1)

- **Vorlage der technisch-organisatorischen Maßnahmen**
- **Sorgfältige Auswahl**
- **Schriftliche Erteilung des Auftrags**
  (10 Punkte des § 11 BDSG bzw. §80 SGB X)
- **Erstmalige Prüfung der technischen und organisatorischen Maßnahmen, d.h. vor der Datenverarbeitung**
  - **Vor-Ort-Kontrolle**
  - **Vorlage von Bescheinigungen, Zertifikaten oder Berichten**
    über durchgeführte Datenschutz- und Datensicherheits- analysen
    (z.B. BSI IT-Grundschutz-Zertifizierung; TÜV; Wirtschaftsprüfungs-gesellschaften; ISO/IEC 27001; vom betrieblichen Datenschutzbeauftragten; ITIL)
    Cave: laut Datenschutzbeauftragten NRW reicht 27001 alleine nicht aus
  - **Beantwortung und Überprüfung eines Fragebogens**
    Datensicherheitskonzept beim Auftragnehmer
- **Dokumentation der Kontrolle**
- **Festlegung der regelmäßigen Kontrolle**
- **Beginn der Verarbeitung**

Auftragsverarbeitung: Vertragsgestaltung (2)

- Genauer Leistungsumfang der zu erbringenden Arbeiten
- Dauer der Datenspeicherung, Aufbewahrung und Kopieren von Datenträgern
- Transport- und Versendungsformen des Datenmaterials, verschließbare Transportbehälter, bzw. Verschlüsselung des Datenmaterials, Zeitpunkt und Ort der Anlieferung und Abholung von Datenmaterial bzw. des Zugangs zu den Daten, Regelung des Transportrisikos, Verfahren bei der Übergabe (Protokollierung, Lieferscheine), empfangsberechtigte Personen
- Kompetenz- und Pflichtenabgrenzung
- Festlegung über Einzelweisungen durch den Auftraggeber; anweisungsberechtigte Personen des Auftraggebers
- notwendige Sicherheitsmaßnahmen nach § 9 BDSG und der Anlage zu § 9 BDSG
- Vernichtung / Entsorgung von Schriftstücken und sonstigen Datenträgern durch den Auftragnehmer nach der Verarbeitung; Vernichtung von Test- und Ausschussmaterial
- Dokumentation der Auftragsabwicklung beim Auftragnehmer, inklusive eines Kontrollrechtes durch den Auftraggeber, Prüfungspflichten für beide Seiten im Hinblick auf die ordnungsgemäße Auftragserledigung
- Maßnahmen beim Verlust von Datenträgern, bei Störungen des Verarbeitungsablaufs und bei besonderen Vorkommnissen
- Bedingungen für die Beauftragung von Subunternehmen durch den Auftragnehmer
- Vertragslaufzeit bzw. Kündigungsmöglichkeiten
- Vertragsstrafen bei Datenschutzverletzungen
- Verpflichtungen der Vertragspartner bei Beendigung der Geschäftsbeziehungen

Beispiele für Auftragsdatenverarbeitung

- **Druck von Visitenkarten**
  - **Mitarbeiterdaten**
  - **Funktion**
- **Personalmanagement**
  - **Gehälter**
  - **Krank- und Fehlzeiten**
- **Webseiten-Hosting**
  - **Logdateien**
  - **Mitarbeiterpräsentation**
- **Wartung und Pflege (vor Ort oder via Fernwartung)**
  - **Installation, Wartung, Pflege und Prüfung von Netzwerken, Hardware und Software**
  - **Parametrisierung von Software**
  - **Programmentwicklungen /-anpassungen /-umstellungen, Fehlersuche, Tests**
  - **Durchführungen von Migrationen im Produktivsystem**

Diskussion


Vereinfachen Sie Ihre Kommunikation:
Hmmm...
ääh...
räusper...
(schluck!)
Nein.
Ich denke...
Man könnte...
unter Umständen...
möglicherweise...
...denkbar wäre...
Ja.