
Einführung ins Datenschutzrecht

Henry Krasemann

CAU-Vorlesung
29.10.2018



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Organisatorisches I: Material

- Die Folien der Veranstaltungen werden auf der Seite <https://www.datenschutzzentrum.de/vorlesungen/> zur Verfügung gestellt
- Gesetzestexte auf www.datenschutzzentrum.de/gesetze/: Dürfen auch für die Klausur verwendet werden. Unterstreichungen und Hervorhebungen sind erlaubt. Ebenso Paragraphenverweise in der Form „=> § 3 VIII“ nicht aber Anmerkungen mit Wörtern oder Text.
- Insbesondere Art. 1 bis 39 DSGVO

ULD

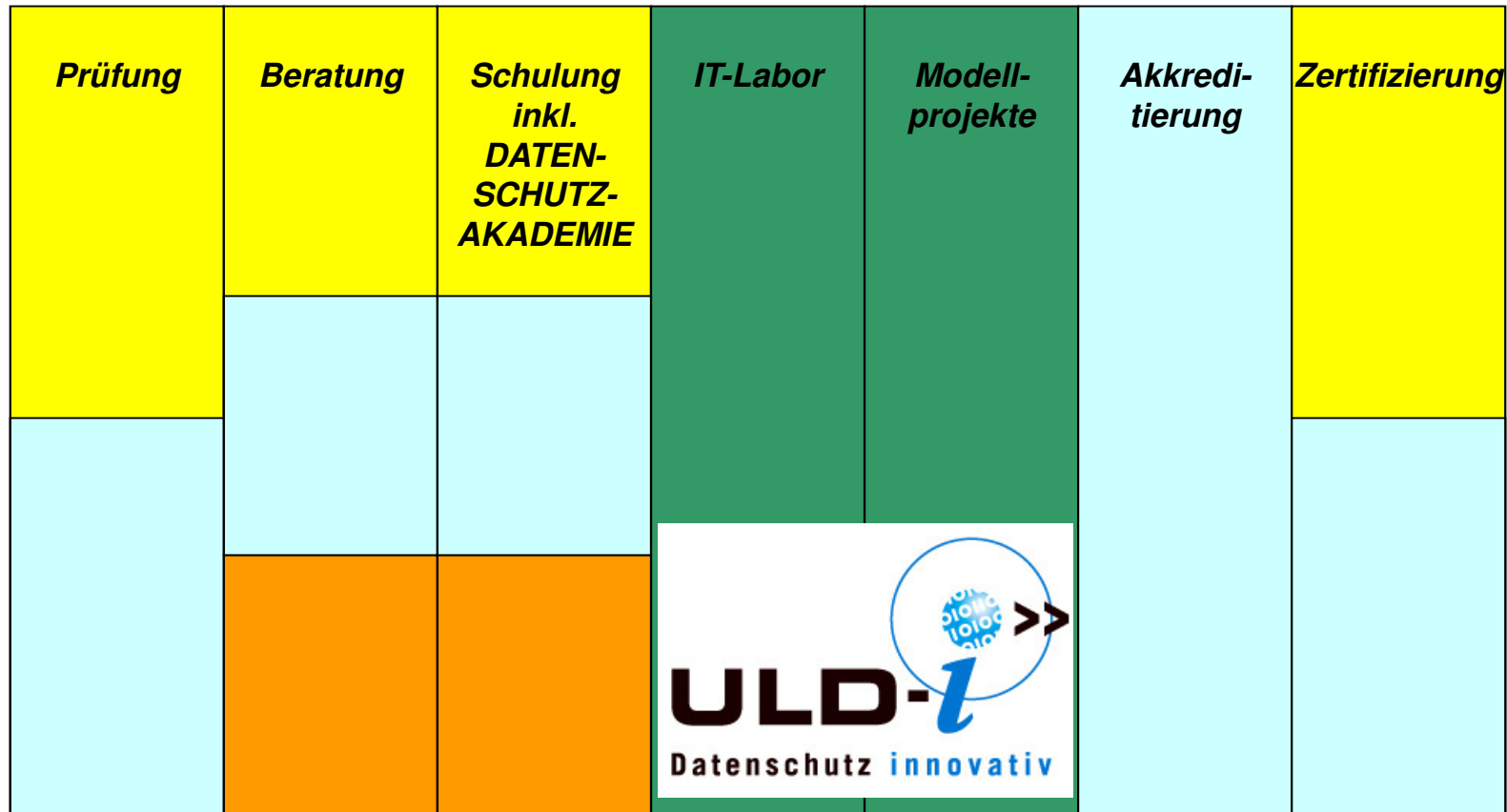


Organisatorisches II

- **Prüfungsleistung: Klausur über alle Bestandteile der Veranstaltung**
- **Üblicher Aufbau im Datenschutzrecht: Freitext-Fragen, Multiple Choice, evtl. ein kleiner Fall**
- **Eine alte Übungsklausur finden Sie auf unserer Webseite**



Kurzvorstellung: Was macht das ULD?



Primäre Adressaten:

- Öffentl. Verwaltungen
- Unternehmen
- Bürger, Kunden, Patienten

- Wirtschaft, Wissenschaft, Verwaltung

Projekte

