

Webinar

DSGVO – (einige) Veränderungen und
Folgen für den Hochschulbereich.

17.5.2018 via e-teaching.org

Prof. Dr. iur. Tobias Keber Hochschule der Medien Stuttgart keber@hdm-stuttgart.de

+49 711 8923 2718 Twitter: @datenreiserecht

Wer?

- Professur für **Medienrecht und Medienpolitik** in der digitalen Gesellschaft, Hochschule der Medien (HdM) Stuttgart
- Institut für Digitale Ethik (IDE), Hochschule der Medien Stuttgart
- Zuvor: Rechtsanwalt
- Vorsitzender des Wissenschaftlichen Beirats der Gesellschaft für Datenschutz und Datensicherheit (GDD)
- Kommentierung Art. 25 DSGVO (erscheint am 25.5.2018) in:



Agenda

- **Teil I: Basics**
 - **Überblick Datenschutzrecht**
 - **Europäische Vorgaben: von der Richtlinie zur Verordnung**
 - **DSGVO: Grundlagen, Prinzipien, Neuerungen**
- **Teil II: Konkrete(re)s**
 - **Privacy by Design und Privacy by Default**
 - **Lernplattformen und Datenportabilität**
 - **Learning Analytics und Folgenabschätzung**
 - **Hochschulkommunikation und Social Media**

Vorab

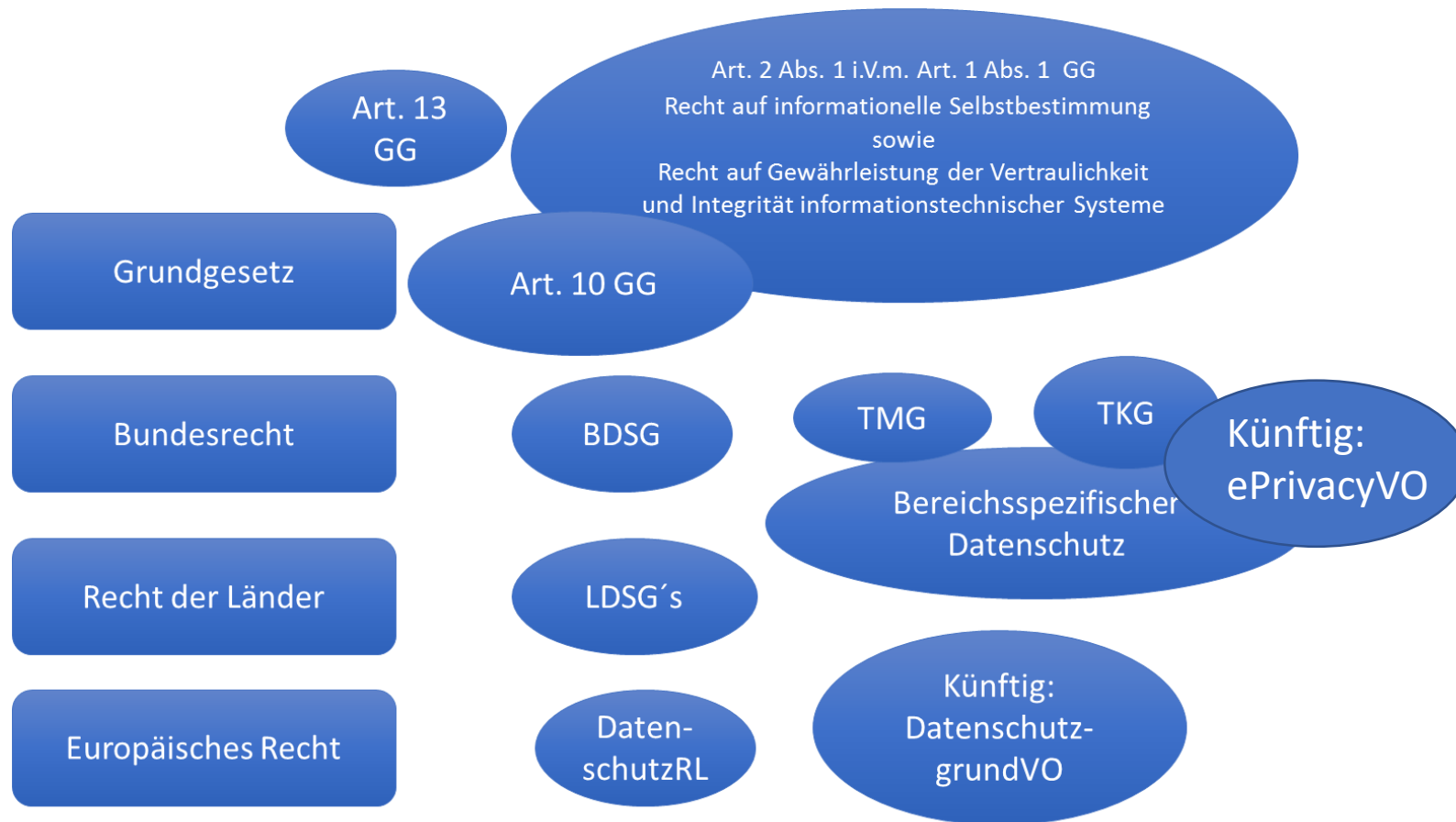
Vorab: don't panic.

