# Verarbeitung im Auftrag

# Was ist Auftragsverarbeitung?

# Auftragsverarbeitung, Funktionsübertragung, Gemeinsame Verarbeitung – Was ist was?

| | Auftragsverarbeitung | Gemeinsame Verarbeitung | „Funktionsübertragung“ |
|---|---|---|---|
| Grundsatz | Weisungsgebundene Verarbeitung von Daten durch Auftragnehmer | (Gleichberechtigte) Partnerschaft mit gemeinsamer Verantwortung | Eigenverantwortliche Entscheidung des Auftragnehmers über die Art und Weise der Datenverarbeitung |
| Erlaubnistatbestand | Verantwortlicher verfügt über einen Erlaubnistatbestand | Die gemeinsam an der Verarbeitung Beteiligten haben einen (gemeinsamen) Erlaubnistatbestand | – Verantwortlicher hat Erlaubnistatbestand zur Übermittlung<br>– Verantwortliche einen für seine Verarbeitung |
| Voraussetzung für Verarbeitung | Vertrag oder sonstiges Rechtsinstrument | Aufteilung der Pflichten gemäß Art. 26 (und entsprechende vertragliche Regelung / Vereinbarung) | Auftragnehmer braucht einen eigenen Erlaubnistatbestand zur Datenverarbeitung |

# Auftragsverarbeitung: Unterschied „altes“ Recht vs. „neues“ Recht

| Regelung | „Altes“ Recht | „Neues“ Recht |
|---|---|---|
| Sprachliche Unterschiede | Auftraggeber – Auftragnehmer<br>Auftragsdatenverarbeitung | Verantwortlicher – Auftragsverarbeiter<br>Auftragsverarbeitung |
| Formale Unterschiede | „Regelung“ | Vertrag oder anderes Rechtsinstrument (schriftlich) |
| Auswahl Dienstleiter | sorgfältig und unter besonderer Berücksichtigung der technischen und organisatorischen Maßnahmen | muss hinreichende Garantien im Hinblick auf geeignete technische und organisatorische Maßnahmen bieten |
| Ort der Datenverarbeitung | EU / EWR | Weltweit |
| Dokumentationspflichten | Auftraggeber | Verantwortlicher, Auftraggeber |
| Hinweispflicht bei rechtswidrigen Weisungen | Nicht geregelt<br>(war aber in vielen Verträgen enthalten) | Pflicht |
| Unterauftragsverarbeitung | Umgang muss „geregelt“ werden | Nur mit Zustimmung Verantwortlicher |
| Haftung gegenüber Betroffenen | Auftraggeber | Verantwortlicher, Auftraggeber |
| Bußgeld | Auftraggeber | Verantwortlicher, Auftraggeber |

# Begriffsbestimmungen

# Begriffsbestimmungen

## Was ist womit gemeint?

- Verarbeitung im Auftrag
  - Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter (Auftragnehmer) nach Weisung und im Auftrag des Verantwortlichen (Auftraggeber)
- Weisung
  - Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers
- Unterauftragnehmer
  - Vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmer zur Erbringung der Leistungen gegenüber dem Auftraggeber benötigt
- Drittland
  - Land außerhalb EU/EWR

# Pflichten des Verantwortlichen

# Rechenschaftspflicht

## Pflicht zum Nachweis der Einhaltung der Vorgaben der DS-GVO

- Art. 5 Abs. 2 DS-GVO
  Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen **Einhaltung nachweisen**
- Art. 24 DS-GVO
  Verantwortliche setzt technische und organisatorische Maßnahmen zum Schutz der von der Verarbeitung betroffenen Person um; **diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert**

# Dokumentationspflichten

## Nachweispflichten bedingen Dokumentation

- Verantwortlicher muss nachweisen
  - Kriterien für die Auswahl des Auftragsverarbeiters,
  - Einhaltung Vorgaben Art. 32 DS-GVO (Sicherheit Verarbeitung)
  - Gewährleistung der Rechte der betroffenen Person
  - Durchführung und das Ergebnis einer Vor-Ort-Prüfung (wenn durchgeführt)
  - → Nachweis muss für gesamte Dauer der Verarbeitung geführt werden
- Verzeichnis von Verarbeitungstätigkeiten

