Karlsruher Institut für Technologie

Zentrum für Angewandte Rechtswissenschaft

Grundlagen des DS-Rechts
Historie, Anwendung & Systematik

Dr. Christoph Werner

Vorlesung Datenschutzrecht
WS 2025/2026, UE 4/15

20.11.2025

wooclap.com Code: AEBRNN

Agenda

1. **Fortsetzung zu UE 3/15 – Grundrechte im öffentlichen Datenschutz**

a) Exkurs: Sicherheitslücken

b) Chatkontrolle

c) Palantir in BW

2. **Systematik des Datenschutzrechts**
3. **Historie der DSGVO**
4. **Anwendungsbereich der DSGVO**
5. **Systematik DSGVO**

1. Grundrechte im öffentlichen Datenschutz

Schutzpflichtdimension („Privater Datenschutz“)	Abwehrdimension („Öffentlicher Datenschutz“)
Betrifft das Verhältnis zwischen Bürger:innen	Betrifft das Verhältnis Bürger:in - Staat
Ausgleich zwischen konkurrierenden Grundrechtspositionen (z.B. unternehmerische Freiheit vs. Datenschutzgrundrecht)	Staat kann sich selbst nicht auf Grundrechte berufen; Grundrechte wirken nur zur Abwehr staatlicher Eingriffe (z.B. Schutz vor Überwachung)

- Volkszählungsurteil
- (Quellen-)TKÜ
- Vorratsdatenspeicherung
- Online-Durchsuchung

1. Grundrechte im öffentlichen Datenschutz

1. Grundrechte im öffentlichen Datenschutz
a) Exkurs: Sicherheitslücken

Sowohl für die *Online-Durchsuchung* als auch die *Quellen-TKÜ* sind offene Sicherheitslücken in informationstechnischen Systemen notwendig. Wie muss der Staat mit erkannten und gemeldeten Sicherheitslücken umgehen?

1. Grundrechte im öffentlichen Datenschutz
a) Exkurs: Sicherheitslücken

BVerfG Urteil [1] Rn. 44: Indessen verlangt die grundrechtliche Schutzpflicht [Computergrundrecht] eine Regelung darüber, wie die Behörde bei der Entscheidung über ein Offenhalten unerkannter Sicherheitslücken den

Zielkonflikt zwischen
- dem notwendigen Schutz vor Infiltration durch Dritte einerseits und [Erfüllung der Schutzpflicht]
- der Ermöglichung von Quellen-Telekommunikationsüberwachungen andererseits aufzulösen hat.

Der Behörde *muss eine Abwägung* der gegenläufigen Belange für den Fall aufgegeben werden, dass ihr eine **Zero-Day-Schutzlücke** bekannt wird.

Es ist sicherzustellen, dass die Behörde **bei jeder Entscheidung über ein Offenhalten einer unerkannten Sicherheitslücke** einerseits die Gefahr einer weiteren Verbreitung der Kenntnis von dieser Sicherheitslücke ermittelt und andererseits den Nutzen möglicher behördlicher Infiltrationen mittels dieser Lücke quantitativ und qualitativ bestimmt, **beides zueinander ins Verhältnis** setzt und **die Sicherheitslücke an den Hersteller meldet**, wenn nicht das Interesse an der Offenhaltung der Lücke überwiegt.

[1] BVerfG, Beschl. v. 08.06.2021 – 1 BvR 2771/18 „IT-Sicherheitslücken“

1. Grundrechte im öffentlichen Datenschutz
b) Chatkontrolle

Idee/Motivation:

- Aufdeckung der Verbreitung kinderpornographischen Materials
- Hierzu sollen flächendeckend, dauerhaft und anlasslos Inhalte (Bilder, Videos und URLs) auf (E-Mail, SMS, OTT-Messenger) und Hosting Providern (einschließlich Social Media) mithilfe von Datenbanken und KI gescannt und ggf. gemeldet werden

Verschiedene technische Ansätze:

- Backdoor in Verschlüsselung (Serverseitiges Scanning)
- Übermitteln und prüfen vor dem Verschlüsseln (Clientseitiges Scanning)

Umsetzung in EU-VO 2022/0155, Gesetzgebungsprozess läuft seit 2022

- Verpflichtendes Scanning vorerst am Widerstand Deutschlands und anderer Mitgliedstaaten gescheitert