- Identitätsmanagement – PrimeLife, PRIME und FIDIS
- Europäisches Datenschutz-Gütesiegl - EuroPriSe
- Anonymität im Internet - AN.ON
- Datenschutz in Online-Spielen – DOS
- Audit für Biobanken – bdc-Audit
- Datenschutz in Bürgerportalen
- Europäische Melderegisterauskunft - RISER
- Verbraucherdatenschutz und Datenschutzrecht im Scoring
- Datenschutzerfordernungen für die Forschung – PRISE
- Virtuelles Datenschutzbüro – www.datenschutz.de



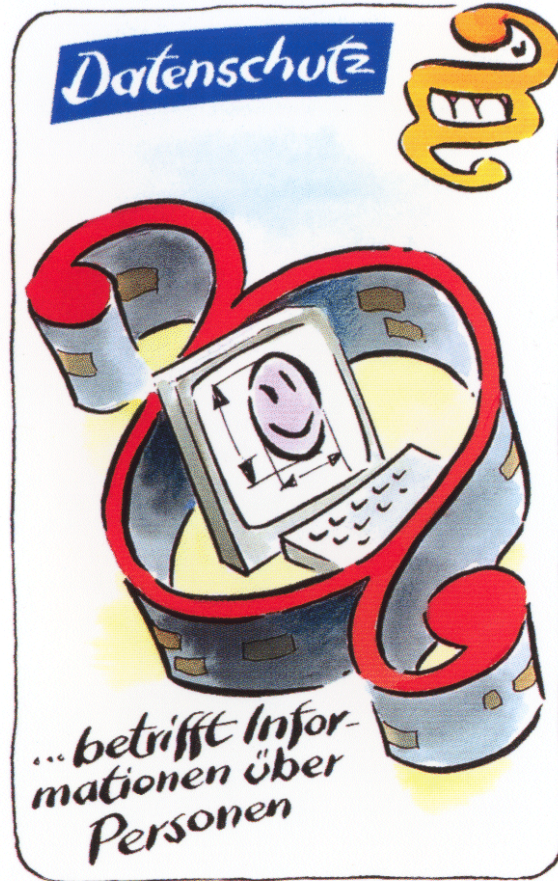
TAUCIS



Warum gibt es Datenschutzrecht?



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein



Entwicklung des Datenschutzes I

- **Anfang der 70er Jahre: Computer in Verwaltung und Wirtschaft**
- **1970: erstes Datenschutzgesetz in Hessen als erstes allgemeines Datenschutzgesetz der Welt**
- **1977: Bundesdatenschutzgesetz**
 - **Einführung von Datenschutzbeauftragten**
 - **Automatisierte Datenverarbeitung**
 - **Schutz personenbezogener Daten**
- **1978: Landesdatenschutzgesetz Schleswig-Holstein**
- **1981: alle Bundesländer haben ein LandesDSG**
- **1983: Volkszählungsurteil**