- **Don't panic – we all survived the Y2K-Bug**
- **Wir müssen arbeitsfähig bleiben (Art. 5 Abs. 3 GG, §§ 2, 3 LHG)**
- **Datenschutz ist wichtig, aber kein Supergrundrecht**
- **Aufsichtsbehörden haben Zähne bekommen, aber das bedeutet nicht, dass sie bissig geworden sind (Ronellenfitsch)**
- **(Weitere) Handreichungen muss und wird es geben**

Teil I: Überblick DSGVO

Hintergrund, Rechtscharakter, Grundprinzipien

Überblick Datenschutzrecht - Rechtsquellen



Hintergrund zur DSGVO - Basisdaten

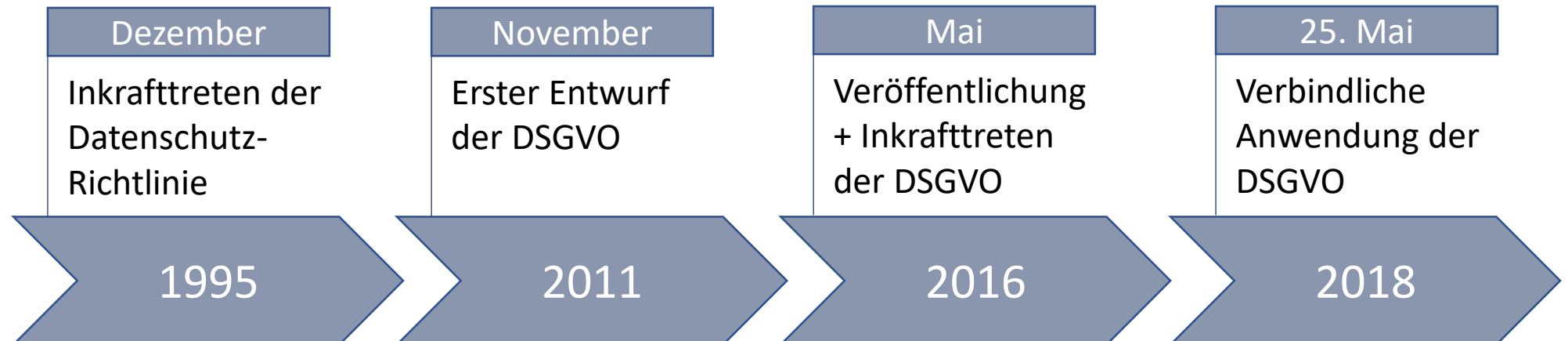


Titel: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG
Kurz: Datenschutz-Grundverordnung (DSGVO)

Rechtsnatur: Verordnung (unmittelbar geltend) *mit Öffnungsklauseln*

Geltungsbereich: Europäische Union

Zeitliche Abfolge:



DSGVO – Ziele/Ideen



Modernisierung des Datenschutzrechts

EU-weite *einheitliche Standards* zum Datenschutz

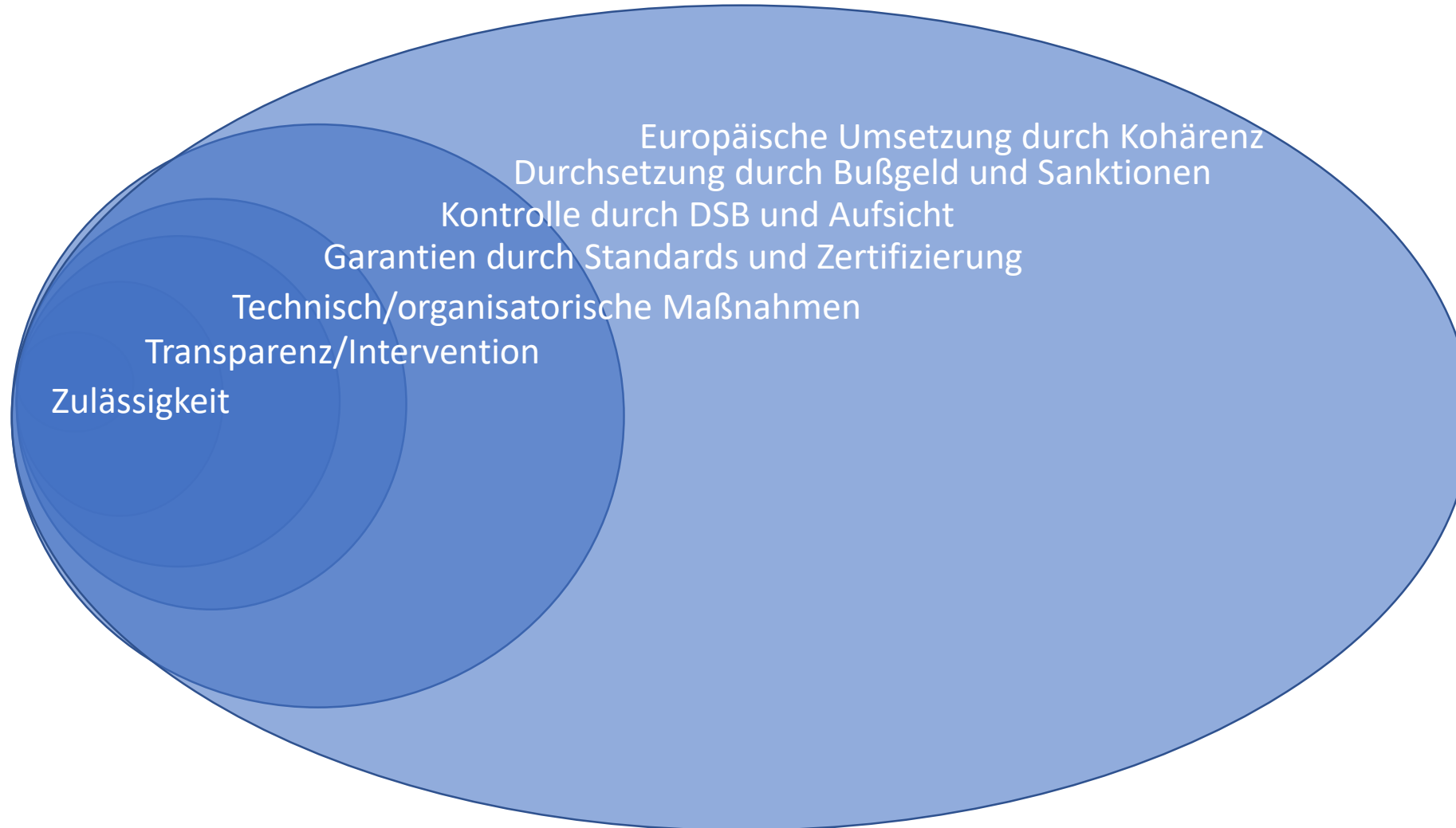
EU-weite *Stärkung* des Datenschutz

EU-weite *Kooperationen der Aufsichtsbehörden*

Verordnung - Rechtscharakter

- DSGVO: allgemeine Regelung mit unmittelbarer Geltung (Verordnungen müssen nicht wie Richtlinien umgesetzt werden)
- Grundsatz: Vollharmonisierung im nicht-öffentlichen Bereich
- Ersetzt grds. nationales Datenschutzrecht, führt zur Unanwendbarkeit entgegenstehender nationaler Regelungen
- ABER: Öffnungsklauseln (Richtlinien-Charakter im öffentlichen Bereich)

DSGVO: Übersicht



Grundprinzipien der DSGVO

Artikel 1 Gegenstand und Ziele

- Schutz der Grundrechte und Grundfreiheiten natürlicher Personen
- insbesondere deren Recht auf Schutz personenbezogener Daten und
- der freie Verkehr personenbezogener Daten

Artikel 2 Sachlicher Anwendungsbereich

- Ganz oder teilweise Automatisierte Verarbeitung personenbezogener Daten
- Nichtautomatisierte Verarbeitung von personenbezogener Daten

Artikel 5 Grundsätze für die Verarbeitung

- Rechtmäßigkeit
- Datensparsamkeit
- Zweckbindung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Artikel 6 Rechtmäßigkeit der Datenverarbeitung

Erfüllung mind. einer Bedingung:

- Einwilligung
- Erfüllung/Verarbeitung eines Vertrages
- Schutz lebenswichtiger Interessen



