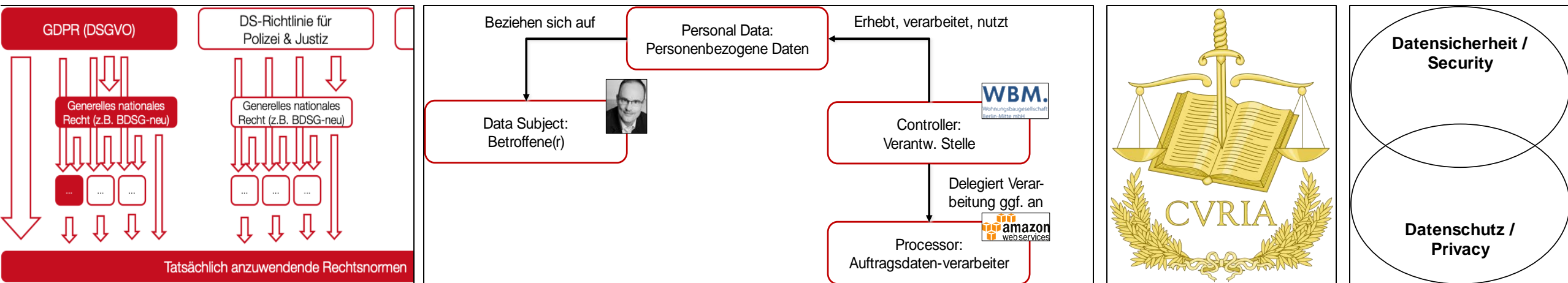


# Information Governance

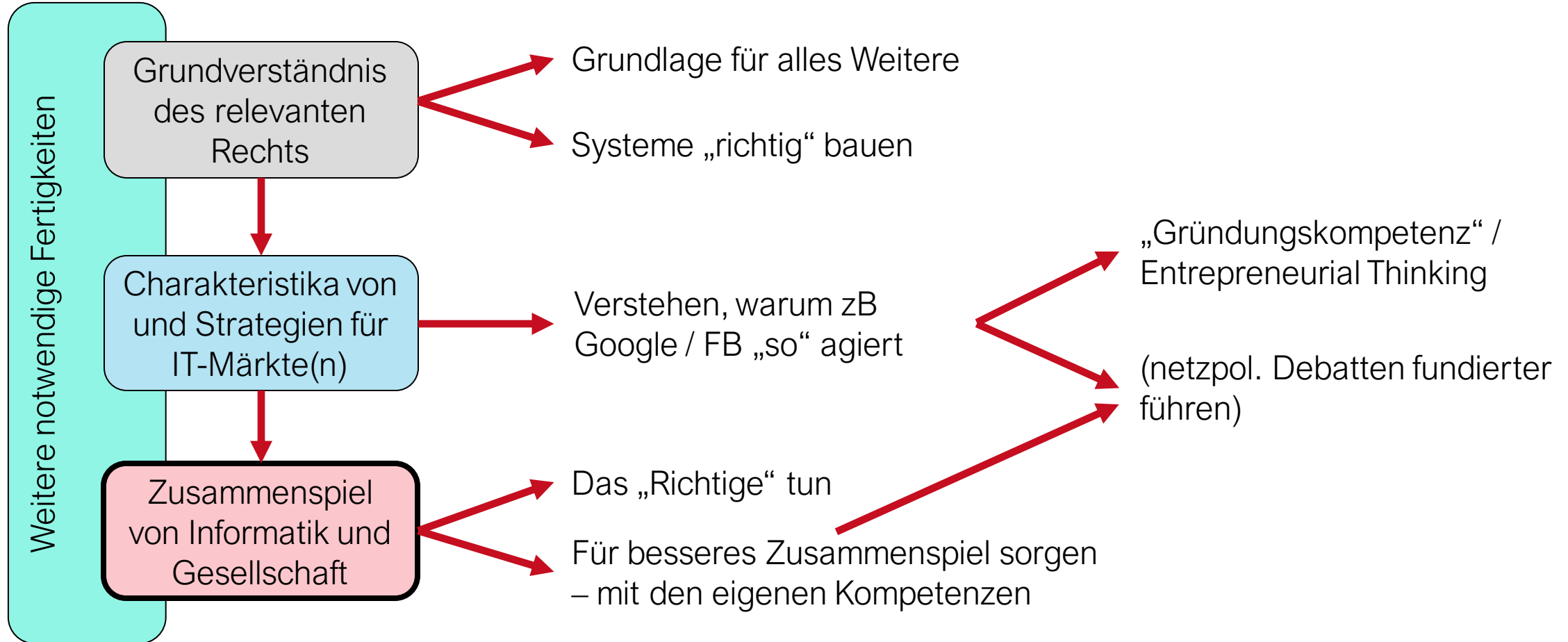
## Lesson 08: Datenschutz 1 – Rechtliche Grundlagen



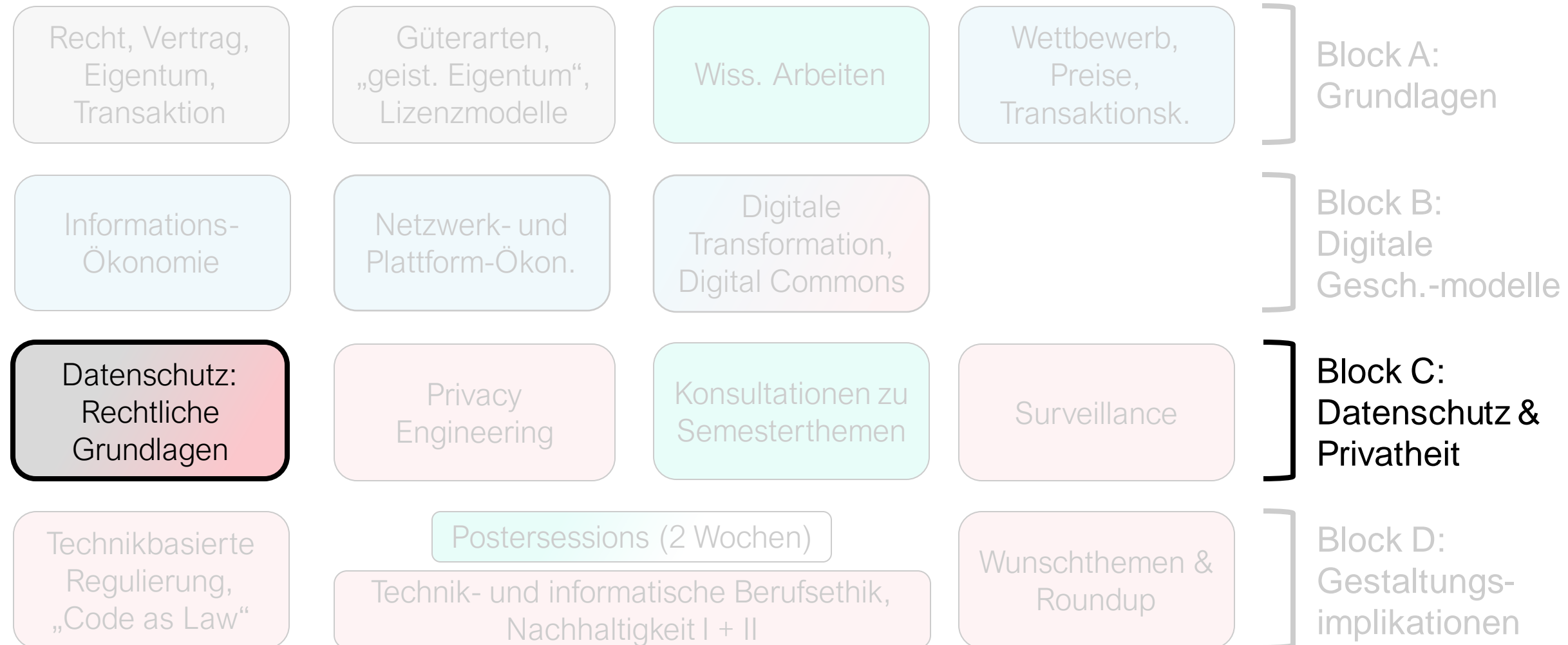
Frank Pallas

Information Systems Engineering  
TU Berlin

# Information Governance – „Riding Skills“



# Information Governance – Thematischer Überblick



# Lesson 08: Datenschutz 1 – Rechtliche Grundlagen



Hintergrund, Architektur & Ziele des Datenschutzrechts

Rechtliche Rollen und „Personenbezogene Daten“

Internationale Transfers

Neun Prinzipien des Datenschutzrechts

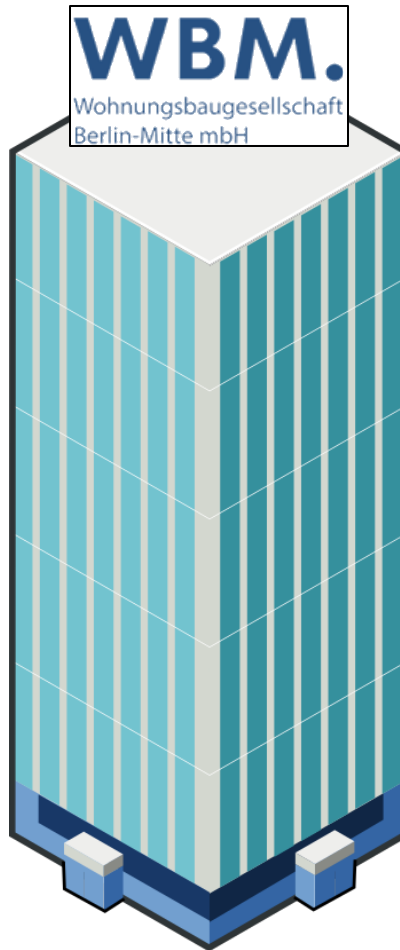
# Stellen Sie sich vor...



Sie haben nach Studienabschluss ein lukratives Angebot als „Chief System Architect Connected Buildings“ von einer großen Berliner Wohnungsbaugesellschaft angenommen.

Sie bekommen den Auftrag, die Backend-Architektur zur intelligenten Vernetzung des Gebäudebestands zu entwerfen.

# Stellen Sie sich vor...



„Entwerfen Sie ein tragfähiges Backend zur intelligenten Vernetzung des Gebäudebestands“

???

## Stellen Sie sich vor...



Sie haben nach Studienabschluss ein lukratives Angebot als „Chief System Architect Connected Buildings“ von einer großen Berliner Wohnungsbaugesellschaft angenommen.

Sie bekommen den Auftrag, die Backend-Architektur zur intelligenten Vernetzung des Gebäudebestands zu entwerfen.

## Was tun Sie?

## Option 1:

**I'm Feeling Lucky**

(„Ist halt mein Job“)



## Option 2:

# I-A-N-A-L

(„I am not a lawyer“)

<https://en.wikipedia.org/wiki/IANAL>

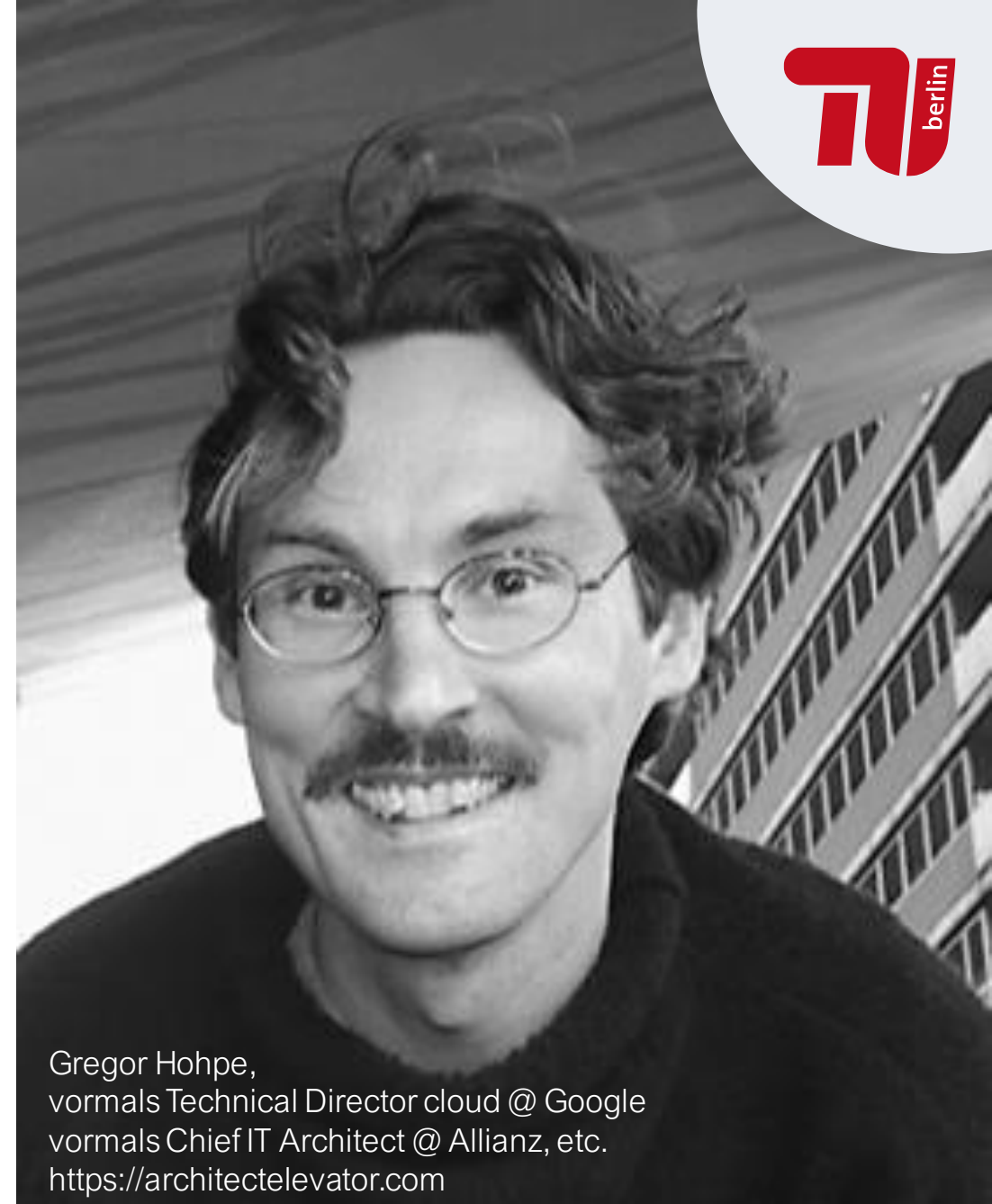
(„Nicht mein Job, darüber nachzudenken“)

## Recap: „Riding the Elevator“

“Architects [...] are able to convey technical topics to upper management without losing the essence of the message. Conversely, they **understand the company strategy and can translate it into technical decisions** that support it.

This is what I call the architect elevator: architects ride the elevator up and down to move between the board room and the engine room of a large enterprise. Such a direct linkage has become more important than ever [...]

The value of the architects in this scenario should not be measured by how "high" they travel, but by how many floors they span. [...]"



Gregor Hohpe,  
vormals Technical Director cloud @ Google  
vormals Chief IT Architect @ Allianz, etc.  
<https://architectelevator.com>

Rekordbußgeld wegen Datenschutzverstößen

UPDATE 05.11.2019, 16:47 Uhr

## Deutsche Wohnen muss 14,5 Millionen Euro Strafe bezahlen

Das Unternehmen soll sensible Mieterdaten rechtswidrig gespeichert haben. Berliner Politiker bezeichnen die Höhe des Bußgelds als „Paukenschlag“. VON JULIUS BETSCHKA, ROBERT KIESEL UND SEBASTIAN CHRIST



Die Deutsche Wohnen hat in Berlin mehr als 100 000 Wohnungen. FOTO: PAUL ZINKEN/DPA

<https://www.tagesspiegel.de/25191038.html>

## Datenschutzbußgelder gegen Unternehmen

Im Verfahren um ein Bußgeld nach der DS-GVO gegen die Deutsche Wohnen SE hat der Generalanwalt am Europäischen Gerichtshof Campos Sánchez-Bordona seine Schlussanträge vorgelegt. Danach können die Datenschutzbehörden Bußgelder direkt gegen Unternehmen verhängen. Dies setzt aber den Nachweis eines vorsätzlichen oder fahrlässigen Handelns eines Mitarbeiters voraus.

<https://rsw.beck.de/aktuell/daily/meldung/detail/eugh-generalanwalt-datenschutzbusse-gegen-unternehmen>

### Datensammelwut

## 14-Millionen-Bußgeld gegen Deutsche Wohnen landet vor EU-Gericht

Deutsche Wohnen sammelt massenhaft Kopien von Personalausweisen, Kontoauszügen und anderen sensiblen Dokumenten von Mieter\*innen. Eigentlich müsste der Immo-Konzern nicht mehr erforderliche Daten löschen – doch das tat er jahrelang nicht. Der Fall landet nun vor dem Europäischen Gerichtshof.