1. Grundrechte im öffentlichen Datenschutz
b) Chatkontrolle

Aktueller Entwurfsstand (Nov. 2025)

- **Nur noch „freiwilliges“ clientseitiges Scanning von Anbietern gefordert:**

- Art. 4 Abs. 1 VO-E 2022/0155 : Haben Anbieter von Hosting-Diensten und Anbieter von Diensten der zwischenmenschlichen Kommunikation ein Risiko festgestellt, dass der Dienst für den Zweck des sexuellen Missbrauchs von Kindern im Internet […] werden könnte, **so ergreifen sie alle angemessenen, auf dieses Risiko zugeschnittenen Maßnahmen, um dieses Risiko wirksam zu minimieren.** Die Maßnahmen zur Risikominderung beschränken sich auf einen *identifizierbaren Teil oder eine identifizierbare Komponente des Dienstes* oder, *soweit möglich, auf bestimmte Nutzer oder bestimmte Gruppen oder Arten von Nutzern*, ohne die Wirksamkeit der Maßnahme zu beeinträchtigen.

  → Befürchtung: unbestimmte Pflichtennorm, die dann faktisch doch wieder clientseitiges Scanning erzwingt.

1. Grundrechte im öffentlichen Datenschutz
b) Chatkontrolle

Kritik:

- Durch anlasslose Prüfung: massive Beeinträchtigung des Datenschutzes für alle
- Hohes Risiko von false-positive-Meldungen bei noch unbekanntem Material und damit ggf. vertieften Persönlichkeitsrechtsverletzungen
- „Dass das hehre Ziel des Kinderschutzes herhalten soll, um ein solches Instrument zu etablieren, ist mindestens fragwürdig.“ (*Sylvia Ruge*, Hauptgeschäftsführerin des DAV, siehe becklink 2026110)

  → (berechtigtes) Dammbruch-Argument
- Starkes Ausweichverhalten und damit mangelnde Wirksamkeit zu befürchten

Vorübergehende Ausnahme erlaubt freiwillige Chatkontrolle bereits jetzt die **EU-VO 2021/1232**

- Gilt für nummernunabhängige interpersonelle Kommunikationsdienste (Art. 2 Nr. 7 EECC)

  → E-Mail + Messenger-Dienste
- läuft im April 2026 aus

1. Grundrechte im öffentlichen Datenschutz
c) Palantir in BW

- Einsatz der Software „Gotham“ von Palantir Technologies Inc. (USA) ab dem zweiten Quartal 2026, entsprechende Änderungen des Polizeigesetzes am 12.11.2025 im Landtag beschlossen [1]

- Datenanalysesoftware, die Daten aus unterschiedlichen Quellen und Datenbanken durchsuchen und analysieren kann (wohl sog. Data Mining, d.h. die automatisierte, auch KI-gestützte Generierung neuer Erkenntnisse aus den Querverbindungen der gespeicherten Datensätze)

- Datenschutzrechtlich insbesondere fraglich:
  a. Hinreichend bestimmte Rechtsgrundlage
  b. Reichweite des Eingriffs (welche Daten werden genutzt)

Quelle und Copyright:
https://en.wikipedia.org/wiki/File:Saruman_uses_the_Palantir.jpg

[1] https://www.swr.de/swraktuell/baden-wuerttemberg/landtag-beschliesst-nutzung-von-palantir-100.html

1. Grundrechte im öffentlichen Datenschutz
c) Palantir in BW

Karlsruher Institut für Technologie

a) hinreichend bestimmte Rechtsgrundlage

§ 47a Abs. 1 LPolG BW-E

Der Polizeivollzugsdienst kann nach Maßgabe der Absätze 2 bis 7 in polizeilichen Dateisystemen gespeicherte **personenbezogene Daten auf einer Analyseplattform automatisiert zusammenführen, verknüpfen, abgleichen, aufbereiten, auswerten und bewerten (automatisierte Datenanalyse),** wenn

1. dies zur Gefahrenabwehr erforderlich ist, [verkürzt]
2. bestimmte Tatsachen die Annahme rechtfertigen, dass
   a) innerhalb **eines überschaubaren Zeitraums** auf eine **zumindest ihrer Art nach konkretisierte Weise eine Straftat von erheblicher Bedeutung** begangen wird, die auch im Einzelfall schwer wiegt,
   b) die automatisierte Datenanalyse zur Verhütung dieser Straftat **erforderlich** ist und
   c) die Verwirklichung der Straftat zu einer Gefahr für das geschützte Rechtsgut führen würde,
3. bestimmte Tatsachen die Annahme rechtfertigen, dass besonders schwere Straftaten begangen werden sollen und die automatisierte Datenanalyse zur Verhütung dieser Straftaten erforderlich ist.