DSGVO

Grundprinzipien der DSGVO

Artikel 3
Räumlicher Anwendungsbereich



Artikel 12-21
Rechte der betroffenen Person



DSGVO

Artikel 83
**Allgemeine Bedingungen für die
Verhängung von Geldbußen**



Grundprinzipien der DSGVO – Artikel 3

Räumlicher Anwendungsbereich – „Marktortprinzip“

- Die DSGVO ist nicht nur für die in der Europäischen Union niedergelassenen Unternehmen relevant (sog. Marktortprinzip, Art. 3 Abs. 2).
- Voraussetzung ist, dass sich ein Angebot von (unentgeltlichen) Waren oder Dienstleistungen an einen **nationalen Markt in der EU** richtet (lit. a), oder eine Datenverarbeitung zur **Verhaltensbeobachtung** betroffener Personen in der EU erfolgt (lit. b).
- **Der Anwendungsbereich erstreckt sich also grds. auch auf außereuropäische Unternehmen, die auf dem europäischen Markt agieren, selbst wenn Sie keine eigenständige Niederlassung im Gebiet der europäischen Union unterhalten (z.B. auch Facebook oder Google).**
- Dadurch sollen **gleiche Wettbewerbsbedingungen** für alle Unternehmen geschaffen werden, nachdem das BDSG lediglich „im Inland“ erhobene Daten dem deutschen Datenschutzrecht unterwarf (§ 1 Abs. 5 Satz 2 BDSG) und insoweit Unklarheiten bezgl. dessen Anwendbarkeit entstanden sind.

Quelle: BfDI – Info 6

Artikel 4: Definitionen

1. “personenbezogene Daten” alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden “betroffene Person”) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

Artikel 4: Definitionen

2. “Verarbeitung” jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten 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;

Artikel 4: Definitionen

5. “Pseudonymisierung” die Verarbeitung personenbezogener Daten in einer Weise, 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;

Artikel 4: Definitionen

7. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden

Artikel 5 und 6 DSGVO

Artikel 6: Rechtmäßigkeit der Verarbeitung

- u.a.: Einwilligung, Vertrag, gesetzl. Gestattungsnorm, lebenswichtige Interessen, Interessenabwägung

Artikel 5: Grundsätze

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Rechenschaftspflicht!
Accountability (Art. 5 Abs. 2)
Nachweispflicht

Artikel 5 und 6 Details

- Verarbeitung von Daten ist nur rechtmäßig, wenn eine **Einwilligung** oder eine andere in dieser Vorschrift normierte Ausnahme vorliegt (Art. 5 Abs. 1 lit. a i.V.m. Art. 6 Abs. 1), d.h. wenn
 - die Verarbeitung für die **Erfüllung eines Vertrags** erforderlich ist (Art. 6 Abs. 1 lit b), oder
 - die Verarbeitung zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich ist (lit. c), oder
 - die Verarbeitung erforderlich ist, um **lebenswichtige Interessen** der betroffenen Person zu schützen (lit. d), oder
 - **die Verarbeitung zur Erfüllung hoheitlicher Aufgaben erforderlich ist (lit. e), oder**
 - **zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist (lit. f).**
 - **(P) gilt nicht für Behörden für Verarbeitung in Erfüllung ihrer Aufgaben – Hochschulen = Behörde in diesem Sinne?**
- Generell muss die Verarbeitung der personenbezogenen Daten **dem Zweck angemessen** sein (Art. 5 lit. b u. c).
- Auch **Prinzip der Datensparsamkeit** („Datenminimierung“) genannt, Art. 5 lit. c).

DSGVO und ihre „Umsetzung“ im nationalen Recht

- Die DSGVO gilt in den Mitgliedstaaten unmittelbar und braucht daher nicht in nationales Recht umgewandelt werden (sog. **Anwendungsvorrang, Art. 288 Abs. 2 AEUV**).
- **Mitgliedstaaten können jedoch eigene, ergänzende Regelungen setzen (jedoch lediglich dort, wo durch DSGVO gesetzl. vorgesehen, sog. „Öffnungsklauseln“, s.o.).**
- In der Bundesrepublik Deutschland erfolgte diese Rechtsetzung z.B. durch das Datenschutz-Anpassungs-Umsetzungs-Gesetz (**DSAnpUG-EU**), insbes. in Hinblick auf **Datenverarbeitung öffentlicher Stellen (Art. 86)** sowie im Beschäftigtenkontext (Art. 88).
- Die DSGVO ersetzt nicht nur das Bundesdatenschutzgesetz (BDSG), sondern auch viele weitere Bundesgesetze, die Regelungen zum Datenschutz beinhaltet haben (z.B. SGB, TKG, TMG, etc.). Diese sind hiervon (inhaltlich oder auch formell) betroffen und werden von dieser überlagert (z.B. datenrechtliche Regelungen des § 11 ff. TMG; hierbei auch geplante **E-PrivacyVO** zu beachten).