03.01.2022 um 14:11 Uhr - Alexander Fanta - in Datenschutz - 4 Ergänzungen

<https://netzpolitik.org/2022/datensammelwut-14-millionen-bussgeld-gegen-deutsche-wohnen-landet-vor-eu-gericht/>

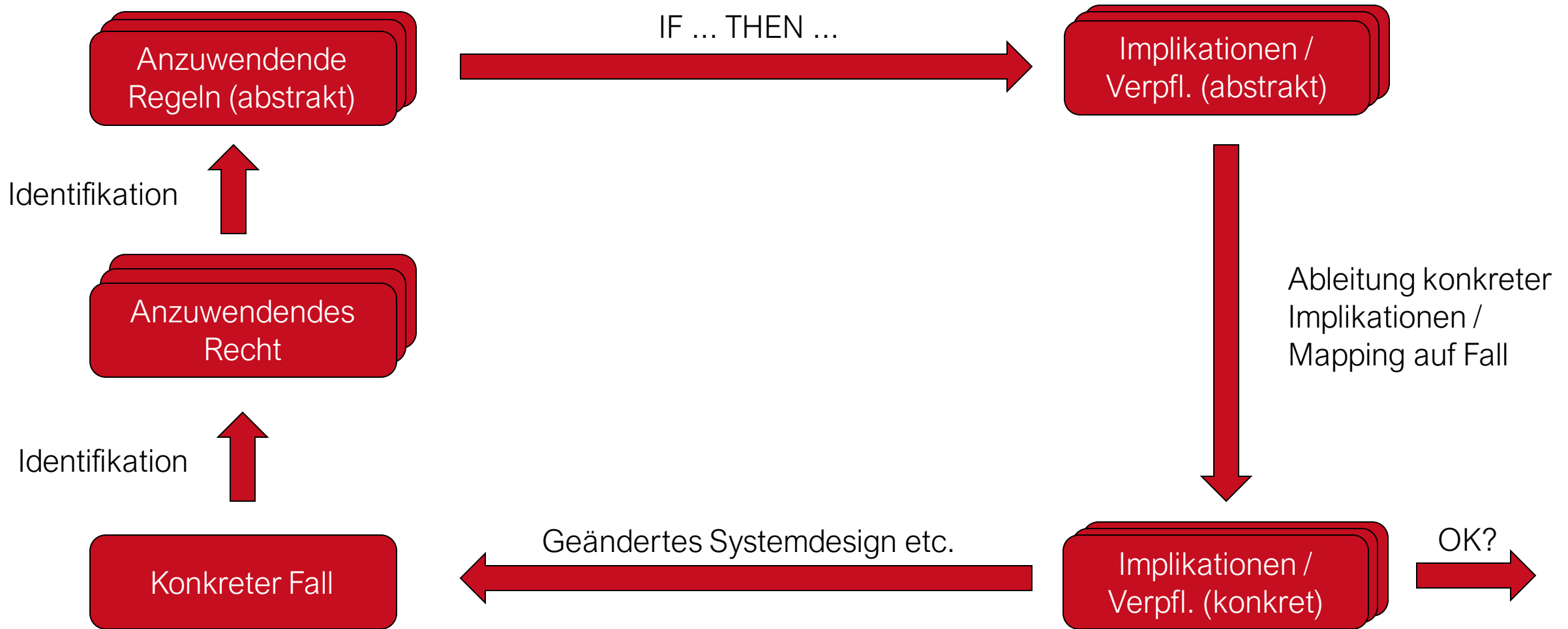
(zu beachten: Hier (noch) kein Fall von Gebäudeautomation und auch nach >4 Jahren noch nicht rechtskräftig)

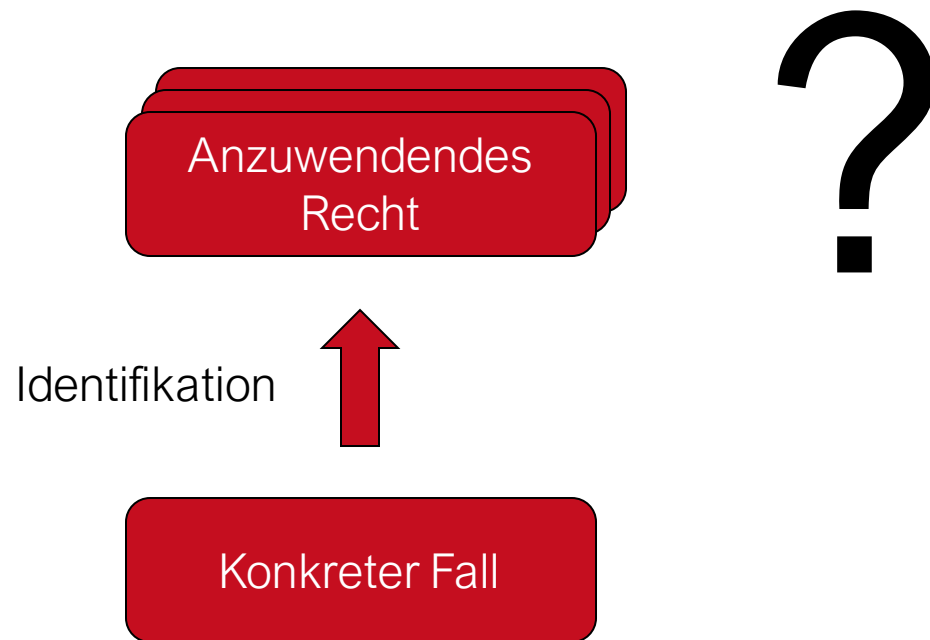
## Option 3:

„Worum geht's da eigentlich?“

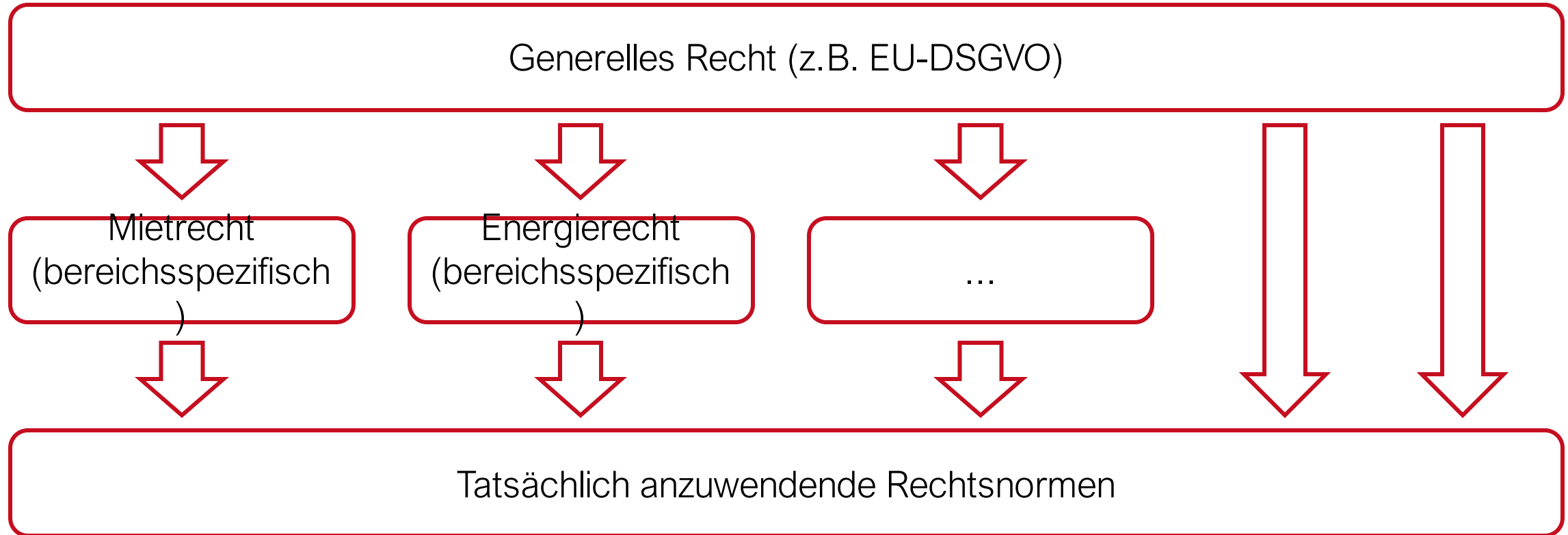
„Was heißt das für uns / mich?“

→ **Datenschutz**





# „Bereichsspezifische Normen“



→ Für Informatiker\*innen: „Partial Override in abgeleiteten Klassen“

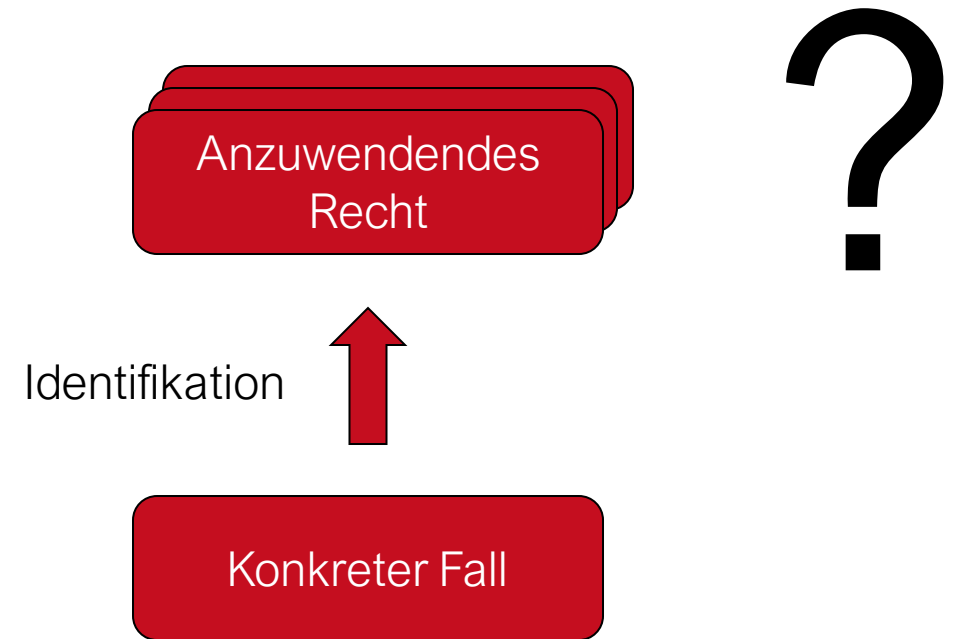
# Datenschutzrecht

Seit Mai 2018 meist anzuwenden:

- EU Datenschutzgrundverordnung (DSGVO)
- International bekannt als „General Data Protection Regulation“ (GDPR)

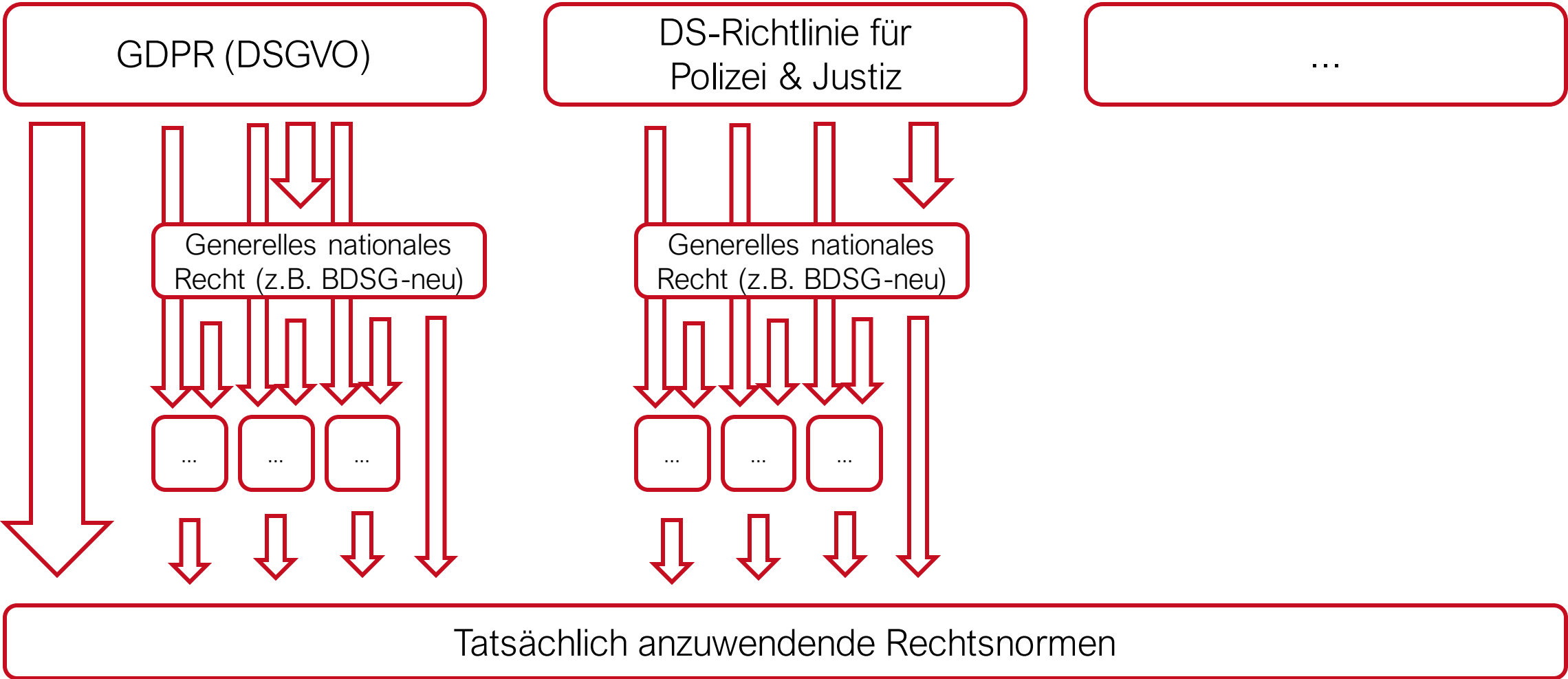
Wichtig:

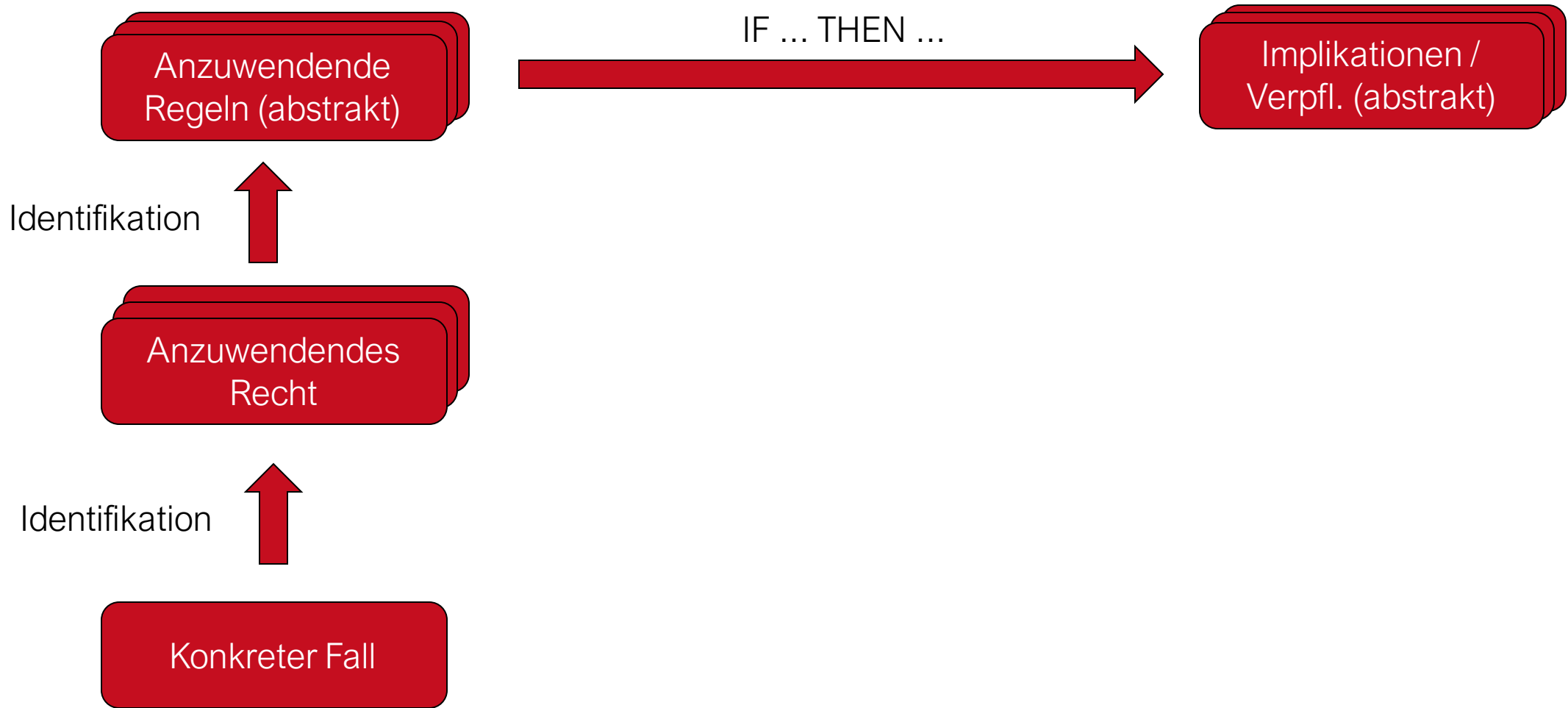
- Nicht anzuwenden u.A. im Bereich Sicherheit & Justiz
- Bereichsspezifische Normen auch hier
- Außerdem: Nationale Anpassungen ähnlich „bereichsspezifisch“ (in Teilen)