# Dokumentationspflichten

## Nachweispflichten bedingen Dokumentation

- Pflicht zum Vertragsabschluss (schriftlich)
  - Inhaltliche Vorgaben aus Art. 28 Abs. 2, 3, 4 DS-GVO
    (siehe auch Muster-Vertrag zur Auftragsverarbeitung für das Gesundheitswesen*)
  - Weitere Vorgaben bzgl. Verarbeitung im Auftrag nicht zwingend Vertragsbestandteil, muss aber ggf. nachgewiesen werden, z.B.
  - Art. 27 DS-GVO: Nicht in der Union niedergelassene Verantwortlichen oder Auftragsverarbeitern benötigen Vertreter in der Union
  - Artt. 44ff DS-GVO: Verarbeitung in Drittstaaten

# Pflichten des Auftragsverarbeiters: Informationspflichten

## Art. 33 „Meldung von Verletzungen des Schutzes personenbezogener Daten“

- Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der für die Verarbeitung **Verantwortliche** ohne unangemessene Verzögerung und möglichst **binnen höchstens 72 Stunden,** nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde
- es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt
- Falls die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden erfolgt, ist ihr eine Begründung beizufügen
- Wenn dem **Auftragsverarbeiter** eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem für die Verarbeitung Verantwortlichen ohne unangemessene Verzögerung

# Pflichten des Auftragsverarbeiters: Informationspflichten

## Art. 33 „Meldung von Verletzungen des Schutzes personenbezogener Daten“

- Die Meldung enthält mindestens folgende Informationen
  - eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Datenkategorien und der ungefähren Zahl der betroffenen Datensätze;
  - den Namen und die Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen
  - eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
  - eine Beschreibung der von dem für die Verarbeitung Verantwortlichen **ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes** personenbezogener Daten und gegebenenfalls zur Eindämmung ihrer möglichen nachteiligen Auswirkungen
- Der Verantwortliche dokumentiert Verletzungen unter Beschreibung aller im Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen.
- Die Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

# Pflichten des Auftragsverarbeiters: Informationspflichten

## Art. 33 „Meldung von Verletzungen des Schutzes personenl

Innerhalb von 72 Stunden nach Ereignis: sportlich...

- Die Meldung enthält mindestens folgende Informationen
  - eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Datenkategorien und der ungefähren Zahl der betroffenen Datensätze;
  - den Namen und die Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen
  - eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
  - eine Beschreibung der von dem für die Verarbeitung Verantwortlichen **ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes** personenbezogener Daten und gegebenenfalls zur Eindämmung ihrer möglichen nachteiligen Auswirkungen
- Der Verantwortliche dokumentiert Verletzungen unter Beschreibung aller im Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen.
- Die Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

# Pflichten des Auftragsverarbeiters: Informationspflichten

## Art. 33 „Meldung von Verletzungen des Schutzes personenbezogener Daten“

- Bestel … Daten ein hohes … für die Verarb… von der Verletz…
- Die Be… die *Art der Ve…* Artikel 31 Absat…
- Sorgt … das hohe Risiko … nach nicht mehr … on entfallen

**Benachrichtigt wird**

1. **Bei eingetretener Datenpanne**
2. **Bei Wahrscheinlichkeit des Eintretens einer Datenpanne**

**Beispiel:**

- **Gestohlener Laptop, gut verschlüsselte Festplatte -> wohl keine Benachrichtigung erforderlich**
- **Gestohlener Laptop, keine Verschlüsselung -> Benachrichtigung wohl erforderlich**

# Pflichten des Auftragsverarbeiters: Informationspflichten

## Art. 33 „Meldung von Verletzungen des Schutzes personenbezogener Daten“

- Bestel … Daten ein hohes … für die Verarb… von der Verletz…
- Die Be… die *Art der Ve…* Artikel 31 Absat…
- Sorgt … das hohe Risiko … nach nicht mehr … on entfallen

**Benachrichtigt wird**

1. **Bei eingetretener Datenpanne**
2. **Bei Wahrscheinlichkeit des Eintretens einer Datenpanne**

**Beispiel:**

- **Gestohlener Laptop, gut verschlüsselte Festplatte -> wohl keine Benachrichtigung erforderlich**
- **Gestohlener Laptop, keine Verschlüsselung -> Benachrichtigung wohl erforderlich**