ULD



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

BVerfG Online-Durchsuchung Schutz informationstechn. Systeme

- **Bundesverfassungsgericht 27. Februar 2008**
 - Sachverhalt:
Verfassungsschutzgesetz NRW sah Möglichkeit der Online-Durchsuchung vor.
 - Urteil: Gesetz ist verfassungswidrig, weil unverhältnismäßig. Schwere des Eingriffs muss besonders schwerwiegende Gefahr gegenüberstehen
 - Eingriffsvoraussetzungen:
 - Tatsächliche Anhaltspunkte für...
 - konkrete Gefahr für ein...
 - überragend wichtiges Rechtsgut (Leib, Leben, Freiheit der Person, Bestand des Rechtsstaates)
 - Ein Ermächtigungsgesetz muss vorsehen:
 - richterliche Anordnung
 - Vorkehrungen für Schutz des Kernbereichs privater Lebensführung
 - Erhebung aus laufendem Telekommunikationsvorgang unterfällt Art. 10 GG
- ⇒ **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**

ULD



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Weltweit

- OECD 1980: „Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten“
 - Kein Völkerrecht, sondern nur Empfehlungen
- „Richtlinien zur Verarbeitung personenbezogener Daten in automatisierten Dateien“ der Generalversammlung der Vereinten Nationen (UN) vom Dezember 1990
- „Privacy-Shield-Abkommen“ USA – EU

- Art. 8 EU-Grundrechtecharta
 - Grundrecht auf Datenschutz
- EG-Datenschutzrichtlinie 95/46/EG
 - Allgemeiner Rahmen
 - Wird gerade überarbeitet
- Richtlinie 2002/58/EG (überarbeitete Fassung von 2009)
 - Telekommunikation / Internetdienste
- Richtlinie 2006/24/EG
 - Vorratsdatenspeicherung
- **Ab 25. Mai 2018: Datenschutz-Grundverordnung**
- **Ab ??? ePrivacy-Verordnung**

Deutschland

- [Datenschutz-Grundverordnung (ab 25.05.2018)]
- Bundesdatenschutzgesetz (BDSG)
 - Allgemeine Datenschutzregelungen
 - Für Bundesbehörden und Privatwirtschaft
- Landesdatenschutzgesetze
 - Für Landesbehörden
- Telekommunikationsgesetz (TKG)
 - Telekommunikationsdienste
- Telemediengesetz (TMG)
 - Telemediendienste (u. a. Webseiten)
- Sozialgesetzbücher, Strafgesetzbuch ...

Aufsichtsstellen in Deutschland

- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
 - Bundesbehörden
 - Sonderzuweisungen: Telekommunikations-Unternehmen, Postwesen
- Landesbeauftragte für Datenschutz
 - Landesbehörden
 - Privatwirtschaft mit Sitz im jeweiligen Bundesland



Anwendungsbereich der DSGVO und des BDSG

Zweck der DSGVO, des BDSG und anderer
Rechtsvorschriften

Geschichte der DSGVO

- In Kraft seit 24. Mai 2016 / Anwendung ab: 25. Mai 2018
- Maßgeblicher Autor: Jan Philipp Albrecht (bald SH-Minister)
- **70 Öffnungsklauseln** (Regelungsaufträge und Regelungsoptionen) für nationalen Gesetzgeber
- Neu: keine Unterscheidung öffentlicher / privater Bereich
- Neues Problem: Welche Übersetzung nehmen wir denn?
 - 30. April 2018: Sprachliche Anpassungen („grundsätzlich“) etc.
- Verhältnis zu anderen Gesetzen?
 - Problem: ePrivacy-Bereich / KunstUrhG etc.
- Neu: Aus Artikel 29 Gruppe wird Datenschutzausschuss
- **One-Stop-Shop:** einfacher für Verbraucher(innen)
- **Kohärenzmechanismus:** Einigung der Aufsichtsbehörden

Zweck der DSGVO

Zweck der DSGVO: Art. 1:

Diese Verordnung enthält Vorschriften zum **Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten** und zum freien Verkehr solcher Daten.

Diese Verordnung **schützt die Grundrechte und Grundfreiheiten natürlicher Personen** und insbesondere deren Recht auf Schutz personenbezogener Daten.

