1. Informationen zur Vorlesung

Termine, Literatur etc.

Terminübersicht

- 25.05.2018 - Vorlesung
- 01.06.2018 - Vorlesung
- 08.06.2018 - Vorlesung
- 15.06.2018 - Vorlesung
- 22.06.2018 - Vorlesung
- 06.07.2018 - Probeklausur
- Xx.08.2018 - Klausur

FAQ zu Vorlesung/Klausur: mitserv-dmz.fh-wedel.de:2121/Weiß

Kontakt zum Dozenten: weiss@gdd.de

Grobgliederung

- Rechtsgrundlagen und –systematik
- Zulässigkeit der Verarbeitung
- Transparenz
- Betroffenenrechte
- Aufsicht & Sanktionen
- Beschäftigtendatenschutz
- Zusammenarbeit mit Dienstleistern
- Werbung
- Videoüberwachung
- Technisch-organisatorische Maßnahmen

Literatur

- Recht allgemein
  - Engisch, Einführung in das juristische Denken, 11. Aufl. (*Bearbeiter: Würtenberger/Otto).*

- Kommentare Datenschutzrecht
  - Gola, DS-GVO
  - Kühling/Buchner, DS-GVO
  - Paal/Pauly, DS-GVO

- Einführungen Datenschutzrecht
  - BfDI, Info 6, 5. Aufl. 2017 (https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.html)
  - Schneider, Datenschutz nach der EU-Datenschutz-Grundverordnung
  - Kühling/Seidel/Sivridis, Datenschutzrecht, 3. Aufl.
  - Taeger, Datenschutzrecht
  - Gola/Reif, Praxisfälle Datenschutzrecht, 2. Aufl.

Gesetzestexte

Schwartmann / Jaspers (Hrsg.)

Datenschutzgrundverordnung und Bundesdatenschutzgesetz

Vorschriftensammlung

Inhaltsverzeichnis
Vorwort

Versandkostenfrei

lieferbar (3-5 Tage)

21,99 €
inkl. MwSt.

In den Warenkorb

Auf die Merkliste

Webcode: beck-shop.de/bvxalz

Ausgedruckte Gesetzestexte sind während der Klausur erlaubt. Zu finden auf dem Handoutserver /Weiß

2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.1 Die Rechtssystematik und -grundlagen

Recht und Rechtstaat

Artikel 20 Abs. 3 des Grundgesetzes:

„Die Gesetzgebung ist an die verfassungsmäßige Ordnung, die vollziehende Gewalt und die Rechtsprechung sind an Gesetz und Recht gebunden.“

- Der Gedanke, der hinter dem Rechtsstaatsprinzip steht, ist, dass die Ausübung aller staatlichen Gewalt umfassend an das Recht gebunden werden soll.

Vorschriften (Arten)

- Verfassung
- (formelle) Gesetze
- Rechtsverordnungen
- Satzungen
- Richtlinien
- Verwaltungsvorschriften
- Tarifverträge
- Betriebs- und Dienstvereinbarungen

Vorschriften (Bestandteile)

§ 4 BDSG – Videoüberwachung öffentlich zugänglicher Räume

(1) [1]Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. [2]Bei der Videoüberwachung von

1. öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-,
2. Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs

gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse.

(2) Der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind durch […]

Juristische Arbeitsmittel

- Gesetze
- Kommentare/Fachliteratur
- Gesetzgebungsmaterialien
- Gerichtsentscheidungen (Urteile & Beschlüsse)
- Behördenentscheidungen
- Juristische Methodik und Auslegungslehre

Meilensteine des Datenschutzrechts

- 1890 – „Right to privacy“ (Warren/Brandeis)
- 1970 – Erstes dt. Datenschutzgesetz in Hessen
- 1977 – Bundesdatenschutzgesetz
- 1978 – Erstes Datenschutzgrundrecht in NRW
- 1983 – Urteil Volkszählung
- 2004 – Urteil Großer Lauschangriff
- 2008 – Urteil Computergrundrecht
- 2010 – Urteil Vorratsdatenspeicherung
- 2016 – EU-Datenschutz-Grundverordnung

Charta der Grundrechte der Europäischen Union (GRCh)

Art. 7 - Achtung des Privat- und Familienlebens
Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Art. 8 - Schutz personenbezogener Daten
(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) [1]Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. [2]Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Informationelle Selbstbestimmung

- Grundrecht
- Unterfall des sog. „Allgemeinen Persönlichkeitsrechts“
- Zusammensetzung aus Art. 1 und 2 Grundgesetz (GG):

Art. 1 Abs. 1 S. 1 GG: Die Würde des Menschen ist unantastbar.
Art. 2 Abs. 1 GG: Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit […].

Volkszählung 1983

§ 2 Volkszählungsgesetz

Die Volkszählung und Berufszählung erfaßt:
1. Vornamen und Familiennamen, Anschrift, Telefonanschluß, Geschlecht, Geburtstag, Familienstand, rechtliche Zugehörigkeit oder Nichtzugehörigkeit zu einer Religionsgesellschaft, Staatsangehörigkeit;
2. Nutzung der Wohnung als alleinige Wohnung, Hauptwohnung oder Nebenwohnung (§ 12 Abs. 2 des Melderechtsrahmengesetzes);
3. Quelle des überwiegenden Lebensunterhaltes;
4. Beteiligung am Erwerbsleben, Eigenschaft als Hausfrau, Schüler, Student;
5. erlernten Beruf und Dauer der praktischen Berufsausbildung, höchsten Schulabschluß an allgemeinbildenden Schulen, höchsten Abschluß an einer berufsbildenden Schule oder Hochschule sowie Hauptfachrichtung des letzten Abschlusses;
6. bei Erwerbstätigen sowie Schülern und Studenten Namen und Anschrift der Arbeitsstätte oder Ausbildungsstätte, hauptsächlich benutztes Verkehrsmittel und Zeitaufwand für den Weg zur Arbeitsstätte oder Ausbildungsstätte; […]

Volkszählung 1983

§ 3 Volkszählungsgesetz

(1) Die gebäudestatistischen Fragen erfassen bei Gebäuden mit Wohnraum und bei ständig bewohnten Unterkünften Anschrift, Art und Baujahr sowie den Eigentümer oder an seiner Stelle den Nießbrauchberechtigten oder denjenigen, der Anspruch auf Übereignung oder auf Einräumung oder Übertragung eines Erbbaurechts oder Nießbrauchs hat.
(2) Die wohnungsstatistischen Fragen erfassen:
1. Art, Größe, Ausstattung und Verwendungszweck, Art der Beheizung und der Heizenergie sowie Bezugsjahr der Wohnung, Wohnverhältnis, Förderung der Wohnung mit Mitteln des sozialen Wohnungsbaus sowie Zahl und Nutzung der Räume;
2. bei vermieteten Wohnungen außerdem die Höhe der monatlichen Miete;
3. bei leerstehenden Wohnungen außerdem die Dauer des Leerstehens.
[...]

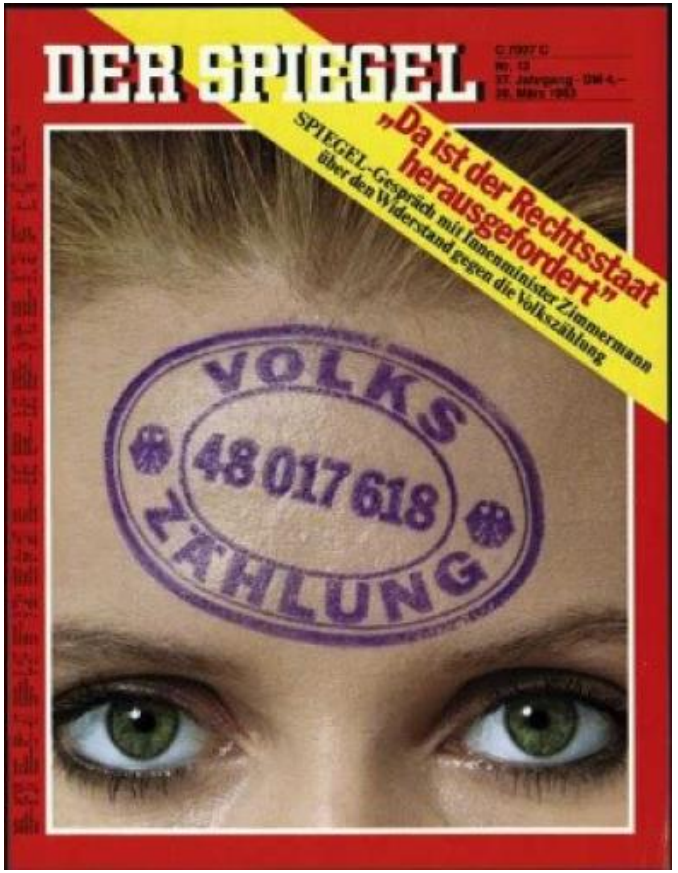
Volkszählung 1983

§ 4 Volkszählungsgesetz:

Die Arbeitsstättenzählung erfaßt:
1. bei allen nichtlandwirtschaftlichen Arbeitsstätten und Unternehmen
a) Namen, Bezeichnung, Anschrift, Telefonanschluß und Zahl der Sprechstellen, Art der Niederlassung, Art der ausgeübten Tätigkeit oder Art des Aufgabengebietes der Arbeitsstätte und des Unternehmens, Eröffnungsjahr, Angaben über Neuerrichtung oder Standortverlagerung, Träger der Arbeitsstätte bei Anstalten, Einrichtungen von Behörden oder der Sozialversicherung sowie von Kirchen, Verbänden oder sonstigen Organisationen,
b) Zahl der tätigen Personen nach Geschlecht, Stellung im Betrieb, Zahl der Teilzeitbeschäftigten sowie Zahl der ausländischen Arbeitnehmer nach Geschlecht,
c) Summe der Bruttolöhne und Bruttogehälter des vorhergehenden Kalenderjahres;
2. bei Hauptniederlassungen und einzigen Niederlassungen außerdem
a) Eintragung des Unternehmens in die Handwerksrolle,
b) Rechtsform des Unternehmens;
3. bei Hauptniederlassungen zusätzlich zu den Angaben nach den Nummern 1 und 2 für jede Zweigniederlassung
a) Namen, Bezeichnung, Anschrift, Art der ausgeübten Tätigkeit oder des Aufgabengebietes, […]

Volkszählungsurteil

Bundesverfassungsgericht:
„Die durch dieses Gesetz angeordnete Datenerhebung hat Beunruhigung auch in solchen Teilen der Bevölkerung ausgelöst, die als loyale Staatsbürger das Recht und die Pflicht des Staates respektieren, die für rationales und planvolles staatliches Handeln erforderlichen Informationen zu beschaffen.“



„Volkszählungsurteil“
des Bundesverfassungsgerichts vom 15.12.1983

„Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe von dem allgemeinen Persönlichkeits-recht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. ***Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“***

➔ **Recht auf informationelle Selbstbestimmung**

➔ **Zweites Bundesdatenschutzgesetz vom 20. Dezember 1990**

Richtlinie 95/46/EG
des Europäischen Parlaments und des Rates
zum Schutz natürlicher Personen bei der
Verarbeitung personenbezogener Daten und zum freien
Datenverkehr vom 24. Oktober 1995

Drittes Bundesdatenschutzgesetz vom 22. Mai 2001

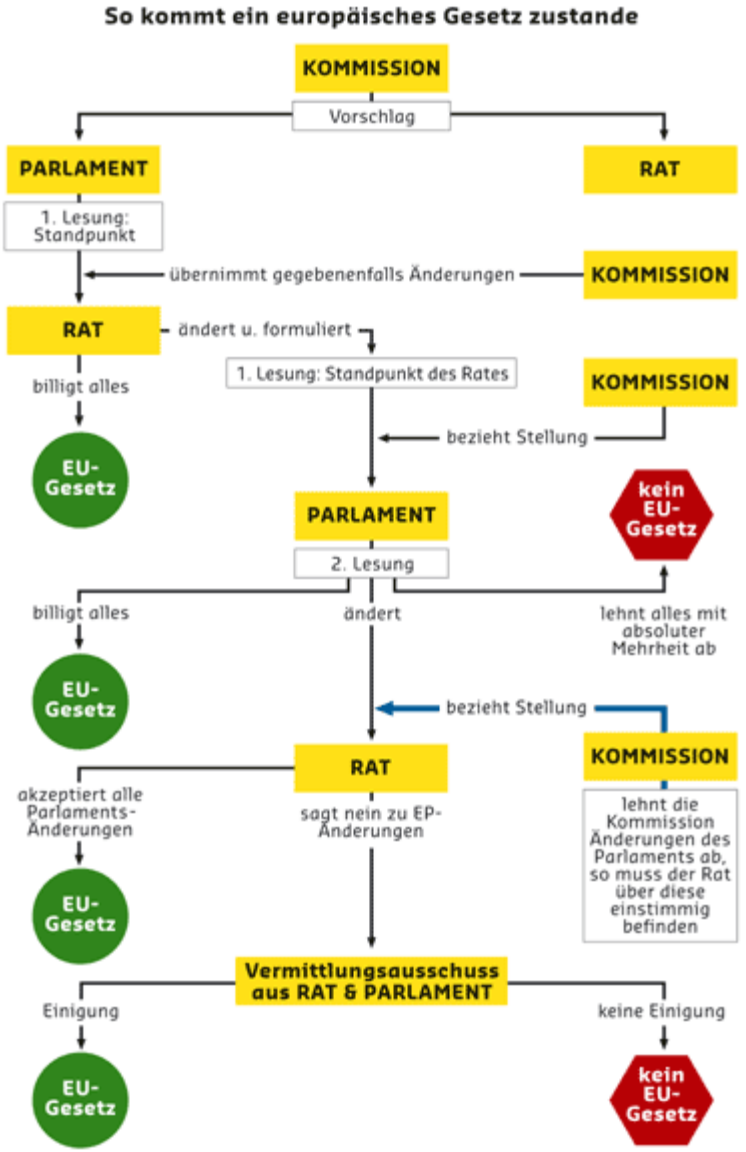
Aufgrund der Datenschutzskandale: Gravierende Änderungen des Bundesdatenschutzgesetzes überwiegend mit Wirkung vom 1. September 2009; Ergänzung um ein Beschäftigtendatenschutzgesetz zunächst ausgesetzt

25.05.2018: Anwendung der EU-Datenschutz-Grundverordnung

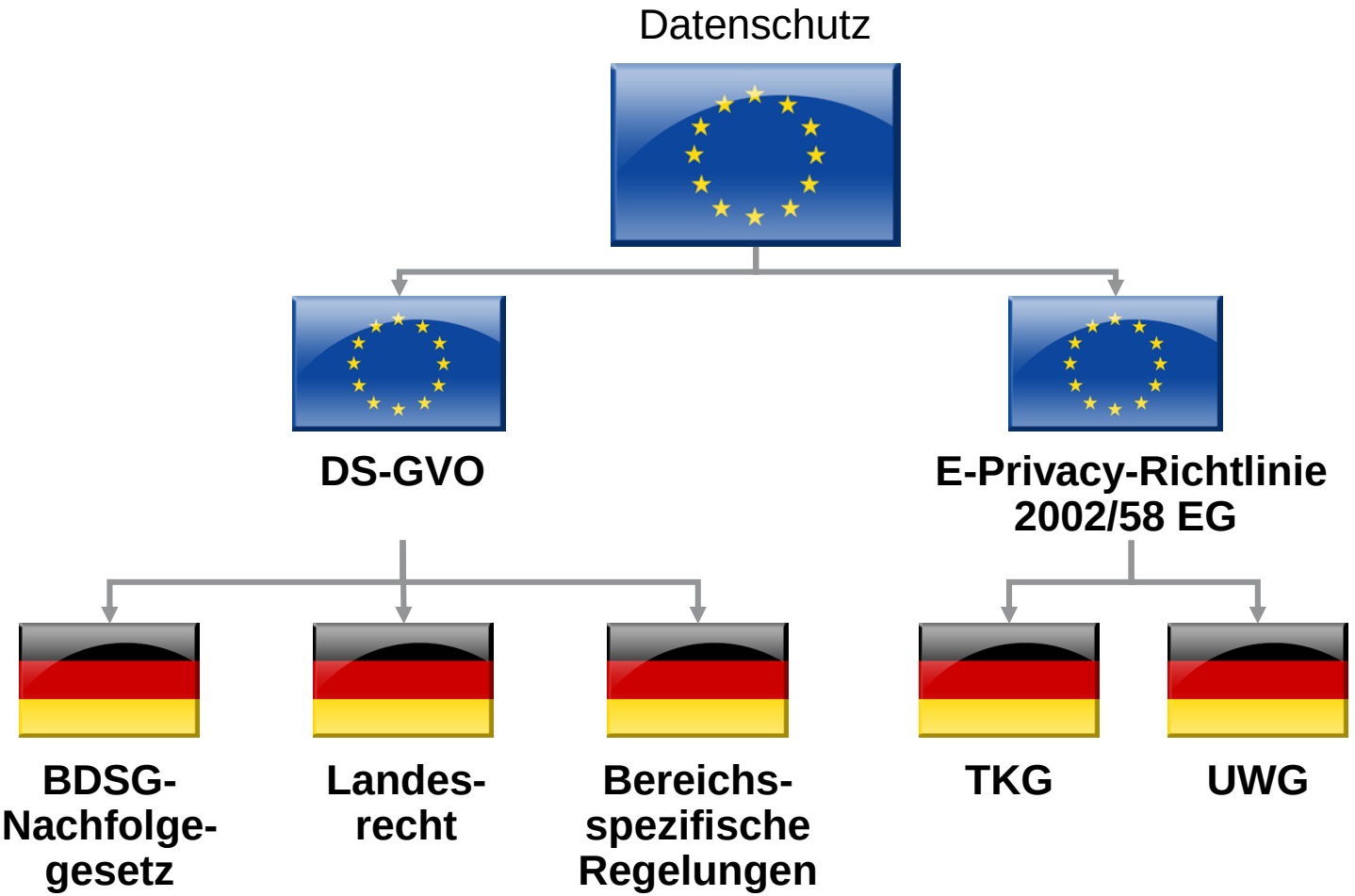
Nach Art. 99 DSGVO:
„ … Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedsstaat.“

- Die DSGVO ist eine allgemeine Regelung mit unmittelbarer innerstaatlicher Geltung
  -> **„Durchgriffswirkung“**
- Grundsätzliche Vollharmonisierung im nicht-öffentlichen Bereich
- Ersetzt nationales Datenschutzrecht, führt grds. zur Unanwendbarkeit entgegenstehender nationaler Regelungen
- Öffnungsklauseln für nationalen Gesetzgeber in bestimmten Bereichen – Richtlinien-Charakter im öffentlichen Bereich
  - Zweijährige Anpassungsphase für Rechtsbereinigung und Folgeänderungen

Wie kommt ein europäisches Gesetz zustande?



Der Datenschutz ab dem 25.05.2018



Bereichsübergreifende Regelungen:

- EU-Datenschutz-Grundverordnung (DS-GVO)
- Bundesdatenschutzgesetz (BDSG)
- Landesdatenschutzgesetze (LDSG)
- Kirchliche Datenschutzgesetze (DSG-EKD; KDO)

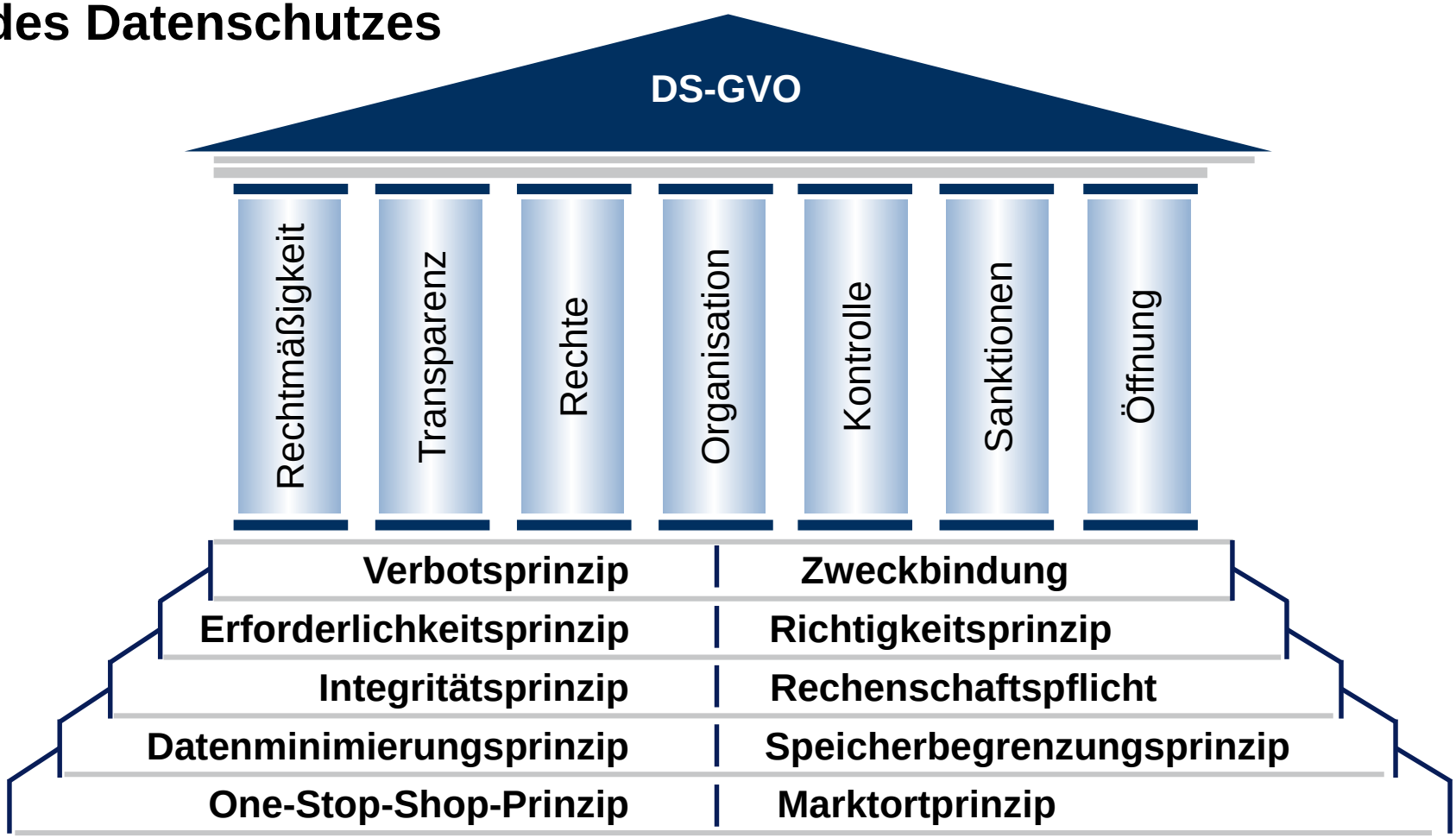
Bereichsspezifische Regelungen:

- **Bundesgesetze**, z.B.
  - Sozialgesetzbuch, insbesondere SGB I und X
  - Betriebsverfassungsgesetz (BetrVG)
  - Abgabenordnung (AO)
  - Gesetz über den unlauteren Wettbewerb (UWG)
  - Urheberrechtsgesetz (UrhG)
  - Strafgesetzbuch (StGB)
  - Telekommunikationsgesetz (TKG)
  - Telemediengesetz (TMG)

Aufbau der DS-GVO

	Art.	EG
Kapitel I: Allgemeine Bestimmungen	1 – 4	1 – 37
Kapitel II: Grundsätze	5 – 10	38 – 57
Kapitel III: Rechte der betroffenen Person	12 – 23	**58** – 73
Kapitel IV: Verantwortlicher und Auftragsverarbeiter	24 – 43	74 – 100
Kapitel V: Übermittlung pb Daten an Drittländer oder an int. Organisatio	44 – 50	101 – 116
Kapitel VI: Unabhängige Aufsichtsbehörden	51 – 59	117 – **129**
Kapitel VII: Zusammenarbeit und Kohärenz	60 – 76	**130** – 140
Kapitel VIII: Rechtsbehelfe, Haftung und Sanktionen	77 – **84**	141 – 152
Kapitel IX: Vorschriften für besondere Datenverarbeitungssituationen	85 – **91**	153 – 165
Kapitel X: Delegierte Rechtsakte und Durchführungsrechtsakte	92 – 93	166 – 170
Kapitel XI: Schlussbestimmungen	**94** – 99	171 – 173

Grundprinzipien des Datenschutzes



Lehrveranstaltung Datenschutz

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	▪ Verarbeitung auf rechtmäßige Weise ▪ nach dem Grundsatz von Treu und Glauben ▪ in einer für den Betroffenen nachvollziehbaren Weise
Zweckbindung	▪ Erhebung für festgelegte, eindeutige und rechtmäßige Zwecke ▪ Verbot der Weiterverarbeitung in einer mit diesen Zwecken nicht zu vereinbarenden Weise
Datenminimierung	▪ Beschränkung auf das für den Zweck der Verarbeitung angemessene und sachlich relevante sowie notwendige Maß
Richtigkeit	▪ sachlich richtige und ggf. aktuellste Daten, ▪ Vorsehen von Maßnahmen zur unverzüglichen Löschung oder Berichtigung von unzutreffenden Daten
Speicherbe-grenzung	▪ Speicherung mit Personenbezug höchstens so lange, wie es für die Verarbeitungszwecke erforderlich ist
Integrität und Vertraulichkeit	▪ geeignete TOM zum angemessenen Schutz der Daten insbes. vor unbefugter oder unrechtmäßiger Verarbeitung, zufälligem Verlust, zufälliger Zerstörung oder Schädigung