1. Grundrechte im öffentlichen Datenschutz
c) Palantir in BW

Karlsruher Institut für Technologie

b) Reichweite des Eingriffs

§ 47a Abs. 3 LPolG BW-E

Zum Zweck der automatisierten Datenanalyse **können eigene Vorgangsdaten, Falldaten, Daten aus polizeilichen Auskunftssystemen und Daten aus dem polizeilichen Informationsaustausch** zusammengeführt werden.

Verkehrsdaten, Daten aus Asservaten, Daten im Sinne des Satzes 1 aus gezielten Abfragen in landesfremden Datenbeständen, **Daten in gesondert geführten staatlichen Registern** sowie einzelne gesondert gespeicherte Daten aus Internetquellen **können ergänzend einbezogen werden**, soweit dies im Einzelfall erforderlich ist.

Daten in gesondert geführten staatlichen Registern

„beispielsweise Daten aus dem Melderegister, dem Zentralen Verkehrsinformationssystem (ZEVIS) oder dem Waffenregister, die durch gezielte Abfragen in die Analyse einbezogen werden können“ [1]

[1] Gesetzesbegründung, Lt. BW Drs. 17/9748

1. Grundrechte im öffentlichen Datenschutz
c) Palantir in BW

Karlsruher Institut für Technologie

b) Beispielsfall

„Terrorverdächtige aus dem Ausland sollen sich auf dem Weg nach Deutschland befinden. **Was könnte ihr Ziel sein, wer ihre Helfer vor Ort?** Die Ermittler [und andere Behörden] haben zwar alle möglichen Daten gespeichert, etwa [aus Melderegister, Grundbuch, ZEVIS], bei Verkehrskontrollen, Zeugenbefragungen oder auch aus sensiblen Bereichen wie einer heimlichen Telefonüberwachung. Doch um Daten eines Verdächtigen zusammenzuführen, etwa zu Autokennzeichen oder Adresse, müssen Polizisten in unterschiedlichen Systemen und Formaten forschen“ was entsprechend zeitintensiv ist. [1]

Weitere Probleme:

- In einem freiheitlichem Rechtsstaat gewünschter Zustand, dass keine individuellen, ganzheitlichen Akten zu jeder Person vorliegen
- Unklar inwieweit Unbeteiligte erfasst werden: hier „Helfer“
- Ggf. Fehler durch verbundenen KI-Einsatz

- Zusätzlich wird Abhängigkeit der Sicherheitsbehörden von einem Privatunternehmen kritisiert

[1] zitiert aus becklink 2035194

2. Systematik des DS-Rechts

Allgemein

EU-Recht	DSGVO	Gilt in allen Mitgliedstaaten unmittelbar enthält alle wesentlichen Regelungen zum Datenschutz
Bundesrecht	BDSG	Gilt für öffentliche Stellen des Bundes (Bundesverwaltung), richtet den BfDI ein und enthält besondere Vorschriften für nicht-öffentliche Stellen, z.B. zum Arbeitnehmerdatenschutz
Landesrecht	LDSG	Gilt für öffentliche Stellen des Landes (Landesverwaltung) und die Gemeinden und richtet die LfDIs ein

2. Systematik des DS-Rechts

	Allgemein	*Zusätzliche bereichsspezifische Regelungen*
EU-Recht	DSGVO	ePrivacy-RL Nur für elektronische Kommunikation
Bundesrecht	BDSG	TDDDG (Umsetzung ePrivacy-RL) BPolG
Landesrecht	LDSG	LPolG

3. Historie der DSGVO

Vorgängerregelung: Datenschutzrichtlinie 95/45/EG, DS-RL

- Galt von 13.12.1995 – 24.05.2018; ab 25.05.2018 durch DSGVO ersetzt.
- war als Richtlinie nicht unmittelbar verbindlich, Umsetzung in Deutschland **BDSG a.F.**

