

Datenschutzrecht

Episode 1: Einführung

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 Grundzüge des Datenschutzrechts.

Lernziel 2:

Sie kennen die wesentlichen gesetzlichen Grundlagen des Datenschutzrechts.

Lernziel 3:

Sie kennen die Voraussetzungen, unter denen personenbezogene Daten verarbeitet werden dürfen.

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.

Rechtsgrundlagen

- **Europäische Datenschutz-Grundverordnung** gilt für:
 - öffentliche und nicht-öffentliche Stellen
- **Bundesdatenschutzgesetz** gilt für:
 - öffentliche Stellen des Bundes (z.B. Bundesministerien, Statistisches Bundesamt, Bundesgerichte)
 - öffentliche Stellen der Länder (z.B. Landesbehörden, Landesgerichte, Hochschulen), soweit der Datenschutz nicht durch Landesdatenschutzgesetze geregelt ist
 - nichtöffentliche Stellen (z.B. natürliche und juristische Personen)
- **Datenschutzgesetze der Länder** (z.B. Bremisches Ausführungsgesetz zur DSGVO) gilt für:
 - öffentliche Stellen der Länder (z.B. Hochschulen)

Sachlicher Anwendungsbereich der DSGVO

- DSGVO gilt bei der Verarbeitung **personenbezogener Daten** von **natürlichen, lebenden Personen**
 - „alle Informationen, die sich auf eine **identifizierte** oder **identifizierbare natürliche** Person beziehen“. Identifizierbar ist nach Art. 4 Nr. 1 DSGVO eine natürliche Person, wenn sie „direkt oder indirekt“ identifiziert werden kann, wie die Zuordnung einer Person:
 - zu einer Kennung wie einem Namen,
 - zu einer Kennnummer,
 - zu Standortdaten,
 - zu einer Online-Kennung (IP-Adressen, Cookies)
 - zu einem oder mehreren besonderen Merkmalen, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der natürlichen Person sind.

Anonyme Daten

- Anonyme Daten werden in der DSGVO gesetzlich nicht definiert.
- Anonyme Daten sollen vom Anwendungsbereich der DSGVO nicht erfasst werden, so dass ihre Verarbeitung keinen datenschutzrechtlichen Restriktionen unterliegt (Erwägungsgrund 26).

Pseudonymisierte Daten

- Sonderfall personenbezogener Daten sind pseudonymisierte Daten. Nach Art. 4 Nr. 5 DSGVO ist unter „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise zu verstehen, dass die *„personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.“*
 - Beispiel Pseudonyme: Personalnummer, Kennzahl, Phantasiename bei der Nutzung von Online-Diensten, Verschlüsselung

Pseudonymisierte Daten

- Im Gegensatz zu anonymen Daten sind pseudonymisierte Daten personenbezogene Daten (Erwägungsgrund 26) und fallen in den Regelungsbereich der DSGVO.
- gegenüber sonstigen personenbezogenen Daten sind sie aber privilegiert, weil sie ohne Kenntnis zusätzlicher, getrennt aufbewahrter Informationen einer identifizierten Person nicht zugeordnet werden können.

Räumlicher Anwendungsbereich der DSGVO

- Unterhalten Verantwortliche oder Auftragsverarbeiter in der Europäischen Union eine **Niederlassung**, gilt die DSGVO, soweit die Datenverarbeitung mit der durch die Niederlassung ausgeübten Tätigkeit im Zusammenhang steht. Unerheblich ist, ob die Datenverarbeitung in Europa stattfindet (Art. 3 Abs. 1 DSGVO - **Niederlassungsprinzip**).
- Wenn Verantwortliche oder Auftragsverarbeiter personenbezogenen Daten von Personen verarbeiten, die sich in der Union befinden, im Zusammenhang mit dem **Angebot von Waren oder Dienstleistungen** oder das Verhalten betroffener Personen **beobachten**, soweit ihr Verhalten in der Union erfolgt (Art. 3 Abs. 2 DSGVO - **Marktortprinzip**).

Verantwortlicher für die Datenverarbeitung

- Natürliche oder juristische Personen,
 - Behörden,
 - Einrichtungen oder andere Stellen,
- die allein oder gemeinsam mit anderen über die **Zwecke und Mittel der Verarbeitung von personenbezogenen Daten** entscheiden (sog. „Verantwortliche“, Art. 4 Nr. 7 DSGVO).