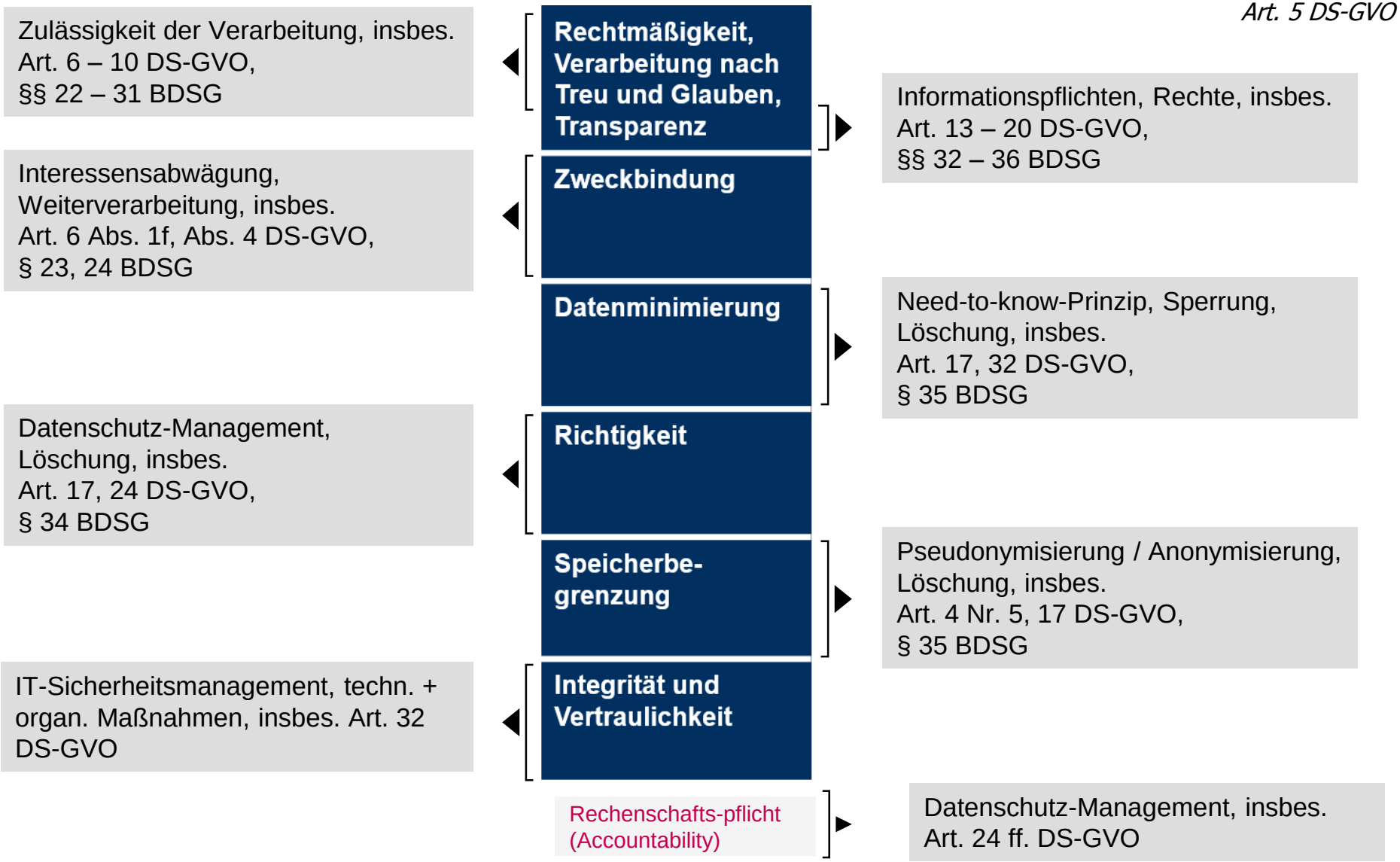
Rechenschafts-pflicht (Account-ability):

- **Verantwortung und**
- **Nachweis-pflicht**

für die Einhaltung dieser Prinzipien

Lehrveranstaltung Datenschutz

Art. 5 DS-GVO



2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO

2.2.1 Die wichtigsten Begriffe

Lehrveranstaltung Datenschutz

Sachliche Anwendbarkeit DS-GVO

Anwendung der DS-GVO

Personenbezogene Daten
= jede Information über natürliche Personen

+

Automatisierte oder für beziehungsweise in einem Dateisystem erfolgende Verarbeitung

Ausnahmen bei Verarbeitung durch

Natürliche Personen
Verarbeitung ausschließlich für persönliche und familiäre Zwecke

Öffentliche Stellen
zum Beispiel Datenverarbeitung durch Sicherheitsbehörden, Organe der EU (aber: spezielle gesetzliche Regelungen)

Lehrveranstaltung Datenschutz

Artikel 4 Nr. 1 DS-GVO

Personenbezogene Daten:

alle Informationen über

- eine identifizierte oder identifizierbare
- natürliche Person

Lehrveranstaltung Datenschutz

Artikel 4 Nr. 1 DS-GVO

Person ist direkt zu identifizieren ⟷ **Person ist indirekt zu identifizieren, insbes. mittels Zuordnung zu**

einer Kennung wie:

- einem Namen,
- einer Kennnummer,
- Standortdaten,
- einer Online-Kennung

einem oder mehreren besonderen Merkmalen

die Ausdruck sind der

- physischen,
- physiologischen,
- genetischen,
- psychischen,
- wirtschaftlichen,
- kulturellen oder
- sozialen

Identität dieser natürlichen Person

Lehrveranstaltung Datenschutz

personenbezogene Daten

Artikel 4 Nr. 1 DS-GVO

pseudonyme Daten

Artikel 4 Nr. 5 DS-GVO

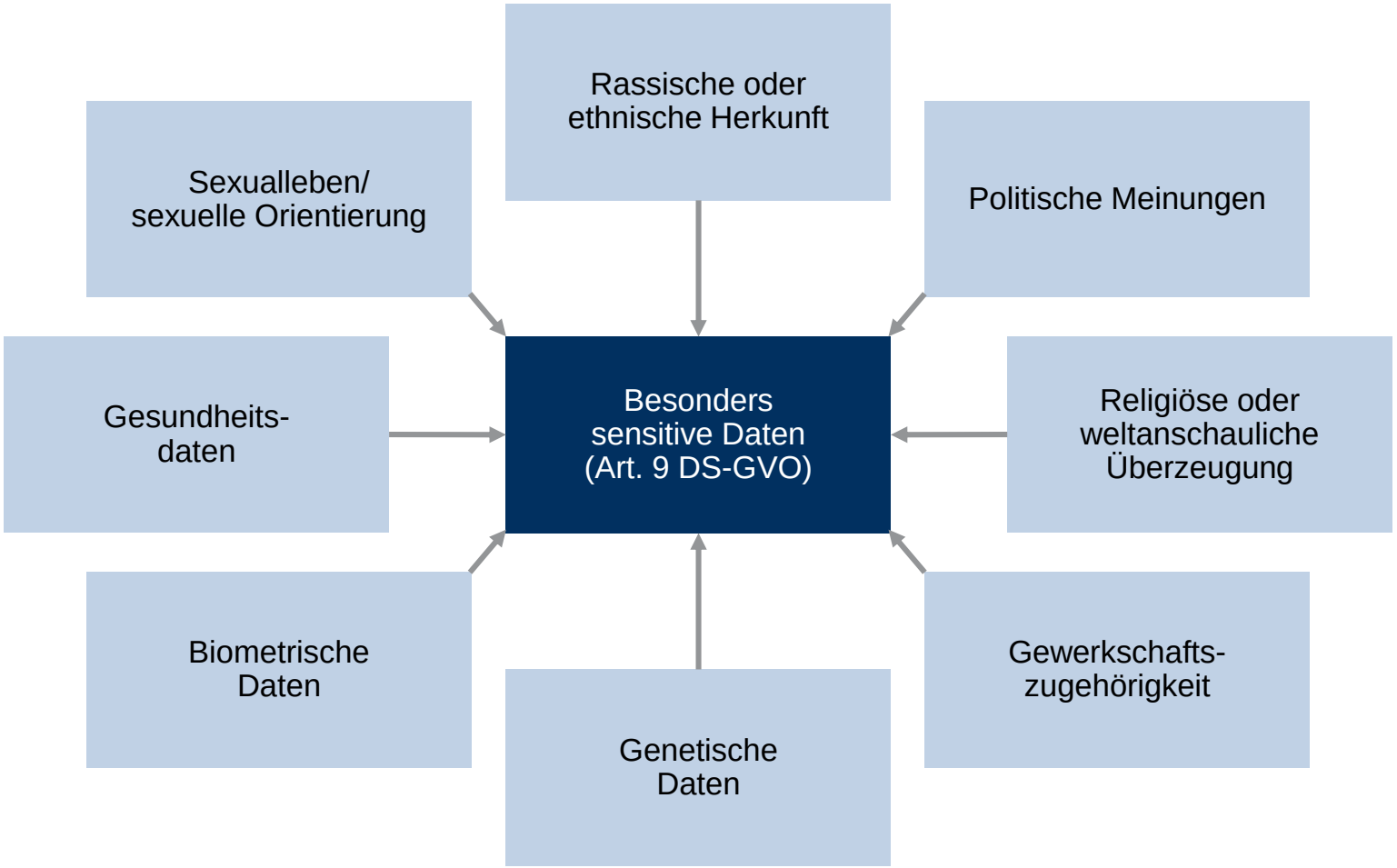
anonyme Daten

EG 26 DS-GVO

sonstige Daten

Lehrveranstaltung Datenschutz

(Art. 9 DS-GVO)



Lehrveranstaltung Datenschutz

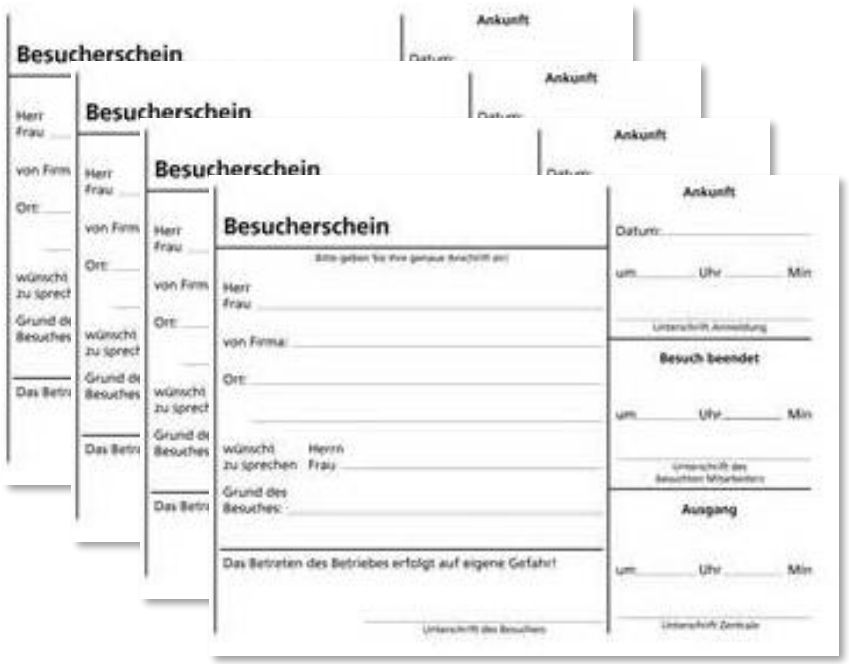
Art. 2 Abs. 1, Art. 4 Nr. 2 DS-GVO

(Automatisierte) Verarbeitung ist

- **jeder Vorgang oder jede Vorgangsreihe (Umgang)**
- **mit personenbezogenen Daten**
- **mit oder ohne Hilfe automatisierter Verfahren**

Lehrveranstaltung Datenschutz

Artikel 4 Nr. 6 DS-GVO



- Strukturierter Aufbau
- Nach bestimmten Kriterien zugänglich
- Auswertbar
- Unabhängig von ihrer Führung

Räumliche Anwendbarkeit DS-GVO

Jede sich in der EU aufhaltende natürliche Person genießt Schutz vor Verarbeitungen ihrer personenbezogenen Daten durch Verantwortliche und Auftragnehmer, die …

… von der EU aus agieren

… von außerhalb der EU agieren und Personen in der EU
- Dienstleistungen anbieten
- in ihrem Verhalten beobachten

Die Folgen

GDPR bad news =/ Posteingang x

Christian at DBinbox [redacted]bbestellen
an Steffen

Englisch › Deutsch Nachricht übersetzen

Hi! You probably haven't heard from me in a while. I'm Christian - I made a service you signed up for called DBinbox.com that makes it easy to receive files.

I've got some sad news for you if you're a DBinbox customer in the EU, or if you use DBinbox to receive files from people in the EU: you can't use DBinbox after this Friday :(

Why? GDPR is impossible for me to comply with as a small business. Small as in: DBInbox is run entirely by me and my girlfriend.

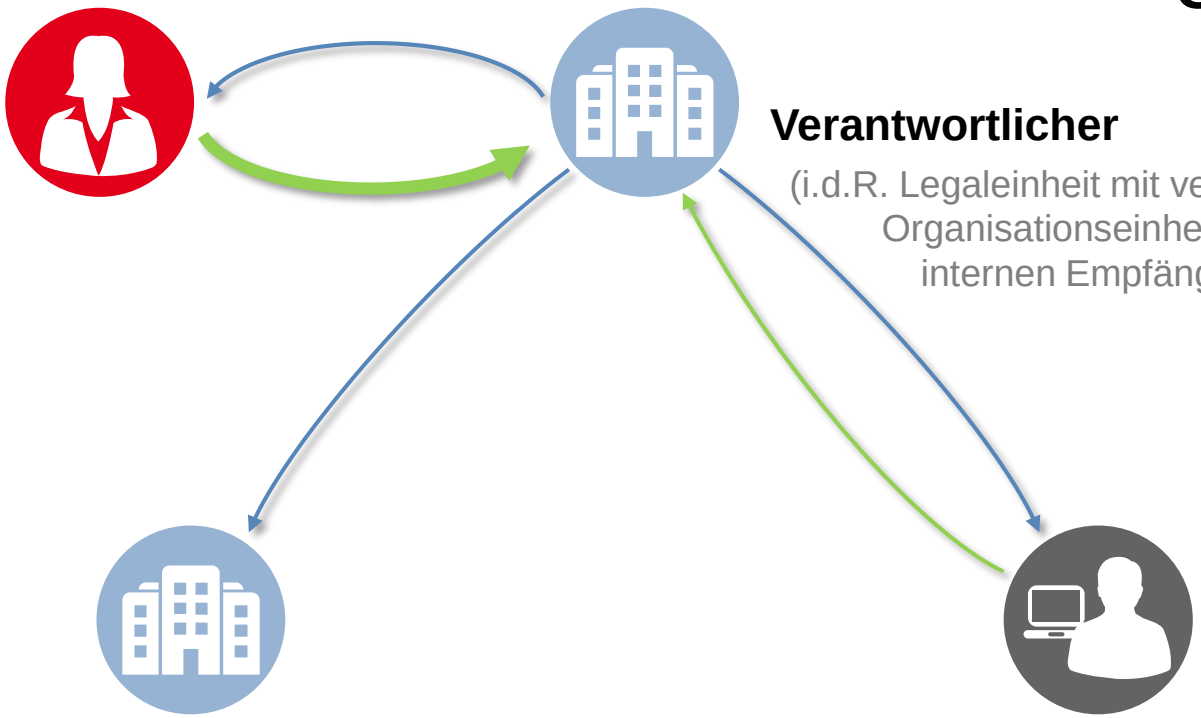
Am I totally anti-privacy and trying to be the next Zuckerberg selling all of your data? Man, absolutely not. Your privacy is super important, and it makes me physically angry when I hear about poorly-built websites leaking passwords.

Here are some great things I think every web service should be doing that GDPR enforces (from the GDPR Compliance Checklist):

Here's some things GDPR requires that I can't do:

- Appoint a representative within the EU - "If you have a business outside of the EU and you collect data on EU citizer accountant - I can't financially justify hiring another professional just to handle GDPR stuff.
- Accept a $20M euro penalty if I can't prove that my users didn't consent to my GDPR compliant privacy policy.
- Be able to prove who has ever seen any of the data I collect.

Beteiligte in der DS-GVO



Verantwortlicher

(i.d.R. Legaleinheit mit verschiedenen Organisationseinheiten als internen Empfängern)

Dritter

(Empfänger außerhalb des Verantwortlichen, außer betroffene Person)

Auftragsverarbeiter

(Fiktion: Empfänger innerhalb der verantwortlichen Stelle)

Lehrveranstaltung Datenschutz

„Verantwortlicher“:
Stelle, die
- allein oder
- gemeinsam mit anderen

über die
- Zwecke und
- Mittel

der Verarbeitung entscheidet

Art. 4 Nr. 7 DS-GVO

„Empfänger“:
Stelle,
- der personenbezogene Daten offengelegt werden,
- unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht

Art. 4 Nr. 9 DS-GVO

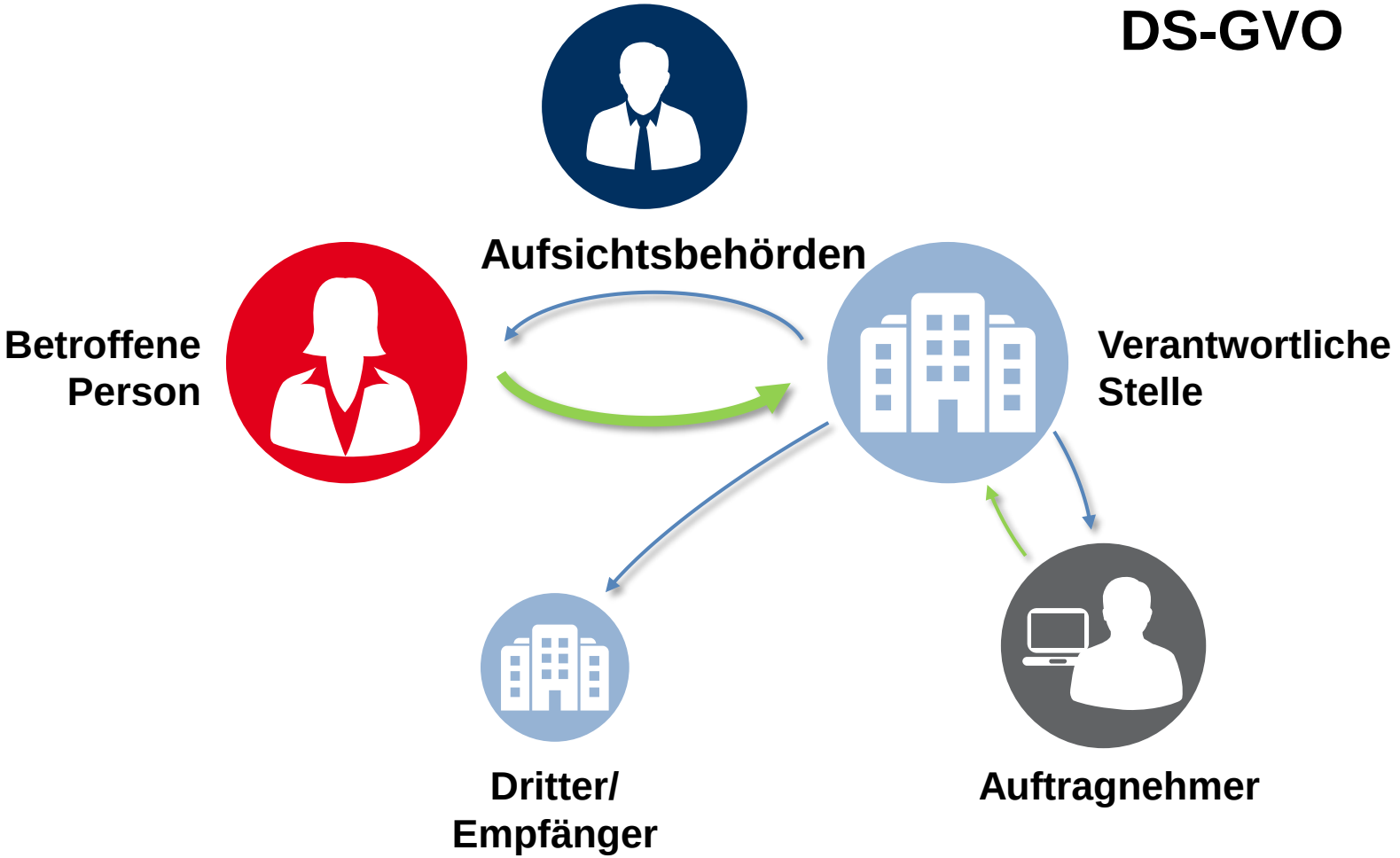
„Dritter“:
Stelle außer
- der betroffenen Person,
- dem Verantwortlichen,
- dem Auftragsverarbeiter

Art. 4 Nr. 10 DS-GVO

„Auftragsverarbeiter“:
Stelle,
die personenbezogene Daten
im Auftrag
des Verantwortlichen verarbeitet

Art. 4 Nr. 8 DS-GVO

Akteure der DS-GVO



2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO

2.2.2 Zulässigkeit der Verarbeitung

Lehrveranstaltung Datenschutz

Art. 6 DS-GVO

DAS DATENSCHUTZRECHT verbietet grundsätzlich den Umgang mit personenbezogenen Daten, erlaubt diese aber unter bestimmten Voraussetzungen (Verbot mit Erlaubnisvorbehalt).

DATENUMGANG ist nur zulässig, wenn er ...

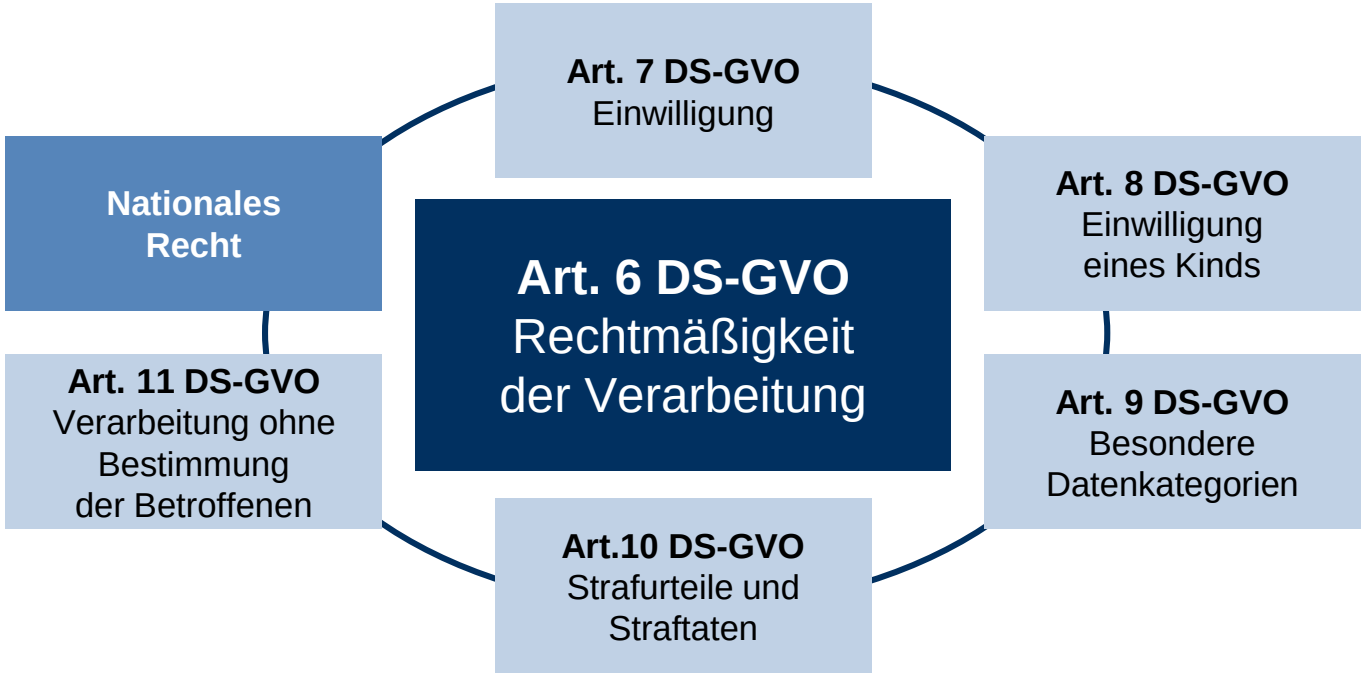
durch das Datenschutzrecht (DS-GVO, BDSG) selbst ...
Beispiel: Zur Durchführung eines Vertrages

oder durch eine besondere Rechtsvorschrift ...
Beispiel: Steuern, Abgaben

oder durch die Einwilligung des Betroffenen ...
Beispiel: Einverständniserklärung zur Datennutzung

... erlaubt und dem Betroffenen transparent gemacht wird.