Prüfungsraster

- Gibt es eine datenschutzrechtliche Regelung in der DSGVO?
- Lässt diese Regelung den Mitgliedstaaten einen Regelungsspielraum?
- Wurde der Regelungsspielraum in Deutschland genutzt?
- Durch Bundes- oder Landesrecht?
- Wurden die Grenzen des mitgliedstaatlichen Spielraums beachtet?

Grundprinzipien der DSGVO

Artikel 3 **new**
Räumlicher Anwendungsbereich

Artikel 12-21 **new**
Rechte der betroffenen Person

DSGVO

Artikel 83 **new**
**Allgemeine Bedingungen für die
Verhängung von Geldbußen**

Grundprinzipien der DSGVO – Artikel 12-21

Rechte der betroffenen Person - Übersicht

Information:

- Zweck & Rechtsgrundlage der Verarbeitung
- Name und Kontaktdaten des Verantwortlichen

Transparenz:

- Präzise, verständlich und leicht zugänglich
- Klare und einfache Sprache

Auskunft:

- Verarbeitungszweck
- (Geplante) Dauer der Verarbeitung
- Offenlegung gegenüber Dritten

Einschränkung:

- Unrechtmäßigkeit der Verarbeitung
- Bestritt der Richtigkeit

Datenübertragbarkeit:

- Übermittlung der Daten

Widerspruch:

- Direktwerbung

Vervollständigung

Berichtigung

Löschung („Recht auf Vergessenwerden“):

- Unrechtmäßigkeit der Verarbeitung
- Zweck der Erhebung nicht mehr notwendig

Rechte der betroffenen Person

Details

- Art. 12 DSGVO normiert die Anforderungen an die **Transparenz**, die Art der **Kommunikation** sowie die **Modalitäten** für die Ausübung der Rechte der betroffenen Person. Beispiele:
 - Betroffene müssen in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form über die Verarbeitung ihrer Daten informiert werden (Art. 12 Abs. 1 Satz 1).
 - Verantwortliche müssen betroffener Person die Ausübung ihrer Rechte erleichtern (Abs. 2).
- Art. 13 f. DSGVO sehen einen umfangreichen Katalog **proaktiver Benachrichtigungspflichten** vor, wobei danach differenziert wird, ob die Daten bei der betroffenen Person (Art. 13 DSGVO) oder bei Dritten (Art. 14 DSGVO) erhoben werden. Beispiele:
 - Zum Zeitpunkt der Erhebung muss die betroffene Person über Namen und Kontaktdaten des Verantwortlichen und den Zweck der Verarbeitung informiert werden (Art. 13 Abs. 1 lit. a, c).
 - Darüber hinaus über die Dauer der Speicherung (Abs. 2 lit. a), das Recht auf Auskunft/Berichtigung/Löschung/Einschränkung (lit. b) oder ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist (lit. e).

Rechte der betroffenen Person

Details

- Nach Art. 15 DSGVO hat die betroffene Person ein **Recht auf Auskunft**, ob und welche Daten, insbesondere zu welchem Zweck (Abs. 1 lit. a) die Daten erhoben werden.
- Nach Art. 16 DSGVO hat die betroffene Person ein **Recht auf Berichtigung** unrichtig erhobener Daten.
- Nach Art. 17 DSGVO hat die betroffene Person unter bestimmten Voraussetzungen das Recht, die **Löschung** ihrer Daten (sog. „**Recht auf Vergessenwerden**“) zu verlangen.
 - Dabei besteht auch die Pflicht eines Datenverantwortlichen, der die Daten veröffentlicht hat, datenverarbeitende Dritte über das Löschbegehren des Betroffenen zu informieren (Abs. 2).
- Art. 18 DSGVO normiert das **Recht auf Einschränkung der Verarbeitung**, z.B. wenn die Richtigkeit der Daten in Frage steht
- Das **Recht auf Datenübertragbarkeit** (Art. 20) gibt betroffenen Personen unter bestimmten Voraussetzungen einen Anspruch, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen und maschinenlesbaren Dateiformat zu erhalten (z.B. um den Wechsel zu einem **anderen Anbieter** zu erleichtern).

Technischer und organisatorischer DS

Artikel 25

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

new

Artikel 35

Datenschutz-Folgenabschätzung

new

DSGVO

Artikel 37

Benennung eines Datenschutzbeauftragten

Pflicht, wenn:

- Öffentliche Stelle
- Datenverarbeitung als Kerntätigkeit

Hauptaufgabe:

Überwachung der Einhaltung datenschutzrechtlicher Vorschriften

Technischer und organisatorischer DS – Artikel 25 Abs. 1

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Privacy by Design: „Datenschutz durch Technikgestaltung“

Ergreifen technischer und organisatorischer **Maßnahmen** (TOMs) zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung (im **Entwicklungsstadium**), z.B.