Erlaubnis zur Datenverarbeitung

- Jede Datenverarbeitung bedarf nach Art. 6 Abs. 1 DSGVO einer Rechtsgrundlage, dies sind insbesondere:
 - **Einwilligung** der betroffenen Person in die Verarbeitung personenbezogener Daten für einen oder mehrere bestimmte Zwecke (Art. 6 Abs. 1 Satz 1 lit. a) DSGVO),
 - Erfüllung eines **Vertrages** (Art. 6 Abs. 1 Satz 1 lit. b) DSGVO)
 - Erfüllung einer **rechtlichen Verpflichtung** (Art. 6 Abs. 1 Satz 1 lit. c) DSGVO)
 - Wahrnehmung einer **Aufgabe im öffentlichen Interesse** (Art. 6 Abs. 1 Satz 1 lit. e) DSGVO)
 - Datenverarbeitung ist aufgrund **berechtigter Interessen** des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (Art. 6 Abs. 1 Satz 1 lit. f) DSGVO) - **Wertungsfrage!!**

Datenschutzrechtliche Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DSGVO)

- Art. 4 Nr. 11 DSGVO Begriffsbestimmung
 - „jede **freiwillig** für den bestimmten Fall, in **informierter Weise** und **unmissverständlich abgegebene Willenserklärung in Form einer Erklärung** oder einer **sonstigen eindeutigen bestätigenden Handlung**, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.“
- Art. 7 DSGVO: Bedingungen für die Einwilligung
 - **Dokumentation der Einwilligung** durch den Verantwortlichen (Art. 7 Abs. 1 DSGVO)
 - Bei einer Einwilligung durch schriftliche Erklärung hat die „....*Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen,.....*“ (Art. 7 Abs. 2 DSGVO).
 - Betroffene Person hat ein jederzeitiges **Widerrufsrecht** (Art. 7 Abs. 3 DSGVO)

Besondere Datenkategorien (Art. 9 DSGVO)

- Verarbeitung besonderer Kategorien personenbezogener Daten (definiert in Art. 9 Abs. 1 DSGVO, z.B. genetische Daten, biometrische Daten, Gesundheitsdaten) ist grundsätzlich verboten.
- In Art. 9 Abs. 2 lit. a) - j) DSGVO sind Ausnahmen vom Verbot in Abs. 1 definiert, wie insbesondere:
 - die betroffene Person hat in die Datenverarbeitung **ausdrücklich eingewilligt** (Art. 9 Abs. 2 lit. a) DSGVO), soweit keine zwingende Verbotsnorm vorliegt,
 - zur Wahrung lebenswichtiger Interessen, soweit die betroffene Person nicht einwilligen kann (Art. 9 Abs. 2 lit. c) DSGVO),
 - für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche Forschungszwecke und statistische Zwecke (Art. 9 Abs. 2 lit. j) DSGVO).

Informationspflichten

- Betroffene muss bei der **Erhebung personenbezogener Daten** und bei jeder **Zweckänderung** durch den Verantwortlichen informiert werden (Art. 12 - 14 DSGVO) über:
 - Zweck und Rechtsgrundlage der Datenverarbeitung,
 - ggf. Empfänger der personenbezogenen Daten,
 - Speicherdauer,
 - Name und Kontaktdaten des Verantwortlichen,
 - Rechte der Betroffenen,
 - Möglichkeit eine Einwilligung jederzeit zu widerrufen,
 - Beschwerderecht bei einer Aufsichtsbehörde,
 - soweit die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, ist die Betroffene darüber zu informieren, aus welcher Quelle die personenbezogenen Daten stammen.
- Informationen müssen in präziser, transparenter, verständlicher, leicht zugänglicher Form und in klarer und einfacher Sprache erfolgen.

Auftragsverarbeitung (Art. 28 DSGVO)

- Auftragsverarbeitung liegt vor, wenn eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet:
 - Verantwortlicher darf personenbezogene Daten weitergeben, ohne dass dazu eine ausdrückliche Einwilligung oder sonstige gesetzliche Grundlage vorliegen muss.
 - Auftragsverarbeiter darf die personenbezogenen Daten nur auf Weisung des Verantwortlichen verarbeiten (Art. 29 DSGVO).
 - Verantwortlicher muss prüfen, ob Auftragsverarbeiter hinreichende Garantien dafür bietet, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften erfolgt.
 - Für die Auftragsverarbeitung ist ein Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter zu schließen, der die Aufgabe des Auftragsverarbeiters umschreibt.

Pflichten des Verantwortlichen - Rechenschaftspflicht

- Der Verantwortliche (Art. 4 Nr. 7 DSGVO) ist für die Einhaltung der **datenschutzrechtlichen Grundsätze** gemäß Art. 5 Abs. 1 DSGVO verantwortlich und muss dessen Einhaltung auch nachweisen können (Art. 5 Abs. 2 DSGVO):
 - Rechtmäßigkeit und Transparenz,
 - Zweckbindung,
 - Datenminimierung,
 - Richtigkeit,
 - Speicherbegrenzung,
 - Integrität und Vertraulichkeit.
- Verantwortlicher hat Verletzungen des Schutzes personenbezogener Daten binnen 72 Stunden nach Bekanntwerden an die Aufsichtsbehörde zu melden (Art. 33 DSGVO).

