

# Datenschutzrecht

## Episode 2: Blick in die Praxis

**Prof. Dr. Iris Kirchner-Freis, LL.M.Eur.**

Direktorin, Institut für IT-, Medien- und Immaterialgüterrecht (MLS LEGAL),  
Bremen

Professorin für Deutsches und Europäisches IT-, Medien- und  
Immaterialgüterrecht am Fachbereich 3 – Informatik, Universität Bremen

# Übersicht der Lerneinheit

Episode 1:  
Einführung

**Episode 2:**  
**Blick in die Praxis**

Episode 3:  
Interview

# Lernziele der Episode

## Lernziel 1:

Sie kennen die Anforderungen des Datenschutzrechts, insbesondere der Europäischen Datenschutz-Grundverordnung (DSGVO), an die Verarbeitung von personenbezogenen Daten.

## Lernziel 2:

Sie kennen wesentliche Anforderungen an die Umsetzung der DSGVO in der Praxis.

# Neues Datenschutzrecht

- Seit dem 25.5.2018 richtet sich das Datenschutzrecht in Europa nach der Datenschutz-Grundverordnung (DSGVO), im Einzelnen ergänzt durch datenschutzrechtliche Bestimmungen der Mitgliedstaaten. In Deutschland ist am 25.5.2018 ein neues Bundesdatenschutzgesetz (BDSG) in Kraft getreten.

# Formen der Datenverarbeitung

- DSGVO gilt bei der **Verarbeitung personenbezogener Daten** von **natürlichen, lebenden Personen**
  - **personenbezogene Daten** sind „alle Informationen, die sich auf eine **identifizierte** oder **identifizierbare natürliche** Person beziehen“ (Art. 4 Nr. 1 DSGVO):
    - z.B. Name und Anschriften von Kunden, Mitarbeitern, Partnern, Lieferanten, Dienstleistern etc.
  - Begriff der **Verarbeitung** ist weit zu verstehen (Art. 4 Nr. 2 DSGVO)
    - z.B. Erheben, Verändern, Speichern, Weitergeben, Löschen, etc.

# Umsetzung der DSGVO in der Praxis

- Wesentliche erste Schritte zur Umsetzung der DSGVO und der nachweisbaren Erfüllung in der Praxis:
  - Benennung eines Datenschutzbeauftragten erforderlich?
  - Erstellung eines Verfahrensverzeichnisses
  - Umsetzung eines Maßnahmenplans, soweit sich aus dem Verfahrensverzeichnis entsprechender Handlungsbedarf ergibt.
  - Einhaltung von Datensicherheit
  - Erstellung von Datenschutzinformationen und Abschluss von notwendigen Verträgen wie z.B. im Bereich der Auftragsdatenverarbeitung.

# Umsetzung der DSGVO: Datenschutzbeauftragter

- **Handelt es sich um eine Behörde oder öffentliche Stelle?**
  - Alle Behörden und öffentlichen Stellen mit Ausnahme von Gerichten, die Daten verarbeiten, haben die Pflicht einen Datenschutzbeauftragten zu bestellen (Art. 37 Abs. 1 lit. a) DSGVO)

# Umsetzung der DSGVO: Datenschutzbeauftragter

- **Handelt es sich um eine nicht-öffentliche Stelle?**
  - Soweit mindestens 10 Personen ständig mit der automatisierten Verarbeitung beschäftigt sind (Art. 38 Abs. 1 BDSG), ist ein Datenschutzbeauftragter zu bestellen,
  - Besteht die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der **Durchführung von Verarbeitungsvorgängen ...zur systematischen Überwachung** oder in der Verarbeitung **besonderer Kategorien von Daten** (Art. 9 DSGVO) oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO), sind sie verpflichtet einen Datenschutzbeauftragten zu bestellen (Art. 37 Abs. 1 lit. b) und lit. c),



# Umsetzung der DSGVO: Datenschutzbeauftragter

- **Handelt es sich um eine nicht-öffentliche Stelle?**
  - Sofern der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vornehmen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO unterliegen, oder
  - Personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeiten (§ 38 Abs. 1 Satz 2 BDSG).

# Datenschutzbeauftragter: Aufgaben (Art. 39 DSGVO)

- **Unterrichtung und Beratung** des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten,
- **Überwachung** der Einhaltung der Datenschutzvorschriften,
- **Schulung** der mit der Datenverarbeitung betrauten Mitarbeiter,
- Auf Anfrage **beratende Funktion** bei der Datenschutz-Folgenabschätzung,
- **Zusammenarbeit** mit der Aufsichtsbehörde
- Datenschutzbeauftragter berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder Auftragsverarbeiters (Art. 38 Abs. 3 S. 3 DSGVO).
- Datenschutzbeauftragter ist **nicht weisungsgebunden** (Art. 38 Abs. 3 S. 1 DSGVO).

# Datenschutzbeauftragter: Benennung

- Art. 37 Abs. 5 DSGVO verlangt eine Benennung auf der Grundlage folgender persönlicher Eigenschaften des Datenschutzbeauftragten:
  - berufliche Qualifikation und Fachwissen sowie
  - Eignung zur Erfüllung der dem Datenschutzbeauftragten durch Art. 39 zugewiesenen Aufgaben (Zuverlässigkeit)
- Möglich ist die Bestellung eines internen oder externen Datenschutzbeauftragten.