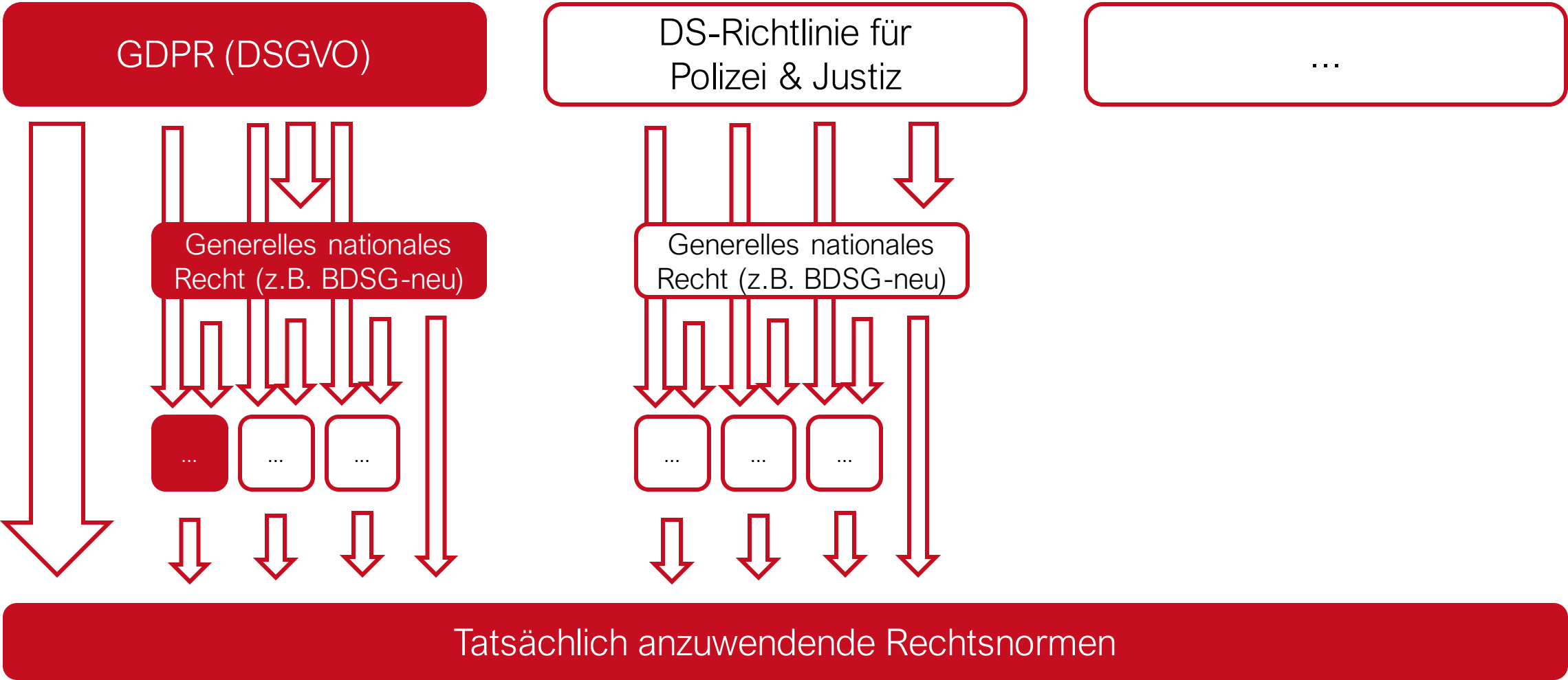


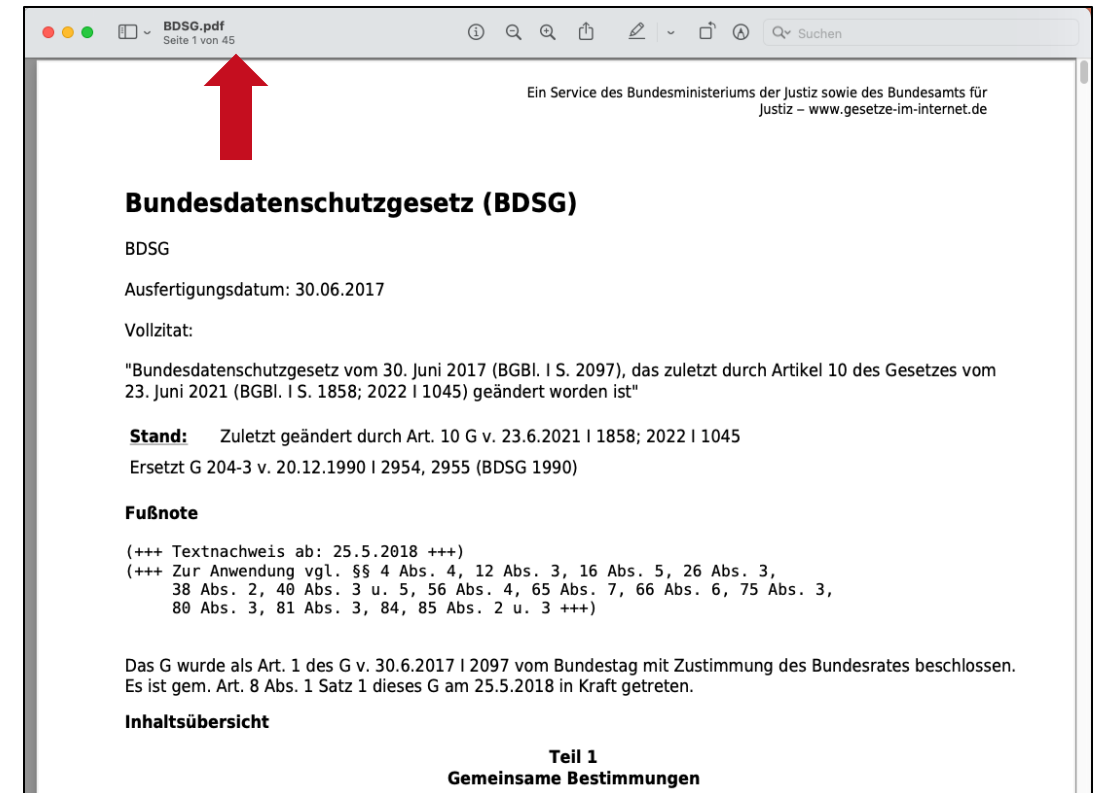
# DSGVO und weitere anzuwendende Rechtsnormen

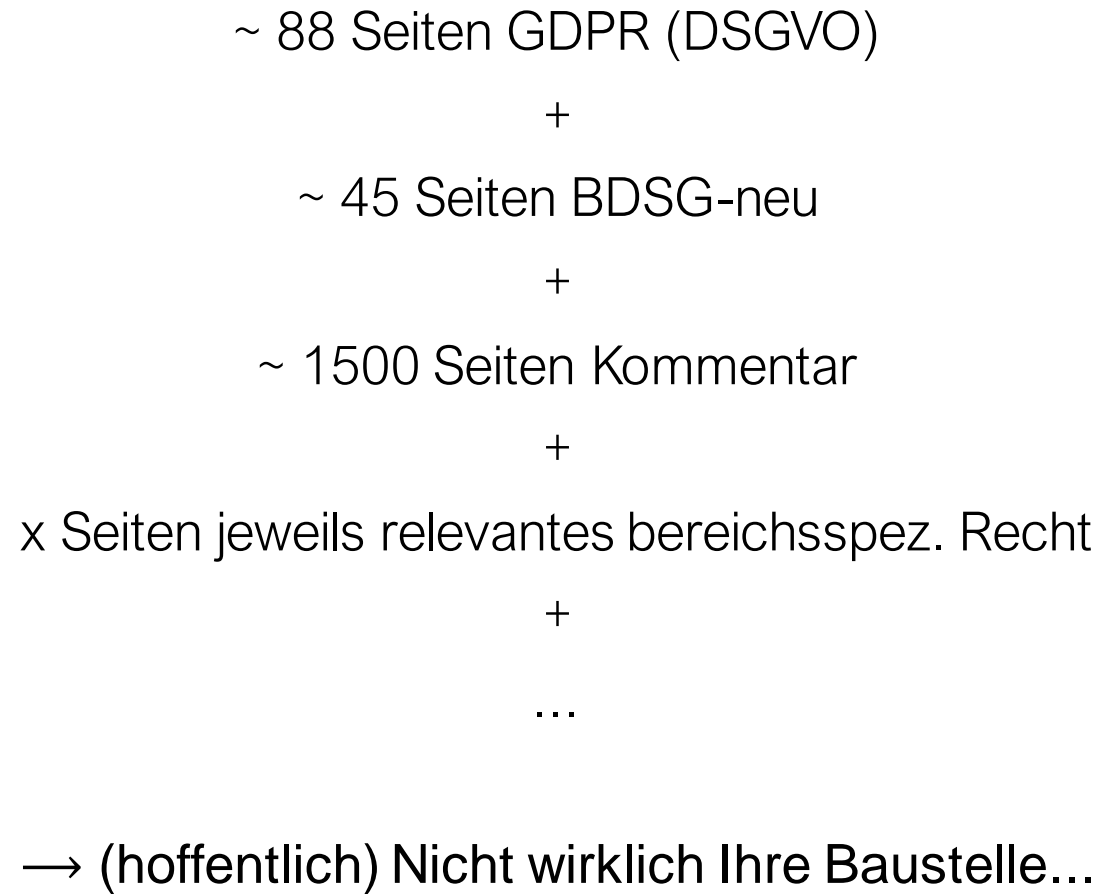




# DSGVO und weitere anzuwendende Rechtsnormen





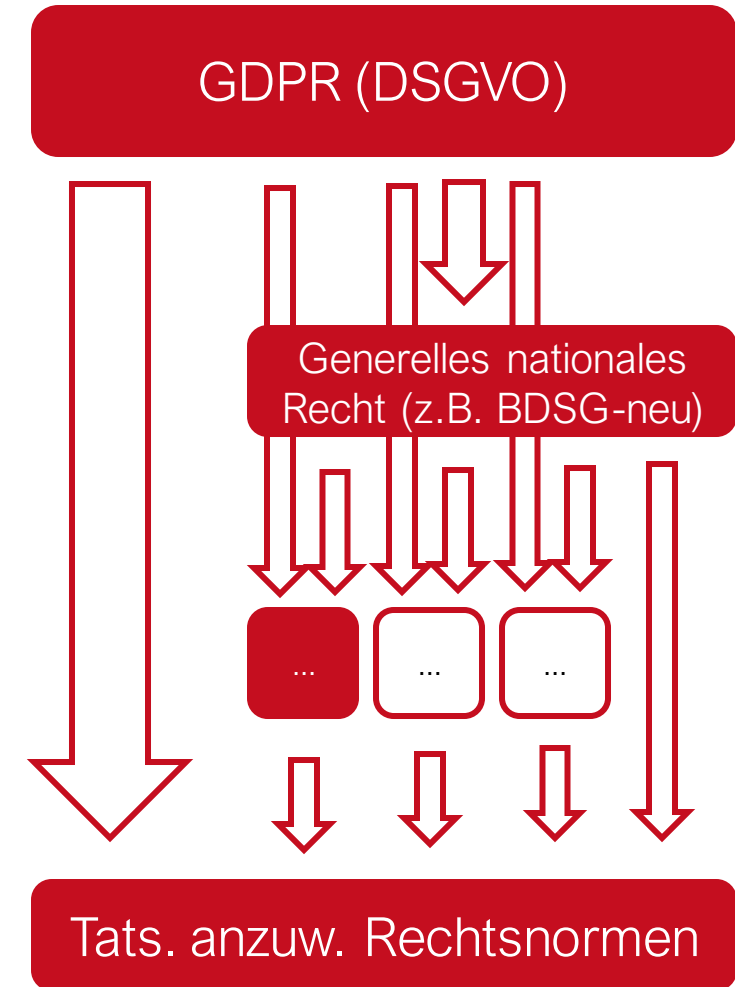


# Datenschutzrecht

- Tatsächlich anzuwendendes Recht im Datenschutz ergibt sich aus einer Vielzahl unterschiedlicher Gesetze etc.
- In den meisten Fällen GDPR als Startpunkt
- Nationale Umsetzungen, bereichsspezifische Regelungen (Mietrecht, Energierecht, Gesundheitsrecht, Hochschulrecht, ...)

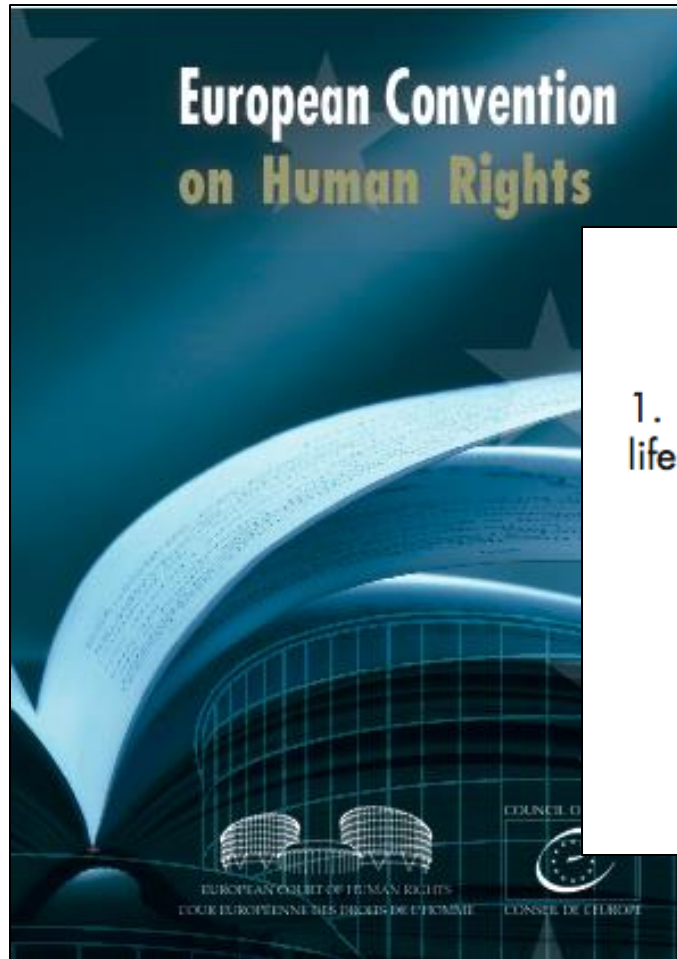
→ „Übersichtlichkeit ist anders“

→ Sinnvoller Detailgrad für Informatiker\*innen?



# Grundlegende Konzepte / Prinzipien

# GDPR: Rechtlicher Anker / Ziele

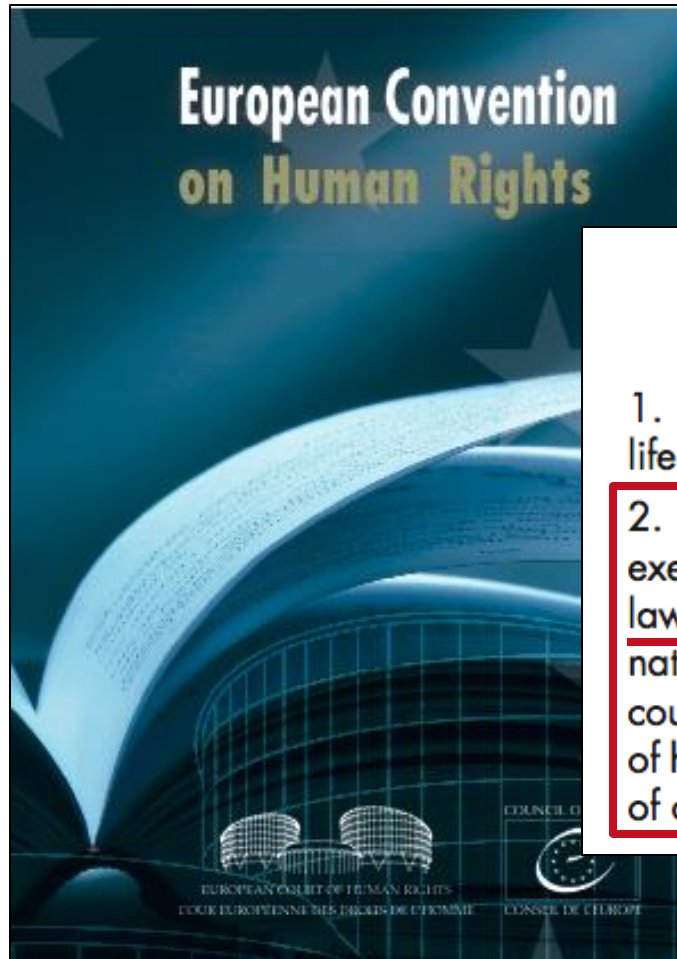


## ARTICLE 8

### **Right to respect for private and family life**

1. Everyone has the right to respect for his private and family life, his home and his correspondence.



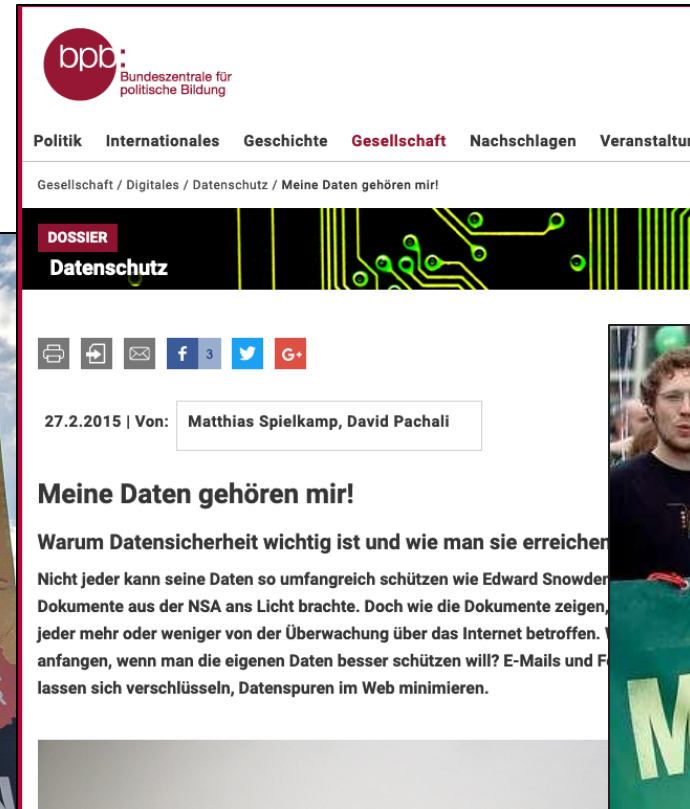
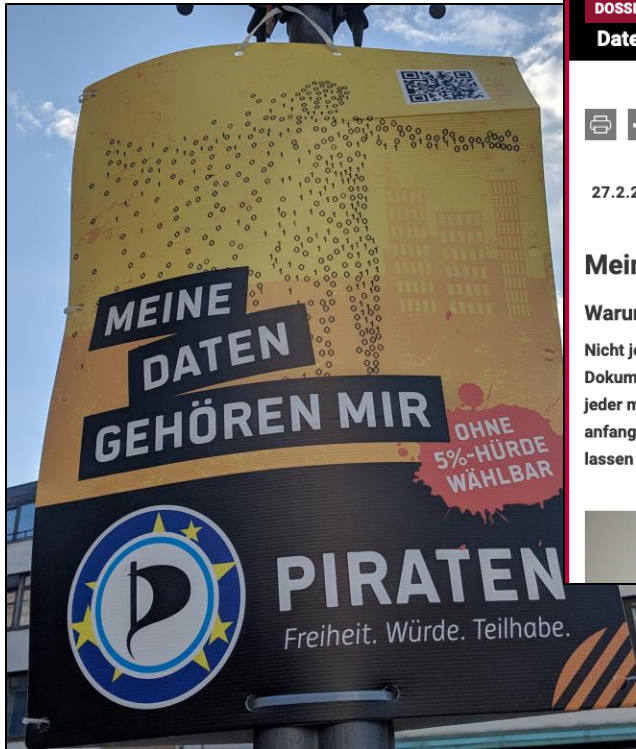