- Pseudonymisierung
- Verschlüsselung
- Nutzerauthentifizierung



Unter Berücksichtigung:

*Stand der Technik +
Implementierungskosten*

*Art, Umfang und
Zwecke der Verarbeitung*

*Eintrittswahrscheinlichkeit und
Schwere des Risikos*

Technischer und organisatorischer DS – Artikel 25 Abs. 2

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Privacy by Default: „Datenschutz durch datenschutzfreundliche Voreinstellungen“

Verarbeitung grundsätzlich nur personenbezogener Daten, deren Verarbeitung für den **jeweiligen bestimmten Verarbeitungszweck erforderlich** ist (= Werkeinstellungen datenschutzfreundlich ausgestalten)

Ziel: Nutzer schützen, die weniger technikaffin sind („Privacy Paradox“)



Was tun bei Unsicherheit mit Artikel 25?

Ein genehmigtes **Zertifizierungsverfahren** gemäß Artikel 42 DSGVO kann als Faktor herangezogen werden!

Technischer und organisatorischer DS

Artikel 25

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen



Artikel 35

Datenschutz-Folgenabschätzung



Artikel 40 und Artikel 42
Zertifizierung und Verhaltensregeln



DSGVO

Artikel 37

Benennung eines
Datenschutzbeauftragten

Pflicht, wenn:

- Öffentliche Stelle
- Datenverarbeitung als Kerntätigkeit

Hauptaufgabe:

Überwachung der Einhaltung datenschutzrechtlicher Vorschriften

Technischer und organisatorischer DS – Artikel 35

Datenschutz-Folgenabschätzung

Artikel 35 Abs. 1 DSGVO

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, 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, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.



Technischer und organisatorischer DS – Artikel 35

Datenschutz-Folgenabschätzung

Instrument des „Risikomanagements“:

Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch systematische Beschreibung der geplanten Verarbeitungsvorgänge

Notwendig, wenn:

- Verarbeitung besonders sensibler Daten
- Voraussichtlich hohes Risiko für Rechte und Freiheiten natürlicher Personen durch Verarbeitung (insb. bei Verwendung neuer Technologien)



Folgenabschätzung durchführen – wann genau?



Art. 29 Gruppe WP 248

- Nach der Leitlinie gilt es als je wahrscheinlicher, desto mehr der aufgelisteten Kriterien vorliegen. Als Faustregel soll gelten, dass eine Folgenabschätzung bei Erfüllung von zwei oder mehr Kriterien durchgeführt werden muss.
- Die Kriterien sind: (1) Scoring, Profiling, Evaluation, z. B. Einschätzung der Kreditwürdigkeit, Behavioral Marketing etc., (2) automatisierte Einzelfallentscheidungen, (3) systematische Überwachung, (4) Verarbeitung sensibler Daten, (5) umfangreiche Datenverarbeitungen (bezogen auf die Anzahl betroffener Personen und Datenkategorien, die Dauer der Verarbeitung, die geographische Ausdehnung), (6) das Zusammenführen oder Abgleichen von Datenbeständen, wenn Betroffene nicht damit rechnen können, (7) die Verarbeitung von Daten besonders schutzbedürftiger Personen, (8) Neuartigkeit von Verarbeitungsvorgängen, Verwendung neuer Technologien (bspw. Fingerabdrucksensoren oder Gesichtserkennung), (9) Verarbeitungen, die es betroffenen Personen erschweren, ihre Rechte auszuüben oder eine Leistung in Anspruch zu nehmen, z.B. die Beurteilung der Kreditwürdigkeit durch eine Bank vor der Vergabe eines Darlehens

Grundprinzipien der DSGVO

Artikel 3 **new**
Räumlicher Anwendungsbereich

Artikel 12-21 **new**
Rechte der betroffenen Person

DSGVO

Artikel 83 **new**
**Allgemeine Bedingungen für die
Verhängung von Geldbußen**

Grundprinzipien der DSGVO – Artikel 83

Allgemeine Bedingungen für die Verhängung von Geldbußen

Geldbußen nach Art. 83 Abs. 4 DSGVO

- *Art. 33 DSGVO: Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde*
- *Art. 35 DSGVO: Datenschutz-Folgenabschätzung*

Geldbußen von bis zu **10 000 000 EUR** oder bis zu **2 %** des gesamten **weltweit erzielten Jahresumsatzes** (höherer Betrag)

Geldbußen nach Art. 83 Abs. 5 DSGVO

- *Art. 6 DSGVO: Rechtmäßigkeit der Verarbeitung*
- *Art. 12-21 DSGVO: Rechte der Betroffenen*