Anwendungsbereich

Umfang:

Diese Verordnung gilt für die **ganz oder teilweise automatisierte** Verarbeitung personenbezogener Daten sowie für die **nichtautomatisierte** Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Keine Anwendung:

- Außerhalb Unionsrecht
- Außen- und Sicherheitspolitik
- Ausschließlich persönliche oder familiäre Tätigkeiten
- Verhütung, Ermittlung etc. von Straftaten

Räumlicher Anwendungsbereich

Art. 3 DSGVO

- Verarbeitung personenbezogener Daten
 - Tätigkeit einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union
 - Verarbeitungsort egal
- Verarbeitung personenbezogener Daten betroffener Personen in der Union
 - Verarbeiter außerhalb der Union
 - Anbieten von Waren/Dienstleistungen betroffenen Personen in der Union (Zahlung egal)
 - Verhalten von Personen innerhalb der Union beobachten

Personenbezogene Daten

Art. 4 Nr. 1 DSGVO

Natürliche Person

- Kein Schutz für juristischer Personen mangels Menschenwürde. Aber: Schutz der natürlichen Person hinter der juristischen Person (Unternehmer)

Alle Information bezogen auf Person

- Es gibt kein belangloses Datum unter den Bedingungen der automatischen Datenverarbeitung (Volkszählungsurteil).
- Alle Informationen, die über die Bezugsperson etwas aussagen.

Identifizierte oder identifizierbare Person

- Aus den Angaben muss sich ergeben, dass sie sich auf eine Person beziehen.



Persönliche oder familiäre Tätigkeiten

- Ausnahme vom Anwendungsbereich der DSGVO
- Persönliche oder familiäre Tätigkeiten, Art. 2 Abs. 2 lit. c DSGVO
 - Abgrenzung des Bereichs persönlicher Lebensführung von beruflicher und geschäftlicher Sphäre.
 - Äußerer Rahmen, organisatorische Anlage und inhaltliche Konzeption müssen persönliche/familiäre Zwecksetzung erkennen lassen.
 - Beispiel: Nutzung einer Adressdatei auf PC von Familie und Freunden, private Fotosammlung, Urlaubsbilder.
 - Nicht aber: Mitgliederliste eines Vereins, private Homepage, Social networks.
 - Bei intensiven Rechtseingriffen: Abwehransprüche aus BGB möglich

ULD



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Anonymisierung, Pseudonymisierung



Rechtsfolgen

- Gesetze nicht anwendbar für **anonyme Daten**
- Anwendbar, aber erweiterte Verarbeitungsbefugnisse bei **pseudonymen Daten**

ULD



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Stadien der Datenverarbeitung

- **Früher: Erheben => Verarbeiten => Nutzen**
- **Heute:** Art. 4 Nr. 2 DSGVO:
 - „Verarbeitung“: jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;



Wie funktioniert das Datenschutzrecht?



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Sechs Goldene Regeln des Datenschutzes

- **Rechtmäßigkeit**
 - Gesetz, Einwilligung, Vertrag, Dienst- oder Betriebsvereinbarung
- **Zweckbindung**
 - Verwendung nur für Erhebungszweck
- **Datenminimierung und Speicherbegrenzung**
 - Verarbeitung nur soweit für Erhebungszweck erforderlich
- **Transparenz und Betroffenenrechte**
 - Unterrichtung über Verwendung, Auskunfts-/Berichtigungs-/Löschrechte
- **Datensicherheit und Richtigkeit**
 - Technische und organisatorische Maßnahmen, Integrität und Vertraulichkeit
- **Kontrolle**
 - Interner / externer Datenschutzbeauftragter; Audit

Konkret: Art. 5 DSGVO

Personenbezogene Daten müssen:

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (**„Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“**);
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken (**„Zweckbindung“**);
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**„Datenminimierung“**);
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden (**„Richtigkeit“**);

Art. 5 DSGVO 2. Teil

- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen **nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist**; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („**Speicherbegrenzung**“);
- in einer Weise verarbeitet werden, die eine **angemessene Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („**Integrität und Vertraulichkeit**“);



Art. 6 DSGVO: Zentrale Befugnisnorm

- Datenverarbeitung ist nur (!) rechtmäßig, wenn:
 - **Einwilligung**
 - **Vertragserfüllung**
 - **Erfüllung rechtlicher Verpflichtung**
 - Lebenswichtige Interessen
 - Ausübung öffentliche Gewalt
 - **Wahrung berechtigter Interessen (sofern Interessen des Betroffenen nicht überwiegen)**