## ARTICLE 8

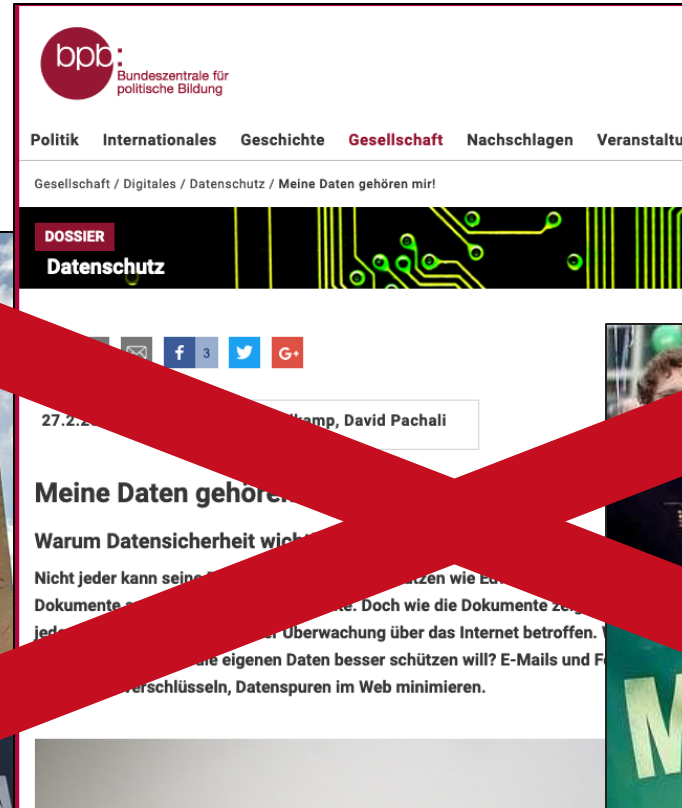
### Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

# „Dateneigentum“



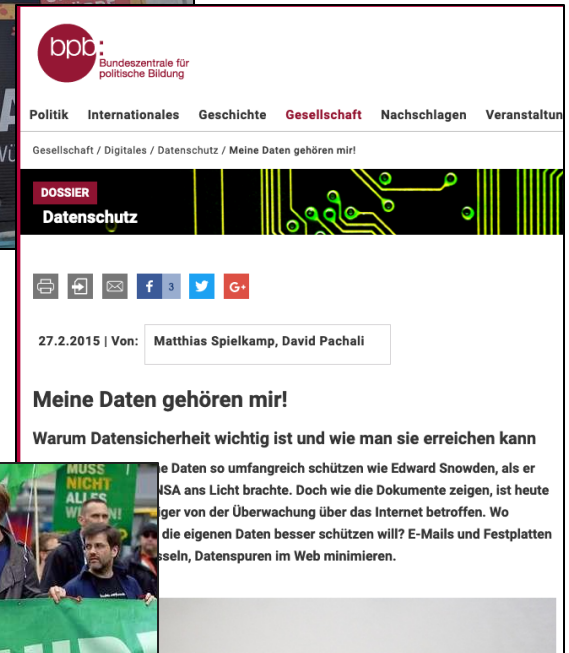
# „Dateneigentum“





# Datenschutzrecht

- Im Datenschutz geht es nicht um „Eigentum“ („Nutzungs- und Verfügungsrechte“, „Daten verkaufen“, ...) sondern um Grund- / Menschenrechte
- In D auch: **Menschenwürde**, allg. Persönlichkeitsrecht (etwa BVerfG vom 6.11.2019: 1 BvR 16/13 - Recht auf Vergessen I)
- Möglichkeit **gesetzlicher Einschränkungen** – z.B. für funktionierende Gesellschaft – von Beginn an angelegt (z.B. in der Europäischen Menschenrechtskonvention)
- Datenschutzrecht wie GDPR setzt konkrete Regeln, um allgemein gehaltene Grund-/Menschenrechte operationalisierbar auszugestalten



# Grundlegende Konzepte / Prinzipien

# Lesson 08: Datenschutz 1 – Rechtliche Grundlagen



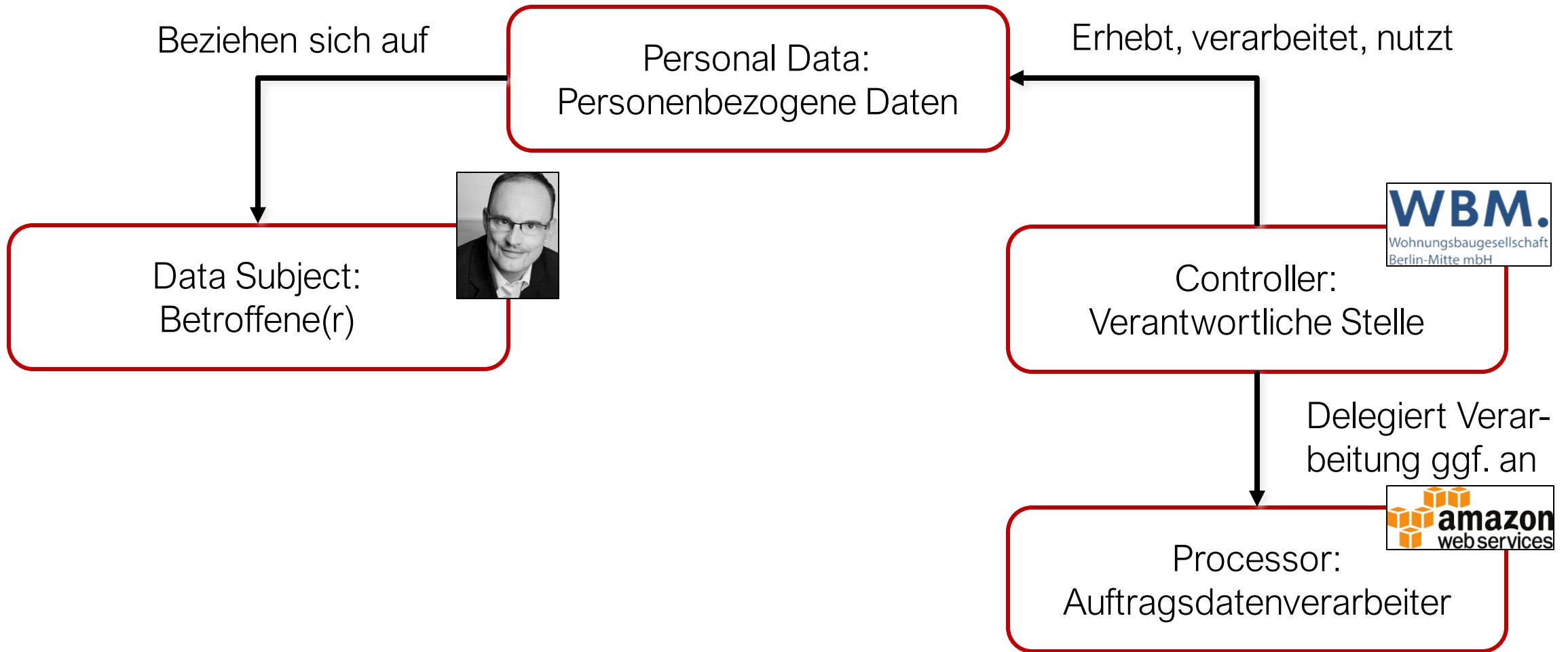
Hintergrund, Architektur & Ziele des Datenschutzrechts

Rechtliche Rollen und „Personenbezogene Daten“

Internationale Transfers

Neun Prinzipien des Datenschutzrechts

# GDPR: Wichtigste Begrifflichkeiten



# GDPR: Anwendungsbereich

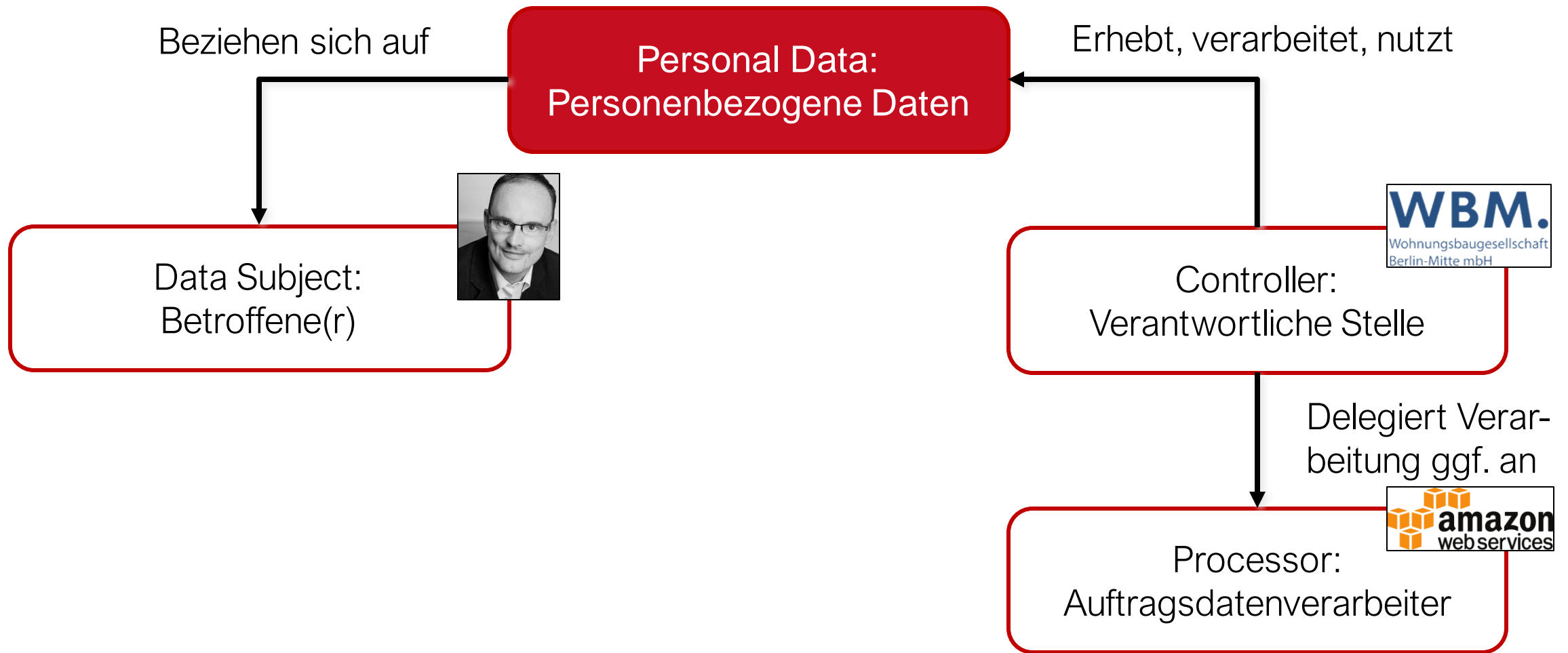
## Art. 2 – Sachlicher Anwendungsbereich:

- (1) 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.
- (2) Diese Verordnung findet **keine Anwendung** auf die Verarbeitung personenbezogener Daten:  
[außerhalb des Anwendungsbereichs des Unionsrechts; Aktivitäten mit Bezug zu Grenzkontrollen, Asyl, etc.; rein persönliche/familiäre Tätigkeiten („**Haushaltsausnahme**“); **Strafverfolgung, öffentliche Sicherheit, ...**]



→ Ohne personenbezogene (oder „personenbeziehbare“)  
Daten keine Anwendbarkeit der GDPR  
(und des Datenschutzrechts im Allgemeinen)

# GDPR: Wichtigste Begrifflichkeiten



# GDPR: „Personenbezogene Daten“

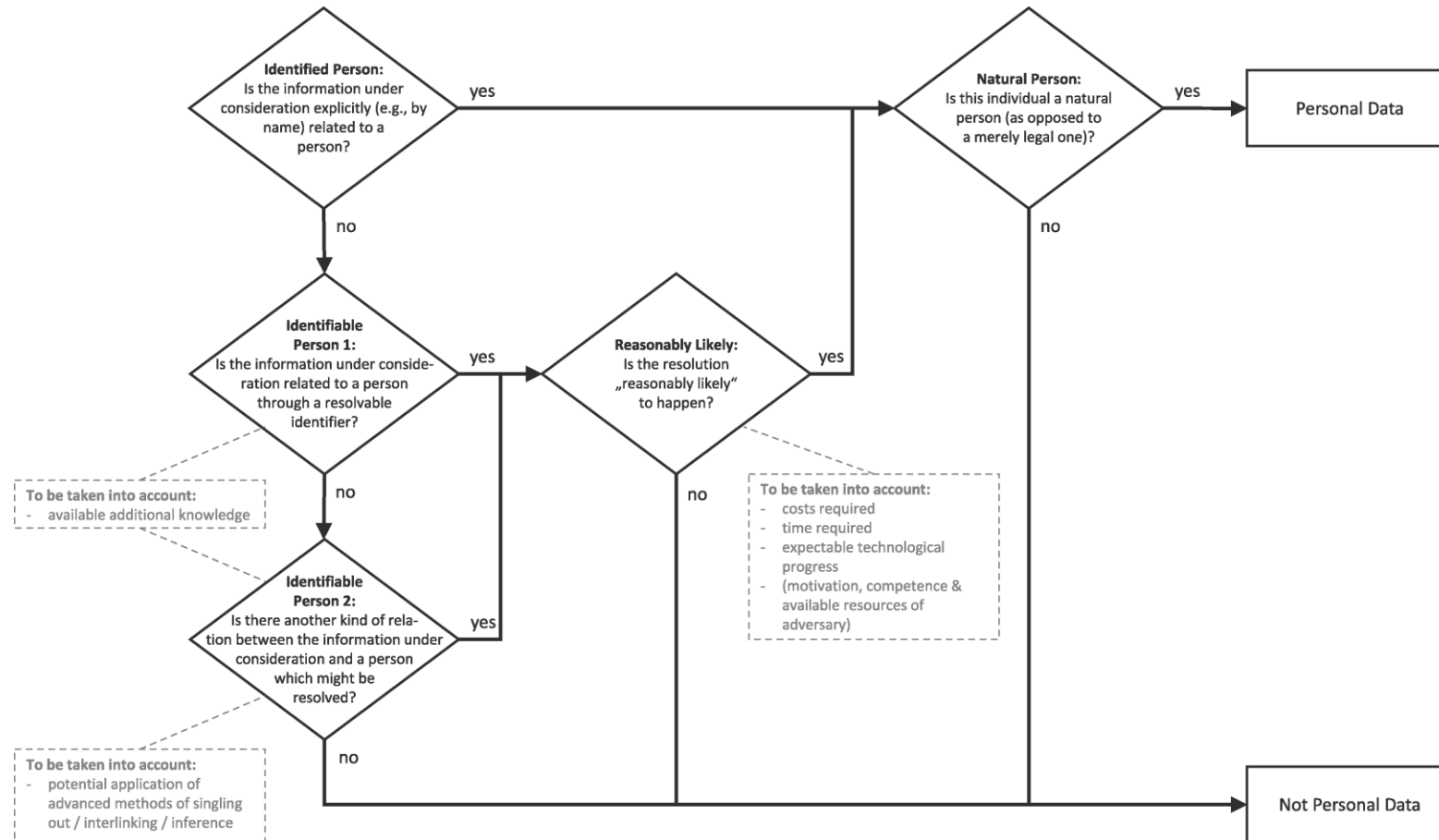
## Art. 4 – Begriffsbestimmungen:

[...]

(1) „personenbezogene Daten“ [sind] 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 [...] **identifiziert werden kann**;


# GDPR: „Personenbezogene Daten“



Finck / Pallas (2020): They who must not be identified—distinguishing personal from non-personal data under the GDPR - <https://academic.oup.com/idpl/article/10/1/11/5802594>

# „Personenbezogene Daten“?


BESTELLUNG AUFGEGEBEN 13. November 2023	SUMME €66,35	VERSANDADRESSE FRANK PALLAS	BESTELLNR. 302-1570684-5307547 <a href="#">Bestelldetails anzeigen</a>   <a href="#">Rechnung</a>
<b>Zugestellt: 14.11.2023</b> Die Sendung wurde einem Hausbewohner übergeben.		<a href="#">Lieferung verfolgen</a>	
 <b>FIBARO The Heat Controller Head / Z-Wave Plus Heizungsthermostat, Heizkörperthermostat, FGT-001</b> Rücksendung bis zum 31.01.2024 möglich.		<a href="#">Produkt-Support erhalten</a>	
<a href="#">Nochmals kaufen</a> <a href="#">Deinen Artikel anzeigen</a>		<a href="#">Artikel zurücksenden oder ersetzen</a>	
		<a href="#">Geschenkbestätigung teilen</a>	
		<a href="#">Schreib eine Produktrezension</a>	
<a href="#">Bestellung archivieren</a>			

BESTELLUNG AUFGEGEBEN 8. November 2023	SUMME €14,99	VERSANDADRESSE FRANK PALLAS	BESTELLNR. 302-6079221-4146705 <a href="#">Bestelldetails anzeigen</a>   <a href="#">Rechnung</a>
<b>Zugestellt: 10.11.2023</b> Die Sendung wurde einem Hausbewohner übergeben.		<a href="#">Lieferung verfolgen</a>	
 <b>D'CASA - Kapselbehälter aus Plexiglas, für 13 Dolce Gusto-Kapseln oder 40 Nespresso-Kapseln</b> Rücksendung bis zum 31.01.2024 möglich.		<a href="#">Artikel zurückgeben</a>	
<a href="#">Nochmals kaufen</a> <a href="#">Deinen Artikel anzeigen</a>		<a href="#">Geschenkbestätigung teilen</a>	
		<a href="#">Verkäufer-Feedback abgeben</a>	
		<a href="#">Schreib eine Produktrezension</a>	
<a href="#">Bestellung archivieren</a>			




Informationsgehalt? Natürliche Person identifizierbar für wen?