Geldbußen von bis zu **20 000 000 EUR** oder bis zu **4 %** des gesamten **weltweit erzielten Jahresumsatzes** (höherer Betrag)

Grundprinzipien der DSGVO – Artikel 83

Allgemeine Bedingungen für die Verhängung von Geldbußen

- Gegen **Behörden und sonstige öffentliche Stellen** des Bundes können auch in Zukunft keine Geldbußen verhängt werden (vgl. Art. 83 Abs. 7 i.V.m. bislang fehlender nationaler Regelung).
- Auf jeden Fall Befugnisse der Aufsicht nach Art. 58 DSGVO:
 - Verwarnung (lit. a und b),
 - Anweisungs- und Anordnungsbefugnisse (lit. c, d, e, g und h) und die Sanktionsbefugnisse (lit. f, h, i und j)
- Aufsichtsrechtliche Maßnahmen sind möglich
- Dagegen steht der Rechtsweg offen: Klagen gegen aufsichtsrechtliche Maßnahmen sind möglich und haben aufschiebende Wirkung, Verwaltungsgericht muss gegebenenfalls dem EuGH vorlegen (das dauert...)

Teil II: Konkrete(re)s

Dokumentieren, nachweisen, informieren

- Einhaltung der Datenschutzgrundsätze (Art. 5 Abs. 2 DSGVO),
- Einhaltung der erforderlichen technisch-organisatorischen Maßnahmen (Art. 24 DSGVO) sowie Vorgaben zur Datensicherheit (Art. 32 DSGVO)
 - [Zur Datensicherheit vgl. auch Checkliste via DAV](#)
 - ...u.a. Zugangskontrolle, Zugriffskontrolle, Erstellen eines Backup- & Recoverykonzepts, Erstellen eines Notfallplans
 - Zur Datensicherheit vgl. [auch das SDM des ULD](#)
 - (P) Die unverschlüsselte Mail eines Studierenden, der ärztliches Attest übermittelt, um Abwesenheit zu entschuldigen

Dokumentieren, nachweisen, informieren

- Einsatz geeigneter Auftragsverarbeiter, Art. 28 DSGVO
 - Druckaufträge an externe Dienstleister für Visitenkarten, Webhosting, Einsatz von Web-Analysediensten
 - Google Analytics auf der Studiengangsseite?
- Führung eines Verarbeitungsverzeichnisses, Art. 30 DSGVO
 - Abbildung sämtlicher relevanter Prozesse
 - Auch was man unterlässt und vernichtet, muss dokumentiert werden
 - DSK [Kurzpapier Nr. 1 - Verzeichnis von Verarbeitungstätigkeiten - Art. 30 DSGVO](#)
 - [Muster Verarbeitungsverzeichnis](#)

Dokumentieren, nachweisen, informieren

Meldung und Dokumentation von Datenschutzvorfällen, Art. 33 DSGVO (Data Breach Notification)

- Eine Meldung an die Aufsichtsbehörde hat immer zu erfolgen, es sei denn, dass die Datenpanne „voraussichtlich nicht zu einem Risiko“ für den Betroffenen führt.
 - (P) Das Ende des Dienstrechners?

Informations- und Auskunftspflichten gegenüber den Betroffenen (Art. 13 - 15 DSGVO).

- Die Betroffenen sind in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer einfachen und klaren Sprache“ von der Verarbeitung ihrer personenbezogenen Daten zu unterrichten, Art. 12 Abs. 1 DSGVO
 - Erklären Sie Vorgänge der Datenverarbeitung (Zweck, Speicherfristen, Rechtsgrundlage, bei Interessenabwägung auch die tragenden Gründe) umfassend, verständlich, vollständig und nachweislich (Webseite)

Löschpflichten

- (P) der dienstliche (oder gemischt dienstlich private?) E-Mail Account: wann hat sich der Zweck welcher E-Mail erledigt - Löschkonzept?
- (P) Verkettete Daten in Archiven und Backups
- Aufbewahrungsfristen zu Prüfungszwecken, zu statistischen Zwecken oder nach Steuerrecht

Recht auf Vergessenwerden und Datenübertragbarkeit

„Recht auf Vergessenwerden (Art. 17 DSGVO)

- Absatz 3: Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist
 - a zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
 - d 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

Recht auf Datenübertragbarkeit (Art. 20 DSGVO).

- Auch für Lernplattformen (Moodle)?
- In der Regel (-), da in der Regel Rechte Dritter (Gruppenarbeiten) entgegenstehen

Privacy by Design und by Default: Moodle

Art. 25 DSGVO regelt die Grundsätze des „Datenschutzes durch Technik und datenschutzrechtliche Voreinstellungen“.