# Pflichten des Auftragsverarbeiters

# Pflichten des Auftragsverarbeiters

## Bisher bekannte Pflichten: ADV-Vertrag & Co.

- Auftragsverarbeiter darf personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten (Art. 28 Abs. 3 lit a, Art. 29)
- Auftragsverarbeiter muss gewährleisten, dass **alle** zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b)
  - Cave: alle = keine Beschränkung auf Beschäftigte des Auftragsverarbeiters; gilt somit auch für Beschäftigte von Unteraufragnehmern, Verantwortlichen
- Auftragsverarbeiter muss erforderliche technische und organisatorische Maßnahmen (Art. 28 Abs. 3 lit. c i. V. m. Art. 32)
- Auftragsverarbeiter muss Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und unterstützen (Art. 28 Abs. 3 lit. h)
- Auftragsverarbeiter darf ohne schriftliche Genehmigung des Verantwortlichen keinen Unterauftragsverarbeiter beauftragen (Art. 28 Abs. 2)

# Pflichten des Auftragsverarbeiters

## Informationspflichten

- Auftragsverarbeiter muss Verantwortlichen **unverzüglich informieren**, falls er meint, dass eine **Weisung gegen die DS-GVO oder andere Datenschutzbestimmungen verstößt** (Art. 28 Abs. 3 Satz 3)
- Auftragsverarbeiter muss Verantwortlichen **unverzüglich über eine Verletzung des Schutzes** personenbezogener Daten **informieren** (Art. 33 Abs. 2)
- Beachtung Anforderungen Datenschutzbeauftragter (ordentliche Bestellung, weisungsfrei, frühzeitige Einbindung in alle Verarbeitungstätigkeiten, Ressourcen ausreichend, ...) (Art. 38)

# Pflichten des Auftragsverarbeiters

## Neue Pflichten

- Auftragsverarbeiter außerhalb der EU müssen schriftlich einen Vertreter in der Union bestimmen (Art. 27 Abs. 1, 3)
- Nach Abschluss der Verarbeitung: personenbezogenen Daten löschen oder zurückgeben (Art. 28 Abs. 3 lit. g)
- Auftragsverarbeiter muss alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung stellen (Art. 28 Abs. 3 lit. h)
- Auftragsverarbeiter muss einem Unterauftragsverarbeiter dieselben Datenschutzpflichten auferlegen, die der Auftragsverarbeiter mit dem Verantwortlichen vereinbarte (Art. 28 Abs. 4)
- Der Auftragsverarbeiter führt (soweit keine Ausnahmetatbestände vorliegen) ein schriftliches (beinhaltet auch die Möglichkeit der Nutzung eines elektronischen Formates) Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung
  - Verzeichnis muss auf Anfrage der Aufsichtsbehörde zur Verfügung gestellt werden
- Verarbeitung in Drittländern nur unter Einhaltung der in den Artt. 44-50 DS-GVO beschriebenen Anforderungen statthaft

# Pflichten des Auftragsverarbeiters

## Unterstützung des Auftraggebers

Auftragsverarbeiter muss Auftraggeber (Verantwortlichen) unterstützen

- Umsetzung der Rechte von betroffenen Personen (Art. 28 Abs. 3 lit. e)
- Sicherheit der Verarbeitung (Art. 32)
- Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33)
- Meldung von Verletzungen des Schutzes personenbezogener Daten an den Betroffenen (Art. 34)
- Datenschutz-Folgenabschätzung (Art. 35)
- Vorherige Konsultation der Aufsichtsbehörde (Art. 36)

# Pflichten des Auftragsverarbeiters

## Unterstützung bei der Umsetzung der Rechte von betroffenen Personen

**Recht auf**

- **Transparenz (Art. 12)**
  - Verantwortlicher informiert über Betroffenenrechte
  - Informationen müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form vorliegen
  - Mitteilungspflicht Artt. 15ff innerhalb 4 Wochen, ggfs. Info über Fristverlängerung durch Verantwortlichen
  - Unentgeltlich
- **Information (Artt. 13, 14)**
  - Vor Beginn der Datenverarbeitung
  - Cave Auskunftsrecht: neu ist Auskunft bzgl. Speicherdauer bzw. – falls nicht möglich – Darlegung der Kriterien für die Festlegung dieser Dauer
- **Auskunft (Art. 15)**
  - Informationen nur an identifizierte Personen (Betroffene) weitergeben
  - Cave: Betroffenen bzgl. Zweckänderung informieren
- **Berichtigung ( Art. 16)**