Gesetzgebungsverfahren: dauerte 3 Jahre, erheblicher Lobbyeinfluss
Dokumentarfilm: https://www.bpb.de/themen/daten/democracy/254255/der-dokumentarfilm-democracy/

Wichtige Neuerungen der DSGVO [1]

- Neues Recht auf Datenübertragbarkeit, Art. 20 DSGVO
- Pflicht zur Datenschutzfolgenabschätzung, Art. 35 DSGVO
- Anforderungen an Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
- Deutlich höherer Bußgeldkatalog (bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes)

[1] vgl. Hornung, ZD 2012, 99

4. Anwendungsbereich DSGVO

4. Anwendungsbereich DSGVO

Art. 2 DSGVO Sachlicher Anwendungsbereich

(1) Diese Verordnung gilt für die ganz oder teilweise **automatisierte Verarbeitung personenbezogener Daten (Alt. 1)** sowie **für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Alt.2).**

Personenbezogenes Datum,
Art. 4 Nr. 1, Erw.-Gr. 26
(siehe im Detail nächste UE 5/15)

Automatisierte Verarbeitung (Art. 4 Nr. 2)

Einsatz elektronischer Datenverarbeitungssysteme (EDV), Computer, Smartphones, digitale Speichermedien, Kopierer

Nicht-Automatisierte Verarbeitung mit Dateisystem (Art. 4 Nr. 2, Nr. 6)

Strukturierte „Papiersammlung“, z.B. Personalakten

Nicht erfasst: unstrukturierte Notizen

4. Anwendungsbereich DSGVO

Art. 2 DSGVO Sachlicher Anwendungsbereich

(1) Diese Verordnung gilt für die ganz oder teilweise **automatisierte Verarbeitung personenbezogener Daten (Alt. 1)** sowie **für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Alt.2).**

Personenbezogenes Datum,
Art. 4 Nr. 1, Erw.-Gr. 26
(siehe im Detail nächste UE 5/15)

Verarbeitung (Art. 4 Nr. 2 DSGVO)

jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten **Vorgang (en: operation)** 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;

4. Anwendungsbereich DSGVO

Art. 2 DSGVO Sachlicher Anwendungsbereich

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,
b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen [gemeinsame Außen- und Sicherheitspolitik, Art. 21 ff. EUV],
c) durch natürliche Personen zur Ausübung **ausschließlich persönlicher oder familiärer Tätigkeiten [Haushaltsausnahme]**,
d) **durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung**, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit [*u.a. Fälle zur Quellen-TKÜ, Vorratsdatenspeicherung, Online-Durchsuchung von DSGVO ausgeschlossen]*

Außerdem keine Anwendung für den Bereich der elektronischen Kommunikation (EPrivacy-RL, Art. 95 DSGVO, da spezieller geregelt)

Beispielsfall Haushaltsausnahme:

Getrennt lebende Familie, V, M, K: Die M installiert eine „Überwachungsapp“ auf dem Smartphone ihrer Tochter, welche Standortabfragen ermögliche. V ist davon nicht begeistert, schließlich könne M nun auch seinen Standort tracken, wenn er mit seiner Tochter (K) unterwegs sei. Kann er sich auf das Datenschutzrecht berufen und somit ggf. die Verarbeitung unterbinden oder greift (trotz Trennung) die Haushaltsausnahme?

Beispielsfall Haushaltsausnahme:

Getrennt lebende Familie, V, M, K: Die M installiert eine „Überwachungsapp“ auf dem Smartphone ihrer Tochter, welche Standortabfragen ermögliche. V ist davon nicht begeistert, schließlich könne M nun auch seinen Standort tracken, wenn er mit seiner Tochter (K) unterwegs sei. Kann er sich auf das Datenschutzrecht berufen und somit ggf. die Verarbeitung unterbinden oder greift (trotz Trennung) die Haushaltsausnahme?