- Umsetzung bei Moodle: nicht unmittelbar für den Unterrichtszweck notwendige Daten: default „off“

Auftragsdatenverarbeitung (Art. 28 DSGVO):

- Überprüfung der ADV-Verträge auf Anpassungsbedarfe

Erfordernis einer Datenschutz-Folgenabschätzung, soweit eine Verarbeitung voraussichtlich hohe Risiken für die persönlichen Rechte und Freiheiten der Betroffenen zur Folge hat (Art. 35 DSGVO). Insbesondere die Eintrittswahrscheinlichkeit und Schwere der möglichen Risiken sind zu bewerten und Maßnahmen zur Eindämmung der Risiken zu prüfen.

- Relevant bei Learning Analytics

Social Media und Folgenabschätzung

Social-Media-Kanäle und Folgenabschätzung (vgl dazu Orientierungshilfe LfDI BaWü)

- Auf individuellen Anwendungsfall zugeschnittene Erforderlichkeitsprüfung
 - Geht mit Verzicht eine signifikante Beeinträchtigung der Aufgabenerfüllung einher?
 - Gleich das (potentielle) Plus an Reichweite das Minus an Datensparsamkeit aus?
- Transparentes und öffentlich zugängliches Social-Media-Konzept
 - Nach außen zu dokumentierender (externer) Bereich der SMG, d.h. SMK
 - Zweck, Art, Umfang, Verantwortlichkeiten
- Crossmedia-Gebot
- Evaluationsgebot

Sonderproblem Social Media Monitoring

Im Gegensatz zum BDSG a.F. kein (weit reichendes) Privileg der DSGVO hinsichtlich öffentlich zugänglicher Daten - lediglich das Verbot der Verarbeitung sensibler Daten gilt nicht, wenn die Daten offenkundig vom Betroffenen öffentlich gemacht wurden (Art. 9 Abs. 2 lit. e) DSGVO).

- Art. 6 Abs. 1 lit. f DSGVO (?)
- Informationspflichten nach Art. 14 DSGVO
- Art. 22 DSGVO

Die Hochschulkommunikation bleibt arbeitsfähig!

Mythos: KUG wegen DSGVO künftig (ab 25.5.) unanwendbar, daher Anfertigen und Verbreiten von Personenaufnahmen via Social Media durch Hochschulkommunikationen künftig ohne Einwilligung nicht möglich.

BMI: Falsch!

„**Die Ansicht, das Kunsturhebergesetz werde durch die DSGVO ab dem 25. Mai 2018 verdrängt, ist falsch.** Das Kunsturhebergesetz stützt sich auf Artikel 85 Abs. 1 DSGVO, der den Mitgliedstaaten nationale Gestaltungsspielräume bei dem Ausgleich zwischen Datenschutz und der Meinungs- und Informationsfreiheit eröffnet. **Das Kunsturhebergesetz steht daher nicht im Widerspruch zur DSGVO,** sondern fügt sich als Teil der deutschen Anpassungsgesetzgebung in das System der DSGVO ein. Eine gesetzliche Regelung zur Fortgeltung des Kunsturhebergesetzes ist nicht erforderlich. Ebenso führen die Ansätze anderer Mitgliedstaaten, die sich in allgemeiner Form zum Verhältnis von Datenschutz und Meinungs- und Informationsfreiheit verhalten, in der praktischen Umsetzung nicht weiter und führen nicht zu mehr Rechtssicherheit.

Die grundrechtlich geschützte Meinungs- und Informationsfreiheit fließt zudem unmittelbar in die Auslegung und Anwendung der DSGVO ein, insbesondere stellen sie berechnigte Interessen der verantwortlichen Stellen nach Art. 6 Abs. 1 lit. f) DSGVO dar. **Die DSGVO betont, dass der Schutz personenbezogener Daten kein uneingeschränktes Recht ist, sondern im Hinblick auf seine gesellschaftliche Funktion und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden (Erwägungsgrund 4).** Zu den von der DSGVO in diesem Zusammenhang genannten Grundrechten zählt ausdrücklich auch die Freiheit der Meinungsäußerung und Informationsfreiheit.“

...also noch einmal:
don't panic.

Links

[Linkliste DSK Papers](#)

[LfDI Social Media und öffentliche Stellen – Folgenabschätzung & Co](#)

[GDD DSGVO Praxishilfen \(für Unternehmen\)](#)

[DSGVO Folgenabschätzung Tool](#)

[Zu Fortgeltung von Einwilligungen via Härting RAe](#)

[FAQ DSGVO via BMI](#)

[Via LfDI Niedersachsen: Datenschutz-Grundverordnung – was ändert sich für die Hochschulen?](#)

Vielen Dank!

Fragen?