Technische und organisatorische Maßnahmen

- **Maßnahmen zur Datensicherheit**, die von dem Verantwortlichen umzusetzen sind, um die Rechte und Freiheiten der Betroffenen zu schützen und sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt (Art. 24 DSGVO), wie z.B.
 - Maßnahmen zur Einhaltung der datenschutzrechtlichen Grundsätze gemäß Art. 5 DSGVO
 - Maßnahmen zur Sicherheit der Verarbeitung (Art. 32 DSGVO)
 - z.B. Pseudonymisierung, Verschlüsselung
 - Datenschutz durch Technikgestaltung und durch datenschutzrechtliche Voreinstellungen (Art. 25 DSGVO)
 - z.B. in Experimente, Evaluationen, Demonstratoren

Verzeichnis von Verarbeitungstätigkeiten

- Jeder Verantwortliche hat ein Verzeichnis aller Verarbeitungstätigkeiten zu erstellen und fortlaufend zu aktualisieren (Art. 30 DSGVO).
 - An welchen Stellen in Unternehmen, Behörden, Vereinen, Projekten etc. werden personenbezogene Daten verarbeitet?
 - z.B. im Rahmen der Administration, Vertrieb, Buchhaltung, Projektevaluation
 - Verzeichnis enthält Angaben wie:
 - Name und Kontaktdaten des Verantwortlichen,
 - Zwecke der Verarbeitung,
 - Kategorien betroffener personenbezogener Daten,
 - Empfänger gegenüber denen personenbezogene Daten offengelegt werden,
 - Fristen für die Löschung,
 - Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO etc.

Benennung eines Datenschutzbeauftragten (Art. 37 DSGVO)

- a) Die Verarbeitung wird von einer **Behörde** oder **öffentlichen Stelle** durchgeführt
 - z.B. Hochschulen haben einen Datenschutzbeauftragten zu benennen - wie auch bei der Beteiligung an einem Forschungsprojekt
- b)/c) Die Kerntätigkeit des Verantwortlichen besteht in der **Durchführung von Verarbeitungsvorgängen ...zur systematischen Überwachung** oder in der Verarbeitung **besonderer Kategorien von Daten** (Art. 9 DSGVO)
 - z.B. bei der Verarbeitung von Gesundheitsdaten/medizinische Daten.
- **Nicht-öffentliche Stellen**, soweit mindestens 10 Personen ständig mit der automatisierten Verarbeitung beschäftigt sind (§ 38 Abs. 1 BDSG)
 - z.B. Unternehmen

Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

- Verantwortlicher hat eine Folgenabschätzung vor der Datenverarbeitung durchzuführen, wenn eine Verarbeitung, insbesondere unter Verwendung **neuer Technologie**, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung **voraussichtlich ein hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge hat, wie insbesondere:
 - systematische und umfassende Bewertung natürlicher Personen mittels Profiling (Art. 35 Abs. 3 lit. a) DSGVO),
 - umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO (Art. 35 Abs. 3 lit. b) DSGVO) oder
 - systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (Art. 35 Abs. 3 lit. c) DSGVO).

Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

- Inhaltliche Anforderungen der Folgenabschätzung (Art. 35 Abs. 7, 8, 9 DSGVO):
 - Systematische Beschreibung der geplanten Verarbeitungsvorgänge sowie ihrer Zwecke,
 - Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,
 - Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen,
 - Beschreibung der Maßnahmen zur Risikoreduzierung.
- Konsultation der zuständigen Aufsichtsbehörde vor Beginn der Datenverarbeitung, soweit ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht (Art. 36 Abs. 1 DSGVO).

Rechte der von der Datenverarbeitung Betroffenen

- Auskunftsrecht (Art. 15 DSGVO)
- Berichtigungsrecht (Art. 16 DSGVO)
- Löschungsrecht und „Recht auf Vergessenwerden“ (Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Widerspruchsrecht (Art. 21 DSGVO)
- Verbot automatisierter Entscheidungen im Einzelfall einschließlich Profiling (Art. 22 DSGVO)

Aufgabe für das Selbststudium

Bitte beantworten Sie die folgenden Fragen und begründen Sie Ihre Antworten:

- Unter welche Voraussetzungen ist eine Datenverarbeitung nach der DSGVO zulässig?
- Nennen sie drei Voraussetzungen einer wirksamen Einwilligung nach der DSGVO.
- Ist es datenschutzrechtlich zulässig,
 - wenn Sie beim Kauf einer Tageszeitung an einem Kiosk nach Ihrem Namen und Ihrer Anschrift gefragt werden und diese Informationen gespeichert werden sollen?
 - wenn Sie beim Kauf eines Buches im Internet nach Ihrem Namen und Ihrer Anschrift gefragt werden und diese Informationen gespeichert werden sollen?

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