Lösung: Erkenntnis des Bundesverwaltungsgericht Österreich (ZD 2025, 646)

- Haushaltsausnahme (+)
- Trennung führt nicht zur Unanwendbarkeit der Haushaltsausnahme, entscheidend ob ein persönliches bzw. familiäres Verhältnis gegeben ist (hier jedenfalls zwischen M und K)
- Nach der Rspr. des EuGH selbst Verarbeitungen unter die Haushaltsausnahme, die „nebenbei das Privatleben anderer Personen betreffen oder betreffen können“ (vgl. EuGH 11.12.2014 – C-212/13, ZD 2015, 77“
- M nutzte Standort-Daten im privaten Verhältnis um T bei der Orientierung in der Stadt zu helfen, sie ggf. bei Verirrung wiederzufinden und ihre Sicherheit (bzw. Ms eigenes Sicherheitsgefühl) zu erhöhen.

4. Anwendungsbereich DSGVO

Art. 3 DSGVO Räumlicher Anwendungsbereich

(1) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer **Niederlassung** eines Verantwortlichen oder eines Auftragsverarbeiters **in der Union** erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.

(2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden**, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter**, wenn die Datenverarbeitung im Zusammenhang damit steht

a) betroffenen Personen **in der Union Waren oder Dienstleistungen anzubieten**, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;

b) das Verhalten **betroffener Personen zu beobachten, soweit ihr Verhalten in der Union** erfolgt.

(3) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt.

4. Anwendungsbereich DSGVO

(P) Datenübermittlung ins Ausland

1. Unternehmen hat Niederlassung in Europa (Art. 3 Abs. 1) und übermittelt aber trotzdem Daten an den Mutterkonzern im Ausland (z.B. Meta, Amazon, Google, etc.) oder
2. Unternehmen hat keine Niederlassung in der EU, sondern ist nur nach dem Marktortprinzip bzw. des Orts der Verhaltensbeobachtung erfasst, Art. 3 Abs. 2 DSGVO → dann findet zwangsläufig eine Datenübermittlung ins EU-Ausland statt

In beiden Fällen (bei 2. str.) müssen nach Art. 45 f. DSGVO bestimmte Voraussetzungen erfüllt werden, d.h. insbesondere:

a) Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO) oder
b) Geeignete Garantien (Art. 46 DSGVO)

4. Anwendungsbereich DSGVO

(P) Datenübermittlung ins Ausland

a) Angemessenheitsbeschluss (Art. 45 DSGVO)

- Wird von der EU-Kommission erlassen
- Voraussetzung: angemessenes, der Sache nach gleichwertiges Datenschutzniveau (siehe auch Art. 45 Abs. 2 DSGVO)
- Rechtsfolge: Datenübermittlung in das entsprechende Land zulässig

Ein solcher Angemessenheitsbeschluss besteht derzeit u.a. für*:

- Kanada
- Israel
- Japan
- Neuseeland
- Schweiz
- Vereinigtes Königreich (bis 27.12.2025, befristet aufgrund neuer Datenschutzgesetze in UK)
- **USA**

*https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/angemessenheitsbeschluesse-der-europaeischen-kommission, zuletzt abgerufen am 31.07.2025

4. Anwendungsbereich DSGVO

Geschichte der Angemessenheitsbeschlüsse zu den USA:

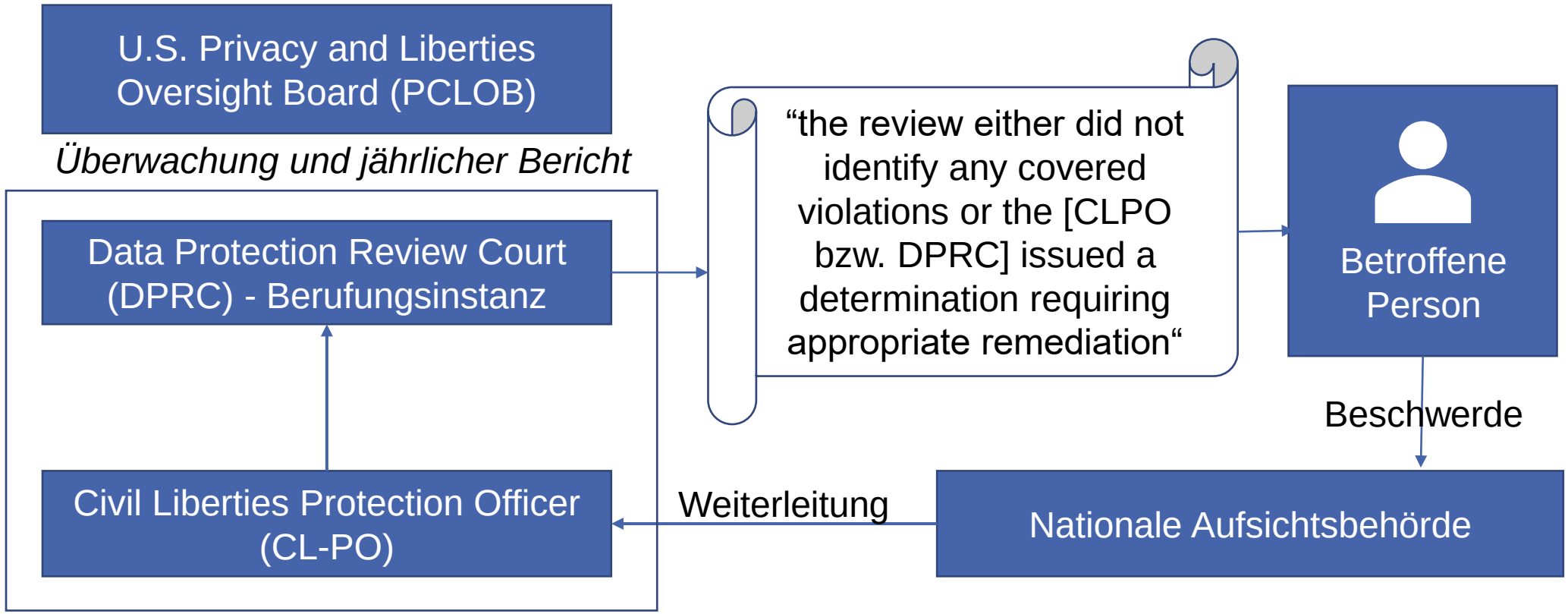
- **Safe Harbor (2000)**
- **EuGH-Urteil: Schrems I (2015)**
- **EU-US-Privacy Shield (2016)**
- **EuGH-Urteil: Schrems II (2020)**
- **EU-US Data Privacy Framework (DPF) (2022)**

Max Schrems (NOYB)
Quelle: https://noyb.eu/de/unser-team-mitglieder-und-partner

**[EuGH, Urteil vom 6.10.2015 – C-362/14;
EuGH, Urteil vom 16.7.2020 – C-311/18]**

4. Anwendungsbereich DSGVO

DPF: Rechtsschutzmechanismus (Executive Order 14086, Sec. 3)



Vgl. Glocker, ZD 2023, 189 (191 f.)

4. Anwendungsbereich DSGVO

Ausblick & Entwicklung seit Donald Trump

- Ob EuGH das EU-US Data Privacy Framework als hinreichend erachtet, ist zweifelhaft. [1]

  Philippe Latombe, frz. Parlamentsabgeordneter ist am 03.09.2025 vor dem EuG gescheitert [1a]

- Donald Trump hat Anfang 2025 alle fünf Mitglieder des PCLOB entlassen bzw.

  zum Rücktritt aufgefordert; entspr. Gerichtsverfahren sind anhängig [2];

  → der PCLOB ist damit bereits jetzt nicht mehr arbeitsfähig (mind. 3 Mitglieder erforderlich) [3]

  → bei dauerhaftem Erfolg: Transparenz/Unabhängigkeit massiv in Frage gestellt

[1] Glocker, ZD 2023, 189 (192 ff.); [1a] DSB 2025, 284 [2] Nebel, CR 2025, 437.[3] Lindner, ZD 2025, 310 (311).