Art. 9 DSGVO: besondere Kategorien

- Verschärfte Bedingungen bei besonderen Kategorien
 - Politische Meinung, ethnische Herkunft, Religion, Weltanschauung, genetische/biometrische Daten, Gesundheit, Sexualität etc.
- Verarbeitung grundsätzlich untersagt
- Ausnahmen:
 - Ausdrückliche Einwilligung
 - Arbeitsrecht / Soziale Sicherheit
 - Lebenswichtige Interessen
 - Offensichtlich öffentliche Daten
 - ...

Einwilligung

„ ... jede **freiwillig** für den **bestimmten Fall**, in **informierter Weise** und **unmissverständlich** abgegebene **Willensbekundung** 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. 4 Nr. 11 DS-GVO)



Was ist wichtig?

- Die Einwilligung muss informiert und freiwillig erfolgen.
- Die Einwilligung muss nicht mehr schriftlich sein.
- Die Einwilligung ist mit Wirkung für die Zukunft widerruflich.



Einwilligung

- Information
 - Welche Daten werden verarbeitet?
 - Wer verarbeitet?
 - Zu welchem Zweck?
 - Speicherdauer?
- Freiwilligkeit
 - Kopplungsverbot ⇒ Lockangebote
 - Wirtschaftliche Abhängigkeit ⇒ Arbeitsverhältnis
- Formalien
 - Hervorhebung der Einwilligungserklärung



Einwilligung eines Kindes

- Bzgl. Dienste der Informationsgesellschaft: 16 Jahre
 - Oder Einwilligung der Eltern
 - Art. 8 DSGVO
- Sonstige Dienste: Einsichtsfähigkeit

Einwilligung

▪ **Widerruflichkeit der Einwilligung**

- Ab jetzt und für die Zukunft: JA
- Für die Vergangenheit: NEIN

• **Probleme**

- Was, wenn Vertrag von Einwilligung abhängig?
- Was, wenn Folgen nicht mehr unumkehrbar?
- Spannungsverhältnis zwischen KunstUrhG und DSGVO



Zweckbindung

Personenbezogene Daten dürfen nur zu dem Zweck verarbeitet und genutzt werden, zu dem sie erhoben worden sind.

Erforderlichkeit

Die Datenverarbeitung ist auf den für Ihren Erhebungszweck notwendigen Umfang zu begrenzen.

- Art
- Umfang
- Dauer der Datenverarbeitung



Erforderlichkeit

Recht auf Löschung (Art. 17 – Recht auf Vergessenwerden)

- Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten **unverzüglich gelöscht werden**, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:
 - Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, **nicht mehr notwendig**.
 - Die betroffene Person **widerruft ihre Einwilligung** [...].
- Die betroffene Person legt gemäß Artikel 21 Absatz 1 **Widerspruch** gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor [...].
- Die personenbezogenen Daten wurden **unrechtmäßig verarbeitet**.
- [...]

Recht auf Löschung

Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten **angemessene Maßnahmen**, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

Beispiel: Daten in Google-Suche

Ausnahmen vom Recht auf Löschung

- Soweit die Verarbeitung erforderlich ist zur Ausübung des Rechts auf freie **Meinungsäußerung und Information**;
- Zur Erfüllung einer **rechtlichen Verpflichtung**, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- Aus Gründen des öffentlichen Interesses im Bereich der **öffentlichen Gesundheit** [...];
- Für im öffentlichen Interesse liegende **Archivzwecke**, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß [Artikel 89](#) Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
- Zur Geltendmachung, Ausübung oder **Verteidigung von Rechtsansprüchen**.



Sperrung / Recht auf Einschränkung der Verarbeitung

- Wenn
 - die **Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten** wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,
 - die Verarbeitung unrechtmäßig ist und die **betroffene Person die Löschung der personenbezogenen Daten ablehnt** und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;
 - der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen** benötigt, oder
 - die betroffene Person **Widerspruch** gegen die Verarbeitung gemäß Artikel 21 Absatz 1 eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Transparenz ***Art. 12 ff. DSGVO***

Die/der Betroffene muss in der Lage sein zu erfahren, wer welche Art von Daten in welchem Umfang und zu welchem Zweck erhebt, verarbeitet oder nutzt.