Zulässigkeit der Verarbeitung



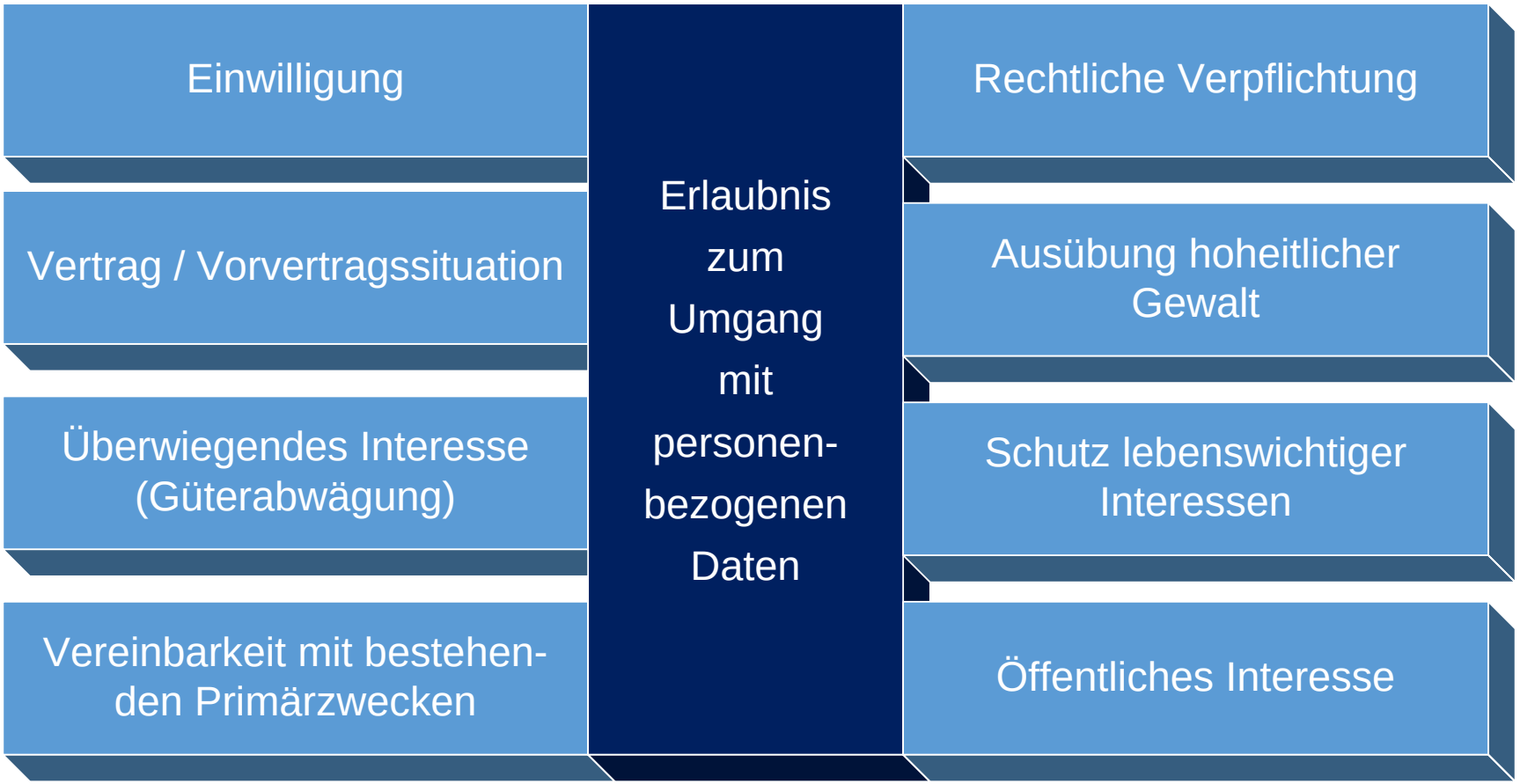
Ergänzende Zulässigkeitsanforderung

Art. 23 DS-GVO
Automatisierte Einzelentscheidung

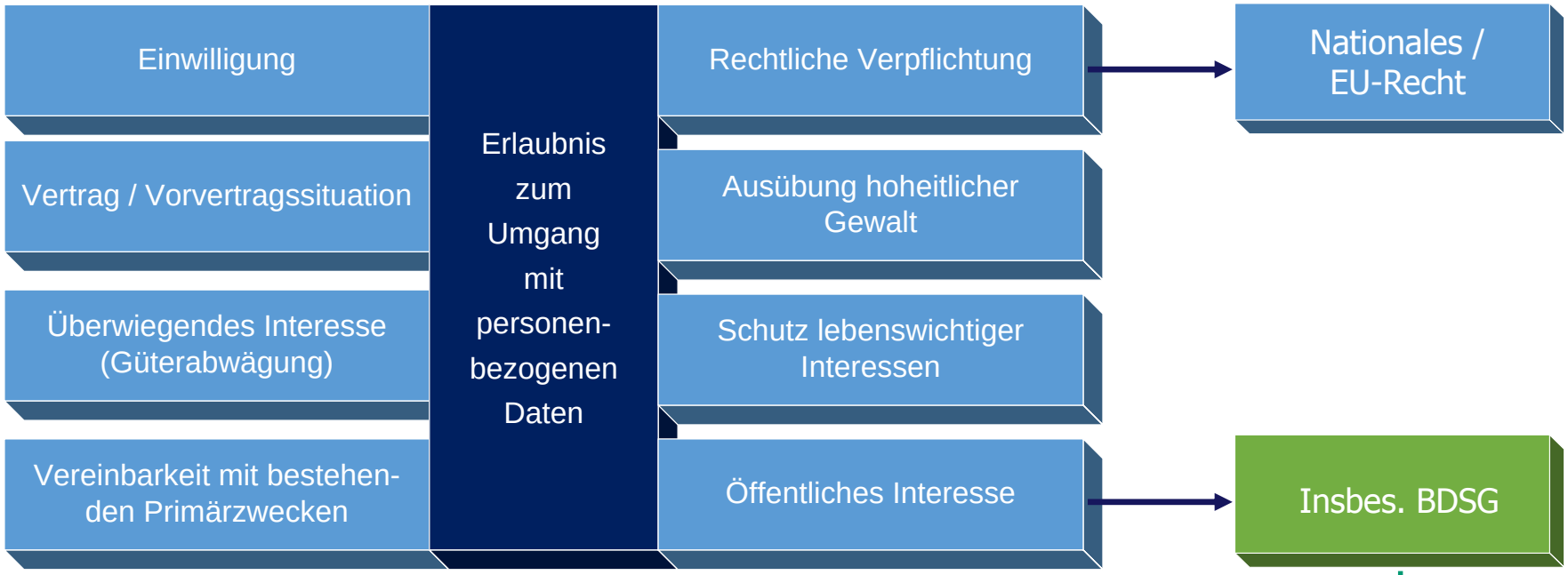
Art. 44 ff. DS-GVO
Übermittlung in Drittländer

Zulässigkeit der Verarbeitung

Art. 6 DS-GVO



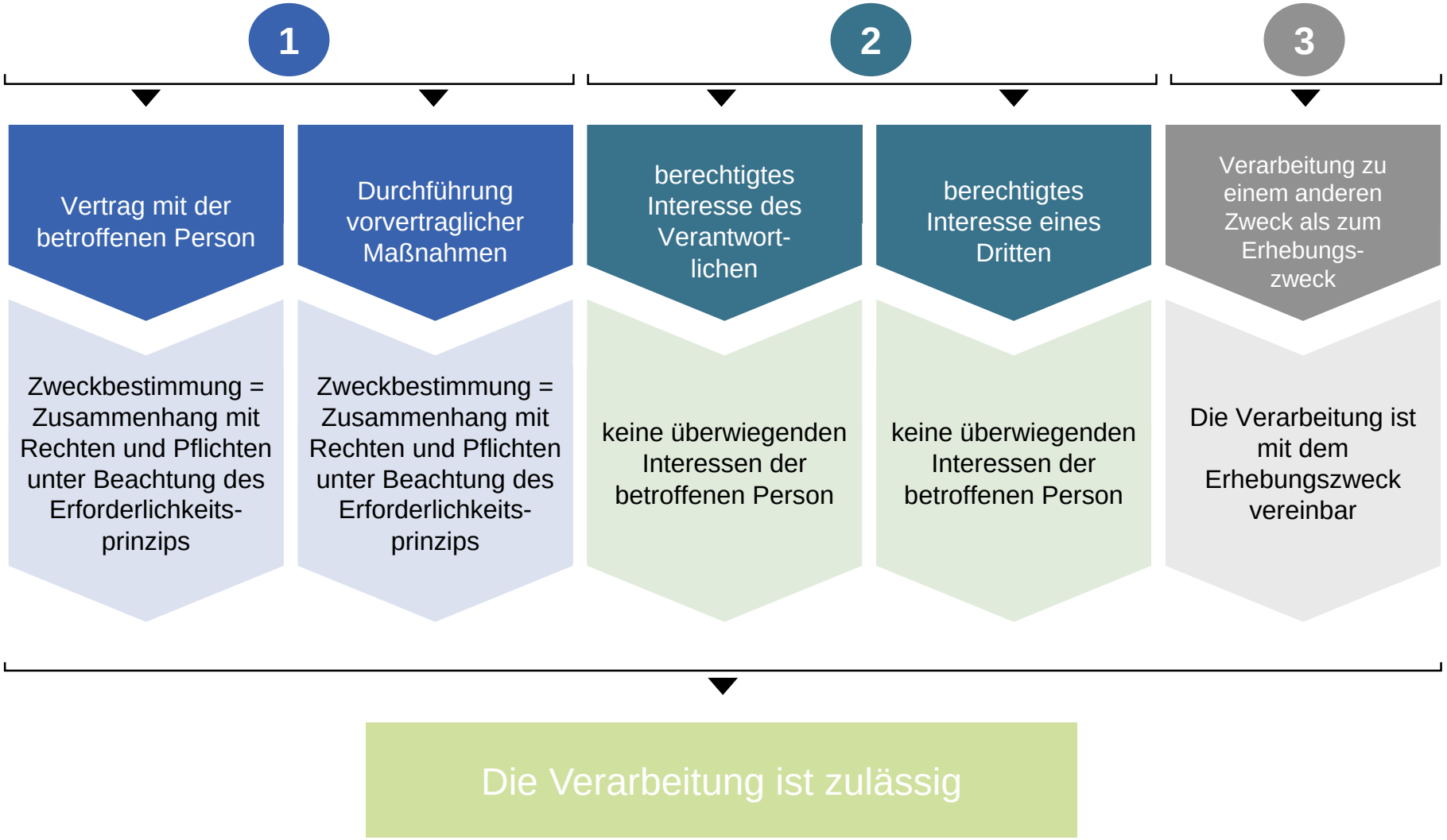
Zulässigkeit der Verarbeitung



- Verarbeitung zu anderen Zwecken
- Verarbeitung im Beschäftigungskontext
- Geheimhaltungspflichtige Daten
- Videoüberwachung

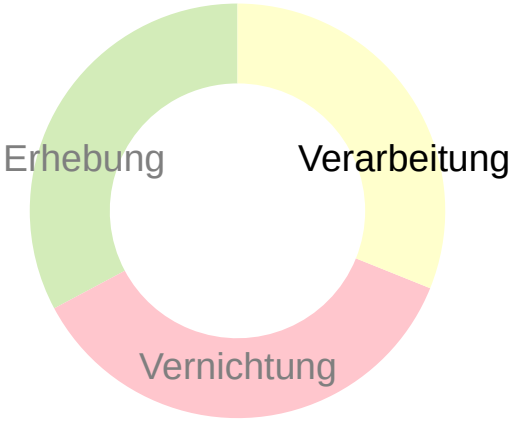
- Datenübermittlung an Auskunfteien
- Scoring
- Verbraucherkredite
- Forschungszwecke

Lehrveranstaltung Datenschutz



Vertrag/vorvertragliche Maßnahmen

Art. 6 Abs. 1 (b) DS-GVO



Vertrag mit der betroffenen Person

Verarbeitung ist **erforderlich**

- für die **Erfüllung** eines Vertrags
- **Vertragspartei die betroffene Person** ist

Durchführung vorvertraglicher Maßnahmen

Verarbeitung ist **erforderlich**

- zur Durchführung **vorvertraglicher Maßnahmen**
- auf **Antrag** der betroffenen Person

Zwischenfall: Onlineshopping

Ihr Unternehmen betreibt einen Webshop.
Bei der Bestellung werden Vorname, Nachname, Geburtsdatum, Adresse, Telefonnummer und Kontodaten erfragt.
Ist dies zur Vertragsabwicklung zu rechtfertigen?

Lösungsskizze

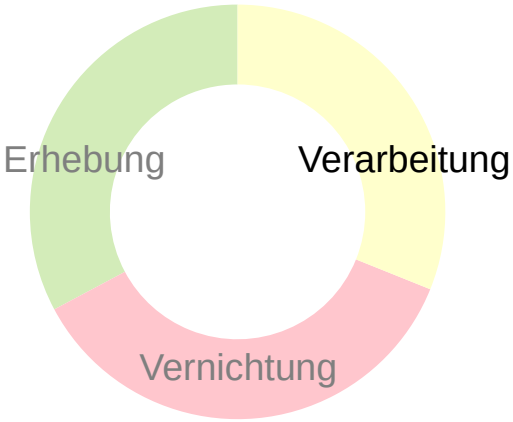
Fragestellung: Ist die Datenverarbeitung rechtmäßig im Sinne von Art. 5 Abs. 1 lit. a DS-GVO?

- Anwendbarkeit der DS-GVO (+), Art. 2 Abs. 1 DS-GVO: ganz oder teilweise automatisierte Verarbeitung. Keine private/familiäre Tätigkeit im Sinne von Art. 2 Abs. 2 lit. c DS-GVO.
  - Personenbezug (+), Art. 4 Nr. 1 DS-GVO
  - Verarbeitung (+), Art. 4 Nr. 2 DS-GVO: Erheben, Speichern
- Rechtmäßigkeit nach Art. 6 Abs. 1 lit. b DS-GVO?
  - die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen“
    - Vorname, Nachname, Adresse (+): Lieferung
    - Kontodaten (+): bei Lastschriftmandat
    - Geburtsdatum?
    - Telefonnummer?

ERGEBNIS: Datenverarbeitung dürfte gemäß Art. 6 Abs. 1 lit. b DS-GVO nur zum Teil **rechtmäßig** sein.

Interessensabwägung

Art. 6 Abs.1 (f) DS-GVO



berechtigtes Interesse des Verantwort-lichen

berechtigtes Interesse eines Dritten

Verarbeitung ist **erforderlich**

- zur Wahrung der **berechtigten Interessen** des Verantwortlichen oder eines Dritten

und

- keine überwiegende **Interessen** oder überwiegende **Grundrechte und Grundfreiheiten** der betroffenen Person, die den Schutz personenbezogener Daten erfordern

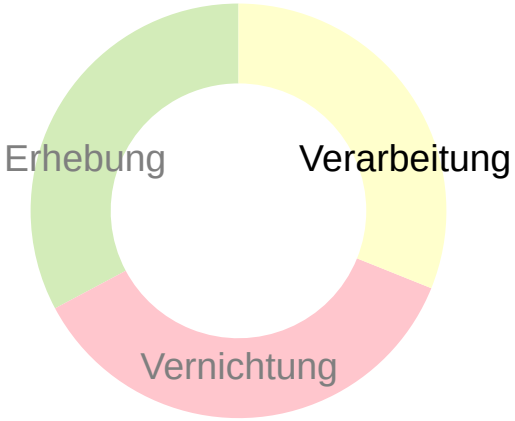
Interessensabwägung

Abwägungskriterien z. B.

- Berücksichtigung der „vernünftigen Erwartungen“ des Betroffenen, „Verbrauchersicht“ (EG 47)
- Konzerninteressen können einbezogen werden (EG 48)

Kompatible Verarbeitung

Art. 6 Abs. 4 DS-GVO



Kompatible Weiterverarbeitung

personenbezogene Daten müssen

- für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und
- dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden

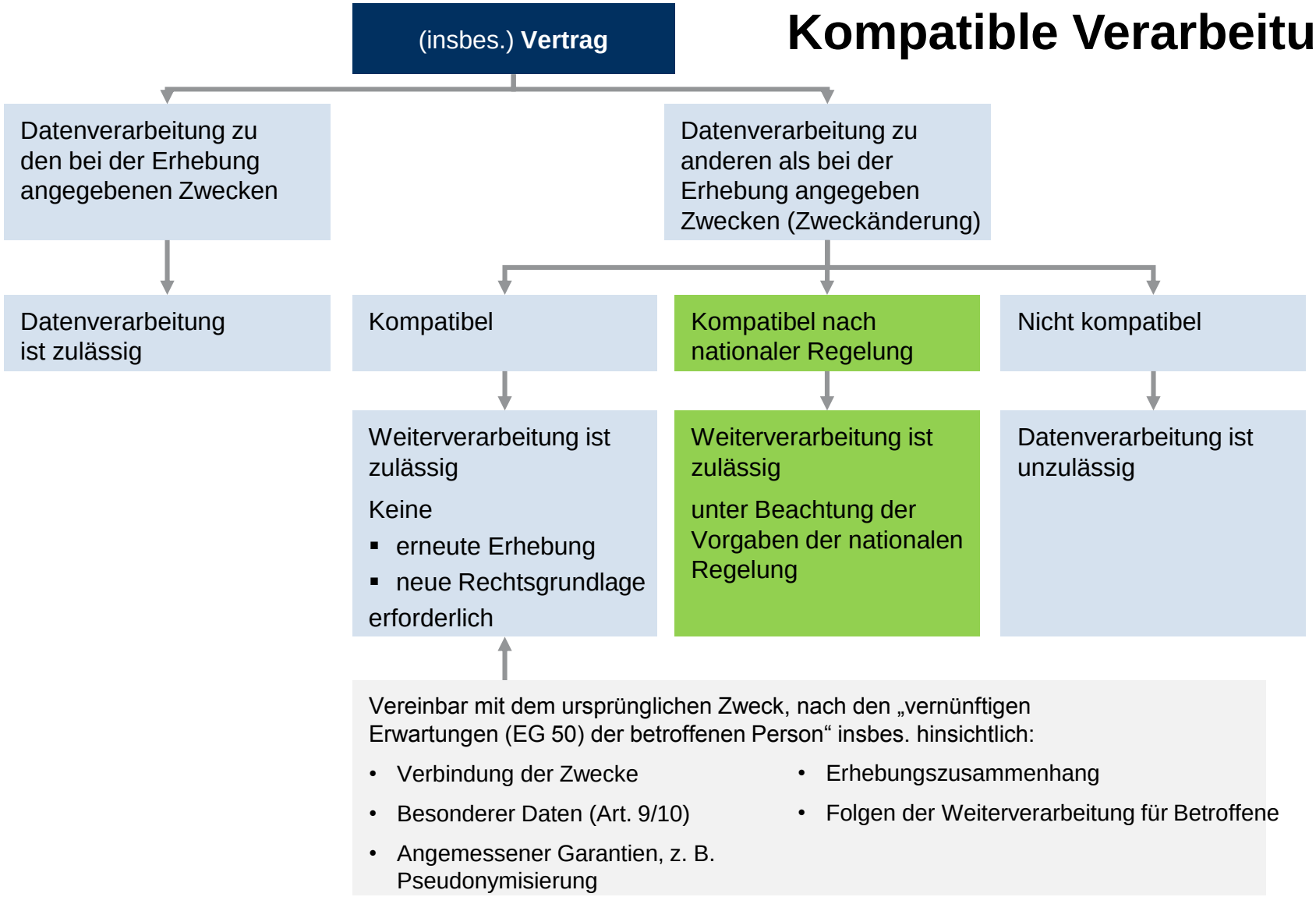
Art. 5 Abs. 1 (b) DS-GVO

Verarbeitung zu einem **anderen Zweck** als zum Erhebungszweck

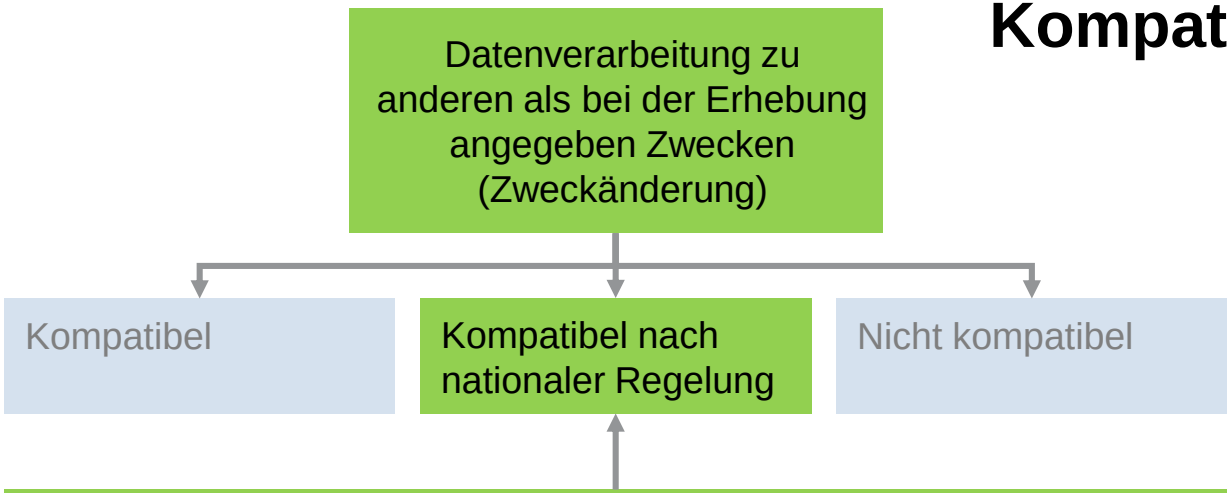
Verarbeitung ist mit dem **Erhebungszweck vereinbar** unter Berücksichtigung insbes. folgender Aspekte:

- **Verbindung** zwischen den Erhebungszwecken und der Weiterverarbeitung,
- **Erhebungszusammenhang**,
- die **Art** der personenbezogenen Daten (s. insbes. Art. 9, 10 DS-GVO),
- möglichen **Folgen** für die betroffenen Personen,
- geeignete **Garantien**, insbes. Verschlüsselung oder Pseudonymisierung

Kompatible Verarbeitung



Kompatible Verarbeitung



Art. 6 Abs. 4 DS-GVO, § 24 BDSG

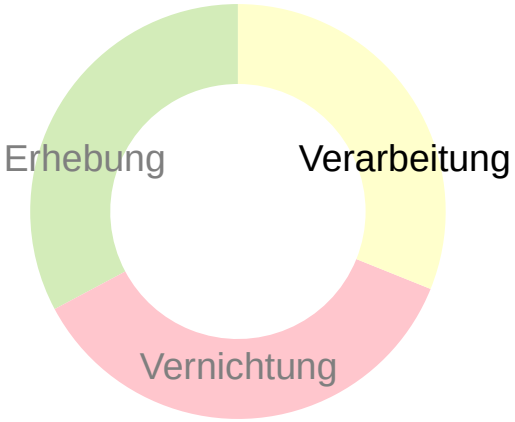
Nach § 24 BDSG kompatible Zwecke für nicht-öffentliche Stellen sind:

- Abwehr von **Gefahren** für die staatliche oder öffentliche Sicherheit oder
- Verfolgung von **Straftaten**
- Geltendmachung, Ausübung oder Verteidigung **zivilrechtlicher Ansprüche**

(Interessensabwägung ist erforderlich)

Achtung: erneute Information erforderlich

Einwilligung



Einwilligung der betroffenen Person

Einwilligung

Einwilligung für einen oder mehrere bestimmte Zwecke:

- **unmissverständlich** abgegebene Willensbekundung (Erklärung oder sonstige eindeutige bestätigende Handlung)
- für den **bestimmten** Fall
- **freiwillig**
- in **informierter** Weise

Art 4. Nr. 11 DS-GVO

Näher konkretisiert:

- Allgemein in Art. 7
- Für Kinder in Art. 8
- In speziellen Rechtsvorschriften, z. B. TMG, TKG, StGB

Einwilligung

Art. 7 DS-GVO

Form

- Verständliche und **leicht zugängliche** Form
- In einer klaren und **einfachen** Sprache
- Klar von den anderen Sachverhalten zu **unterscheiden**
- Ohne **Zwang** zu geben
- **Koppelungsverbot** (Art. 7 Abs. 4)

Widerruflich für die Zukunft

Einwilligung ist nicht verbindlich, wenn sie einen **Verstoß** gegen die DS-GVO darstellt

Es besteht eine **Nachweispflicht** für das Vorliegen der Einwilligung*

* Nach § 26 BDSG im Beschäftigungsverhältnis: schriftlich

Einwilligung bei Kindern

Art. 8 DS-GVO

Bei einem Angebot von „Diensten der Informationsgesellschaft“, das einem Kind direkt gemacht wird, gelten die folgenden Besonderheiten für eine Einwilligung

Kinder

Nach nationalem Recht bis 13 und maximal 16 Jahren

(keine Regelung im BDSG = 16 Jahre)

Voraussetzungen des **Art. 7**

Zusätzlich:

Einwilligung muss durch den **Träger der elterlichen Verantwortung** für das Kind oder mit dessen Zustimmung erteilt werden

Überprüfungspflicht desjenigen, der die Einwilligung einholt/nutzt

Fortgeltung von Einwilligungen

Bisher erteilte Einwilligungen gelten fort, sofern sie der Art nach den Bedingungen der DS-GVO entsprechen (EG 171, S. 3 DS-GVO).

Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen.

Informationspflichten nach Art. 13 DS-GVO müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.

Voraussetzung aber:

- **Freiwilligkeit** („Kopplungsverbot“, Art. 7 Abs. 4 i.V.m. EG 43 DS-GVO),
- **Altersgrenze**: 16 Jahre (soweit im nationalen Recht nichts anderes bestimmt wird; Schutz des Kindeswohls, Art. 8 Abs. 1 i.V.m. EG 38 DS-GVO).

Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 13./14. September 2016)

Zwischenfall: Massenmail

Sie sind Vertriebsmitarbeiter/in in einem mittelständischen Unternehmen.
Sie verschicken eine eMail mit aktuellen Restposten und Sonderangeboten an sämtliche Geschäfts- und Privatkunden.
Die Empfängeradressen bestehen weit überwiegend aus vorname.nachname@firma.de.
Alle Adressen stehen im CC-Feld.

Lösungsskizze

Fragestellung: Ist die Datenverarbeitung rechtmäßig im Sinne von Art. 5 Abs. 1 lit. a DS-GVO?