# „Personenbezogene Daten“?


Frank > Touren > **NOK 2: Rendsburg-Eidervorland-Büsum-104**










Map data © OpenStreetMap-Mitwirkende

 **NOK 2: Rendsburg-Eidervorland-Büsum-104**  

 **04:06** ↔ **104 km** Ø **25,3 km/h** ↗ **180 m** ↘ **190 m**

 Du warst Rennrad fahren.  
9. August 2022

-  Tour bearbeiten
-  Teilnehmende markieren
-  Teilen
-  Zu Collection hinzufügen
-  Mehrtagestour planen
-  Tour neu planen
-  Für GPS-Gerät herunterladen

Informationsgehalt? Natürliche Person identifizierbar für wen?

# „Personenbezogene Daten“?



„Jens Müller“



Informationsgehalt? Natürliche Person identifizierbar für wen?

Aber: Biometrische Daten sind – entgegen der eigentlichen Logik – per Definition personenbezogene Daten (Art. 4(14) GDPR)

# „Personenbezogene Daten“?

100.98.67.102

Informationsgehalt? Natürliche Person identifizierbar für wen?



Want More?

# International Data Privacy Law

[Issues](#) [More Content ▾](#) [Submit ▾](#) [Purchase](#) [Alerts](#) [About ▾](#)


All International Data Pr



**Volume 10, Issue 1**  
February 2020

**Article Contents**

## They who must not be identified—distinguishing personal from non-personal data under the GDPR

 [Michèle Finck](#) ✉, [Frank Pallas](#)

*International Data Privacy Law*, Volume 10, Issue 1, February 2020, Pages 11–36,  
<https://doi.org/10.1093/idpl/ipz026>  
**Published:** 10 March 2020 **Article history ▾**

 PDF  Split View  Cite  Permissions  Share ▾

# GDPR: „Personenbezogene Daten“

## Art. 4 – Begriffsbestimmungen:

[...]

(1) „personenbezogene Daten“ [sind] 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 [...] identifiziert werden kann**;

# „Personenbezogene Daten“

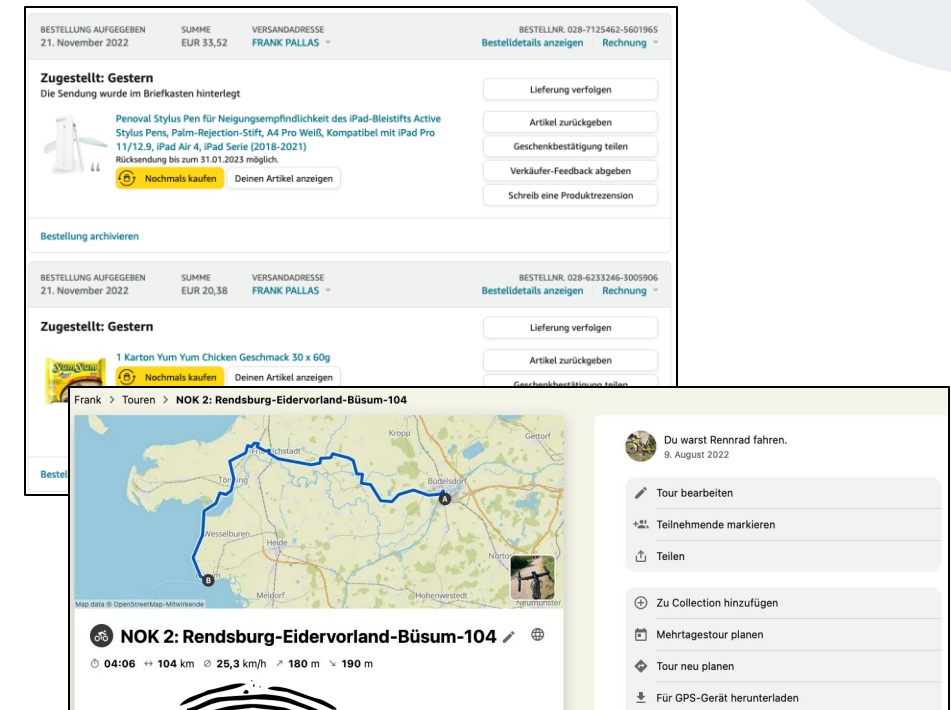
Datenschutzrecht nur anwendbar, wenn personenbezogene Daten vorliegen

Erforderlich für personenbezogene Daten:

- Informationsgehalt
- Identifizierte oder identifizierbare natürliche Person

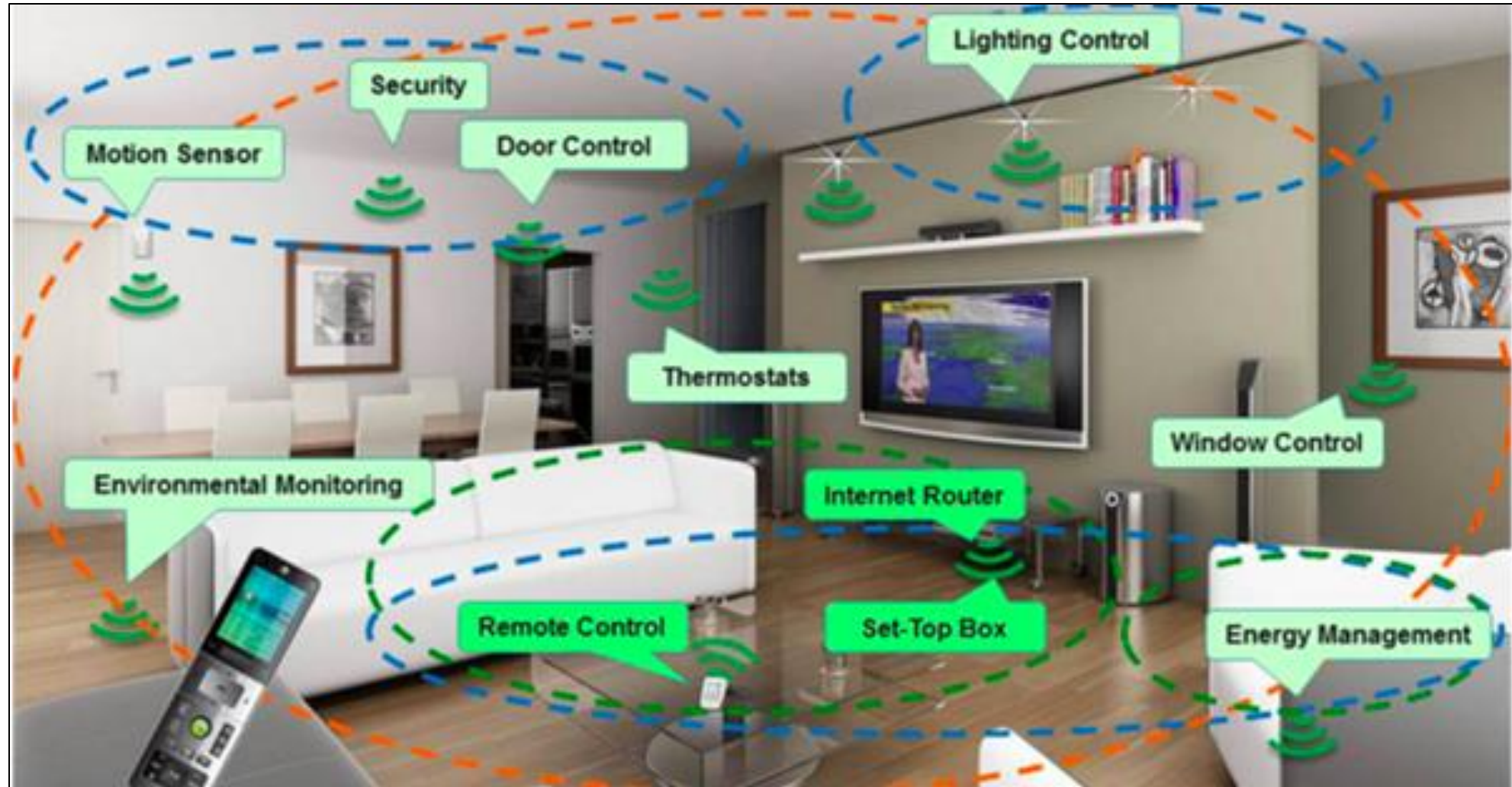
→ Abhängig von Identifizierbarkeit kann ein und dasselbe Datum gleichzeitig personenbezogen (aus Sicht von A) und nicht personenbezogen (aus Sicht von B) sein

→ Intuitiv als personenbezogen empfundene Daten (IP-Adressen) sind teilw. nur Identifier, ermöglichen als solche aber Personenbezug anderer Daten und sind daher ebenfalls schützenswert.

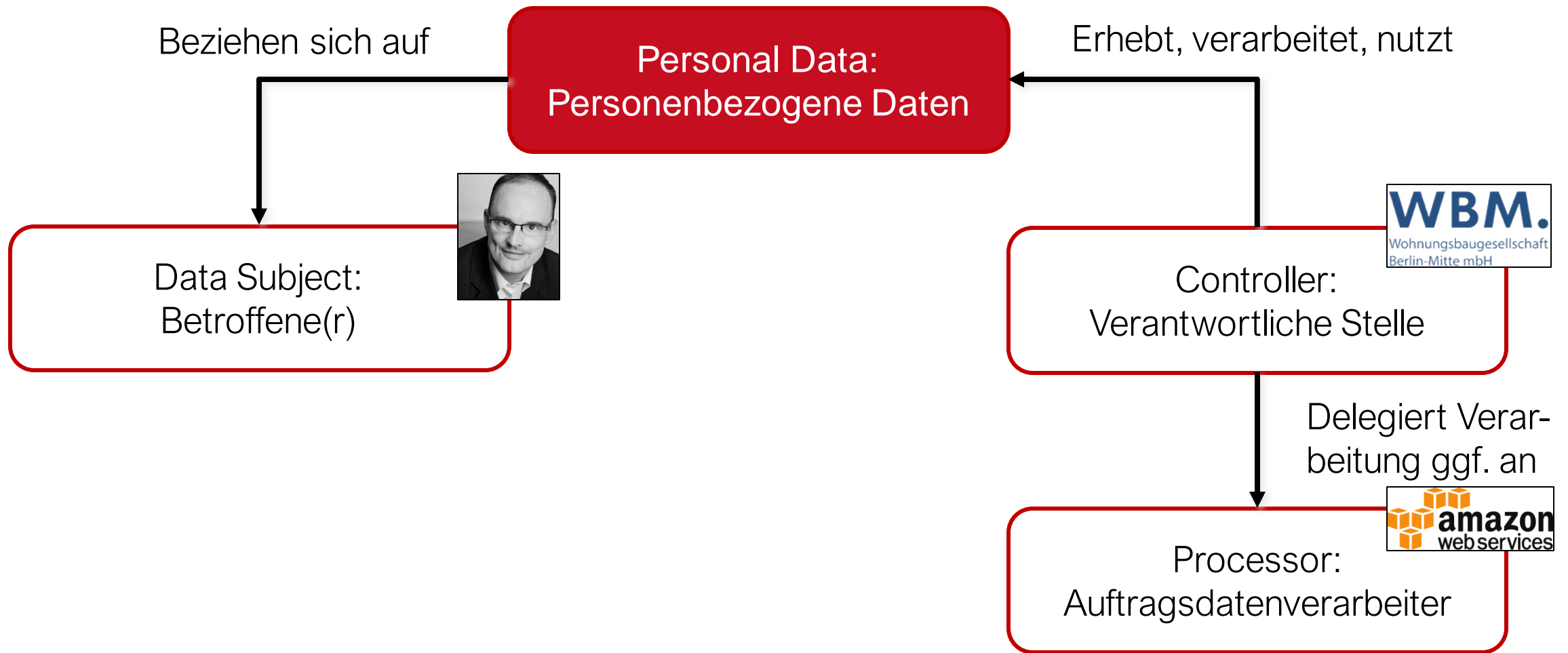


100.98.67.102

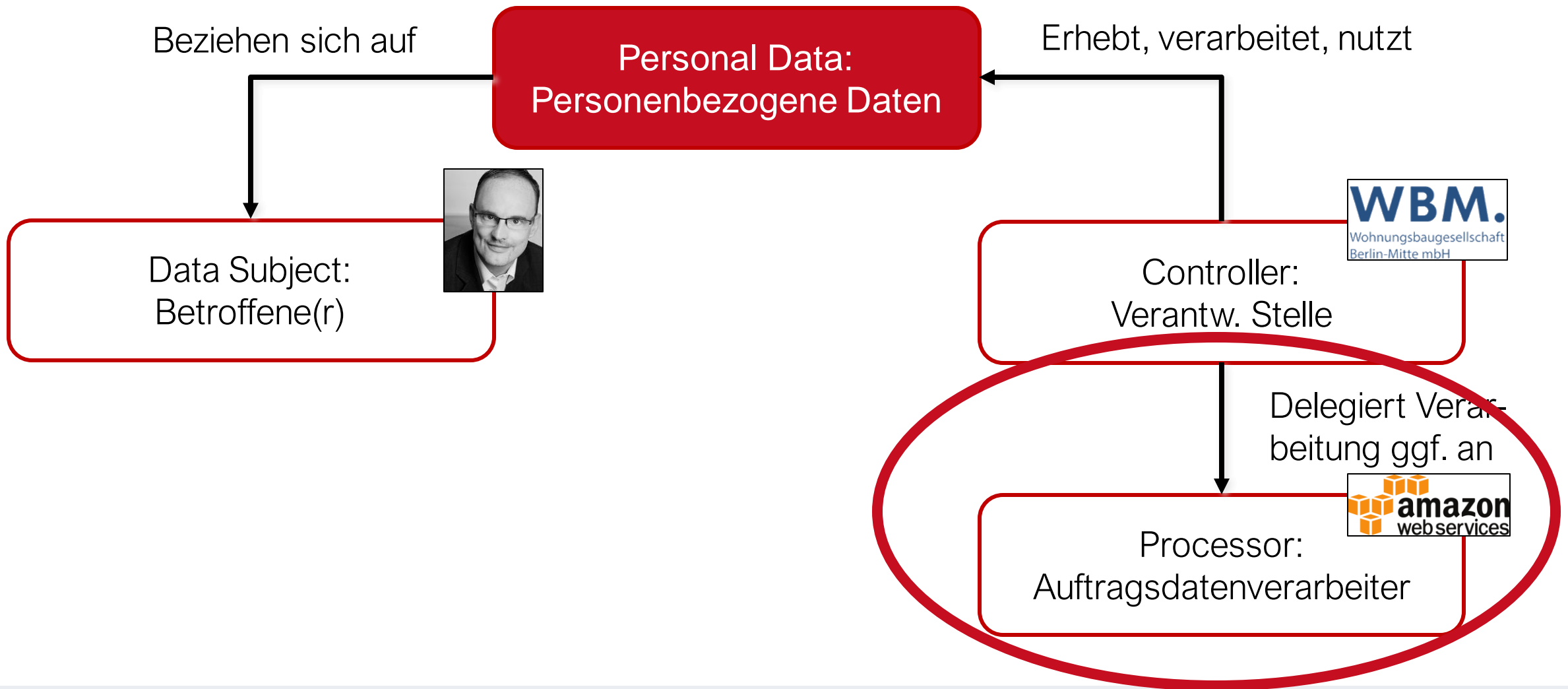
# „Personenbezogene Daten“?



# GDPR: Wichtigste Begrifflichkeiten

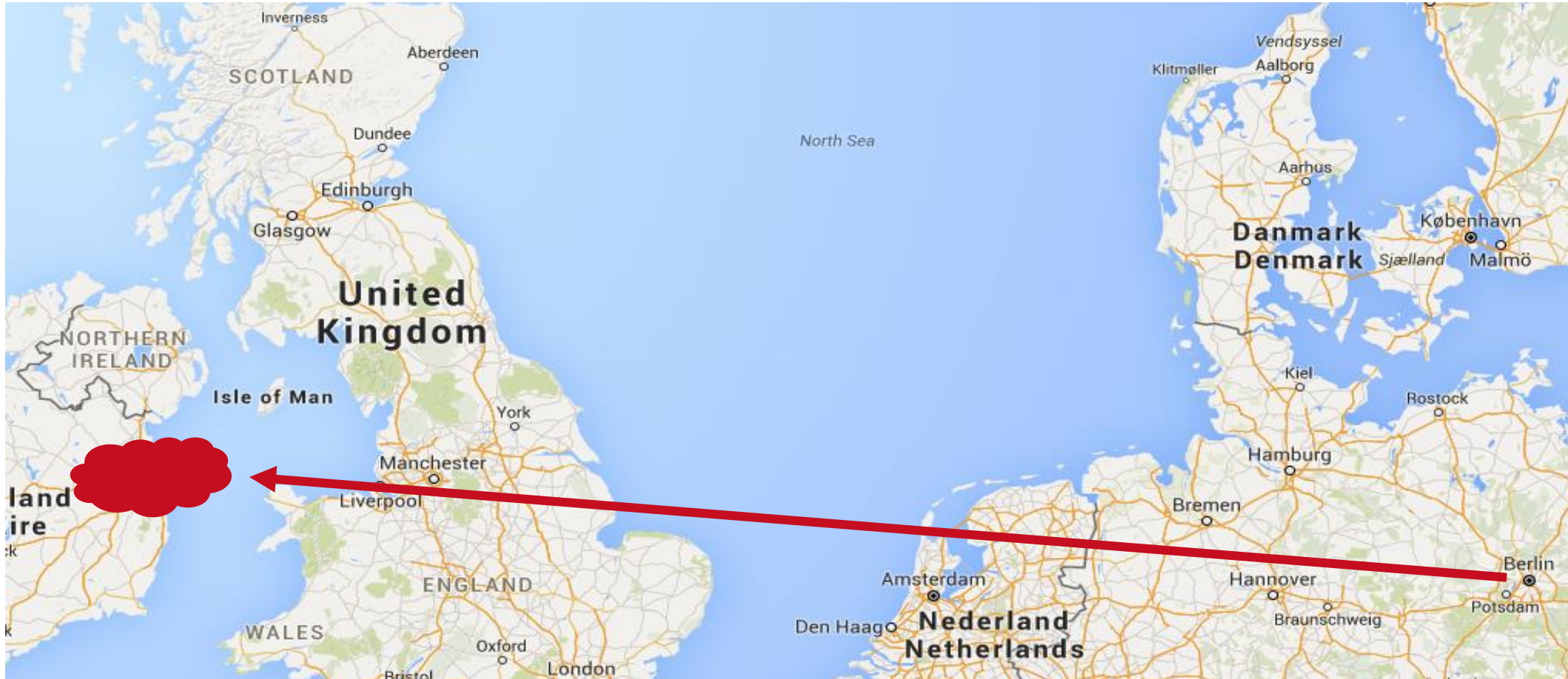


# GDPR: Wichtigste Begrifflichkeiten





# Übermittlung in andere Staaten?



→ Übermittlungen in andere Staaten (z.B. für Cloud Computing) ohne Weiteres zulässig?