- Allgemeine und besondere Informations- und Benachrichtigungspflichten der verantwortlichen Stelle
 - Art. 13 DSGVO (direkte Erhebung)
 - Art. 14 DSGVO (indirekte Erhebung)
- Auskunftsansprüche der Betroffenen (Art. 15 DSGVO)

Transparenz

Auskunftsanspruch, Art. 15 DSGVO

- Inhalt der Daten
- die Verarbeitungszwecke;
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.



Besondere Transparenzverpflichtung

- **Breach Notification, Art. 33 DSGVO**
 - Im Falle einer **Verletzung des Schutzes personenbezogener Daten** meldet der Verantwortliche **unverzüglich und möglichst binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Datensicherheit



Datenschutz setzt technisch und organisatorisch sichere Datenverarbeitung voraus

- Art. 32 ff. DSGVO
- Technische Maßnahmen
- Organisatorische Maßnahmen (innerbetriebliche Organisation)

Schutzziele:

- | | |
|--------------------------|----------------------|
| ▪ Vertraulichkeit | ▪ Transparenz |
| ▪ Integrität | ▪ Nicht- |
| ▪ Verfügbarkeit | Verkettbarkeit |
| ▪ (Belastbarkeit) | ▪ Intervenierbarkeit |

Sanktionen DSGVO

Art. 83 ff. DSGVO

- Geldbußen bis 10 Millionen Euro oder 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres
 - Einwilligung Kind, Zertifizierungsstellen etc.
- Bis 20 Millionen Euro bzw. 4% Jahresumsatz
 - Einwilligungsbedingungen, Rechte des Betroffenen, Transparenz, Drittlandübermittlung etc.
- Alte „Hitliste“ Bußgeldverfahren
 - § 43 Abs. 1 Nr. 3 BDSG (Werbewiderspruchshinweis)
 - § 43 Abs. 1 Nr. 8a BDSG (Auskunft gegenüber Betroffenen)
 - § 43 Abs. 1 Nr. 10 BDSG (Auskunft gegenüber Aufsichtsbehörde)
 - § 43 Abs. 1 Nr. 1 BDSG (Meldepflicht)

Sanktionen nach StGB

- § 201 Verletzung der Vertraulichkeit des Wortes
- § 201a Verletzung des höchst persönlichen Lebensbereichs durch Bildaufnahmen
- § 202 Verletzung des Briefgeheimnisses
- § 203 Verletzung von Privatgeheimnissen (Berufsgeheimnis)

gemäß § 205 ist Strafantrag der Betroffenen für Strafverfolgung erforderlich

- § 202a Ausspähen von Daten



Staatsanwaltschaft kann auch bei besonderem öffentlichen Interesse Strafverfolgung einleiten

- **§ 206 Verletzung des Post- oder Fernmeldegeheimnisses**

Datenschutzbeauftragter ***Art. 37 DSGVO***

- Öffentliche Stellen
- Private Stellen (§ 38 BDSG neu):
 - soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen
 - Datenschutz-Folgenabschätzung nach Artikel 35 erforderlich
 - Zum Zwecke der Übermittlung
 - ...

Aufgaben des DSB

- Hinwirken auf die Einhaltung der DSGVO und anderer Vorschriften über den Datenschutz
- **Beratung**
 - bei der Gestaltung und
 - Auswahl von Verfahren und Datenverarbeitungsmaßnahmen
- **Prüfung** der Einhaltung von Datenschutzvorschriften
 - Vor allem bei der Einführung neuer Verfahren oder
 - Änderung bestehender Verfahren
- **Überwachung** der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme
- **Schulung** der Beschäftigten zu Datenschutzrecht und Erfordernissen des Datenschutzes

Aber...