- Anwendbarkeit der DS-GVO (+), Art. 2 Abs. 1 DS-GVO: ganz oder teilweise automatisierte Verarbeitung. Keine private/familiäre Tätigkeit im Sinne von Art. 2 Abs. 2 lit. c DS-GVO.
  - Personenbezug (+), Art. 4 Nr. 1 DS-GVO: identifizierte oder identifizierbare natürliche Person. (Name, Mail-Adresse, Arbeitgeber, Kundenbeziehung...). **SONDERPROBLEM**: Kontaktadressen von juristischen Personen (poststelle@..., info@... haben idR keinen Personenbezug. Datenschutz nur für natürliche Personen!)
  - Verarbeitung (+), Art. 4 Nr. 2 DS-GVO: Übermittlung
- Rechtmäßigkeit nach Art. 6 DS-GVO?
  - Einwilligung, lit. a (-)
  - Vertragliche Maßnahmen, lit.. b (-)
  - Rechtliche Verpflichtung, lit. c (-)
  - Lebenswichtige Interessen, lit. d (-)
  - Öffentliches Interesse, lit. e (-)
  - Interessenabwägung, lit. f (-)

ERGEBNIS: Datenverarbeitung gemäß Art. 6 Abs. 1 DS-GVO **unrechtmäßig**.

Rubrik: #GDPRFAIL

Rubrik: #GDPRFAIL

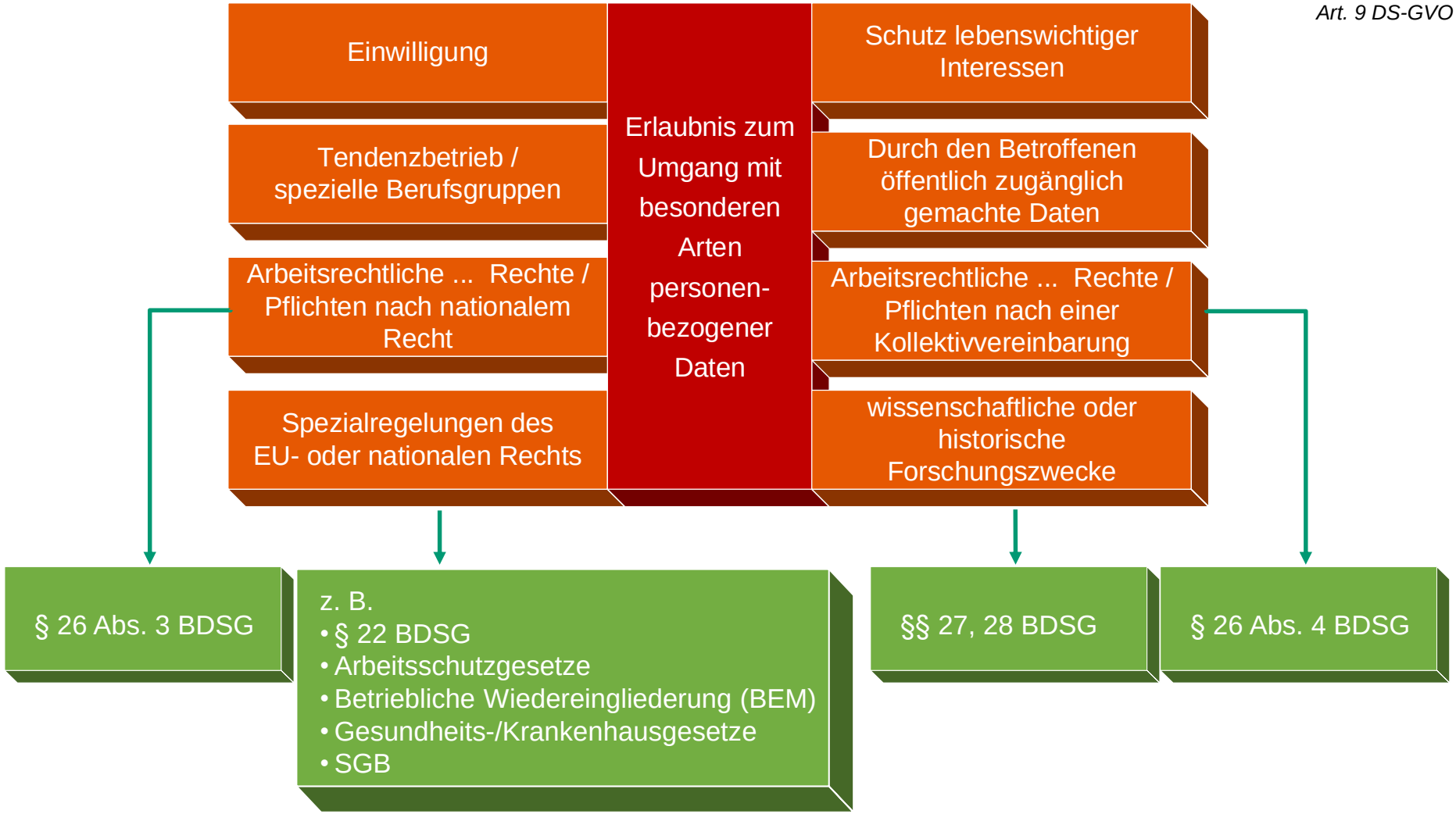
2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO

2.2.3 Zulässigkeit der Verarbeitung besonderer Kategorien von personenbezogenen Daten

Lehrveranstaltung Datenschutz

Art. 9 DS-GVO



Besondere Schutzmaßnahmen sind erforderlich
(s. Art. 25, 32 und 36 DS-GVO; § 22 Abs. 2 BDSG)

Lehrveranstaltung Datenschutz

Verarbeitung besonderer Kategorien personenbezogener Daten zu anderen als bei der Erhebung angegeben Zwecken (Zweckänderung)

Kompatibel nach Art. 6 Abs. 4 DS-GVO

Kompatibel nach nationaler Regelung

Nicht kompatibel

Nach § 24 Abs. 2 BDSG kompatible Zwecke für **nicht-öffentliche Stellen** sind:

- Abwehr von **Gefahren** für die staatliche oder öffentliche Sicherheit oder
- Verfolgung von **Straftaten** oder
- Geltendmachung, Ausübung oder Verteidigung **zivilrechtlicher Ansprüche**

und

- Ausnahmetatbestand liegt vor gemäß
  - Art. 9 Abs. 2 DS-GVO
  - § 22 BDSG
  - § 27 Abs. 1 BDSG (wissenschaftliche und statistische Zwecke)
  - § 28 Abs. 1 BDSG (in öffentlichem Interesse liegende Archivzwecke)

(Interessensabwägung ist erforderlich)

Achtung: erneute Information erforderlich

Zwischenfall: Einwilligung

Sie sind betriebliche/r Datenschutzbeauftragte/r in einem mittelständischen Unternehmen. Die Personalabteilung verlangt Einwilligungserklärungen für die Verarbeitung von Informationen zu Schuhgröße und orthopädischen Einlagen, um ein Rabattsystem bei einem Online-Schuhversand nutzen zu können.

„Bei Weigerung oder Falschangaben kann dies disziplinarische Schritte oder die Auflösung des Beschäftigungsverhältnisses nach sich ziehen.“ Ist das Vorgehen zulässig?

Lösungsskizze

Fragestellung: Ist die Datenverarbeitung rechtmäßig im Sinne von Art. 5 Abs. 1 lit. a DS-GVO?

- Anwendbarkeit der DS-GVO (+), Art. 2 Abs. 1 DS-GVO: ganz oder teilweise automatisierte Verarbeitung.
  Keine private/familiäre Tätigkeit im Sinne von Art. 2 Abs. 2 lit. c DS-GVO.
  - Personenbezug (+), Art. 4 Nr. 1 DS-GVO
  - Verarbeitung (+), Art. 4 Nr. 2 DS-GVO: Erhebung & Übermittlung
- Rechtmäßigkeit durch Einwilligung
  - Einwilligung, Art. 7 DS-GVO iVm § 26 Abs. 2 BDSG (-), da keine freie Entscheidung des Mitarbeiters.
- Rechtmäßigkeit durch sonstigen Erlaubnistatbestand
  - Sonderproblem: Es handelt sich zum Teil um besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DS-GVO (orthopädische Einlagen = Gesundheitsdaten)! Daher gilt § 26 Abs. 3 BDSG vorrangig. Erforderlichkeit der Daten ist nicht gegeben
  - Hinsichtlich der Schuhgröße greifen die allgemeinen Erlaubnisregeln:
    § 26 Abs. 1 BDSG (-). Wenn überhaupt Zwecke des Beschäftigungsverhältnisses betroffen sind, dann jedenfalls nicht für die Durchführung des Verhältnisses erforderlich.
  - Art. 6 Abs. 1 lit. f DS-GVO (-). Hier fehlt es aber genauso an der Erforderlichkeit und dem Überwiegen des Interesses auf Seiten des Arbeitgebers.

ERGEBNIS: Datenverarbeitung entgegen Art. 5 Abs. 1 lit. a DS-GVO unrechtmäßig.

2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO

2.2.3 Transparenz der Verarbeitung

Transparenz der Verarbeitung

Art. 13-14 DS-GVO

- Information bei der Erhebung beim Betroffenen
- Benachrichtigung
- Ausnahme §§ 31, 32 BDSG

Art. 15 DS-GVO

- Auskunftsrecht
- Ausnahme § 33 BDSG

Art. 16-21 DS-GVO

- Berichtigung
- Löschung (Ausn. § 34 BDSG)
- Sperrung
- Übertragbarkeit
- Widerspruch (Ausn. § 35 BDSG)

Art. 12 DS-GVO

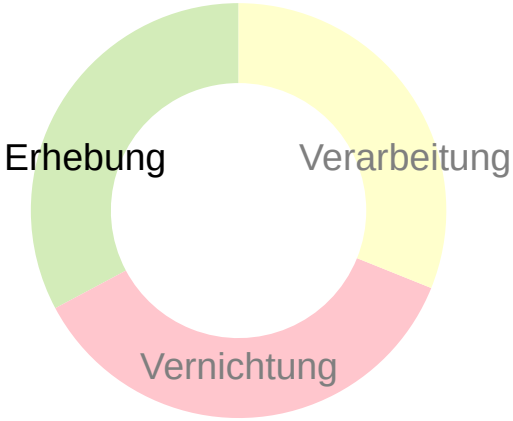
Modalitäten für die transparente Information, Kommunikation und Ausübung der Rechte Betroffenen

Art. 5 Abs. 1 (a) DS-GVO

Prinzip „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“

„Personenbezogene Daten müssen […] auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden“

Informationspflichten



Erhebung
Direkterhebungsgrundsatz fehlt, aber:
Erhebung nach Treu und Glauben/transparent

Beim Betroffenen

Nicht beim Betroffenen/ Zweckänderung

Ausnahme
Wenn und soweit der Betroffene bereits über die Informationen verfügt

Art. 13 DS-GVO
Unterrichtung und Aufklärung

Art. 14 DS-GVO
Benachrichtigung

Ausnahme
Kenntnis, unverhältnismäßig, Erlangung nach nationalem Recht, Geheimhaltungspflicht

Ausnahmen für Weiterverarbeitung nach nationaler Regelung:
§ 32 BDSG
§ 29 Abs. 2 BDSG*

Art. 21 DS-GVO – IMMER:
Hinweis auf Widerspruchsrecht bei
- Direktwerbung
- Interessensabwägung
- Profiling

Weitere Ausnahmen nach nationaler Regelung:
§ 33 BDSG
§ 29 Abs. 1 BDSG*

** Für Geheimnisträger i. S. d. § 203 StGB*

Lehrveranstaltung Datenschutz

Art. 13, 14 DS-GVO

- Alle Zwecke
- Datenkategorien
- Gesetzliche Legitimation
- Interessensabwägung
- Empfänger und Quellen der Daten
- Drittlandübermittlung: geeignete Garantien f. Datenschutzniveau
- Speicherfristen oder Kriterien um die Frist zu bestimmen

+ weitere „allgemeine“ Informationen wie Kontaktdaten des DSB, Beschwerderecht bei der Aufsichtsbehörde, …

Lehrveranstaltung Datenschutz

Information bei Erhebung

Beim Betroffenen

- Ausnahmen nach Art. 13:
  - **Kenntnis** des Betroffenen über die Informationen
- Zusätzliche Ausnahmen bei **Weiter-verarbeitung** nach § 32 BDSG:
  - Bei analog gespeicherten Daten: **unverhältnismäßig** + geringes Interesse an der Information
  - bei Gefährdung der **öffentlichen Sicherheit** oder Ordnung
  - bei Gefährdung **zivilrechtlicher Ansprüche**
  - bei Gefährdung der **vertraulichen Übermittlung** an öffentliche Stellen
- Achtung:
  - Fallweise werden andere Maßnahmen erforderlich wie Bereitstellung der Informationen für die Öffentlichkeit

Nicht beim Betroffenen

- Ausnahmen nach Art. 14:
  - **Kenntnis** des Betroffenen über die Informationen
  - **unverhältnismäßig / unmöglich**
  - Erlangung der Daten aufgrund ausdrücklichen **nationalen Rechts**
  - **Geheimhaltungspflicht**
- Ausnahmen nach § 33 BDSG:
  - bei Gefährdung der **öffentlichen Sicherheit** oder Ordnung
  - bei Gefährdung **anerkannter Geschäftszwecke**
- Achtung:
  - Fallweise werden andere Maßnahmen erforderlich wie Bereitstellung der Informationen für die Öffentlichkeit

Problem: Art des Zugänglichmachens der Informationen

Anforderung an die Information:
leicht zugänglich und **verständlich** sowie in **klarer und einfacher Sprache** abgefasst; ggf. zusätzlich **visuelle Elemente** (delegierter Rechtsakt)

- **Medienbrüche werden nicht ausdrücklich zugelassen**
  (anders etwa Art. 8 Abs. 4 Verbraucherrechterichtlinie)

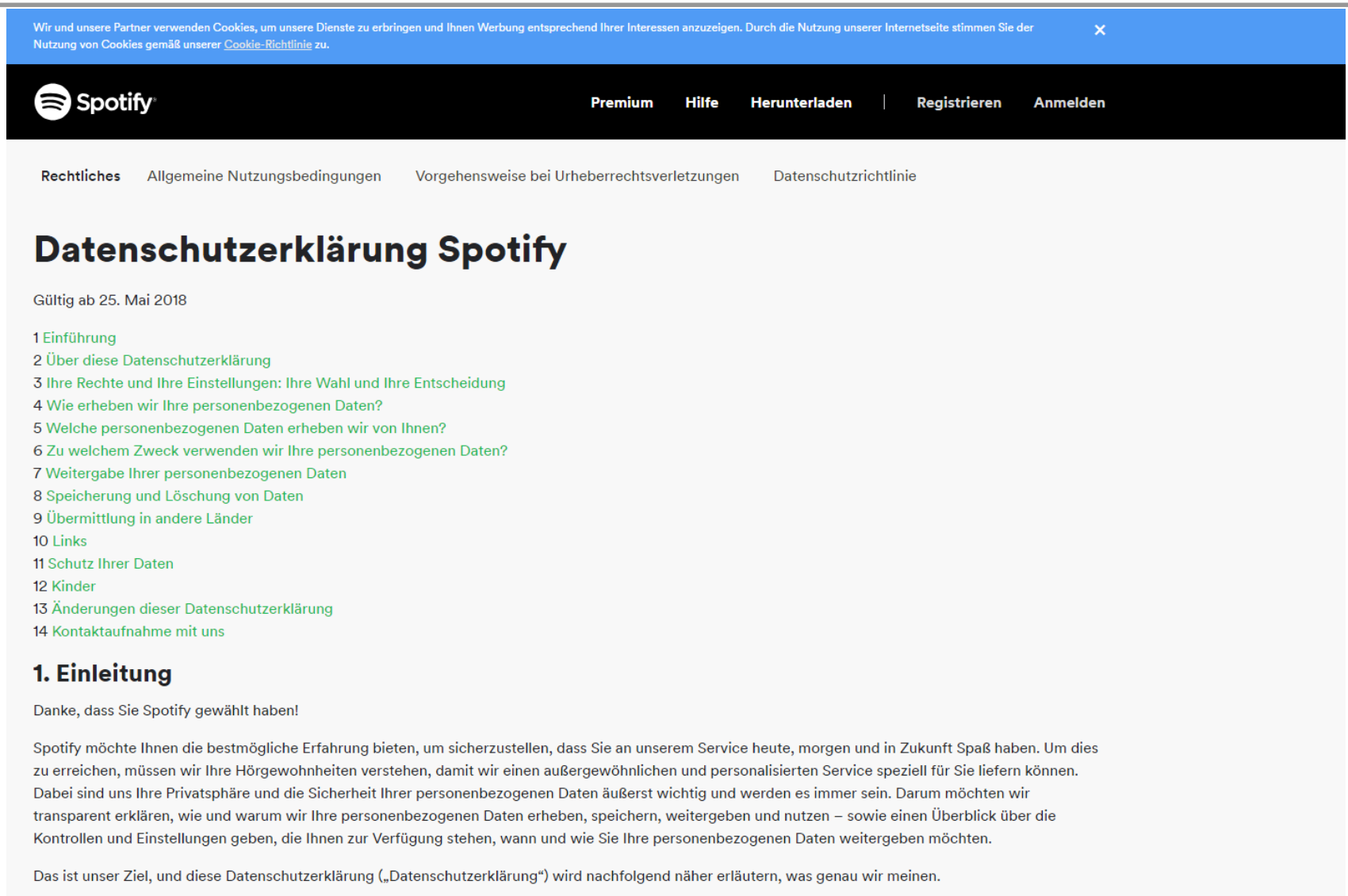
- Aber: Nach **ErwG 58** können Informationen **auch über Webseiten** zur Verfügung gestellt werden

- **Gestuftes Informationsverfahren auch in Zukunft praktikabel**
  - ✓ Möglichkeit der Aufteilung in wesentliche und zusätzliche Infos
  - ✓ Pflicht zum Hinweis auf gestuftes Verfahren
  - ✓ wichtig für kleinteilige Werbemittel, Erhebungen im Callcenter usw.
  - ✓ Weitere Möglichkeiten: Aushang? Hinweis auf Webseite? QR-Code?

Beispiel für eine „gestufte“ Information

*„**Datenschutzinformation:***
Wir sind daran interessiert, Sie als Kunden zu gewinnen, die Kundenbeziehung mit Ihnen zu pflegen und Ihnen Informationen und Angebote zukommen zu lassen. Deshalb verarbeiten wir auf Grundlage von Artikel 6 (1) (f) der Europäischen Datenschutz-Grundverordnung (auch mit Hilfe von Dienstleistern) Ihre Adressdaten und Kriterien zur interessengerechten Werbeselektion, um Ihnen solche Informationen und Angebote von uns und anderen Unternehmen zuzusenden. Wenn Sie dies nicht wünschen, können Sie bei uns jederzeit der Verwendung Ihrer Daten für Werbezwecke widersprechen. Sie erleichtern uns die schnelle Bearbeitung eines Widerspruchs, wenn Sie das Werbemittel beifügen. [OPTIONAL: Sie können den Widerspruch auch per E-Mail senden an: E-MAIL ADRESSE.] Weitere Informationen zum Datenschutz erhalten Sie unter [INTERNETLINK ZUR AUSFÜHRLICHEN DATENSCHUTZINFORMATION].

Unseren Datenschutzbeauftragten erreichen Sie ebenfalls unter unserer Anschrift. “



Wir und unsere Partner verwenden Cookies, um unsere Dienste zu erbringen und Ihnen Werbung entsprechend Ihrer Interessen anzuzeigen. Durch die Nutzung unserer Internetseite stimmen Sie der Nutzung von Cookies gemäß unserer Cookie-Richtlinie zu.

Spotify Premium Hilfe Herunterladen | Registrieren Anmelden

Rechtliches Allgemeine Nutzungsbedingungen Vorgehensweise bei Urheberrechtsverletzungen Datenschutzrichtlinie

Datenschutzerklärung Spotify

Gültig ab 25. Mai 2018

1. Einleitung

Danke, dass Sie Spotify gewählt haben!

Spotify möchte Ihnen die bestmögliche Erfahrung bieten, um sicherzustellen, dass Sie an unserem Service heute, morgen und in Zukunft Spaß haben. Um dies zu erreichen, müssen wir Ihre Hörgewohnheiten verstehen, damit wir einen außergewöhnlichen und personalisierten Service speziell für Sie liefern können. Dabei sind uns Ihre Privatsphäre und die Sicherheit Ihrer personenbezogenen Daten äußerst wichtig und werden es immer sein. Darum möchten wir transparent erklären, wie und warum wir Ihre personenbezogenen Daten erheben, speichern, weitergeben und nutzen – sowie einen Überblick über die Kontrollen und Einstellungen geben, die Ihnen zur Verfügung stehen, wann und wie Sie Ihre personenbezogenen Daten weitergeben möchten.

Das ist unser Ziel, und diese Datenschutzerklärung („Datenschutzerklärung“) wird nachfolgend näher erläutern, was genau wir meinen.

Lehrveranstaltung Datenschutz

Bitte mache dich mit der neuen Fassung vertraut.

Falls diese E-Mail nicht korrekt angezeigt wird, gehen sie bitte zur Online-Version

hhv.de

Hallo Steffen,

Datenschutz und Transparenz unseren Kunden gegenüber sind uns bei HHV wichtig. Heute möchten wir dich darüber informieren, dass wir unsere **Datenschutzrichtlinie aktualisiert** haben.

Die neue Fassung entspricht den Anforderungen der am 25. Mai 2018 in Kraft tretenden **EU-Datenschutz-Grundverordnung** (DSGVO).

Wir haben mehr Details zu den Features und Diensten, die wir anbieten, hinzugefügt, ergänzt um die Auskunft, **wie wir die von uns gesammelten Informationen verwenden**.

Wir haben einige Abschnitte neu strukturiert, um sie **übersichtlicher** zu gestalten.

Da die genannten Punkte nur einige der Updates darstellen, empfehlen wir dir, unsere aktualisierten Datenschutzbestimmungen vollständig zu lesen.

Wir freuen uns auf deinen nächsten Besuch bei HHV.

Viele Grüße aus Berlin,
dein HHV-Team

Datenschutzbestimmungen lesen

?