# Lesson 08: Datenschutz 1 – Rechtliche Grundlagen



Hintergrund, Architektur & Ziele des Datenschutzrechts

Rechtliche Rollen und „Personenbezogene Daten“

**Internationale Transfers**

Neun Prinzipien des Datenschutzrechts



4.5.2016

DE

Amtsblatt der Europäischen Union

L 119/1

I

(Gesetzgebungsakte)

## VERORDNUNGEN

**VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES**

**vom 27. April 2016**

**zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)**

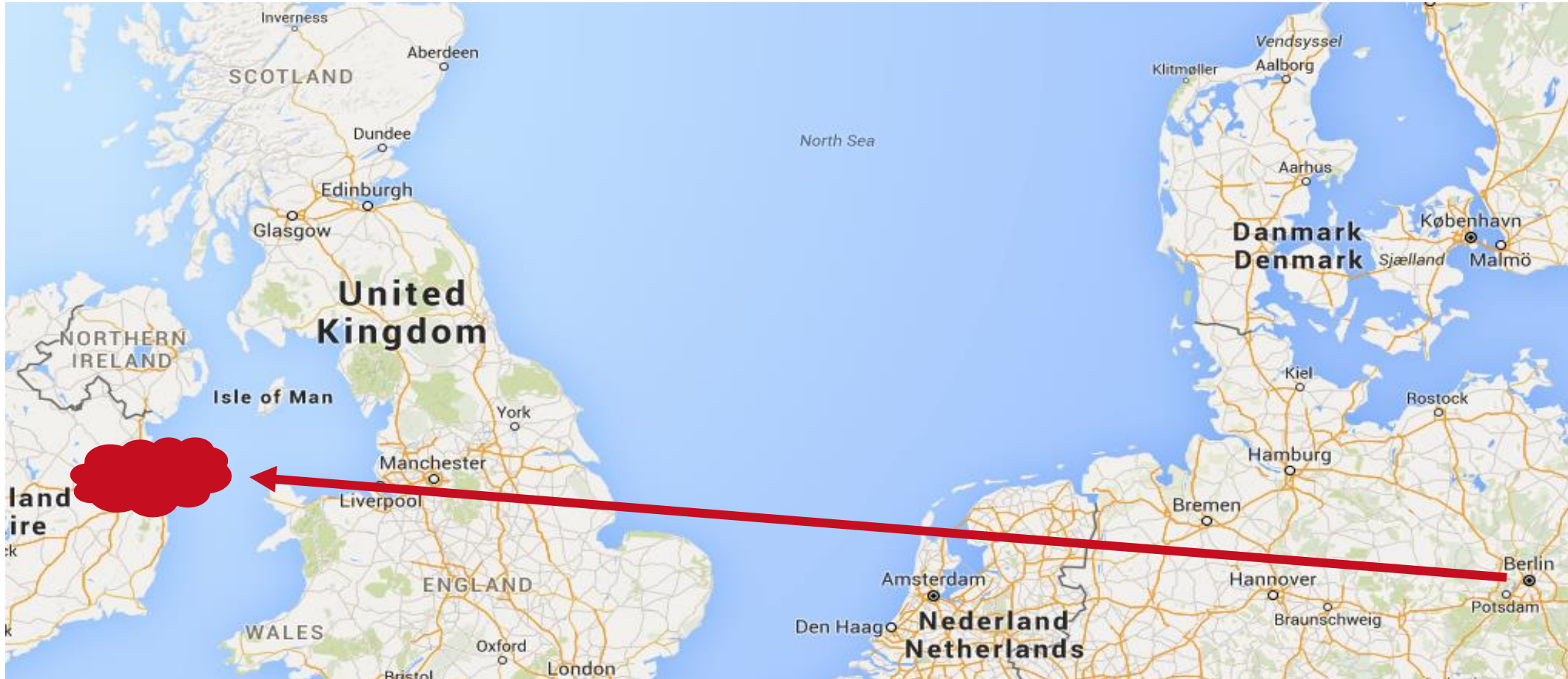
(Text von Bedeutung für den EWR)

# GDPR: „Personenbezogene Daten“

## Art. 1 – Gegenstand und Ziele:

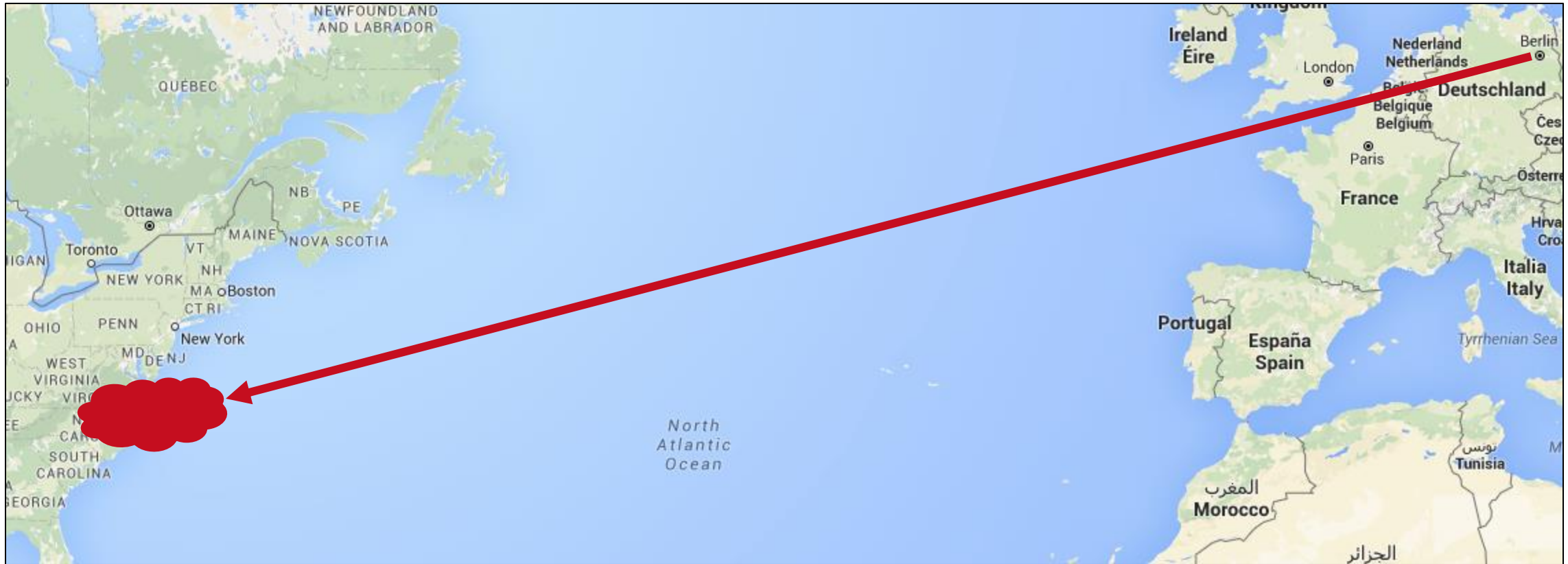
- (1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und **zum freien Verkehr solcher Daten**.
- (2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
- (3) Der **freie Verkehr personenbezogener Daten in der Union** darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

# Freier Verkehr personenbezogener Daten



→ GDPR zieht auf einheitlichen digitalen Markt mit einheitlichen Regeln ab

# Freier Verkehr personenbezogener Daten?



# Freier Verkehr personenbezogener Daten?

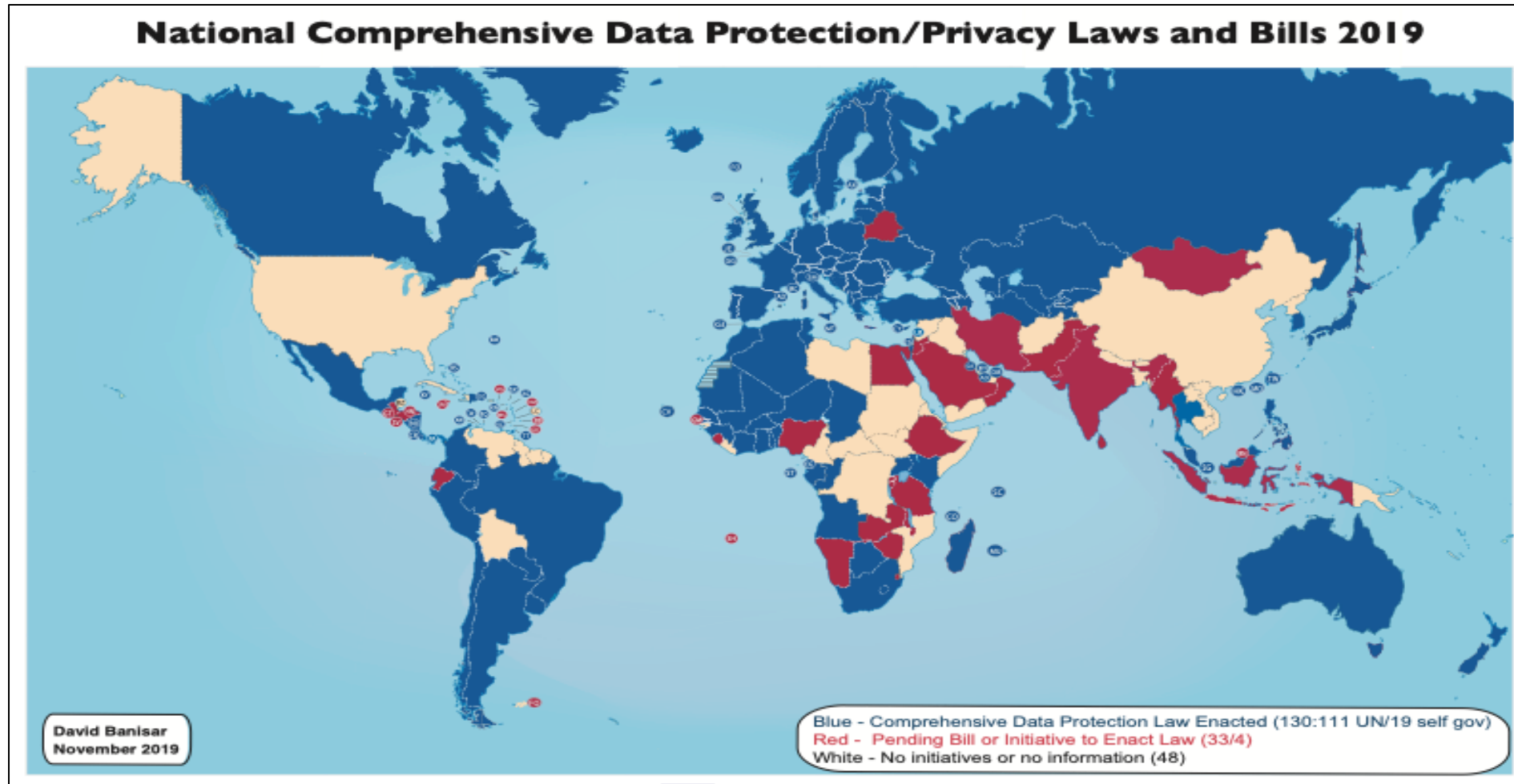
## Art. 44ff GDPR:

Jedwede **Übermittlung** personenbezogener Daten [... zur Verarbeitung ...] an ein Drittland oder eine internationale Organisation [...] **ist nur zulässig**, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen **Bestimmungen dieser Verordnung eingehalten werden**

Eine Übermittlung personenbezogener Daten an ein Drittland [...] darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland [...] ein **angemessenes Schutzniveau** bietet.



# „Angemessenes Schutzniveau“? 2019



Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2019 (Dec. 2019).  
Available at SSRN: <https://ssrn.com/abstract=1951416> or <http://dx.doi.org/10.2139/ssrn.1951416>

# Übermittlung an Drittstaaten ohne „Angemessenes Schutzniveau“?



→ Europäischer Gerichtshof: Vorher existierende Übereinkunft („Safe Harbor Agreement“) bietet kein „Angemessenes Schutzniveau“ („Schrems I“)

# EU-US Privacy Shield



→ Akzeptiert als „Angemessenes Schutzniveau“ im Juli 2016



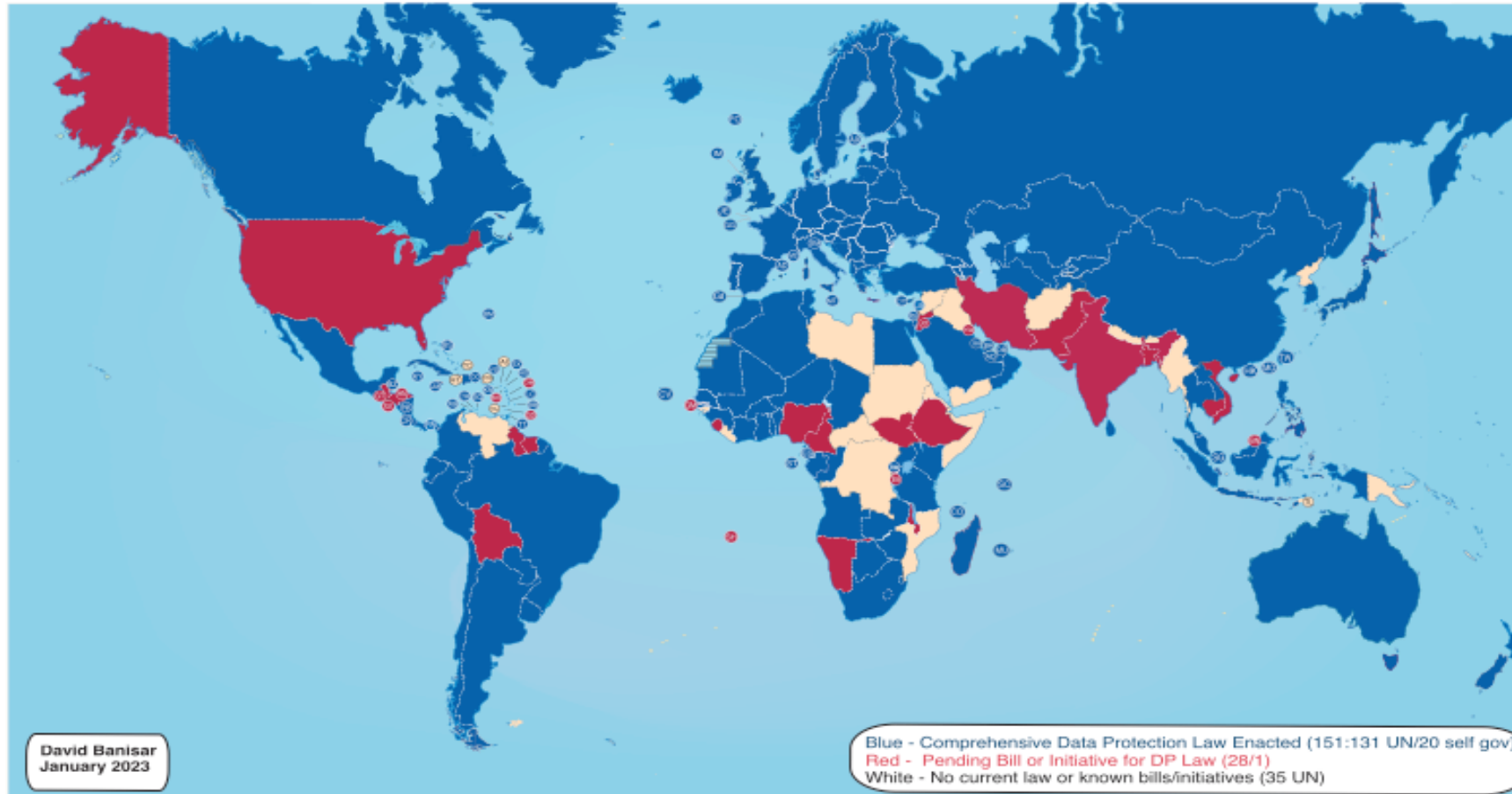
# EU-US Privacy Shield



→ Europäischer Gerichtshof: Auch Privacy Shield bietet kein „Angemessenes Schutzniveau“ („Schrems II“) – aber andere Grundlagen (SCC, ...) möglich

# „Angemessenes Schutzniveau“?

## National Comprehensive Data Protection/Privacy Laws and Bills 2023



Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2023 (Jan 2023).  
Available at SSRN: <https://ssrn.com/abstract=1951416> or <http://dx.doi.org/10.2139/ssrn.1951416>

# „Privacy Shield 2.0“: EU-US Data Privacy Framework



THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)<sup>1</sup>, and in particular Article 45(3) thereof,

Whereas:

[...62 Seiten...]

HAS ADOPTED THIS DECISION:

## *Article 1*

For the purpose of Article 45 of Regulation (EU) 2016/679, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States that are included in the ‘Data Privacy Framework List’, maintained and made publicly available by the U.S. Department of Commerce, in accordance with Section I.3 of Annex I.