- Der DSB ist **nicht verantwortlich** für die Datenverarbeitung, sondern die datenverarbeitende Stelle ist **verantwortliche Stelle**
- Der DSB ist Controller/Berater in Bezug auf die Verarbeitung personenbezogener Daten

Verarbeitungsverzeichnis

- Der Verantwortliche hat die **Pflicht, ein Verzeichnis zu führen**.
- Art. 30 enthält einen ausführlichen Katalog über die im Verzeichnis erforderlichen Angaben.
- Auftragsverarbeiter müssen künftig ein **separates Verzeichnis** über die von Ihnen erbrachten, weisungsgebundenen Tätigkeiten führen.
- Es ist nicht mehr öffentlich zur Verfügung zu stellen.
- Es bestehen Ausnahmen für Betriebe bis 250 Mitarbeiter, sofern keine kritische Datenverarbeitung erfolgt, keine Daten besonderer Kategorien verarbeitet werden, kein Risiko für Rechte und Freiheiten betroffener Personen besteht und die Verarbeitung **nicht nur gelegentlich** erfolgt.

Sonstiges

- Recht auf Datenübertragbarkeit: Art. 20 DSGVO
- Privacy by Design und by Default: Art. 25 DSGVO
- Gemeinsame Verantwortlichkeit: Art. 26 DSGVO
- Datenschutz-Folgenabschätzung: Art.35 DSGVO
 - Wenn hohes Risiko für Rechte und Freiheiten

Verantwortlichkeiten / Auftragsdatenverarbeitung



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Verantwortlichkeit

- **Verantwortlich**
 - Wer personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt
 - Wer andere im Wege der Auftragsdatenverarbeitung für sich tätig werden lässt
- **Auftragsverarbeitung**
 - Datenverarbeitung nach Weisung des Auftraggebers
 - „Verlängerter Arm“ des Auftraggebers
 - Beispiel: DV im Rechenzentrum
 - Gegenteil: Übermittlung an einen Dritten / Gemeinsame Verantwortlichkeit (Art. 26 DSGVO)

Art. 28 DSGVO

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser **Vertrag** bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

- die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
- gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;
- die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
- angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;
- unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;
- nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht,
- dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.
- Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

Auftragsverarbeitung

- Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der **Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen** (Alternative: Zertifizierung). Das Ergebnis ist zu dokumentieren.
- Der Auftragnehmer darf die Daten nur im Rahmen der **Weisungen** des Auftraggebers erheben, verarbeiten oder nutzen.

§ 203 StGB

- Ggf. Keine Auftragsverarbeitung möglich, wenn Verletzung von Privatgeheimnissen
- Gilt für Geheimnisträger wie: Anwälte, Ärzte, Psychologen, Eheberater, Beratungsstellen, Versicherungen, Steuerberater
- Problembereiche: Aktenvernichtung, EDV-Wartung etc.
 - § 203 StGB neu: Erweiterung der Hilfspersonen

Telemedien

- Bisher: § 12 ff. Telemediengesetz
- Werden durch DSGVO ersetzt
- ePrivacy-Verordnung steht aus
- Problembereiche:
 - Tracking über Seiten hinweg
 - Einwilligung erforderlich (siehe DSK-Beschluss)
 - Einwilligung in Cookies?

Sonderfall: Fotografieren

- Unterscheidung: fotografieren (meist erlaubt) und veröffentlichen (i.d.R. nur mit Einwilligung)
- Fotografieren:
 - Ausschließlich persönliche / familiäre Tätigkeit (Art. 2 Abs. 2 Buchst. c DSGVO) -> zulässig (z. B. Urlaubsfotos)
 - Art. 6 Abs. 1 Buchst. f DSGVO: bei vorhandenem berechtigten Interesse des Fotografen, wenn die schutzwürdigen Interessen der abgebildeten Personen nicht überwiegen
 - Problem ggf. Transparenz
- Veröffentlichen:
 - Einwilligung
 - Art. 6 Abs. 1 Buchst. f DSGVO mit Auslegung KunstUrhG oder KunstUrhG direkt

Weitere Informationen

- www.datenschutzzentrum.de/dsgvo:
 - Muster (u.a. Verzeichnis der Verarbeitungstätigkeiten)
 - Kurzpapiere der Datenschutzkonferenz
 - Gesetze
 - Neuigkeiten
 - Meldung Datenschutzbeauftragter



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Vielen Dank!

Noch Fragen?

Henry Krasemann
ULD7@datenschutzzentrum.de
Tel. 0431-988 1398

www.datenschutzzentrum.de