2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO
2.2.4 Datenschutzverletzung

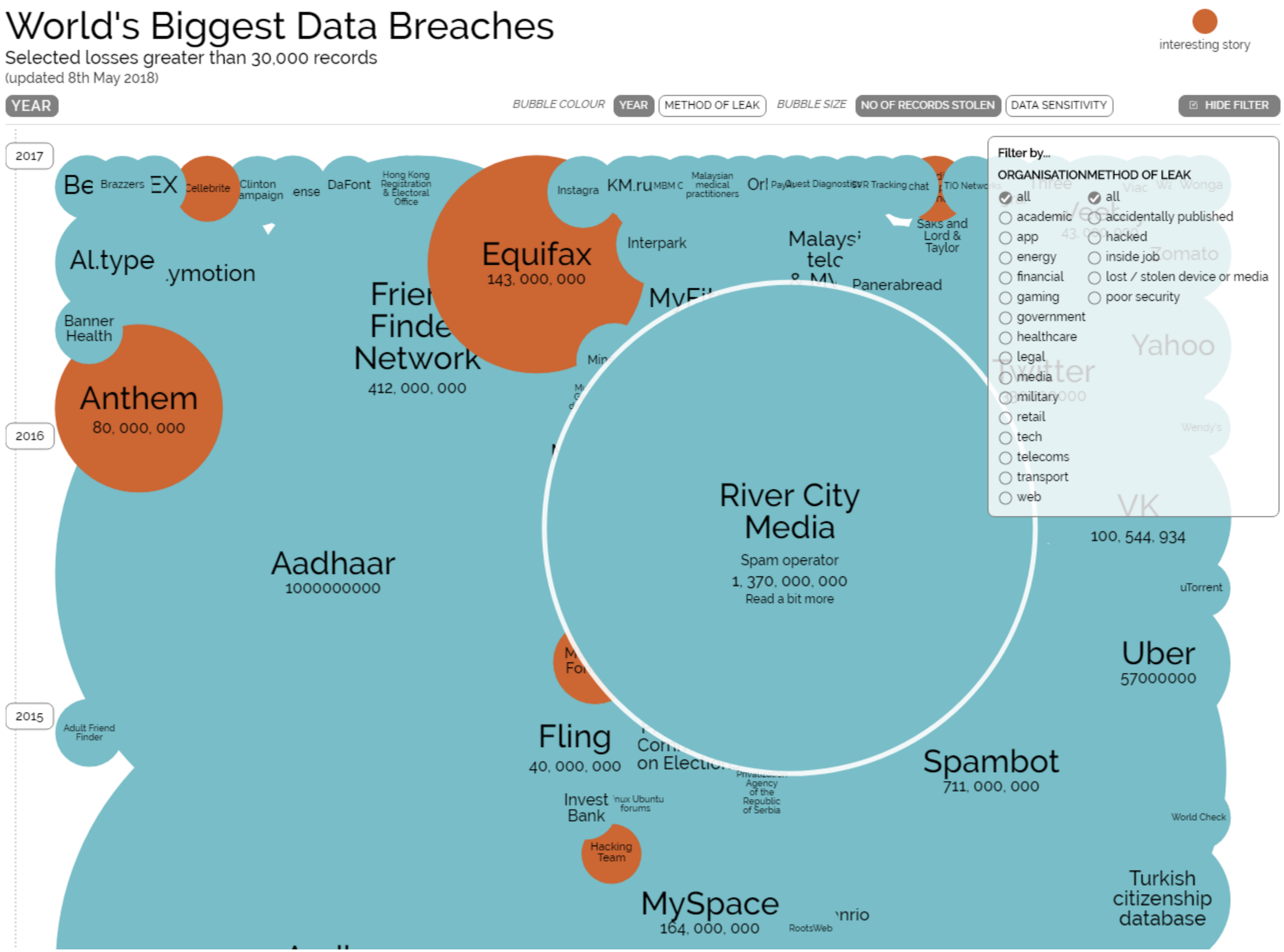
Lehrveranstaltung Datenschutz

(Projekt Datenschutz wurde inzwischen eingestellt)

Datenschutzvorfälle

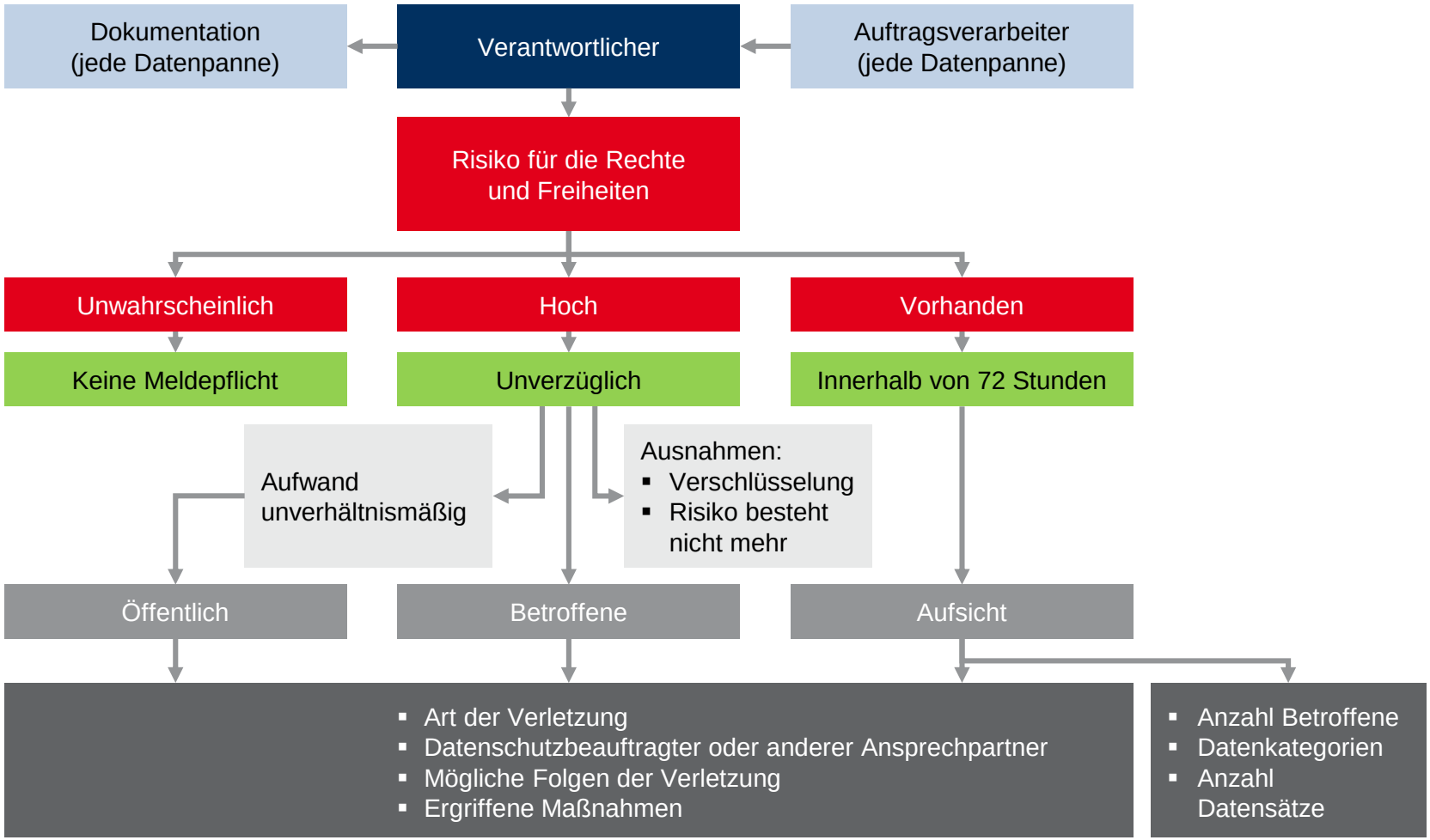
Datum	Ort	Datenherkunft	Organisation	Anz.	Betroffene	Kurzbeschreibung
05.03.14	Frankfurt am Main	Hessisches Wirtschaftsministerium	Behörde	nicht bekannt	Sanktionierte Unternehmen	Ministerium benennt versehentlich Börsensünder
03.03.14	Neufahrn	office discount Vertrieb für Bürobedarf GmbH	Unternehmen	nicht bekannt	Kunden	Office Discount verschickt Kontodaten in unverschlüsselten E-Mails
27.02.14	Bonn	Deutsche Telekom	Unternehmen	Millionen	Kunden	Telekom versendet vollständige Bankverbindungsdaten unverschlüsselt
14.02.14	Neuruppin	Jugend- und Betreuungsamt Neuruppin	Öffentliche Verwaltung	unbekannt	Klienten	Digitale Stifte verantwortlich für Datenpanne bei Jugendamt Neuruppin
12.02.14	Montabaur	1&1 Internet AG	Unternehmen	nicht bekannt	Kunden	1&1 versendet E-Mails mit kompletten Kontodaten
05.02.14	nicht bekannt	nicht bekannt			Nutzer von Fritzbox-Routern	Hacker kapern Fritzbox-Router
03.02.14	Köln	LobbyControl – Initiative für Transparenz und Demokratie e.V.	Verein	wenige	nicht bekannt	Intiative "LobbyControl" versendet E-Mails an falsche Empfänger
03.02.14	Aichach-Schrobenhausen	Unternehmen	Sparkasse Aichach-Schrobenhausen	mehrere Tausend	Kunden	Sparkasse Aichach-Schrobenhausen: Technischer Fehler bei externem Zahlungsdienstleister schuld an Datenpanne
01.02.14	Berlin	Gemeinsames Krebsregister	Behörde	26	Krebspatienten	Datenpanne beim Gemeinsamen Krebsregister
31.01.14	Saarland	Saarländische Polizei	Behörde	über 2.000	Saarländische Polizisten	Polizistenbewertungen versehentlich versendet
31.01.14	Ulm/Neu-Ulm	SWU Stadtwerke Ulm/Neu-Ulm GmbH	Unternehmen	5.400	Kunden	Stadtwerke Ulm/Neu-Ulm verschicken Bankdaten unverschlüsselt
21.01.14	Welver	Gemeinde Welver	Behörde	nicht bekannt	Bürger von Welver	Gemeinde Welver stellt sensible Bürgerdaten ins Internet
20.01.14	nicht bekannt	Hotelkette Hilton	Unternehmen	ca. 1.000	Teilnehmer eines Gewinnspiels	Hilton-Marketingteam verschickt Mailing an offenen Verteiler
23.12.13	Nürtingen	Hewlett-Packard	Unternehmen	ca. 200	Kunden	Dienstleister von HP verschickt Rechnungen an falsche Adresse
20.12.13	Neubrandenburg	Jobcenter Neubrandenburg	Behörde	30	Kunden	Jobcenter sendet Bescheide an falsche Adresse
29.11.13	Neuwied bei Koblenz	Oberfinanzdirektion Koblenz	Behörde	868	Bürger	Bürger findet 868 Briefe der Oberfinanzdirektion Koblenz
22.11.13	Heidelberg	Heidelberger Stadtwerke	Unternehmen	ca. 500	Kunden	Heidelberger Stadtwerke bringen Kundendaten durcheinander
19.11.13	Landkreis Mansfeld-Südharz	Jobcenter Mansfeld-Südharz	Behörde	1	Kunde	Jobcenter verschickt Bescheid an falsche Adresse
06.11.13	Unterföhring	Sky Deutschland	Unternehmen	nicht bekannt	Kunden	Verlust von Kundendaten bei Pay-TV-Sender Sky
04.11.13	München	Talbot Runhof	Unternehmen	98	Kunden	Mode-Label versendet interne Kundendaten in einem Werbe-Mailing

1 2 3 4 5 6 7 8 9 … nächste Seite › letzte Seite »


World's Biggest Data Breaches
Selected losses greater than 30,000 records
(updated 8th May 2018)
interesting story
YEAR
BUBBLE COLOUR
YEAR
METHOD OF LEAK
BUBBLE SIZE
NO OF RECORDS STOLEN
DATA SENSITIVITY
HIDE FILTER
2017
2016
2015
Equifax
143, 000, 000
Anthem
80, 000, 000
Network
412, 000, 000
Aadhaar
1000000000
River City Media
Spam operator
1, 370, 000, 000
Read a bit more
Uber
57000000
Spambot
711, 000, 000
Fling
40, 000, 000
MySpace
164, 000, 000
Turkish citizenship database
100, 544, 934
Filter by...
ORGANISATION
METHOD OF LEAK
all
academic
app
energy
financial
gaming
government
healthcare
legal
media
military
retail
tech
telecoms
transport
web
all
accidentally published
hacked
inside job
lost / stolen device or media
poor security

Verletzung des Schutzes pb Daten

Art. 33, 34 DS-GVO



Informationspflicht an Aufsicht

Art. 33 Abs. 1 DS-GVO

Meldung an Aufsichtsbehörde	• Voraussichtliches Risiko für Rechte und Freiheiten Betroffener • Unverzügliche Meldung, möglichst innerhalb 72 Stunden • Pflicht zur Begründung bei Verzögerung
Inhaltskatalog der Meldung (ggf. schrittweise)	• Beschreibung der Verletzung und der Kategorien der personenbezogenen Daten, Zahl der Betroffenen • Kontaktinformationen des Datenschutzbeauftragten • Beschreibung möglicher Folgen und ergriffener (oder geplanter) Maßnahmen
Auftragsverarbeiter	• meldet unverzüglich an Verantwortlichen

Meldungen nach Art. 33 und Benachrichtigungen nach Art. 34 Abs. 1 DS-GVO dürfen nur mit Zustimmung des Verantwortlichen in einem Strafverfahren (gegen ihn) verwendet werden (§ 42 Abs. 4 BDSG).

Informationspflicht an Betroffene

Art. 34 Abs. 1 DS-GVO

Information Betroffener	• Voraussichtliches **hohes Risiko** für Rechte und Freiheiten Betroffener • Unverzügliche Benachrichtigung in **klarer, einfacher Sprache**
Ausnahmen	• Geeignete technisch-organisatorische Sicherheitsvorkehrungen (etwa durch Verschlüsselung der Daten) • Maßnahmen nach der Verletzung die hohes Risiko für Betroffene ausschließen • Unverhältnismäßig hoher Aufwand (stattdessen öffentliche Bekanntmachung oder ähnliche Maßnahme)
Aufsichtsbehörde	• kann die Benachrichtigung verlangen

Zwischenfall: Hacker John Doe

Um den Zahlungsverkehr noch schneller abzuwickeln, hat die Secret Pay GmbH & Co. KG ein mobiles Bezahlsystem entworfen, das den Nutzern ermöglicht, über eine „App“ weltweit Produkte und Dienstleistungen zu bezahlen. Die hierbei verarbeiteten Daten werden bei einem eingeschalteten Dienstleister im Auftrag von Secret Pay verarbeitet. Durch einen Fehler im Quellcode der App erlangt Hacker „JD“ Zugriff auf Kreditkartendaten von 1000 Kunden. Dies wird umgehend bemerkt.

Beurteilen Sie eine mögliche Meldepflicht von Secret Pay anhand der einschlägigen Normen in der DS-GVO.

Lösungsskizze

Fragestellung: Ist der Zugriff von „JD“ meldepflichtig im Sinne von Art. 33 und 34 DS-GVO?

- Anwendbarkeit der DS-GVO (+), Art. 2 Abs. 1 DS-GVO: ganz oder teilweise automatisierte Verarbeitung.
  Keine private/familiäre Tätigkeit im Sinne von Art. 2 Abs. 2 lit. c DS-GVO.
  - Personenbezug (+), Art. 4 Nr. 1 DS-GVO
  - Verarbeitung (+), Art. 4 Nr. 2 DS-GVO: Erhebung & Übermittlung

- Meldepflicht
  - Informationspflicht geregelt in Art. 33 und 34 DS-GVO
  - Frage: Führt die Verletzung voraussichtlich zu einem Risiko (Art. 33DS-GVO) bzw. zu einem hohen Risiko für Rechte und Freiheiten Betroffener (Art. 34 DS-GVO)?
  - Kreditkartendaten sind betroffen
  - Die Vertraulichkeit der Daten wurde verletzt, da sich JD unbefugt Zugang hierzu verschafft hat
  - Es drohen schwere Beeinträchtigungen für Rechte bzw. schutzwürdige Interessen Betroffener aufgrund eines möglichen Missbrauchs der Kreditkartendaten; ein hohes Risiko ist anzunehmen.
  - Anhaltspunkte für eine Verschlüsselung der Daten bestehen im Übrigen nicht
  - Unverzügliche Meldepflicht an die Aufsichtsbehörde binnen 72 Stunden (Art. 33 Abs. 1 DS-GVO) sowie an den Betroffenen (Art. 34 DS-GVO)

ERGEBNIS: Meldepflicht besteht sowohl gegenüber der Aufsichtsbehörde als auch den Betroffenen.

2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO

2.2.5 Betroffenenrechte

Betroffenenrechte im Überblick

*Dr. Lorenz Franck

Recht auf Auskunft

Art. 15 DS-GVO

Auskunft auf Antrag

Was

- Ob Daten zu seiner Person verarbeitet werden
- Datenkategorien
- Zweck der Verarbeitung
- Empfänger(-kategorien)
- Speicherdauer
- Beschwerderecht bei Aufsicht
- Herkunft
- Bei automatisierter Entscheidung/ Profiling: Logik und angestrebte Wirkung der Verarbeitung
- Unterrichtung über geeignete Garantien beim Drittlandstransfer

Wie

- Identitätsfeststellung (Art. 12 Abs. 6 DS-GVO)
- Ausübung des Auskunftsrechts ist zu „erleichtern“ (Art. 12 Abs. 2 DS-GVO)
- Auskunftserteilung erfolgt:
  - Ohne unangemessene Verzögerung
  - Spätestens innerhalb eines Monats
  - Fristverlängerung um maximal zwei Monate
  - Unentgeltlich, in Ausnahmen Entgelt auf Basis von Verwaltungskosten
  - Schriftlich/Kopie der Daten
  - Elektronisch bei elektronischer Antragsstellung

Ausnahmen vom Auskunftsrecht nach nationalem Recht

Recht auf Auskunft

§ 34 BDSG

Ausnahmen von der Auskunftspflicht

Ausnahmen:

- §§ 27 Abs. 2 (Forschung, Statistik), 28 Abs. 2 (Archive im öffentlichen Interesse), 29 Abs. 1 S. 2 (Geheim-haltungspflichten), 33 Abs. 1 Nrn. 1, 2 lit. b), Abs. 3 BDSG (öffentliche Sicherheit u. Interessen)
- Speicherung nur
  - aufgrund Aufbewahrungs-vorschriften
  - zur Datensicherung/ Datenschutzkontrolle

  und Aufwand unverhältnismäßig und Verarbeitung zu anderen Zwecken durch technische und organisatorische Maßnahmen ausgeschlossen ist (Sperrung)

Maßnahmen:

- Dokumentation der Auskunftsverweigerung
- Begründung gegenüber dem Betroffenen, soweit die Zwecke der Auskunftsverweigerung hierdurch nicht gefährdet werden

Zwischenfall: Auskunftsrecht

Sie sind Datenschutzbeauftragter in einem Versicherungsunternehmen (kein Sozialversicherungsträger!).
In der Tagespresse wird kolportiert, daß Ihr Unternehmen Daten aus Social Media, von Werbepartnern und aus anderen Quellen aggregiert, um individuell zugeschnittene Versicherungsangebote schneidern zu können.

Ein Versicherter verlangt wütend Auskunft über die bei Ihnen gespeicherten Daten. Zu Recht?

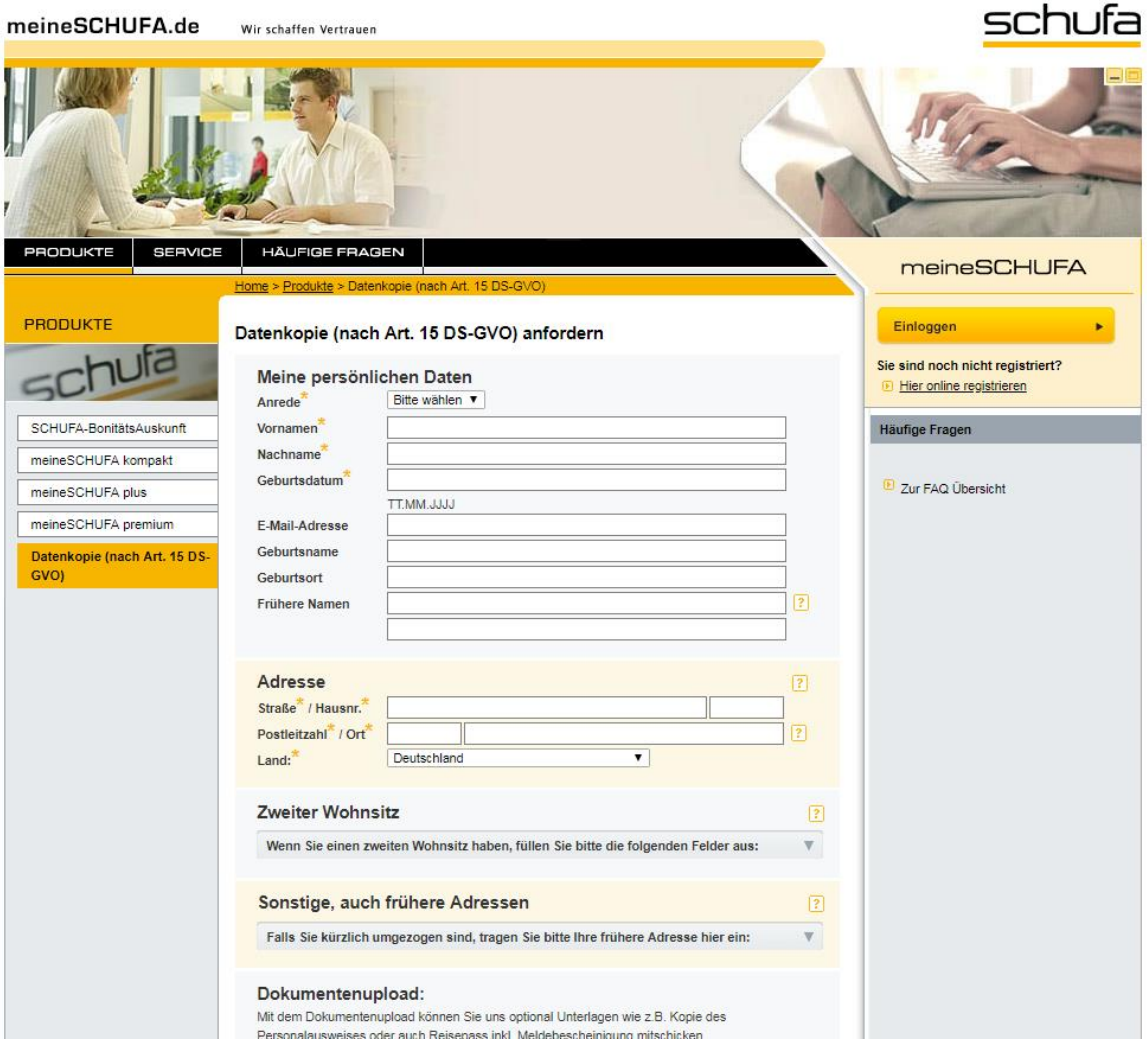
Lösungsskizze

Fragestellung: Besteht ein Auskunftsanspruch nach Art. 15 DS-GVO?

- Anwendbarkeit der DS-GVO (+), Art. 2 Abs. 1 DS-GVO: ganz oder teilweise automatisierte Verarbeitung. Keine private/familiäre Tätigkeit im Sinne von Art. 2 Abs. 2 lit. c DS-GVO. [SONDERPROBLEM: Sozialleistungsträger würden sich nach den SGB I und X richten.]
  - Personenbezug (+), Art. 4 Nr. 1 DS-GVO
  - Verarbeitung (+), Art. 4 Nr. 2 DS-GVO
- Art. 15 Abs. 1 Hs. 1 DS-GVO: „Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten...“
  - Verantwortliche Stelle (+)
  - Betroffener (+)
  - Auskunftsverlangen (+)
- Art. 15 Abs. 1 Hs. 2 litt. a-h DS-GVO (+)
- Ausnahmen?
  - Art. 15 Abs. 4 DS-GVO (-)
  - §§ 27 28, 29, 34 BDSG (jew. in den Grenzen von Art. 23 DS-GVO) (-)

ERGEBNIS: Auskunftsersuchen gemäß Art. 15 Abs. 1 Hs. 1 DS-GVO rechtmäßig. Die Auskunft wird gem. Art. 12 Abs. 5 DS-GVO unentgeltlich erteilt.

Beispiel Auskunftsformular



heise online

IT Mobiles Entertainment Wissen Netzpolitik Wirtschaft Journal Newsticker Foren

TOPTHEMEN: DSGVO COMPUTEX 2018 WINDOWS 10 ANDROID P KRYPTOWÄHRUNG ELEKTROAUTOS TESTS FACEBOOK-DATENSKANDAL

heise online > News > 02/2018 > DSGVO: Folterfragebogen im Selbsttest

DSGVO: Folterfragebogen im Selbsttest

21.02.2018 09:00 Uhr – Jo Bager vorlesen

Die neue EU-Datenschutzgrundverordnung tritt im Mai in Kraft. Sie bringt Verbrauchern neue Rechte und Unternehmen neue Pflichten. c't gibt einen Überblick, hilft Verbrauchern, ihre Rechte geltend zu machen - und testet das Prozedere für Unternehmen.

Die EU-Datenschutzgrundverordnung (DSVGO) kommt. Am 25. Mai wird das riesige Update des europäischen Datenschutzrecht wirksam. Verbraucher können sich über mehr Rechte freuen: Unternehmen müssen genauer über die Verarbeitung der Nutzerdaten informieren, und dürfen sich dabei nicht hinter Juristenkauderwelsch verstecken. Bürger stehen zudem mehr Mittel als bisher zur Verfügung, um zu erfahren, welche Daten Unternehmen über sie speichern, und um diese löschen zu lassen.

Anzeige

Anzeige

Ähnliche Artikel

nachgehakt: Datenschutzgrundverordnung

Ende Mai 2018 tritt die neue Datenschutzverordnung in Kraft, die einheitlich für die gesamte EU gilt. Sie bringt neue Rechte für Verbraucher, aber…

ct

DSGVO: Last-Minute-Hilfe gegen Abmahnungen und Bußgelder

Seit wenigen Tagen ist das neue EU-Datenschutzrecht (DSGVO) wirksam. Wer jetzt noch Hilfe sucht, um die drohende Abmahngefahr zu vermeiden, sollte…

ct 444

c't-Adventskalender: Privacy für Windows-User

Sind Sie auch genervt, wenn Windows mal wieder nach einem Microsoft-Konto verlangt, sich ständig Cortana meldet oder Apps zu viele Rechte wollen?…

ct

Datenportabilität

Art. 20 DS-GVO

Datenportabilität
Art. 20 DS-GVO
(Gilt nur bei Verarbeitung aufgrund Einwilligung oder Vertrag)

Achtung: DS-GVO hat keine Beschränkung auf Internet-dienste!

Erweiterung des Auskunftsrechts + **Erweiterung durch Portierbarkeit**

Der Betroffene kann eine Kopie seiner Daten verlangen, und zwar in einem strukturierten*, gängigen und maschinenlesbaren Format

+

Hinderungsfreie Übermittlung an andere Stelle, gegebenenfalls Direktübermittlung (Abs. 3 DS-GVO)

Ausnahme
Die Portierung beeinträchtigt Rechte und Freiheiten anderer Personen

* Datenbankformat (XML; komma-separierte Liste, SQLite und so weiter)

Lehrveranstaltung Datenschutz

Bereitgestellte Daten

Art. 20 DS-GVO

Pb Daten, die wissentlich und aktiv von Betroffenen „bereitgestellt“ werden

Beispiele der Art. 29-Gruppe:

- Kontodaten (z.B. Postanschrift, Nutzername, Alter) über Online-Formulare
- Play List, Kontakte aus Webmail-Anwendung
- Rohdaten durch Nutzung eines Dienstes (Smart Meter, Suchhistorien, Verkehrsdaten, Daten von Fitnesstrackern)

Negative Abgrenzung

Beispiele der Art. 29-Gruppe:

- Daten von Dritten
- aus Rückschlüssen erzeugte oder abgeleitete Daten z.B. Bonitätsbewertung

Lehrveranstaltung Datenschutz

Art. 20 DS-GVO

Form der Bereitstellung:

Der Betroffene kann eine Kopie seiner Daten verlangen, und zwar in einem strukturierten*, gängigen und maschinenlesbaren Format (Art. 20)

Art. 29-Gruppe:

- Ziel: interoperable Systeme, nicht kompatible Systeme
- Direkte Downloadmöglichkeit
  - für betroffene Person
  - direkt an andere Verantwortliche

(Vorab-)Information

(nach Art. 13 und 14 DS-GVO)

Empfehlung der Art. 29-Gruppe:

- Genaue Erläuterung der unterschiedlichen Datentypen der Portabilität
- Vor jeder Kontoschließung stets Information über das Recht auf Portabilität

Recht auf Widerspruch

Art. 21 DS-GVO

Widerspruchsrecht

„[…] aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung […], die aufgrund von Art. 6 Abs. 1 Buchst. (e) [Wahrnehmung öffentlichen Interesses] oder (f) [Interessensabwägung] erfolgt, […], es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die […] überwiegen."