[https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_23\\_3752](https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752)

# GDPR und Internationale Transfers

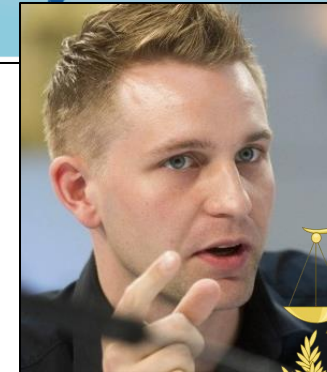
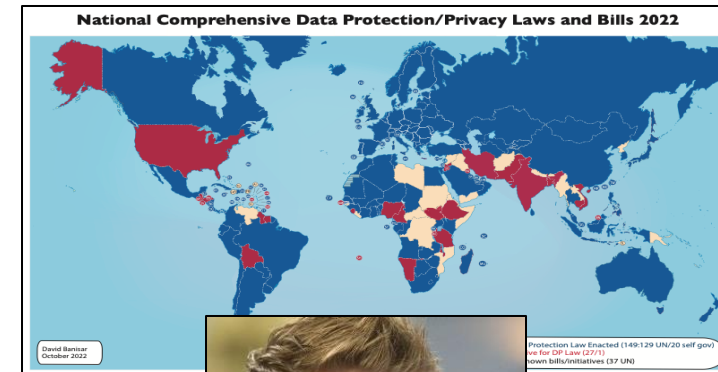
GDPR schützt nicht nur Grundrechte sondern auch freien Verkehr personenbezogener Daten

Innerhalb der EU daher (grundsätzlich) keine Einschränkungen bei grenzüberschreitenden Übermittlungen / Verarbeitungen

Übermittlungen in „Drittstaaten“ außerhalb der EU nur bei „angemessenem Schutzniveau“

Insb. für USA mangels allgemeinen Datenschutzgesetzes (bisher) und ausreichenden Rechtsschutzes nicht gegeben

Safe Harbor → Schrems I → Privacy Shield → Schrems II → EU-US-DPF → ???



Natürliche Personen

Schutz von Grundrechten

Angemessenes Schutzniveau und freier Datenverkehr

# Grundlegende Konzepte / Prinzipien

# 9 Prinzipien

# 9 Kernprinzipien des Datenschutzes

Rechtmäßigkeit (incl. Einwilligung)

Zweckbindung

Datensparsamkeit (incl. Erforderlichkeit)

Transparenz

Richtigkeit

Sicherheit (insb. Vertraulichkeit, Integrität, Verfügbarkeit)

Verantwortlichkeit (incl. nachweisbare Rechtskonformität)

Kontrolle und Durchsetzung

Datenportabilität



# 9 Kernprinzipien des Datenschutzes

Rechtmäßigkeit (incl. Einwilligung)

Zweckbindung

Datensparsamkeit (incl. Erforderlichkeit)

Transparenz

Richtigkeit

Sicherheit (insb. Vertraulichkeit, Integrität, Verfügbarkeit)

Verantwortlichkeit (incl. nachweisbare Rechtskonformität)

Kontrolle und Durchsetzung

Datenportabilität

→ ALLE Kernprinzipien müssen erfüllt werden!  
(z.B. kein „Verzicht“ auf Datensparsamkeit möglich)

# 9 Kernprinzipien des Datenschutzes



Rechtmäßigkeit

„Die Verarbeitung ist **nur rechtmäßig, wenn mindestens eine** der nachstehenden Bedingungen **erfüllt** ist: [...]“

Art 6(1) GDPR

Zentrales Prinzip:  
sog. „Verbot mit Erlaubnisvorbehalt“

„Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:“

[...]

die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist [...] erforderlich [...]

die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich [...]

die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person [...] zu schützen

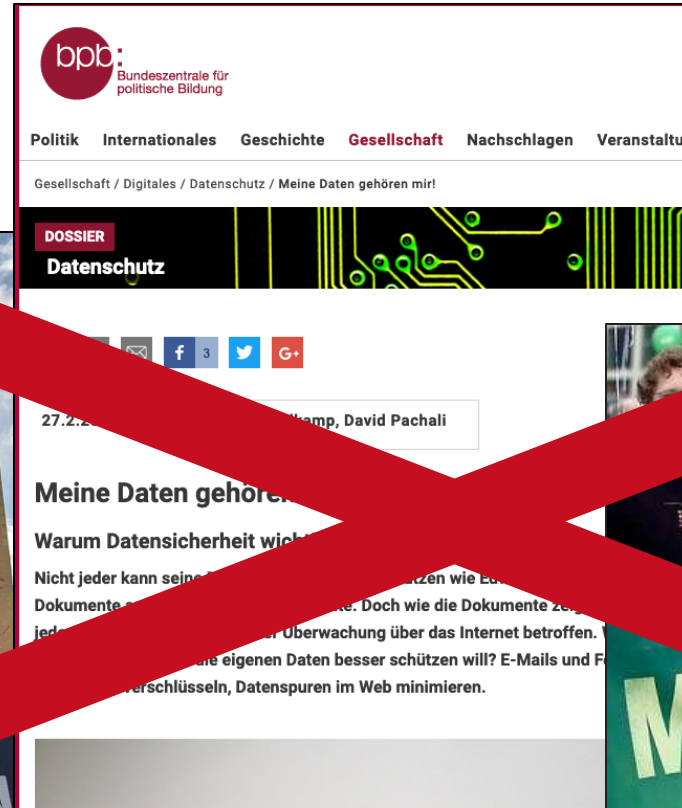
die Verarbeitung ist für die **Wahrnehmung einer Aufgabe** erforderlich, die im **öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt** erfolgt [...]

die Verarbeitung ist zur **Wahrung der berechtigten Interessen des Verantwortlichen** [...] erforderlich, sofern nicht die Interessen [...] betroffenen Person [...] überwiegen

Art 6(1) GDPR

~~„Man muss die Leute immer fragen“~~

# „Dateneigentum“



„Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:“

**Die betroffene Person hat ihre Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten **für einen oder mehrere bestimmte Zwecke gegeben** [...]

die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist [...] erforderlich [...]

die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich [...]

die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person [...] zu schützen

die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt [...]

die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen [...] erforderlich, sofern nicht die Interessen [...] betroffenen Person [...] überwiegen

Art 6(1) GDPR



„‘Einwilligung‘ der betroffenen Person 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(11) GDPR

„Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche **nachweisen können**, [...]“

Art 7 GDPR

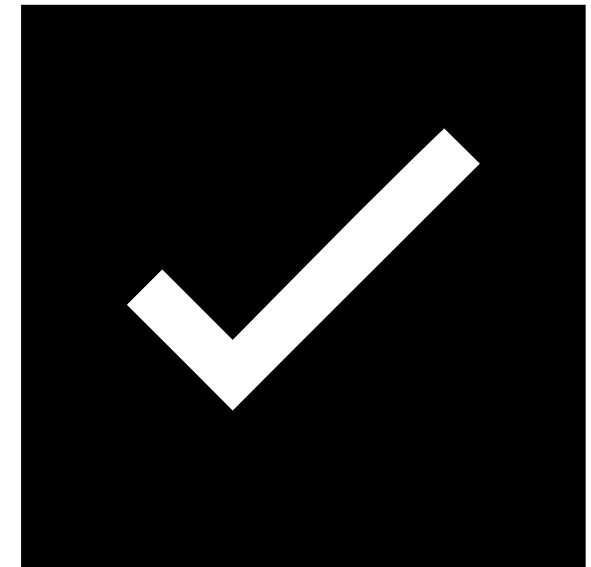
## „Freie und informierte Einwilligung“

(+ div. formale Anforderungen, Widerrufbarkeit, Kopplungsverbot, Mindestalter, ...)

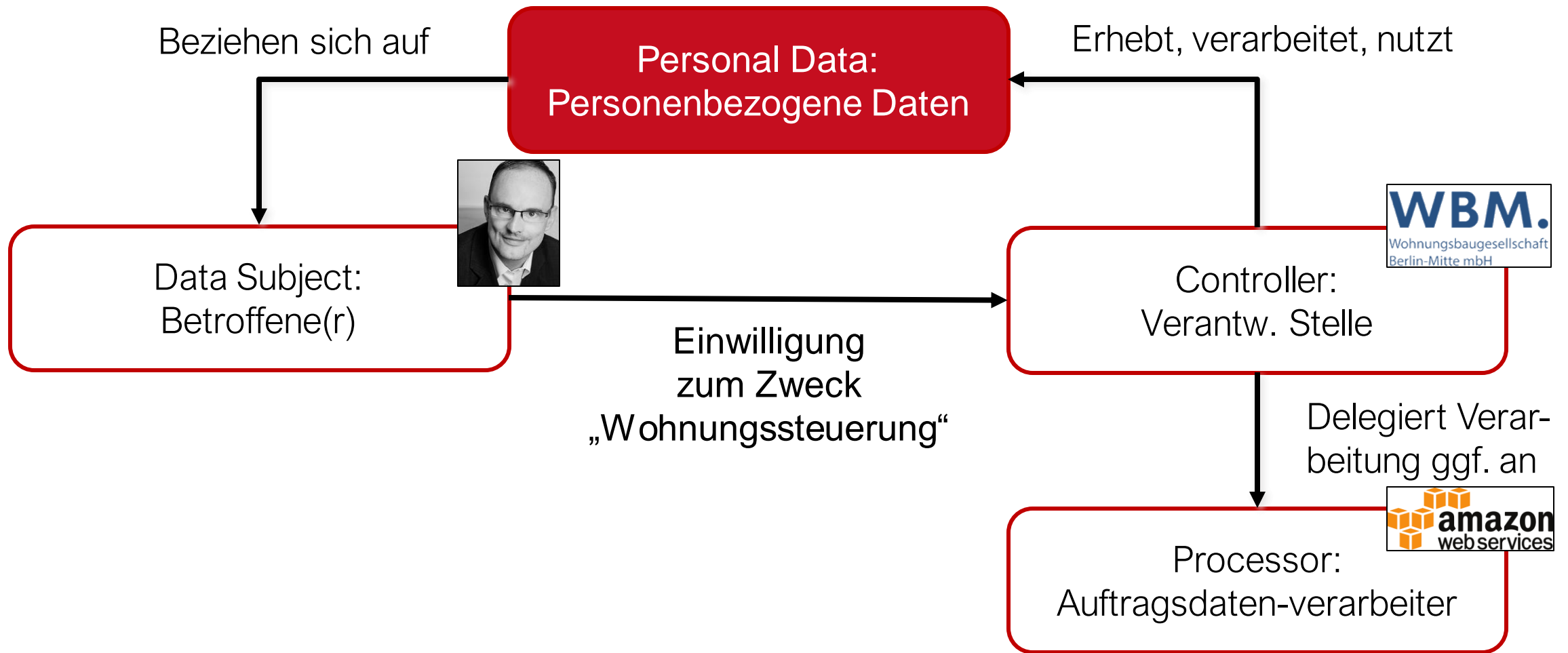
→ Kritisch hinterfragen: Bei welchen Einwilligungen, die sie selbst geben, ist echte Freiwilligkeit und Informiertheit tatsächlich gegeben?

# Rechtmäßigkeit und Einwilligung

- Jede Erhebung, Verarbeitung, ...  
personenbezogener Daten braucht eine  
**Legitimationsgrundlage**
- Dies kann eine individuelle **Einwilligung**  
sein, **muss aber nicht**
- Wenn **Einwilligung**, dann muss diese  
**weiteren Anforderungen** genügen



# GDPR: Wichtigste Begrifflichkeiten



# 9 Kernprinzipien des Datenschutzes



Rechtmäßigkeit (incl. Einwilligung)

Zweckbindung

z.B.

„Personenbezogene Daten müssen [...] für **festgelegte**, eindeutige und legitime **Zwecke** erhoben werden und **dürfen nicht** in einer mit diesen Zwecken nicht zu vereinbarenden Weise **weiterverarbeitet werden**“

Art. 5(1b) GDPR

# Zweckbindung



z.B.

„Personenbezogene Daten müssen [...] für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit **diesen Zwecken nicht zu vereinbarenden Weise** weiterverarbeitet werden“

Art. 5(1b) GDPR



## Zweckbindung – „Zu vereinbarende Zwecke“

„Beruht die **Verarbeitung zu einem anderen Zweck** [...] nicht auf der Einwilligung der betroffenen Person oder [...] so **berücksichtigt** der Verantwortliche — um festzustellen, ob [die Zwecke vereinbar sind] — unter anderem  
[Verbindungen zwischen Zwecken, Erhebungskontext, Art der Daten, mögliche Folgen, existierende Schutzmechanismen]“

Art. 6(4) GDPR

# Zweckbindung – „Zu vereinbarende Zwecke“



# Zweckbindung – „Zu vereinbarende Zwecke“



# Zweckbindung „in the wild“



IMAGE: MANDEL NGAN/POOL/AFP VIA GETTY IMAGES

**MOTHERBOARD**  
TECH BY VICE

**Facebook Doesn't Know  
What It Does With Your  
Data, Or Where It Goes:  
Leaked Document**

<https://www.vice.com/en/article/akvmke/facebook-does-nt-know-what-it-does-with-your-data-or-where-it-goes>

**“We can’t confidently make controlled policy changes or external commitments such as ‘we will not use X data for Y purpose.’ And yet, this is exactly what regulators expect us to do”**

# Zweckbindung

- Verarbeitung personenbezogener Daten grds. nur für ursprüngliche Zwecke
- Zweckänderungen sind (nach GDPR) möglich, aber „Vereinbarkeit“ muss gegeben sein
- Derzeit noch unklar, wie eng „Vereinbarkeit“ zu fassen sein wird



# 9 Kernprinzipien des Datenschutzes

Rechtmäßigkeit (incl. Einwilligung)

Zweckbindung

Datensparsamkeit (incl. Erforderlichkeit)

# Datensparsamkeit / Erforderlichkeit

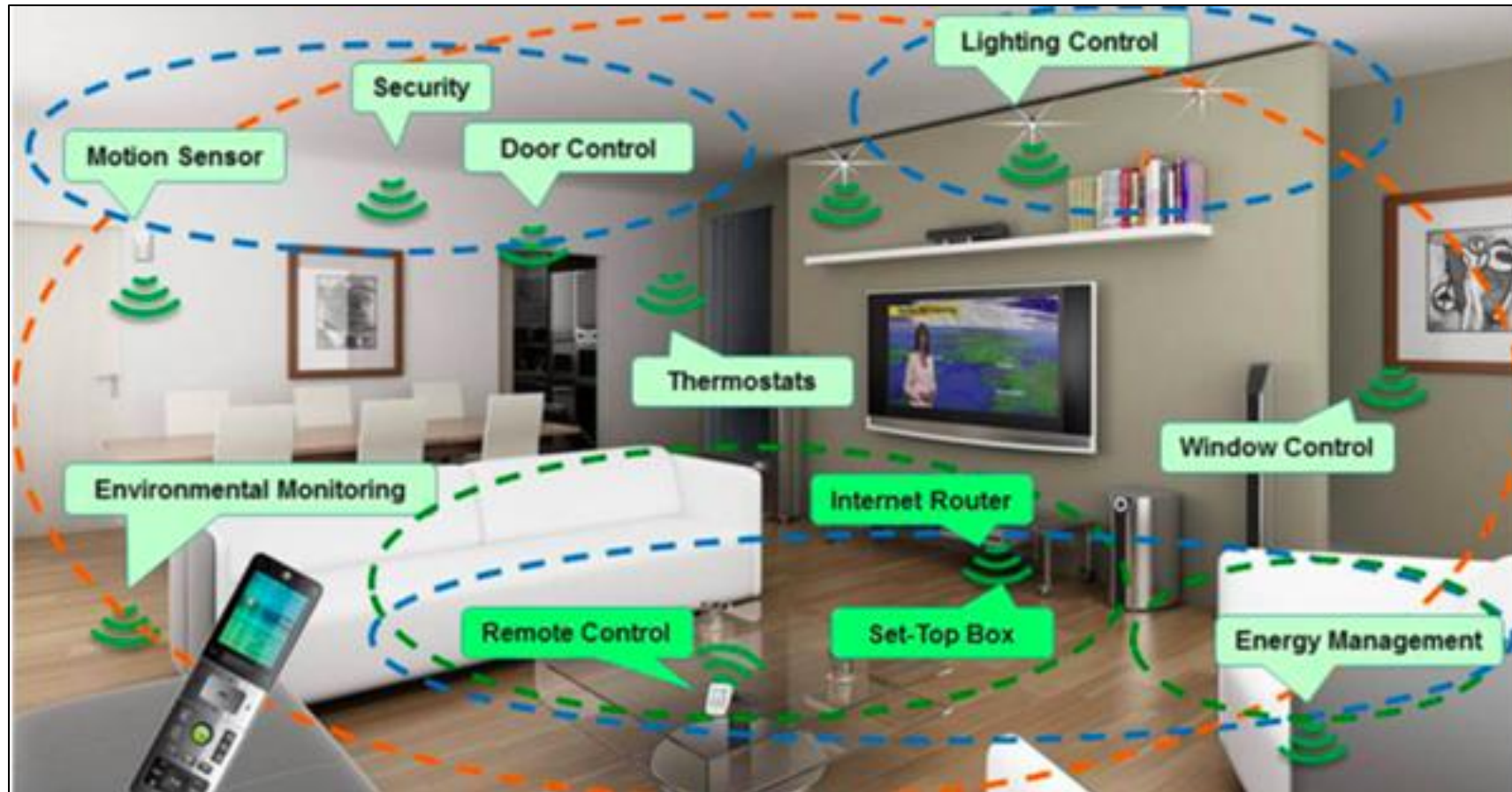
- Erheben, Verarbeiten, etc. ist nur zulässig, wenn es **tatsächlich erforderlich** ist, bei überwiegendem berechtigten Interesse, oder wenn Daten allgemein zugänglich sind.
- Daten sind zu **löschen, anonymisieren, ...**, sobald für Zweck nicht mehr erforderlich
- „**Überschreiben**“ durch Einwilligungen o.ä. **nicht möglich!**

„Personenbezogene Daten müssen [...] dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (‚Datenminimierung‘)“

Art. 5(1c) GDPR



# Datensparsamkeit / Erforderlichkeit



→ Welche Daten sind für welchen Zweck wirklich erforderlich?



# 9 Kernprinzipien des Datenschutzes

Rechtmäßigkeit (incl. Einwilligung)

Zweckbindung

Datensparsamkeit (incl. Erforderlichkeit)

Transparenz

Erhebung bei Betroffenen, Unterrichtung, Auskunftsrechte,  
Informationspflichten, ...

→ Betroffene sollen „**wissen (können), was geschieht**“  
(→ gilt auch jenseits der „informierten Einwilligung“)

# 9 Kernprinzipien des Datenschutzes

Rechtmäßigkeit (incl. Einwilligung)

Zweckbindung

Datensparsamkeit (incl. Erforderlichkeit)

Transparenz

Richtigkeit

z.B.