# Pflichten des Auftragsverarbeiters

## Unterstützung bei der Umsetzung der Rechte von betroffenen Personen

**Recht auf**

- **Löschung (Art. 17)**
  - Ggfs. auch Empfänger über Löschverlangen eines Betroffenen unterrichten
- **Sperrung (Art. 18)**
  - Nach Sperrung: außer Speichern keine Verarbeitung ohne Einwilligung betroffener mehr (abgesehen von drei Ausnahmetatbeständen)
  - Ggfs. muss über Aufhebung Sperrung Betroffener informiert werden
- **Widerspruchsrecht (Art. 21)**
  - Jederzeit möglich, bedarf keiner Einwilligung als Erlaubnistatbestand
- **Auf Widerspruchsrecht hinweisen**
  - Verarbeitung auch bei Widerspruch möglich, wenn „zwingende schutzwürdige Gründe“ die „Interessen, Rechte und Freiheiten“ des Betroffenen überwiegen ➔ Nachweis erforderlich, also dokumentieren
- **Automatisierte Generierung von Einzelentscheidungen einschließlich Profiling (Art. 22)**

# Pflichten des Auftragsverarbeiters

## Unterstützung bei der Umsetzung der Rechte von betroffenen Personen

**Artikel 19 „Mitteilungspflicht im Zusammenhang mit der Berichtigung, Löschung oder Einschränkung“**

- Empfängern, an die Daten weitergegeben wurden, jede Berichtigung, Löschung oder Einschränkung mitteilen
  - ☞ ToDo: Informationssystem anpassen

**Artikel 20 „Recht auf Datenübertragbarkeit“**

- Voraussetzung: Einwilligung oder „Vertrag gemäß Art. 6 Abs. 1 lit. b“

Betroffene haben das

- Recht, Daten „in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“
- Recht, Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermitteln zu lassen
  - ☞ ToDo: Informationssystem anpassen

# Pflichten des Auftragsverarbeiters

## Nähere Betrachtung

- Verzeichnis Verarbeitungstätigkeiten
- Datenschutz-Folgenabschätzung
- Gewährleistung der Sicherheit der Verarbeitung

# Sanktionen

# Sanktionen

## Zwei Fälle sind zu Unterscheiden

1. **Vertrag zur Auftragsverarbeitung liegt vor**
   - Verantwortlicher/Auftragsverarbeiter bei Verstoß gegen die Pflichten gemäß Artt. 8, 11, 25 bis 39, 42 und 43 DS-GVO:
     **„kleines“ Bußgeld**
     (Geldbuße von bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs)

# Sanktionen

## Zwei Fälle sind zu Unterscheiden

2. Vertrag zur Auftragsverarbeitung **liegt nicht vor**
   - **Verantwortlicher**:
     - Übermittlung ohne Rechtsgrundlage = Verstoß gegen Artt. 5-9 DS-GVO
       **„großes“ Bußgeld**
       (Geldbuße von bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs)
     - Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe gem. § 42 BDSG n.F.
   - **Auftragsverarbeiter**: Verarbeitung ohne Rechtsgrundlage = Verstoß gegen Artt. 5-9 DS-GVO
     **„großes“ Bußgeld**

# Sanktionen

## Daher:

**Keine Auftragsverarbeitung ohne Vertrag !!!**

# Vertrag zur Verarbeitung im Auftrag

## Zu regelnde Mindestinhalte

- Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen
- Zur Verarbeitung *befugte* Personen wurden zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht
- Gewährleistung Sicherheit der Verarbeitung (Art. 32 DS-GVO)
- Einsatz weiterer Auftragsverarbeiter („Unterauftragsverarbeiter“) regeln
- Wahrnehmung der Betroffenenrechte, angemessene Unterstützung des Auftragsverarbeiters
- Unterstützung Verantwortlicher durch Auftragsverarbeiter bei
  - Benachrichtigungspflichten (Aufsichtsbehörde, Betroffener)
  - Datenschutz-Folgenabschätzung
- Nach Auftragsende: Löschen oder Rückgabe Daten durch Auftragsverarbeiter
- Informationen bzgl. Einhaltung vertraglicher Bedingungen bereitstellen, Inspektionen erlauben

# Mustervertrag für das Gesundheitswesen

## Muster der Verbände nutzen

- Berufsverband der Datenschutzbeauftragten Deutschlands e. V. (BvD)
  Arbeitskreis Medizin
- Bundesverband Gesundheits-IT e. V. (bvitg)
  Arbeitsgruppe Datenschutz & IT-Sicherheit
- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (gmds)
  Arbeitsgruppe "Datenschutz und IT-Sicherheit im Gesundheitswesen" (DIG)
- Deutsche Krankenhausgesellschaft e. V. (DKG)
- Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD)
  Arbeitskreis "Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen"

Download z.B. unter
http://ds-gvo.gesundheitsdatenschutz.org/html/adv-vertrag.php