Art. 21 Abs. 1 DS-GVO

Widerspruchsrecht

gegen „Direktwerbung"

gegen Profiling für Direktmarketing

Art. 21 Abs. 4 DS-GVO

gegen Profiling

Art. 21 Abs. 4 DS-GVO

Art. 21 Abs. 4 DS-GVO
Ausdrücklicher Hinweis auf die Widerspruchsrechte spätestens bei erster Kommunikation

Recht auf Berichtigung

Art. 16 DS-GVO

Berichtigung (Art. 16)	▪ Berichtigung unrichtiger Daten auf Verlangen ▪ Vervollständigung unvollständiger Daten auf Verlangen ▪ unverzüglich ▪ Information an Empfänger (Art. 19)

Rechte der Betroffenen

Berichtigung

Pflicht des Verantwortlichen

Richtigkeit (Prinzip aus Art. 5)	▪ sachlich richtige und ggf. aktuellste Daten ▪ Vorsehen von Maßnahmen zur unverzüglichen Löschung oder Berichtigung von unzutreffenden Daten

Lehrveranstaltung Datenschutz

Einschränkung der Verarbeitung (Art. 18)	▪ für die Überprüfungsdauer bestrittener Daten ▪ für die Überprüfungsdauer eines Widerspruchs (Art. 21 Abs. 1) ▪ Sperrung unzulässig verarbeiteter Daten auf Verlangen ▪ Zweckverbrauch, aber vom Betroffenen zur Rechtsausübung benötigt

Rechte der Betroffenen

Einschränkung der Verarbeitung / Sperrung

Pflicht des Verantwortlichen

Prinzipien aus Art. 5	**Datenminimierung**	▪ Beschränkung auf das für den Zweck der Verarbeitung angemessene und sachlich relevante sowie notwendige Maß
	Integrität und Vertraulichkeit	▪ geeignete TOM zum angemessenen Schutz der Daten insbes. vor unbefugter oder unrechtmäßiger Verarbeitung, zufälligem Verlust, zufälliger Zerstörung oder Schädigung

Lehrveranstaltung Datenschutz

Einschränkung der Verarbeitung (Art. 18)

- Information an Empfänger (Art. 19)
- Information der betroffen Person bei Aufhebung der erwirkten Sperrung
- Weitere Verarbeitung nur
  - mit Einwilligung
  - zur Ausübung von Rechtsansprüchen
  - zum Schutz einer anderen Person
  - aus wichtigem öffentlichen Interesse nach nationalem Recht

Rechte der Betroffenen

Einschränkung der Verarbeitung / Sperrung

Pflicht des Verantwortlichen

Sperren statt Löschen (§ 35 BDSG)

- wegen Löschaufwand bei **nicht automatisierter** Verarbeitung und geringem Interesse (gilt nicht bei unzulässiger Verarbeitung)
- bei satzungsmäßigen oder vertraglichen Aufbewahrungspflichten
- Bei „Zweckverbrauch“ soweit durch die Löschung schutzwürdige Interessen des Betroffenen gefährdet werden (Unterrichtungspflicht)
- Bei unzulässiger Verarbeitung soweit durch die Löschung schutzwürdige Interessen des Betroffenen gefährdet werden (Unterrichtungspflicht)

Lehrveranstaltung Datenschutz

Recht auf Löschung (Art. 17 Abs. 1)	▪ unverzüglicher Löschanspruch / unverzügliche Löschpflicht bei ▪ „Zweckverbrauch“ ▪ Widerruf der Einwilligung ▪ Widerspruch / Werbewiderspruch ▪ unzulässige Verarbeitung

Rechte der Betroffenen / Pflicht des Verantwortlichen

Löschung

weitere Pflicht des Verantwortlichen

Prinzipien aus Art. 5	**Datenminimierung**	▪ Beschränkung auf das für den Zweck der Verarbeitung angemessene und sachlich relevante sowie notwendige Maß
	Richtigkeit	▪ Vorsehen von Maßnahmen zur unverzüglichen Löschung von unzutreffenden Daten
	Speicherbe-grenzung	▪ Speicherung mit Personenbezug höchstens so lange, wie es für die Verarbeitungszwecke erforderlich ist

Einschränkung der Verarbeitung (Art. 18)	**Löschung** (Art. 17)

Rechte der Betroffenen

Löschung / Einschränkung der Verarbeitung (Sperrung)

Pflicht des Verantwortlichen

Prinzipien aus Art. 5	**Integrität und Vertraulichkeit**	**Daten-minimierung**	**Richtigkeit**	**Speicher-begrenzung**
Sperren statt Löschen (§ 35 BDSG)	▪ wegen Löschaufwand bei **nicht automatisierter** Verarbeitung und geringem Interesse (gilt nicht bei unzulässiger Verarbeitung) ▪ bei satzungsmäßigen oder vertraglichen Aufbewahrungspflichten ▪ Bei „Zweckverbrauch“ soweit durch die Löschung schutzwürdige Interessen des Betroffenen gefährdet werden (Unterrichtungspflicht) ▪ Bei unzulässiger Verarbeitung soweit durch die Löschung schutzwürdige Interessen des Betroffenen gefährdet werden (Unterrichtungspflicht)			

Lehrveranstaltung Datenschutz

Ausgangspunkt

Interesse des Einzelnen, möglichst weitgehend Herr über seine Daten zu bleiben. Personenbezogene digitale Daten sollen daher nicht beliebig lange gespeichert werden

„Digitaler Radiergummi“
Löschpflichten auch hinsichtlich Verweisen im Internet

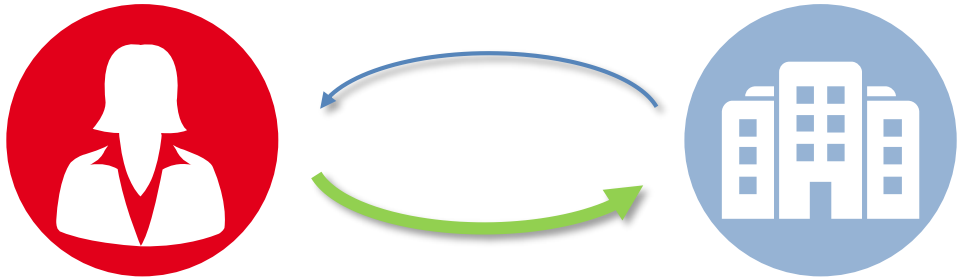
DS-GVO:
Art. 17 Abs. 2 – Recht auf Löschung (Recht auf „Vergessenwerden“)

Umsetzung des „digitalen Radiergummis“

- Information anderer Verantwortlicher über das Verlangen des Betroffenen zur Löschung
  - aller Links zu diesen personenbezogenen Daten oder
  - von Kopien oder Replikationen dieser Daten
- Berücksichtigung der verfügbaren Technologie und der Implementierungskosten

Mitteilungspflicht bei Intervention

Art. 19 DS-GVO



Intervention

- Berichtigung (Art. 16)
- Löschung (Art. 17, § 35 BDSG)
- Einschränkung der Verarbeitung (Art. 18)

Diesbezügliche Mitteilungspflichten nach Art. 19:

- Information der Empfänger über Ausübung der Rechte
- Ausnahme: unverhältnismäßig/unmöglich
- Information des Betroffenen (auf Verlangen) über die informierten Empfänger

Zwischenfall: Löschen impossible

Ex-Mitarbeiter M hegt auch 5 Jahre nach dem Ausscheiden aus dem Unternehmen einen Groll. Zwar wurden inzwischen alle überflüssigen Daten vom Operativsystem gelöscht, er weiß aber, daß die Human-Resources-Datenbank seit Gründung des Betriebes inkrementell auf Magnetbändern gesichert wurde.
Er verlangt nun die Löschung seiner Daten auch aus den Backups.

Zu Recht?

Lösungsskizze

Fragestellung: Besteht ein Löschanspruch gem. Art. 17 DS-GVO?

- Anwendbarkeit der DS-GVO (+), Art. 2 Abs. 1 DS-GVO: ganz oder teilweise automatisierte Verarbeitung. Keine private/familiäre Tätigkeit im Sinne von Art. 2 Abs. 2 lit. c DS-GVO.
  - Verantwortliche Stelle (+)
  - Betroffener (+)
  - Löschverlangen, Art. 17 Abs. 1 lit. a DS-GVO wegen Zweckerreichung (+)

- Ausnahme § 35 Abs. 1 Satz 1 BDSG?
- Wegen besonderer Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich? Beim inkrementellen Backup wird zunächst ein Vollbackup erstellt und sodann jede weitere Änderung zum vorigen Backup erneut gesichert. Zur Wiederherstellung sind das Vollbackup und sämtliche Inkremente erforderlich. [Anders beim differentiellen Backup: Beim differentiellen Backup wird zunächst ein Vollbackup erstellt und sodann jede weitere Änderung zum ersten Vollbackup gesichert. Zur Wiederherstellung sind das Vollbackup und das letzte Diff erforderlich.
- Unverhältnismäßigkeit hier wohl (+)
- ABER: § 35 Abs. 1 BDSG bezieht sich auf die *nicht-automatisierte* Verarbeitung

ERGEBNIS: Löschungsersuchen gemäß Art. 17 Abs. 1 Satz 1 DS-GVO **rechtmäßig, aber nicht durchsetzbar**. Die Sperrung tritt an die Stelle der Löschung.

Lösungsskizze

Gegendarstellung/Korrektur!

Fragestellung: Besteht ein Löschanspruch gem. Art. 17 DS-GVO?

- Anwendbarkeit der DS-GVO (+), Art. 2 Abs. 1 DS-GVO: ganz oder teilweise automatisierte Verarbeitung. Keine private/familiäre Tätigkeit im Sinne von Art. 2 Abs. 2 lit. c DS-GVO.
  - Verantwortliche Stelle (+)
  - Betroffener (+)
  - Löschverlangen, Art. 17 Abs. 1 lit. a DS-GVO wegen Zweckerreichung (+)

- Ausnahme § 35 Abs. 1 Satz 1 BDSG?
- Wegen besonderer Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich? Beim inkrementellen Backup wird zunächst ein Vollbackup erstellt und sodann jede weitere Änderung zum vorigen Backup erneut gesichert. Zur Wiederherstellung sind das Vollbackup und sämtliche Inkremente erforderlich. [Anders beim differentiellen Backup: Beim differentiellen Backup wird zunächst ein Vollbackup erstellt und sodann jede weitere Änderung zum ersten Vollbackup gesichert. Zur Wiederherstellung sind das Vollbackup und das letzte Diff erforderlich.
- Unverhältnismäßigkeit hier wohl (+)
- ABER: § 35 Abs. 1 BDSG bezieht sich auf die *nicht-automatisierte* Verarbeitung

ERGEBNIS: Löschungsersuchen gemäß Art. 17 Abs. 1 Satz 1 DS-GVO **rechtmäßig ~~, aber nicht durchsetzbar~~**. ~~Die Sperrung tritt an die Stelle der Löschung.~~

2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO
2.2.5 Aufsichtsbehörden für den Datenschutz

Lehrveranstaltung Datenschutz

System der Überwachung

EuGH

- Auslegung der DS-GVO
- Kontrolle der Kommissionsentscheidungen

Kommission

- Überwachung der Umsetzung der DS-GVO
- Erlass delegierter Rechtsakte

Europäischer Datenschutzausschuss

- Interpretation der DS-GVO
- Koordination der Zusammenarbeit

DS-GVO

Nationale Gerichte

- Auslegung der DS-GVO und nationaler Datenschutz-Vorschriften

Mitgliedsstaaten

- Ergänzen und modifizieren den Rechtsrahmen

Aufsichtsbehörden

- Überwachung der Umsetzung des Datenschutzes (Zusammenarbeit)

Die Aufsichtsbehörden in 28 Mitgliedsstaaten sollen die einheitliche Anwendung der DS-GVO überwachen und durchsetzen

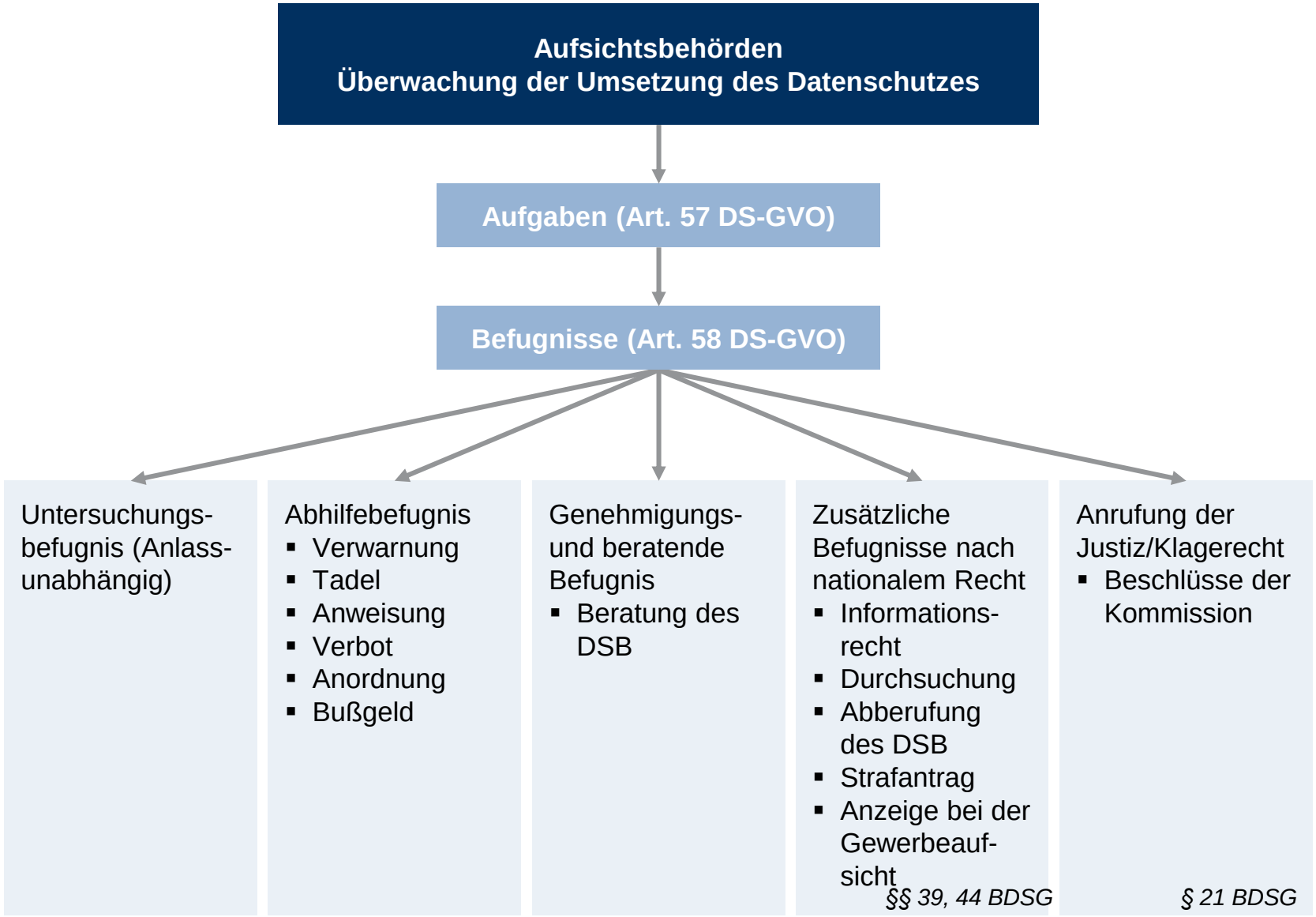
Kapitel VI	Unabhängigkeit der Aufsichtsbehörden
Abschnitt 1	Unabhängigkeit
Abschnitt 2	Zuständigkeit, Aufgaben und Befugnisse

Kapitel VII	Zusammenarbeit und Kohärenz
Abschnitt 1	Zusammenarbeit
Abschnitt 2	Kohärenz
Abschnitt 3	Europäischer Daten-schutzausschuss

Teil 1, Kapitel 4 BDSG	Bundesbeauftragte/r für den Datenschutz und die Informationsfreiheit
Teil 1, Kapitel 6 BDSG,	Rechtsbehelfe
LDSGs	Landesdatenschutzbeauftragte
Teil 2, Kapitel 4 BDSG,	Aufsichtsbehörde für nicht-öffentliche Stellen

Teil 1, Kapitel 5 BDSG	Vertretung im Europäischen Daten-schutzausschuss, zentrale Anlaufstelle, Zusammenarbeit der Aufsichtsbehörden in EU-Angelegenheiten

Lehrveranstaltung Datenschutz



Lehrveranstaltung Datenschutz

Zuständige Aufsichtsbehörde (Art. 55 DS-GVO)

„Jede Aufsichtsbehörde ist für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, ***im Hoheitsgebiet ihres eigenen Mitgliedstaats*** *zuständig.“*

18 Aufsichtsbehörden in Deutschland

EU: Eine Behörde pro Mitgliedstaat

Welche Behörde ist zuständig für Konzerne?

One-Stop-Shop Verfahren

Kriterien für die Identifikation einer federführenden Behörde bei einer grenzüberschreitenden Datenverarbeitung eines Verantwortlichen oder Auftragsverarbeiters (nach Art. 4 Abs. 23)

- Niederlassungen **in mehr als einem Mitgliedstaat** der EU und
- Verarbeitung der Hauptniederlassung von pbD im Rahmen der Tätigkeit dieser Niederlassungen

Achtung:

Es kann auch eine verteilte Verantwortlichkeit bestehen. D.h. Zwecke und Mittel einer Verarbeitung können auch „lokal“ bestimmt werden, so z. B. im Rahmen der Durchführung eines Beschäftigungsverhältnisses.

- **eine einzelne Niederlassung** in der EU,
- die Verarbeitung von pbD hat jedoch **erhebliche Auswirkungen** auf Betroffene **in mehreren Mitgliedstaaten**

Kriterien zu **„erheblichen Auswirkungen“** werden durch die Art. 29-Gruppe vorgeschlagen

Kriterien zu „erheblichen Auswirkungen“

- **eine einzelne** Niederlassung in der EU,
- die Verarbeitung von pbD hat jedoch **erhebliche Auswirkungen** auf Betroffene in mehreren Mitgliedstaaten

Einzelfallbetrachtung, Kriterien:

- Verarbeitungszusammenhang,
- Datenarten
- Zweck der Verarbeitung

Ferner u.a. zu fragen, ob die Verarbeitung

- Rechte der Betroffenen beschränkt, verwehrt oder ihnen Chancen bzw. Möglichkeiten vorenthält,
- Auswirkungen auf einen finanziellen oder wirtschaftlichen Status eines Betroffenen haben kann,
- die Analyse besonderer Arten pbD oder anderer in die Privatsphäre eingreifender Daten – insbesondere solche bei Kindern – beinhaltet,
- einen signifikanten Einfluss auf das Verhalten von Betroffenen hat oder haben kann,
- eine peinliche Situation oder andere negative Ergebnisse, einschließlich einer Rufschädigung, hervorruft,
- ein breites Spektrum an pbD beinhaltet.

Abgrenzung bei Unternehmensgruppen (EG 36)

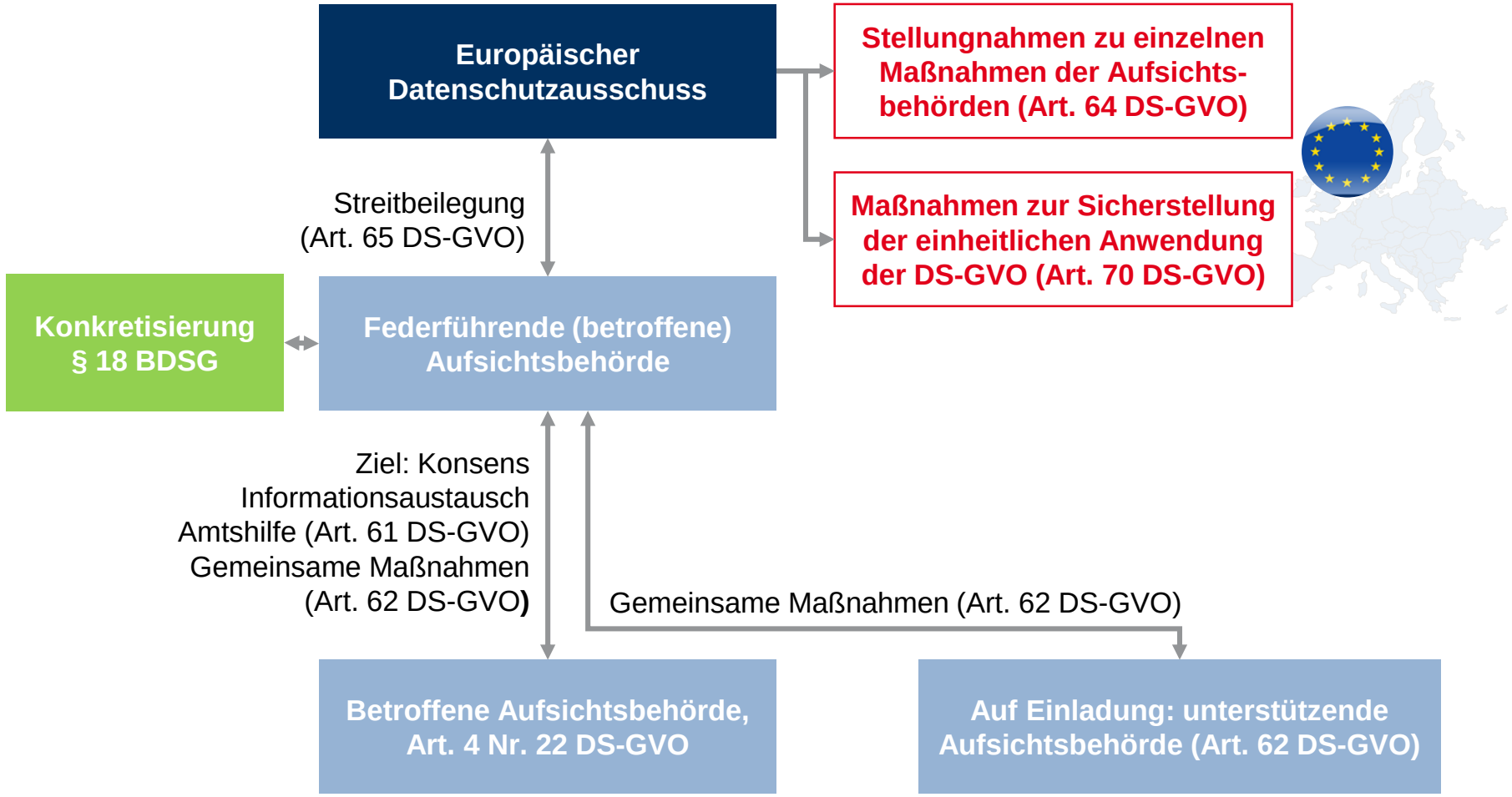
Konkretisierung zur „deutschen Kohärenz“ s. a. **§ 18 BDSG**

- Wo werden faktisch die **Managementaktivitäten** ausgeübt, die Entscheidungen über die **Zwecke und Mittel** einer Datenverarbeitung auf **Basis fester Vereinbarungen** beinhalten.
- Das Vorhandensein und die Nutzung von **technischen Mitteln und Technologien** stellen für sich noch keine bestimmenden Faktoren für die Bestimmung einer Hauptniederlassung dar.