„Personenbezogene Daten müssen [...] **sachlich richtig** und erforderlichenfalls **auf dem neuesten Stand** sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die [...] **unrichtig** sind, unverzüglich **gelöscht oder berichtigt** werden“

Art. 5(1d) GDPR

→ Pflicht des „Controllers“ und Anrecht des „Data Subjects“!

# 9 Kernprinzipien des Datenschutzes

Rechtmäßigkeit (incl. Einwilligung)

Zweckbindung

Datensparsamkeit (incl. Erforderlichkeit)

Transparenz

Richtigkeit

Sicherheit

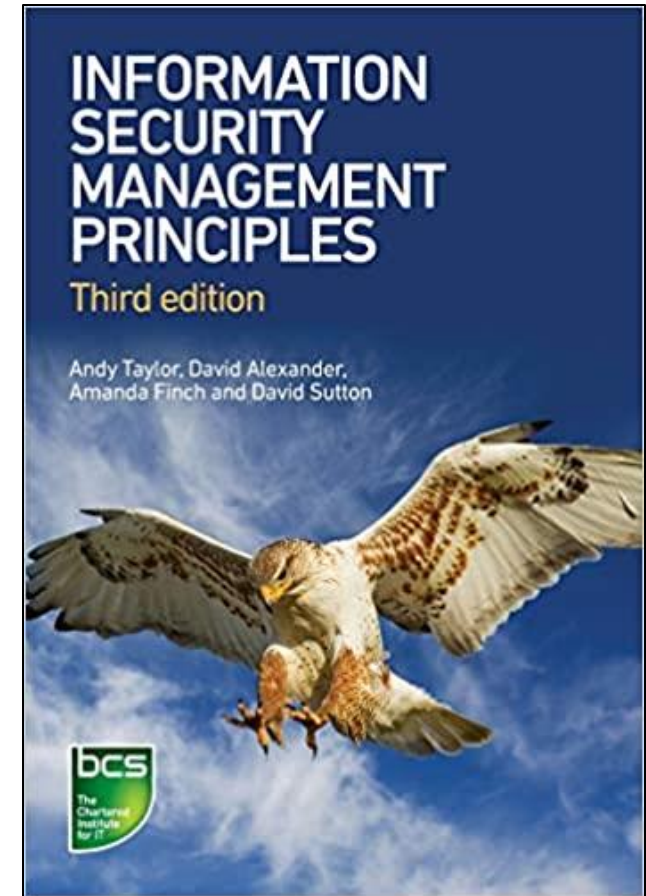
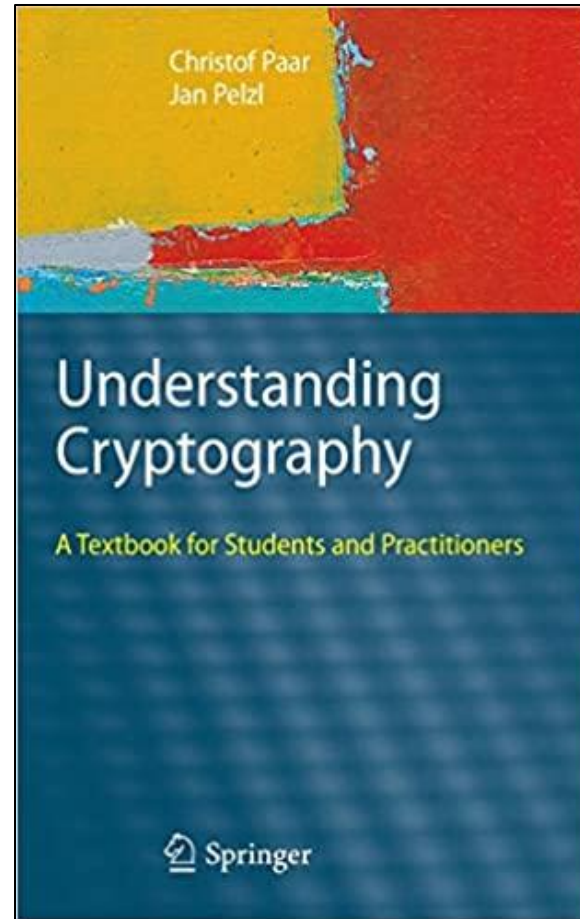
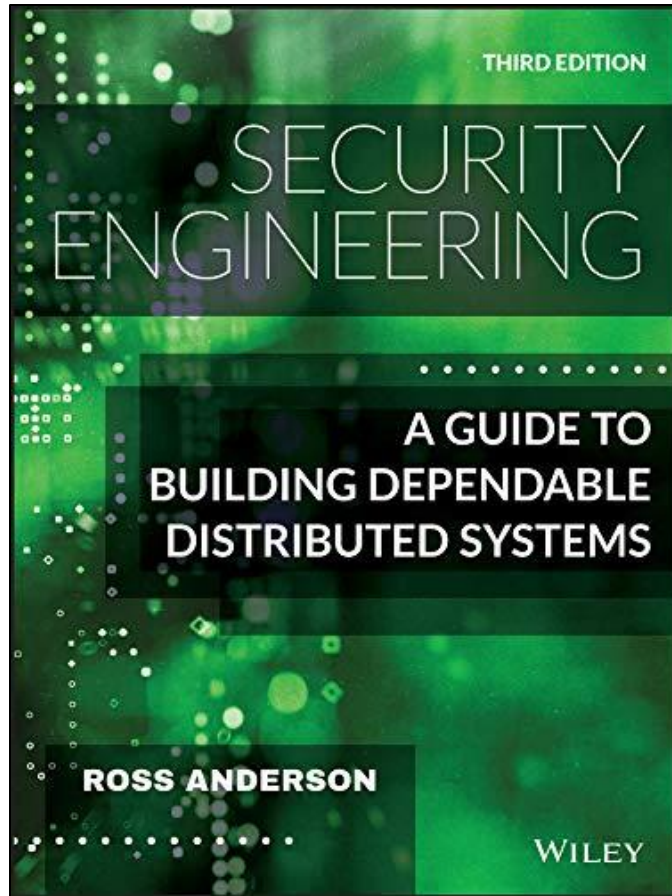
z.B.

„Personenbezogene Daten müssen [...] 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“

Art. 5(1f) GDPR

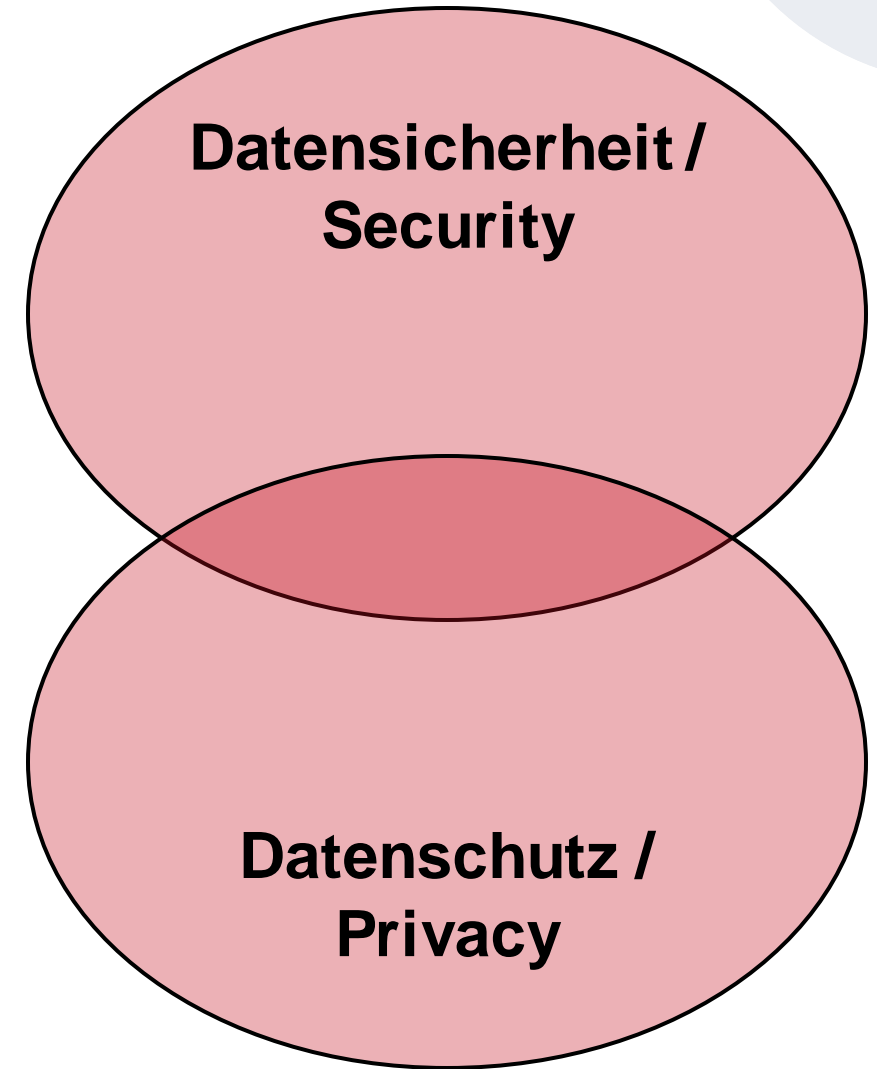
→ **Confidentiality** (Vertraulichkeit), **Integrity** (Integrität), **Availability** (Verfügbarkeit)  
→ **C-I-A**

# Sicherheit



# Datensicherheit / Datenschutz

- (Daten-) Sicherheit als eines von mehreren Kernprinzipien des Datenschutzes
- (Daten-) Sicherheit auch jenseits von Datenschutz auf vielfältige Weise relevant
- Ergo: Überschneidungen; Datenschutz und Datensicherheit sind weder deckungsgleich noch ist das Eine eine Untermenge des Anderen!





# 9 Kernprinzipien des Datenschutzes

Rechtmäßigkeit (incl. Einwilligung)

Zweckbindung

Datensparsamkeit (incl. Erforderlichkeit)

Transparenz

Richtigkeit

Sicherheit (insb. Vertraulichkeit, Integrität, Verfügbarkeit)

Verantwortlichkeit

„Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und **muss** dessen Einhaltung **nachweisen können**“

Art. 5(2) GDPR

„Der Verantwortliche setzt [...] geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den **Nachweis dafür erbringen zu können**, dass die Verarbeitung gemäß dieser Verordnung erfolgt.“

Art. 24(1) GDPR

Belegen von „Rechtsbruch“ → Belegen von Konformität  
(vgl. „Beweislastumkehr“)

## 9 Kernprinzipien des Datenschutzes

Rechtmäßigkeit (incl. Einwilligung)

Zweckbindung

Datensparsamkeit (incl. Erforderlichkeit)

Transparenz

Richtigkeit

Sicherheit (insb. Vertraulichkeit, Integrität, Verfügbarkeit)

Verantwortlichkeit (incl. nachweisbare Rechtskonformität)

**Kontrolle und Durchsetzung**

# Kontrolle und Durchsetzung

„Jeder Mitgliedstaat sieht vor, dass eine oder mehrere **unabhängige Behörden** für die Überwachung der Anwendung dieser Verordnung zuständig“

Art. 51(1) GDPR

„Der **Europäische Datenschutzausschuss** (im Folgenden „Ausschuss“) wird als Einrichtung der Union mit eigener Rechtspersönlichkeit eingerichtet. [...] [Er] besteht aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und [...]“

Art. 68 GDPR

# Kontrolle und Durchsetzung



→ Überwachen, fördern, Beschwerden entgegennehmen, ...,  
Ordnungsgelder verhängen

# Kontrolle und Durchsetzung

„Bei Verstößen [...] Geldbußen von **bis zu 20.000.000 EUR** / 10.000.000 EUR oder im Fall eines Unternehmens von **bis zu 4% / 2% seines gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.“

→ Abhängig vom Artikel, gegen den verstoßen wurde

Art. 83(2, 4, 5) GDPR

→ bis zu 4,6/2,3 Mrd USD für Meta (2023)

→ bis zu 20/10 (>10/5) Mio EUR für WBM 2023  
(60 / 30 Mio EUR für Deutsche Wohnen 2023)

# 9 Kernprinzipien des Datenschutzes

Rechtmäßigkeit (incl. Einwilligung)

Zweckbindung

Datensparsamkeit (incl. Erforderlichkeit)

Transparenz

Richtigkeit

Sicherheit (insb. Vertraulichkeit, Integrität, Verfügbarkeit)

Verantwortlichkeit (incl. nachweisbare Rechtskonformität)

Kontrolle und Durchsetzung

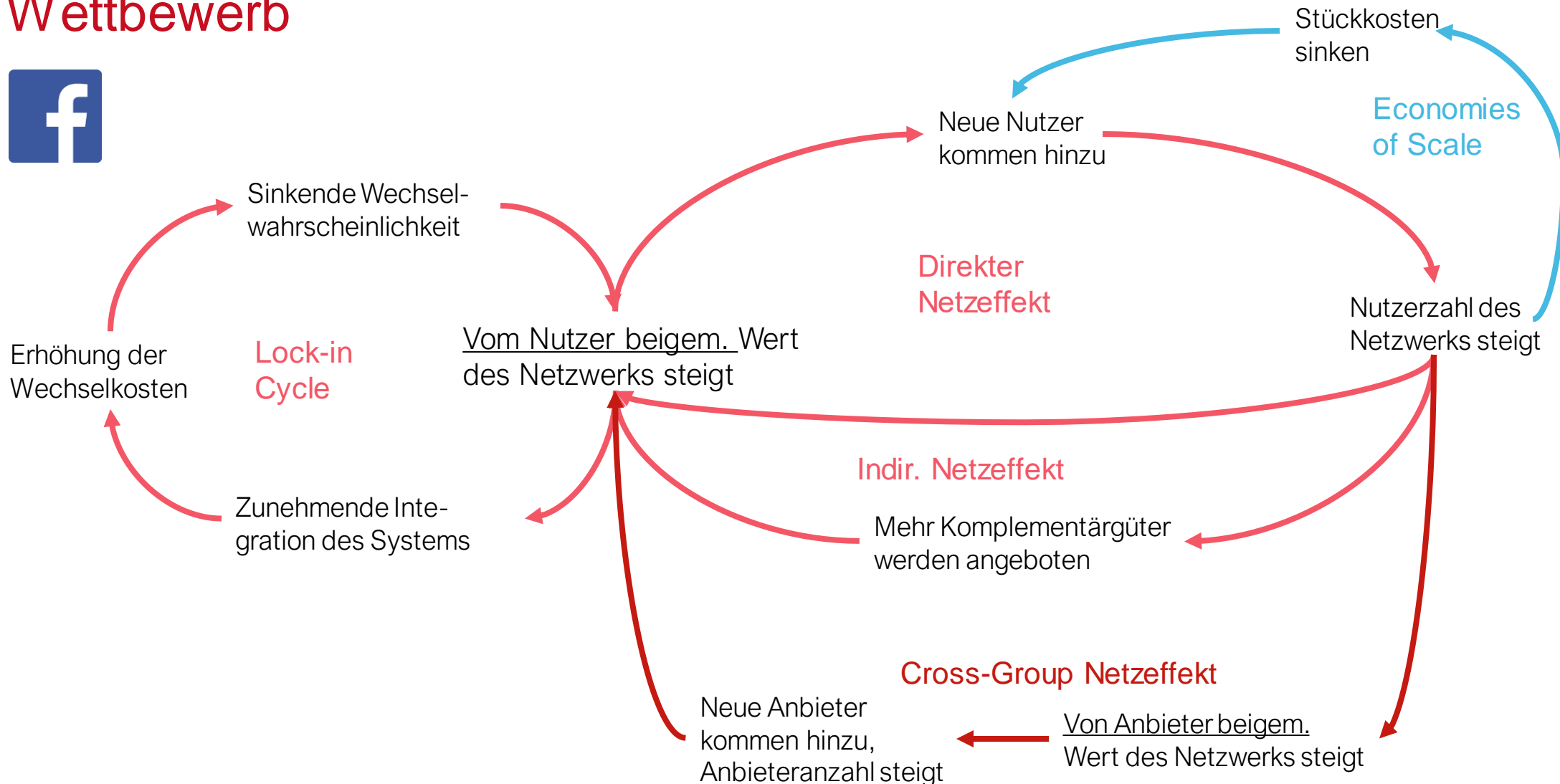
**Datenportabilität**

- „1) Die betroffene Person hat das Recht, **die sie betreffenden personenbezogenen Daten**, die sie einem Verantwortlichen bereitgestellt hat, **in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten**, und sie hat das **Recht, diese Daten** einem anderen Verantwortlichen [...] **zu übermitteln**, sofern [...]
- 2) die betroffene Person das **Recht, zu erwirken, dass die personenbezogenen Daten direkt** von einem Verantwortlichen einem anderen Verantwortlichen **übermittelt werden**, soweit dies technisch machbar ist.“

Art. 20 GDPR



# Datenportabilität – Im Kern nicht Datenschutz sondern Wettbewerb



# 9 Kernprinzipien des Datenschutzes

Rechtmäßigkeit (incl. Einwilligung)

Zweckbindung

Datensparsamkeit (incl. Erforderlichkeit)

Transparenz

Richtigkeit

Sicherheit (insb. Vertraulichkeit, Integrität, Verfügbarkeit)

Verantwortlichkeit (incl. nachweisbare Rechtskonformität)

Kontrolle und Durchsetzung

Datenportabilität

9 + 1 Kernprinzipien

→ nächste Lesson

	30.11.23	<p>Großübung „How to Poster“  <small>(ausnahmsweise in Präsenz)</small>  <b>(via Zoom)</b><sup>[Tutor:innen]</sup></p> <p>Gruppenkonsultation          Poster/Essay  <b>(via Zoom)</b></p>	<p>Großübung</p> <p>Gruppenindividuelle Betreuung  <small>(nach Absprache)</small> <sup>[Tutor:innen]</sup></p>
7	04.12.23	<p>Datenschutz 2: Privacy Engineering <sup>[FP]</sup>  <b>(in Präsenz)</b></p>	<ol style="list-style-type: none"> <li>1. 9+1 Prinzipien: „Privacy by Design“</li> <li>2. Technische Umsetzung von Datensparsamkeit (incl. <i>k</i>-anonymity etc.)</li> <li>3. „Wieviel Security ist angemessen?“, Experimente</li> <li>4. Praktische Beispiele für „Systems-Oriented Privacy Engineering“</li> </ol>

fin