# Umsetzung der DSGVO: Verzeichnisse

- Jeder Verantwortliche hat ein Verzeichnis aller Verarbeitungstätigkeiten zu erstellen und fortlaufend zu aktualisieren (Art. 30 DSGVO)
  - Verzeichnis dient dem Nachweis einer DSGVO-konformen Datenverarbeitung.
  - auf Anforderung der Aufsichtsbehörde muss anhand des Verzeichnisses nachgewiesen werden, welche Verarbeitungsprozesse zu einer bestimmten Zeit aktiv waren.
- Als Verarbeitungstätigkeiten gelten z.B.:
  - Buchhaltungssoftware
  - Adressdatenbanken,
  - Webseiten, Seiten in Sozialen Netzwerken, betriebliches Intranet
  - Urlaubslisten
  - elektronische Personalakten .....

# Umsetzung der DSGVO: Verzeichnis

- Verzeichnis muss keinem bestimmten Aufbau folgen.
- Verzeichnis muss schriftlich oder elektronisch geführt werden (z.B. Word- oder Exceldatei).
  - Aktualisierung z.B. durch Datenschutzbeauftragten oder IT-Dienstleister
  - Kontrolle, ob alle Regeln eingehalten werden, sollte Chefsache sein.
- Für jede einzelne Verarbeitungstätigkeit sind bestimmte Angaben vorgeschrieben:
  - siehe zu den Einzelheiten Episode 1 zum Datenschutzrecht
- Erstellung eines Verzeichnisses ist ein guter Anlass über Effizienz, Nachvollziehbarkeit und Sinnhaftigkeit der eigenen Datenverarbeitung nachzudenken.
  - z.B. Umfang der Datenverarbeitung, Speicherfristen, etc.

# Umsetzung der DSGVO: GAP-Analyse

- Verfahrensverzeichnis ist Ausgangspunkt für eine Lückenanalyse, im Hinblick auf mögliche Schwachstellen jedes einzelnen Verarbeitungsverfahrens. Mögliche Schwachstellen sind insbesondere:
  - Datensparsamkeit
  - Datenrichtigkeit
  - Rechtmäßigkeit
  - Löschfristen
  - Zugriffsrechte
  - Zugangskontrolle
  - Schutz gegen Hacker und Schadsoftware
- Am Ende einer Gap-Analyse steht ein Maßnahmenplan, um Datenschutzkonformität aller Verfahren zu erreichen.

# Umsetzung der DSGVO: Datensicherheit

- Technische und organisatorische Maßnahmen (TOM's), um Sicherheit der verarbeiteten Personendaten zu gewährleisten (Art. 32 DSGVO). Folgende Maßnahmen sind vorgeschrieben:
  - **Verschlüsselung:** z.B. Verschlüsselung von E-Mails mit Verschlüsselungsprogrammen,
  - **Stabilität:** Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme ist auf Dauer sicherzustellen (z.B. durch IT-Fachfirma),
  - **Wiederherstellbarkeit:** Schutz gegen Datenverlust durch fachgerechte Datensicherung (z.B. durch IT-Fachfirma),
  - **Regelmäßige Überprüfung:** Routineprüfung für die Datensicherheit.

# Umsetzung der DSGVO: Datensicherheit

- Technische und organisatorische Maßnahmen (TOM's) sollten dokumentiert werden.
  - Auf diese Dokumentation kann im Verzeichnis verwiesen werden, um der Verpflichtung nachzukommen, die Maßnahmen der Datensicherheit im Verzeichnis zu beschreiben.



# Umsetzung der DSGVO: Datenschutzinformation

- Datenschutzinformationen in Form von Informationspflichten sind in Art. 12 - 14 DSGVO geregelt und umfangreicher als bisher (siehe zu den Einzelheiten Episode 1 zum Datenschutzrecht)
  - Datenschutzerklärungen auf Webseiten müssen überarbeitet werden und an DSGVO angepasst werden.
  - Bei der Verarbeitung von personenbezogenen Daten sind allgemeine Hinweise zur Datenverarbeitung bereitzustellen.
  - Hinweise zur Datenverarbeitung sollten auch in jedem Arbeitsvertrag gegeben werden.
- Abwicklung der Betroffenenrechte (Art. 15 ff. DSGVO) sollte interne geklärt sein.

## Aufgaben für das Selbststudium

Beantworten Sie die folgenden Fragen zur Umsetzung der DSGVO in der Praxis:

- Wann muss ein Datenschutzbeauftragter benannt werden?
- Welche Maßnahmen der Datensicherheit sind zwingend erforderlich?
- Wer hat ein Verzeichnis zu erstellen und was ist darin aufzuführen?
- Was umfassen die Informationspflichten gemäß Art. 12 - 14 DSGVO?

# Literatur und weiterführende Quellen

- *Roßnagel (Hrsg.)*, Das neue Datenschutzrecht, 1. Aufl. 2018.
- *Plath (Hrsg.)*, DSGVO/BDSG Kommentar, 3. Aufl. 2018.
- *Simitis, Hornung, Spiecker (Hrsg.)*, Datenschutzrecht: DSGVO mit BDSG, 1. Aufl. 2019.

# ENDE

Vielen Dank für Ihre Aufmerksamkeit

Weitere Informationen:

[www.mls-legal.de/eGeneralStudies](http://www.mls-legal.de/eGeneralStudies)