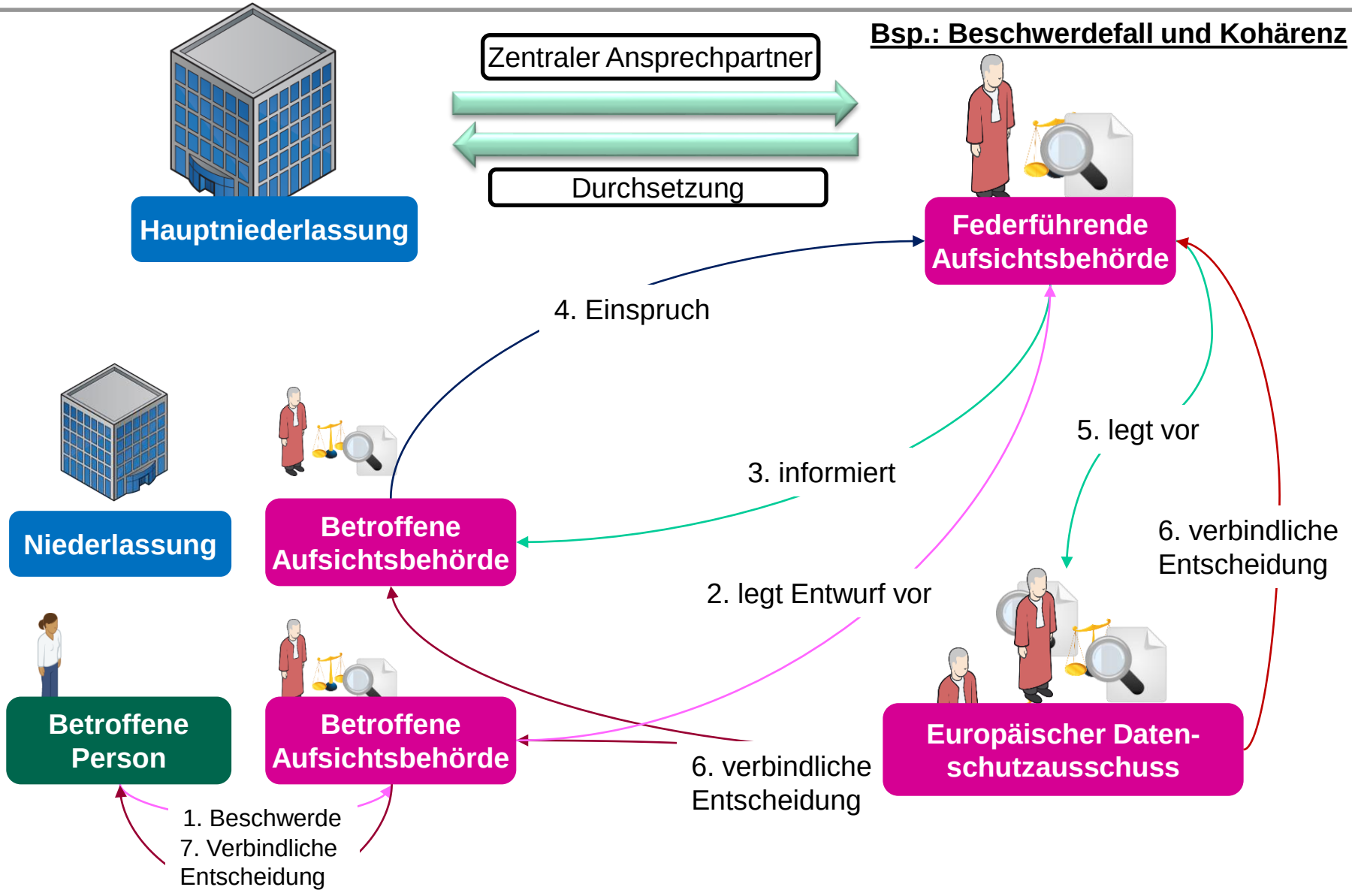
Die – nicht abschließenden – Kriterien nach Art. 29-Gruppe lauten u.a.:

- Wo werden Entscheidungen über die Zwecke und Mittel einer Datenverarbeitung letzten Endes unterzeichnet?
- Wo werden Entscheidungen über Geschäftsaktivitäten, die die Verarbeitung personenbezogener Daten zum Inhalt haben, gefällt?
- Wo liegt die effektive Entscheidungsbefugnis?
- Wo sind der oder die Leiter mit übergeordneten Managementverantwortlichkeiten für grenzüberschreitende Datenverarbeitungen angesiedelt?
- Wo ist der Verantwortliche oder Auftragsverarbeiter als Unternehmen registriert, falls dies in einem einzelnen Hoheitsgebiet erfolgt?

Kohärenz - Zusammenarbeit



Lehrveranstaltung Datenschutz



Kompetenzen der Aufsichtsbehörde

Kontrolle

- Anlassunabhängige Kontrolle
- Informations-, Betretens-, Besichtigungs-, Prüfungs- und Einsichtsrechte
- Datenübermittlungen an andere Aufsichtsbehörden / Zusammenarbeit / Amtshilfe innerhalb der EU
- Herausgabe regelmäßiger Tätigkeitsberichte

Durchsetzungs-/Sanktionsmaßnahmen nach pflichtgemäßen Ermessen

- Eigenständiges Antragsrecht bei BDSG-Straftatbeständen
- Unterrichtung des Betroffenen über Datenschutzverstöße und Anzeige bei den zuständigen Ahndungs- und Verfolgungsbehörden
- Anordnung von Maßnahmen zur Beseitigung festgestellter Verstöße im Hinblick auf die Zulässigkeit der Datenverarbeitung oder technisch-organisatorischer Mängel
- Untersagung des Datenumgangs oder einzelner Verfahren bei schwerwiegenden Verstößen
- Aufforderung zur Abberufung des betrieblichen DSB

Kompetenzen der Aufsichtsbehörde

Beratungspflicht gegenüber DSB und verantwortlicher Stelle

Weitere Kompetenzen

- Meldestelle bei „Datenpannen“ nach Art. 33
- Konsultation im Rahmen der Datenschutz-Folgeabschätzung
- Akkreditierungs- / Zertifizierungsstelle
- Überprüfung vorgelegter Verhaltensregelungen
- Genehmigungsverfahren bei Datentransfer in Nicht-EU/EWR-Staaten ohne angemessenes Datenschutzniveau
- Entwicklung von Standardverträgen zur Auftragsverarbeitung

2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO
2.2.5 Sanktionen bei Datenschutzverstößen

Systematik

Rechtswege

- Beschwerde bei Aufsichtsbehörde
- Gerichtsverfahren gegen Aufsichtsbehörde
- Gerichtsverfahren gegen Verantwortlichen/ Auftragsverarbeiter

- § 44 BDSG näheres zu Klagen gegen den Verantwortlichen oder Auftragsverarbeiter

Vertretung

- Vertretung des Betroffenen durch einen Verband
- Verbandsklagerecht (nach nationalem Recht)

- Klagerecht der Verbraucherverbände nach UKlaG

Sanktionen

- Schadensersatz
- Bußgeld
- Strafe (nach nationalem Recht)

- §§ 41, 43 BDSG Ausgestaltung des Bußgeldverfahrens, Ausweitung auf BDSG
- §§ 41, 42 BDSG Straftatbestände und -verfahren

Lehrveranstaltung Datenschutz

heise online

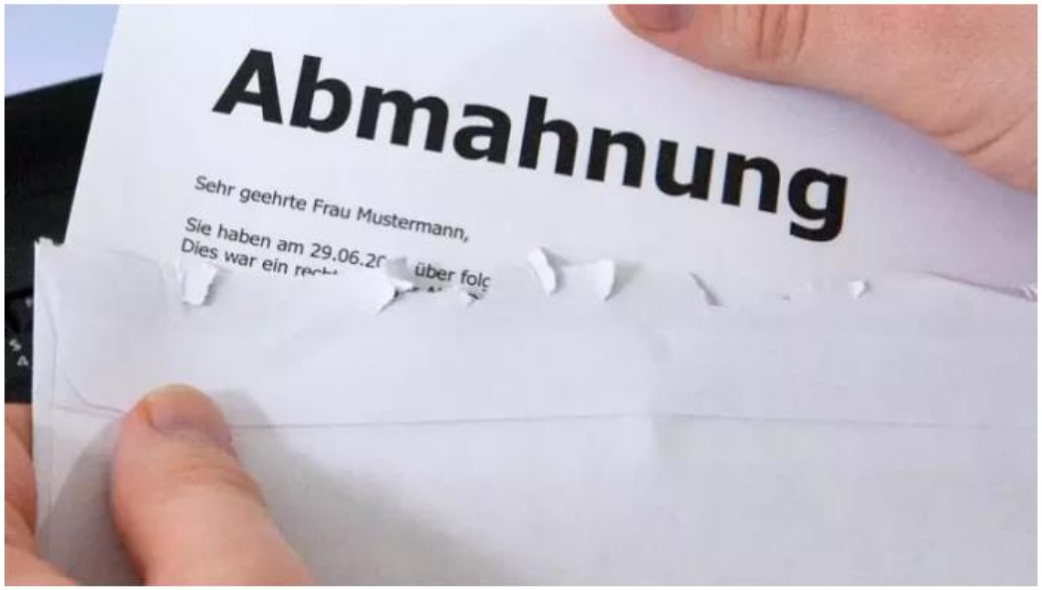
IT Mobiles Entertainment Wissen Netzpolitik Wirtschaft Journal Newsticker Foren

TOPTHEMEN: DSGVO COMPUTEX 2018 WINDOWS 10 ANDROID P KRYPTOWÄHRUNG ELEKTROAUTOS TESTS FACEBOOK-DATENSKANDAL

heise online > News > 05/2018 > DSGVO: Die Abmahn-Maschinerie ist angelaufen

DSGVO: Die Abmahn-Maschinerie ist angelaufen

30.05.2018 14:55 Uhr – Holger Bleich vorlesen



(Bild: dpa, Andrea Warnecke/Illustration)

Ähnliche Artikel

DSGVO: Last-Minute-Hilfe gegen Abmahnungen und Bußgelder

Seit wenigen Tagen ist das neue EU-Datenschutzrecht (DSGVO) wirksam. Wer jetzt noch Hilfe sucht, um die drohende Abmahngefahr zu vermeiden, sollte…

c't 444

Nachbesserungsgesetz soll negative Folgen der DSGVO eindämmen

Weil die deutsche Umsetzung der Datenschutz-Grundverordnung von Normalbürgern die aufwendige Dokumentation

Sind falsche oder fehlende Datenschutzerklärungen abmahnfähig?

Hanseatisches OLG, Urteil vom 27.06.2013 - 3 U 26/12

Wettbewerbsverstoß wegen fehlender Datenschutzhinweise - Bei § 13 Abs. 1 TMG handelt es sich um eine das Marktverhalten regelnde Norm im Sinne von § 4 Nr. 11 UWG.

UWG §§ 3, 4 Nr. 11, 5, 8; TMG §§ 5, 13; HWG § 7 Abs. 1 Nr. 2

KG Berlin, Beschluss vom 29.04.2011 - 5 W 88/11

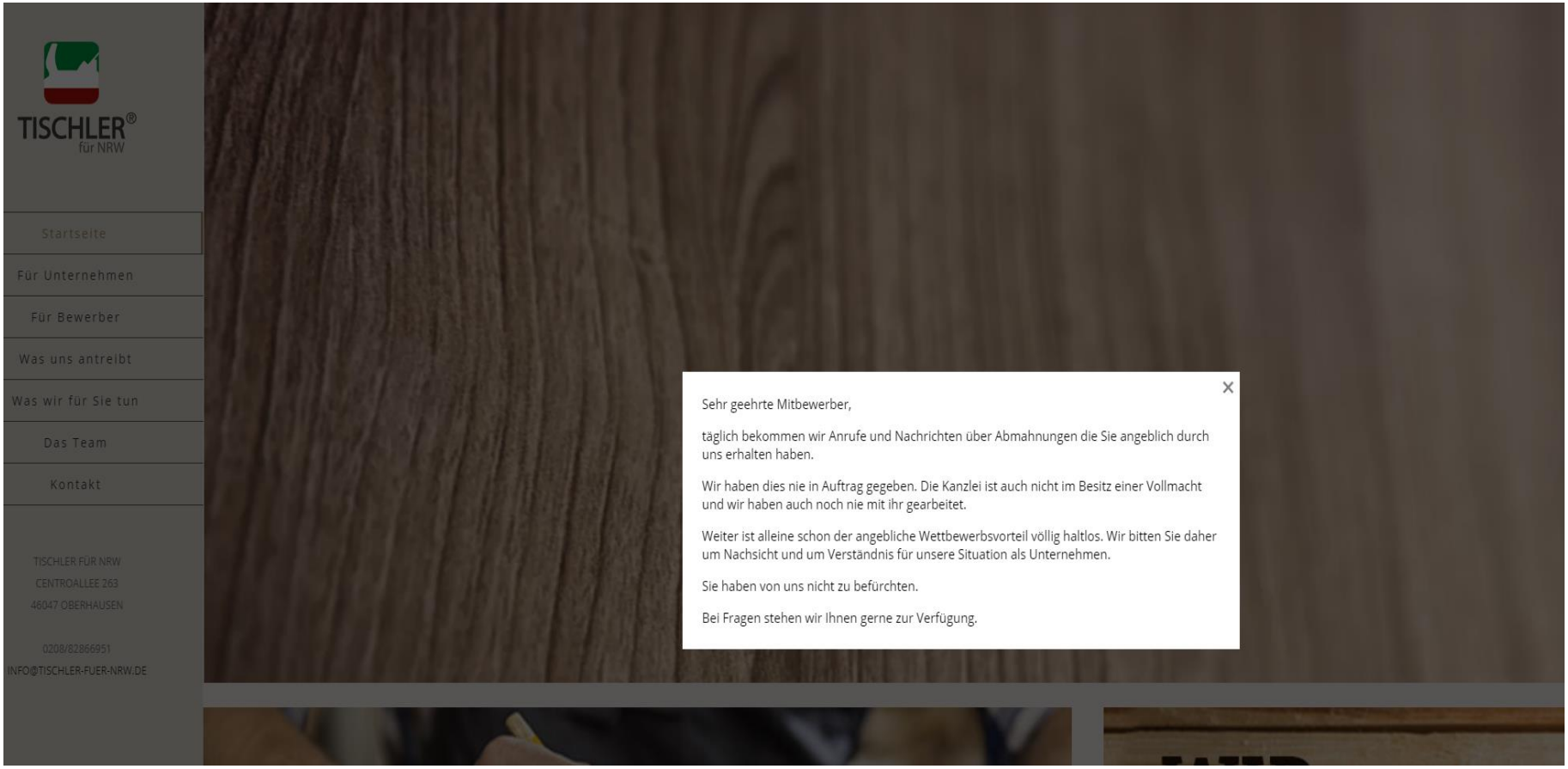
Kein Wettbewerbsverstoß durch Verwendung des facebook "Gefällt-mir"-Button unter Verstoß gegen die Informationspflichten nach § 13 Abs. 1 TMG - Zur Frage, ob ein Verstoß gegen § 13 Abs. 1 TMG als Verstoß gegen eine Marktverhaltensvorschrift im Sinne von § 4 Nr. 11 UWG anzusehen ist.

UWG §§ 3, 4 Nr. 11, 8 Abs. 1 und 3 Nr. 1; TMG §§ 12 Abs. 3, 13 Abs. 1, BDSG § 3

In diesem Sinne betrifft ein Verstoß gegen § 13 Abs. 1 TMG ein Verhalten, das dem Marktverhalten vorausgegangen ist und nur dann als Marktverhaltensvorschrift im Sinne des § 4 Nr. 11 UWG anzusehen ist, wenn ihm eine zumindest sekundäre wettbewerbsbezogene Schutzfunktion innewohnt (vgl. BGH GRUR 2010, 654 - Zweckbetrieb, Rn 18).

a) Diese Schutzfunktion ist im Hinblick auf die Mitbewerber des nach § 13 Abs. 1 TMG Informationspflichtigen nicht zu erkennen. Die Vorschriften im vierten Abschnitt des TMG mit der Überschrift „Datenschutz" verfolgen ebenso wie bereits die Vorgängerregelungen in dem bis zum 28. Februar 2007 gültigen TDDSG das Ziel, „eine verläßliche Grundlage für die Gewährleistung des Datenschutzes im Bereich der Teledienste zu bieten und einen Ausgleich zwischen dem Wunsch nach freiem Wettbewerb, berechtigten Nutzerbedürfnissen und öffentlichen Ordnungsinteressen zu schaffen" (vgl. BT-Drucksache 13/7385, S. 21, zum TDDSG; Schmitz in: Hoeren/Sieber, Handbuch Multimediarecht, 16.2, Rn 15).

Lehrveranstaltung Datenschutz



Bußgeldvorschriften

Bußgeld	Verstöße gegen die Artikel	Wer
Bis zu **10.000.000 Euro** oder im Fall eines Unternehmens bis zu **zwei Prozent seines weltweiten Jahresumsatzes***	8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 43 DS-GVO	Verantwortlicher, Auftragsverarbeiter
	42, 43 DS-GVO	Zertifizierungsstelle
	41 Abs. 4 DS-GVO	Überwachungsstelle
Bis zu **20.000.000 Euro** oder im Fall eines Unternehmens bis zu **vier Prozent seines weltweiten Jahresumsatzes***	5, 6, 7 und 9, 12-22, 44-49, 58 Abs. 1, 2 DS-GVO	Verantwortlicher, Auftragsverarbeiter

Berücksichtigung erschwerender und erleichternder (zum Beispiel Zertifizierung) Tatsachen, aber: in jedem Fall **„wirksam, verhältnismäßig und abschreckend“**

*** Je nachdem, was höher ist**

Quo vadis Bußgeldtatbestand?

Eine privat betriebene „Bußgeldstelle“ und die DSGVO

Ein Privatmann dokumentiert mehr als zehn Jahre lang über 50.000 Verkehrsverstöße und zeigt sie an. In der Regel fertigt er dabei Fotografien an oder macht Videoaufzeichnungen. Die Datenschutzaufsicht versucht, einzugreifen. Am Ende steht ein gerichtlich bestätigtes Bußgeld von sage und schreibe 250 €. Die Datenschutz-Grundverordnung (DSGVO) wird solche Billigtarife künftig nicht mehr zulassen.

Die Zeiten, in denen die Aufsichtsbehörden Datenschutzverstöße nur geringfügig mit Bußgeldern belegen konnten, sind vorbei (Bild: tforgo / iStock / Thinkstock)

Jedem sein Hobby?

Manche Menschen haben spezielle Hobbys. In diesem Fall ist es die Leidenschaft,

Straftatbestand

§§ 42 BDSG

- Verwirklichung eines Tatbestandes aus § 42 BDSG
- Vorsatz
- Handel, Bereicherungs- oder Schädigungsabsicht
- Rechtswidrigkeit und Schuld

+

Antrag durch
- Betroffenen,
- Verantwortlichen
- BfDI oder
- Aufsichtsbehörde

Freiheitsstrafe bis zu 2 bzw. 3 Jahren oder Geldstrafe

Schadenersatz

Art. 82 DS-GVO

Anspruchsberechtigter:

- Jede Person, die wegen Verstoß gegen die DS-GVO Schaden hat

Anspruchsverpflichteter:

- Verantwortlicher
- Auftragsverarbeiter

Verletzungshandlung:

- Datenverarbeitung, die nicht im Einklang mit der DS-GVO steht
- Verstoß gegen Pflichten als Auftragsverarbeiter oder gegen Weisungen

Schaden:

- materieller und
- immaterieller Schaden

Kausalität:

- Rechtswidrige Datenverarbeitung führt zum Schaden

Verschulden:

- Vermutetes Verschulden mit Exkulpationsmöglichkeit

Mehrere Beteiligte

- Gesamtschuldner (inkl. Auftragsverarbeiter)

- Eigenständige verschuldensabhängige Haftungsnorm
- Ersatzpflicht entfällt bei Beachtung der nach den Umständen gebotenen Sorgfalt
  - Beweispflicht des Unternehmens (z.B. im Rahmen der Accountabiliy)
- Ggf. allgemeine Haftungsansprüche z.B. nach dem Bürgerlichen Gesetzbuch (BGB)

Sanktionen gegenüber Beschäftigten

Als Täter eines als Ordnungswidrigkeit sanktionierten Verstoßes

Als Täter eines als Straftat sanktionierten Verstoßes

Arbeitsrechtliche Konsequenzen (Abmahnung, Kündigung)

Haftung sowohl der betroffenen Person als auch dem Arbeitgeber gegenüber

Mögliche Folgen von DS-Verstößen

Verantwortliche Stelle / Unternehmensleitung

- Straftat / Ordnungswidrigkeit
- Vermögensrechtliche Haftung gegenüber dem Betroffenen
- Einschreiten der Aufsichtsbehörde
- Reputationsverlust
- Ggf. Abmahnung (Verbraucher-schutz, Mitbewerber)

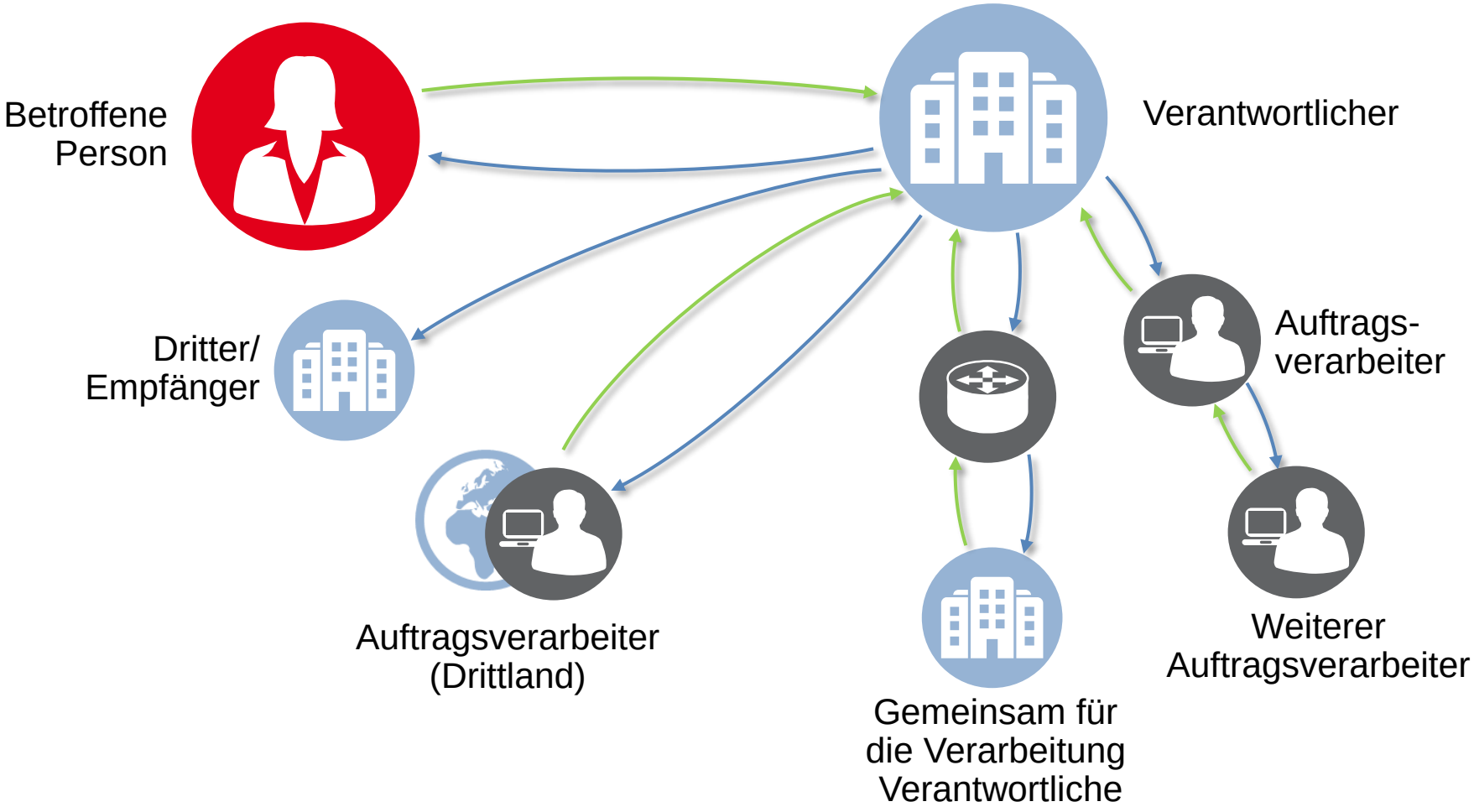
Mitarbeiter

- Straftat / Ordnungswidrigkeit
- Vermögensrechtliche Haftung gegenüber dem Betroffenen bzw. der verantwortlichen Stelle (Ausnahme: leichte Fahrlässigkeit)
- Arbeitsrechtliche Konsequenzen (Abmahnung, Kündigung)

2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO
2.2.6 Auftragsverarbeitung

Zusammenarbeit mit Dienstleistern



Beteiligte - Definitionen

„Verantwortlicher“:
Stelle, die
- allein oder
- gemeinsam mit anderen

über die
- Zwecke und
- Mittel

der Verarbeitung entscheidet

Art. 4 Nr. 7 DS-GVO

„Auftragsverarbeiter“:
Stelle,
- die personenbezogene Daten
- im Auftrag
- des Verantwortlichen

verarbeitet

Art. 4 Nr. 8 DS-GVO

Auftragsverarbeitung *Art. 28 DS-GVO*

Der Verantwortliche bleibt „Herr der Daten“:
- Er bestimmt über die Zwecke der Verarbeitung
- Er bestimmt über die Mittel der Verarbeitung (kann – durch Vertrag – delegiert werden)

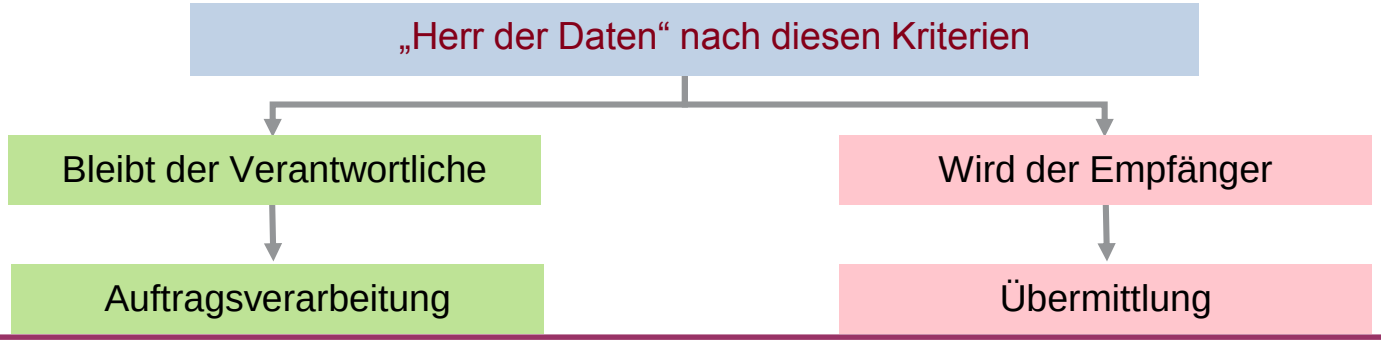
Lehrveranstaltung Datenschutz

Kriterien zur Abgrenzung: Verantwortlicher („Herr der Daten“) entscheidet insbes. über:

- den Zweck der Verarbeitung
- inhaltliche Fragen, die den Kern der Rechtmäßigkeit der Verarbeitung wesentlich betreffen
- wie lange Daten aufbewahrt werden
- wer Zugang zu den verarbeiteten Daten hat

- z. B. durch vertragliche Vorgaben, Weisungen
- Indiz insbes. „Kontakt“ zum Betroffenen
- wen treffen Aufbewahrungspflichten?
- wer hat das „Bestimmungsrecht“?