4. Anwendungsbereich DSGVO

(P) Datenübermittlung ins Ausland

b) Geeignete Garantien (Art. 46 Abs. 1 DSGVO)

Falls kein Angemessenheitsbeschluss vorliegt ist eine Übermittlung möglich, wenn geeignete Garantien nach Abs. 2 vorliegen:

- Behördliche Absprache, lit a)
- Binding Corporate Rules (BCRs), lit b)
- Standardvertragsklauseln (SCCs), lit c), d)
- genehmigte Verhaltensregeln o. Zertifizierungen, lit e), f)

4. Anwendungsbereich DSGVO

(P) Datenübermittlung ins Ausland

b) Geeignete Garantien (Art. 46 Abs. 1 DSGVO)

Ggf. sind auch technische Lösungen vorzusehen, um datenschutzrechtliche Defizite im Empfängerland soweit möglich zu kompensieren, beispielsweise [1]:

- Verschlüsselung
- Pseudonymisierung
- Multi-Party Processing

Ist dies nicht möglich/unzureichend: Übermittlung unzulässig [2]

[1] Schantz in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 46 Rn. 18 [2] Schantz, a.a.O., Rn. 16; EuGH – C-311/18, ZD 2020, 511 Rn. 92, 105.

5. Systematik der DSGVO

Artikel und Erwägungsgründe

Artikel: Rechtsnormen
Erwägungsgründe: Erläuterungen des Gesetzgebers (historische Auslegung)

https://dsgvo-gesetz.de/art-7-dsgvo/
(Unternehmenswebseite)

Art. 7 DSGVO

Bedingungen für die Einwilligung

(1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

Passende Erwägungsgründe

(**32**) Einwilligung, (**33**) Einwilligung zur wissenschaftlichen Forschung, (**42**) Beweislast und Erfordernisse einer Einwilligung, (**43**) Zwanglose Einwilligung

5. Systematik der DSGVO

Kap. I: Allgemeine Bestimmungen

Art. 1: *Gegenstand und Ziele*

Art. 2: *Sachlicher Anwendungsbereich*

Art. 3: *Räumlicher Anwendungsbereich*

Art. 4: Begriffsbestimmungen

Kap. II: Grundsätze

Art. 5: Grundsätze für die Verarbeitung personenbezogener Daten

Art. 6: Rechtmäßigkeit der Verarbeitung

Art. 7: Bedingungen für die Einwilligung

Art. 9: Verarbeitung besonderer Kategorien personenbezogener Daten

5. Systematik der DSGVO

Kap. III: Rechte der betroffenen Personen

Art. 12-14:	Informationspflichten
Art. 15:	Auskunftsrecht
Art. 16:	Recht auf Berichtigung
Art. 17:	Recht auf Löschung
Art. 20:	Recht auf Datenübertragbarkeit
Art. 21:	Widerspruchsrecht
Art. 22:	Automatisierte Entscheidungen

5. Systematik der DSGVO

Kap. IV: Verantwortlicher und Auftragsverarbeiter

Art. 24: Verantwortung des für die Verarbeitung Verantwortlichen

Art. 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Art. 26: Gemeinsam Verantwortliche

Art. 28: Auftragsverarbeiter

Art. 30: Verzeichnis von Verarbeitungstätigkeiten

5. Systematik der DSGVO

Kap. IV: Verantwortlicher und Auftragsverarbeiter (Fort.)

Art. 32: Sicherheit der Verarbeitung

Art. 33: Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Art. 34: Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

Art. 35: Datenschutzfolgenabschätzung

Art. 37ff.: Datenschutzbeauftragte(r)

5. Systematik der DSGVO

Kap. V	Übermittlungen pb. Daten an Drittländer oder an internationale Organisationen (Art. 44-50)
Kap. VI	Unabhängige Aufsichtsbehörden (Art. 51-59)
Kap. VIII	Rechtsbehelfe, Haftung und Sanktionen (Art. 77-84)

Anhang: Wesentliche Lerninhalte

- Unterschiedliche staatliche Datenerhebungsmaßnahmen (öffentlicher Datenschutz) betreffen unterschiedliche Grundrechte (RiSb, Fernmeldegeheimnis, Computergrundrecht)
- Eröffnung sachlicher Anwendungsbereich der DSGVO: Verarbeitung personenbezogener Daten
  Wichtigste Ausnahmen: „Haushaltsausnahme“, Gefahrenabwehr & Polizei, elektronische Kommunikation
- Räumlicher Anwendungsbereich (Niederlassung, Marktortprinzip oder Verhaltensbeobachtung in EU)
- Datenübermittlung ins Ausland entweder auf Basis eines Angemessenheitsbeschlusses oder geeignete Garantien (Art. 45, 46 DSGVO)
- Mit den USA besondere Herausforderungen im Rahmen des Angemessenheitsbeschlusses