- Technische oder organisatorische Fragen können als Entscheidung über die „Mittel“ der Verarbeitung delegiert werden.



Beispiele

Auftragsverarbeitung

- Lohn- und Gehaltsabrechnung oder Finanzbuchhaltung durch RZ
- Cloud-Computing
- Werbeadressenverarbeitung in einem Lettershop,
- Callcenter ohne wesentliche eigene Entscheidungsspielräume
- Auslagerung der E-Mail-Verwaltung oder von sonstigen Datendiensten zu Webseiten
- Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten
- Backup-Sicherheitsspeicherung / Archivierungen
- Datenträgerentsorgung durch Dienstleister,
- Prüfung oder Wartung (z. B. Fernwartung, externer Support), wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann

Übermittlung

- Berufsgeheimnisträge, z. B.
  - Steuerberater,
  - Rechtsanwälte,
  - externe Betriebsärzte,
  - Wirtschaftsprüfer),
- Inkassobüros mit Forderungsübertragung,
- Bankinstitute für den Geldtransfer,
- Postdienstes für den Brieftransport

Eine Beschränkung der Auftragsverarbeitung ergibt sich z. B. aus:
- Speziellen Gesetzen (Berufsrecht)
- § 203 StGB

Pflichten zur Auftragsverarbeitung

Art. 28 DS-GVO

Verantwortlicher  Auftragsverarbeiter

- Sorgfältige Auswahl der Auftragsverarbeiter unter Vorlage „hinreichender Garantien“
- Schriftliche Verträge sind zwingend, Inhalte ergeben sich aus Art. 28
- Offizielle Vertragsmuster können zur Verfügung gestellt werden
- Zustimmungserfordernis für Unterauftragnehmer
- Auftragsverarbeitung im Drittland nur auf Weisung
- Ausdrückliche Kontrollpflicht fehlt zwar, ist aber durch Art. 5 Abs. 2 DS-GVO gefordert
- Bußgeld- und Haftungsbewehrt (gesamtschuldnerische Haftung)

Prüfschritte für den Auftraggeber

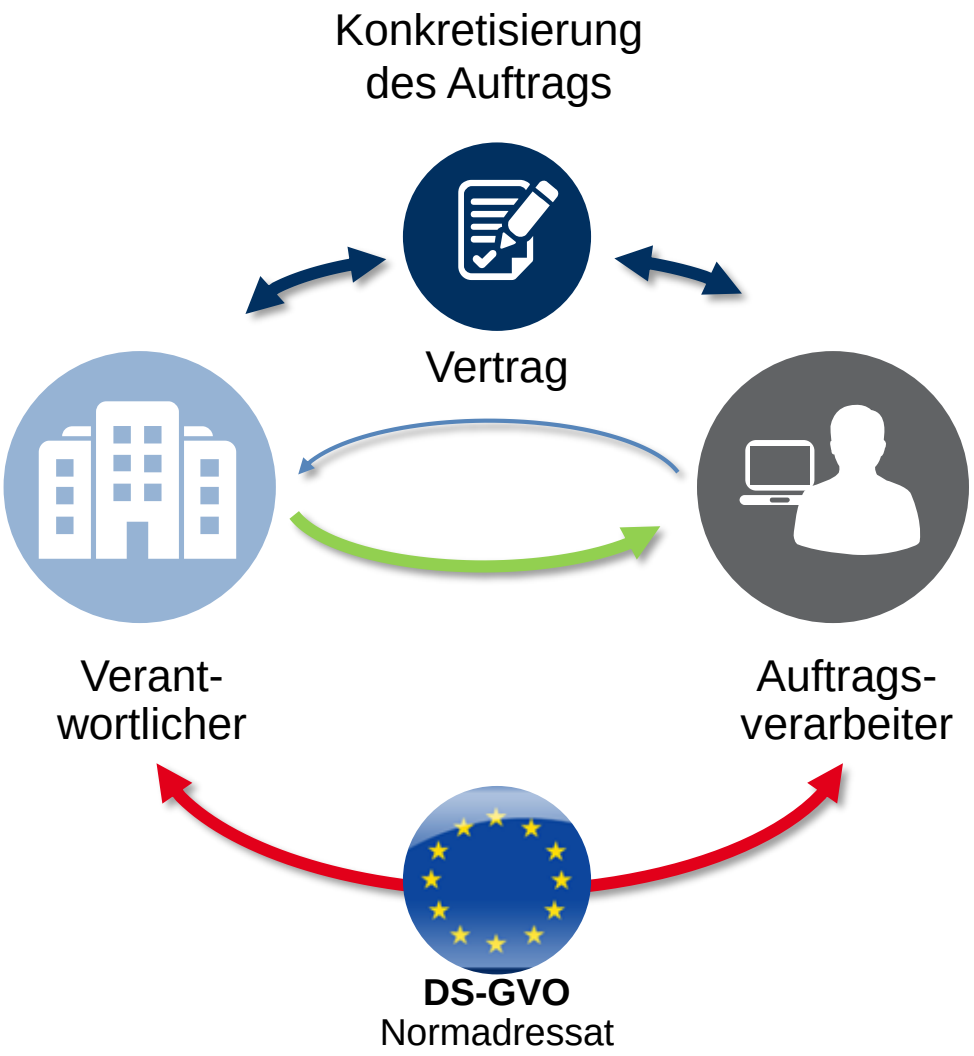
Art. 28 DS-GVO

Verantwortlicher  Auftragsverarbeiter

- Darf der Prozess überhaupt ausgelagert werden?
- Sorgfältige Auswahl des Auftragnehmers unter besonderer Berücksichtigung „hinreichender Garantien“, insbes. hinsichtlich der getroffenen technischen und organisatorischen Maßnahmen
- Schriftlicher Auftrag (Vorgaben insbes. nach Art. 28)
- Überprüfung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen

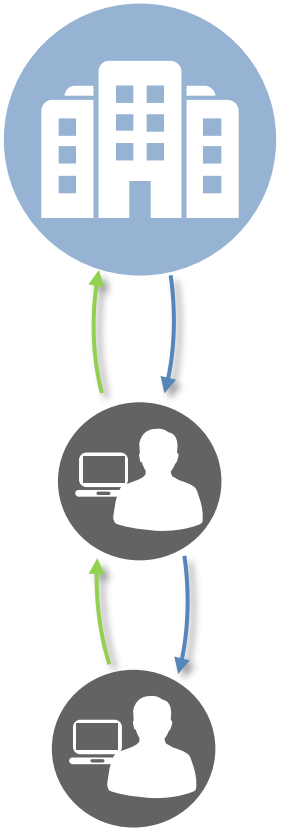
Sicht des Auftragsverarbeiters

- Eigenen Datenschutzpflichten (Datenschutz-/IT-Sicherheitsmanagement)
- Dokumentationspflicht für Auftragsverarbeitungen (Verträge, Weisungen)
- Aufsicht durch die Aufsichtsbehörden, s. insbes. Art. 57, 58
- Gesamtschuldnerische Haftung, s. insbes. Art. 79, 82
- Bußgeld, s. Art. 83



Unterauftragsverhältnisse

Art. 28 DS-GVO



- Auftragsverarbeiter ist Auftraggeber für „weitere Auftragsverarbeiter“:
  - Verantwortlich für Vertrag
  - Haftung für weitere Auftragsverarbeiter
  - Kontrolle der weiteren Auftragsverarbeiter
- Einzel- oder pauschale Zustimmungserfordernis (Dokumentationspflicht)
- Informationspflicht gegenüber dem AG
- Einspruchsrecht des AG bei pauschaler Zustimmung

Zwischenfall: Schick raus.

Die Wedel Group GmbH beauftragt einen Lettershop zur Aussendung eines neuen Werbeschreibens an Kunden. Absprachen zum Datenschutz werden hierbei nicht getroffen. Nachdem der externe Datenschutzbeauftragte der Wedel Group Wochen später Kenntnis von der Beauftragung erlangt hat, weist er die Geschäftsleitung darauf hin, dass gesetzliche Anforderungen zum Datenschutz mit Füßen getreten wurden.

Hat er Recht? Was hätte die Wedel Group beachten müssen?

Lösungsskizze

Fragestellung: Welche datenschutzrechtlichen Pflichten hätten beachtet werden müssen?

- Anwendbarkeit der DS-GVO (+), Art. 2 Abs. 1 DS-GVO: ganz oder teilweise automatisierte Verarbeitung.
  Keine private/familiäre Tätigkeit im Sinne von Art. 2 Abs. 2 lit. c DS-GVO.
  - Personenbezug (+), Art. 4 Nr. 1 DS-GVO
  - Verarbeitung (+), Art. 4 Nr. 2 DS-GVO: Übermittlung

- Auftragsverarbeitung gem. Art. 28 DS-GVO?
  - Lettershopverfahren ist als datenverarbeitende Unterstützungsleistung des Dienstleisters zu sehen und damit eine Auftragsdatenverarbeitung nach Art. 28 DS-GVO
  - Datenschutzvereinbarung mit den Inhalten des Art. 28 Abs. 3 S. 2 DS-GVO notwendig
  - Sorgfältige Auswahl des Dienstleisters vor Auftragserteilung hätte erfolgen müssen unter Vorlage hinreichend geeigneter Garantien für technisch-organisatorische Maßnahmen (Art. 28 Abs. 1 DS-GVO)
  - Regelmäßige Kontrollen der technisch-organisatorischen Maßnahmen und deren Dokumentation sind mit Blick auf Art. 24 Abs. 1 DS-GVO sowie Art. 5 Abs. 2 DS-GVO

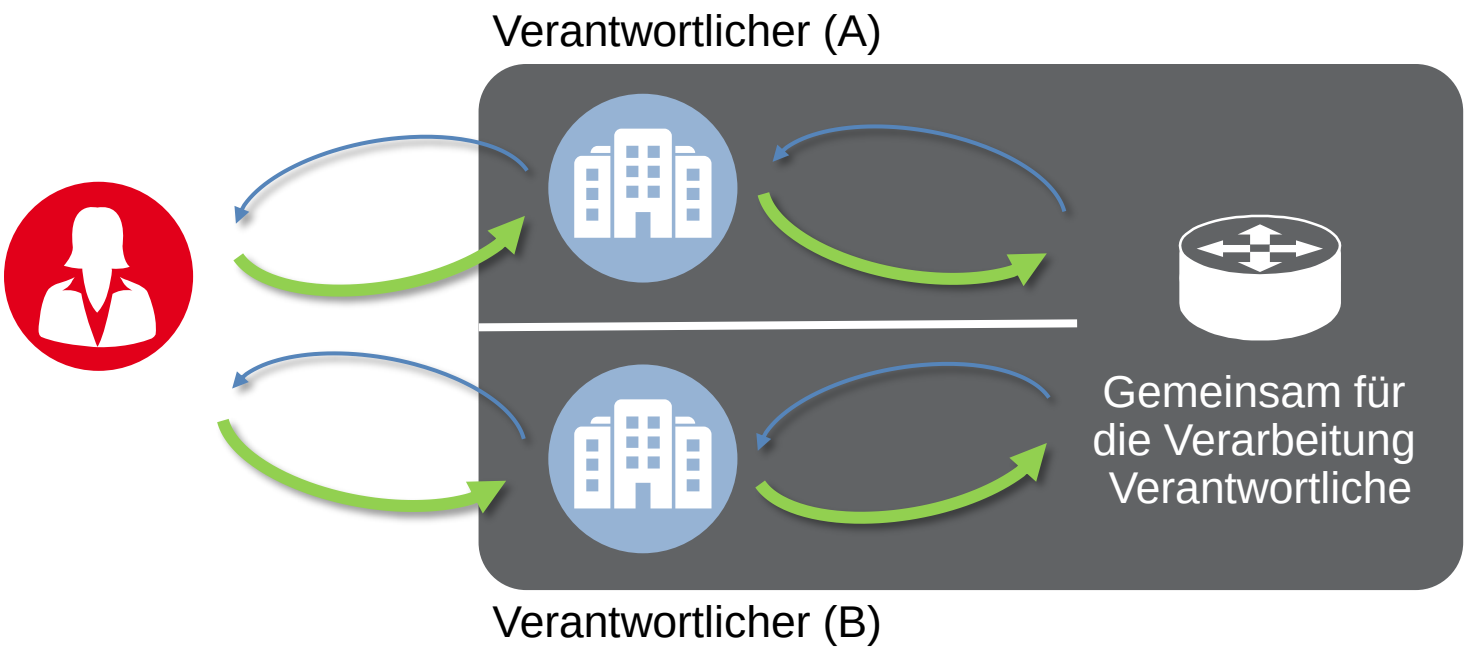
ERGEBNIS: Der externe Datenschutzbeauftrage hat Recht. Die Vorgaben des Art. 28 DS-GVO hätten vorab der Datenübermittlung umgesetzt werden müssen. Ein Verstoß gegen Art. 28 DS-GVO kann gem. Art. 83 Abs. 4 lit. a DS-GVO mit einem Bußgeld bis zu 10.000.000 EUR oder im Falle eines Unternehmens von bis zu 2 % seines weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs geahndet werden.

2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO
2.2.7 Joint Controller

Gemeinsam für die Verarbeitung Verantwortliche

Art. 26 DS-GVO



Zwei oder mehr Verantwortliche legen gemeinsam

- die **Zwecke** der

und

- die **Mittel** zur

Verarbeitung fest

Vereinbarung in transparenter Form:

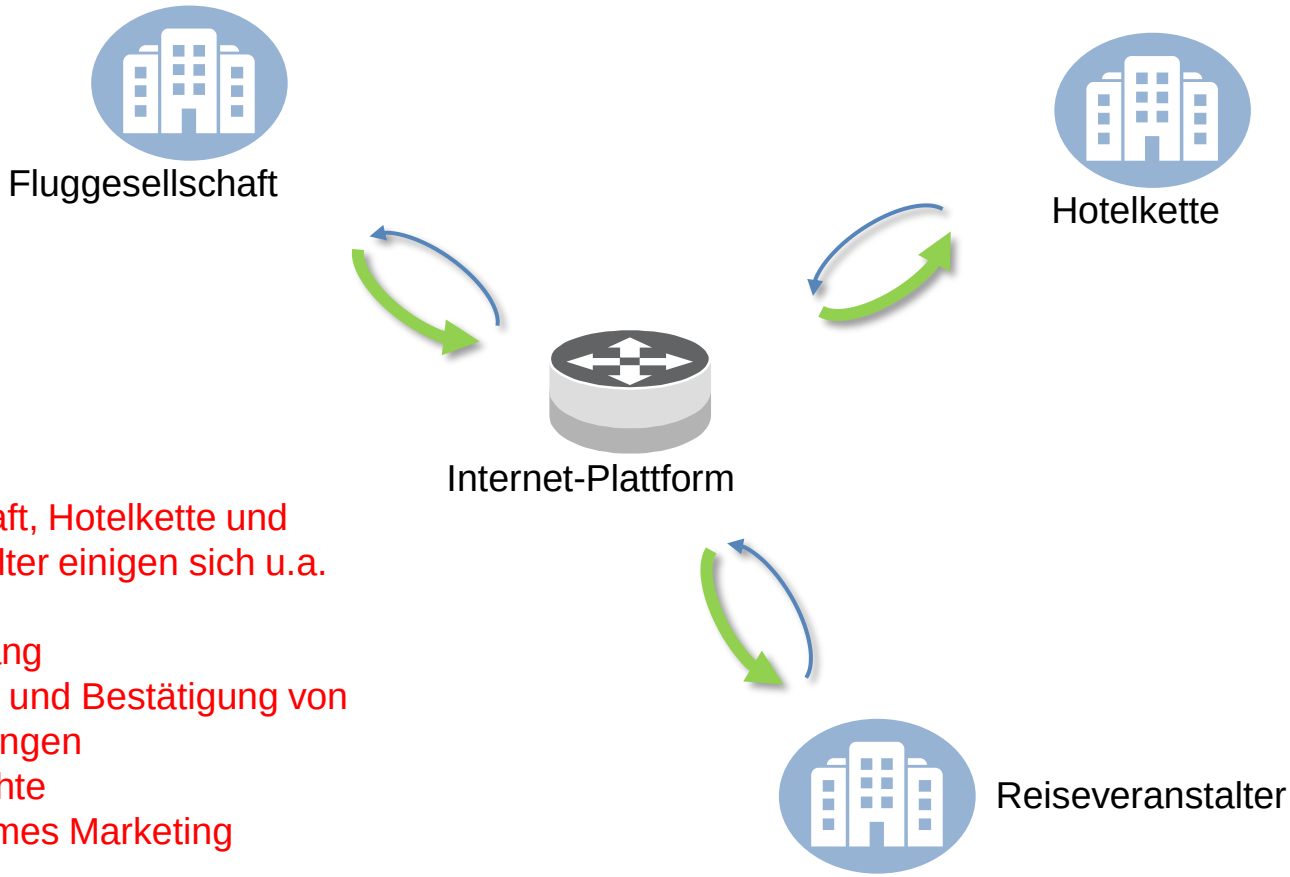
- wer welche Verpflichtung der DS-GVO erfüllt, insbesondere
  - Wahrnehmung der Rechte der betroffenen Person
  - wer welchen Informationspflichten nachkommt
  - es kann eine Anlaufstelle für betroffene Personen angegeben werden
- zu den jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen

Die wesentlichen Inhalte sind den betroffenen Person zur Verfügung zu stellen

Beispiel

Art. 26 DS-GVO

Beispiel: Gemeinsame Internet-Plattform zur Optimierung der Abwicklung von Reisebuchungen



Fluggesellschaft, Hotelkette und Reiseveranstalter einigen sich u.a. hinsichtlich

- Datenumfang
- Zuweisung und Bestätigung von Reservierungen
- Zugriffsrechte
- Gemeinsames Marketing

Facebook Fanpages

DSK
DATENSCHUTZKONFERENZ

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 6. Juni 2018

Die Zeit der Verantwortungslosigkeit ist vorbei: EuGH bestätigt gemeinsame Verantwortung von Facebook und Fanpage-Betreibern

Die unabhängigen Datenschutzbehörden des Bundes und der Länder begrüßen das Urteil des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018, das ihre langjährige Rechtsauffassung bestätigt.

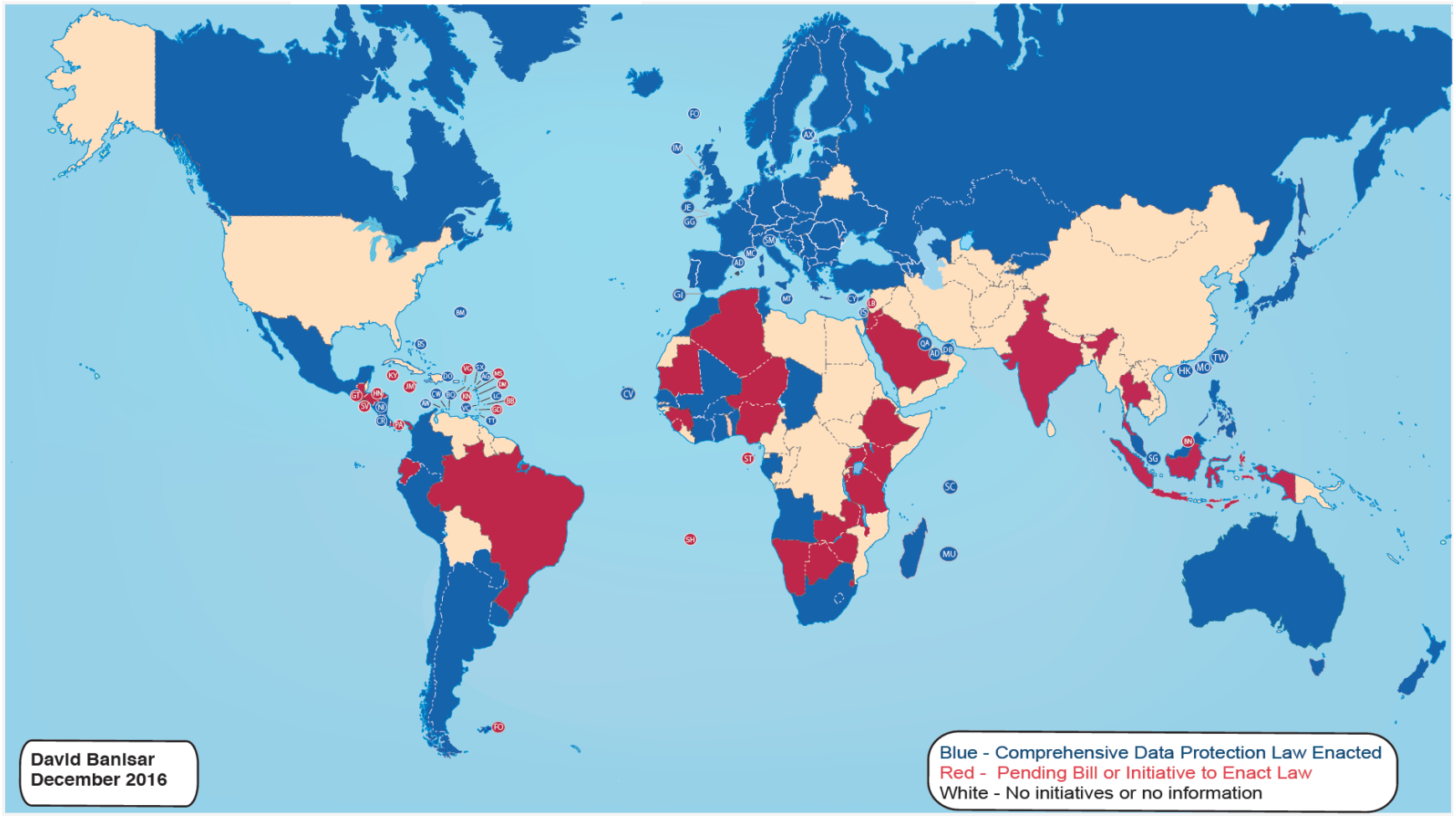
Das Urteil des EuGH zur gemeinsamen Verantwortung von Facebook und den Betreibern einer Fanpage hat unmittelbare Auswirkungen auf die Seitenbetreiber. Diese können nicht mehr allein auf die datenschutzrechtliche Verantwortung von Facebook verweisen, sondern sind selbst mitverantwortlich für die Einhaltung des Datenschutzes gegenüber den Nutzenden ihrer Fanpage.

Dabei müssen sie die Verpflichtungen aus den aktuell geltenden Regelungen der Datenschutz-Grundverordnung (DS-GVO) beachten. Zwar nimmt das Urteil Bezug auf die frühere Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr, doch die vom EuGH festgestellte Mitverantwortung der Seitenbetreiber erstreckt sich auf das jeweils geltende Recht, insbesondere auf die in der DS-GVO festgeschriebenen Rechte der Betroffenen und Pflichten der Verarbeiter.

2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO
2.2.8 Datenübermittlung in Drittländer

National Comprehensive Data Protection/Privacy Laws and Bills 2016



2-Stufen-Prinzip

(Art. 44 ff DS-GVO)

Stufe 1

Ist die Weitergabe von Daten zulässig?

Voraussetzung:

- Erlaubnistatbestände (Kapitel II DS-GVO)

Stufe 2

Ist es zulässig, dass die Daten außerhalb der EU/des EWR verarbeitet werden?

Voraussetzung:

- Angemessenheitsbeschluss (Art. 45)
- Geeignete Garantien (Art. 46)
- Rechtshilfeabkommen (Art. 48)
- Sonderfälle (Art. 49)
- Ausnahmen (Art. 49 Abs. 1 *letzter Satz*)

s.a. DSK - Kurzpapier Nr. 4 - Datenübermittlung in Drittländer

Mechanismen der „2. Stufe“

Zulässigkeit der Übermittlung in Staaten außerhalb der EU/EWR
grundsätzlich nur bei angemessenem Schutzniveau

Anerkennung durch unterschiedliche Mechanismen

- Anerkennung des Rechtssystems einzelner Staaten / Sektoren
- Angemessenheit beim Empfänger

Teilweise ist die Übermittlung genehmigungspflichtig

Fokus:
Geschäftsprozesse, regelmäßiger Datenaustausch

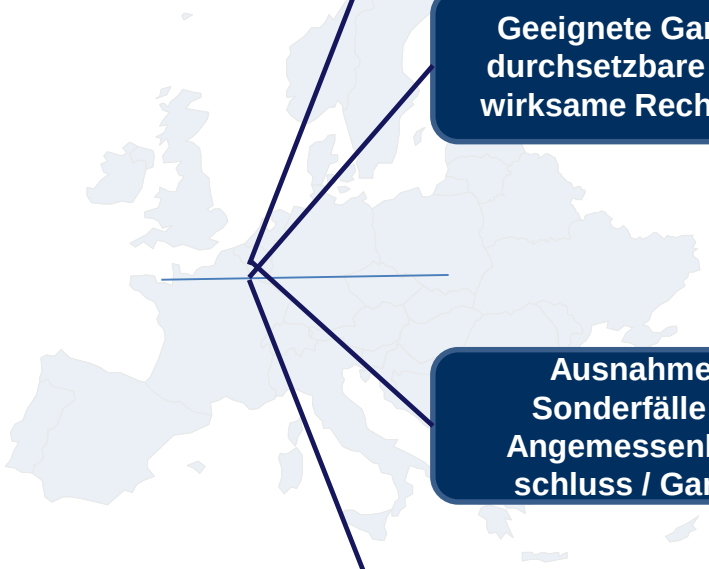
Ausnahmen

Insbesondere im Interesse des Betroffenen

Fokus:
Datenweitergabe im Einzelfall

Lehrveranstaltung Datenschutz

Mechanismen der „2. Stufe“



Angemessenheits-beschluss für Drittland, Gebiet oder Sektor

Übermittlungen genehmigungsfrei; bestehende Beschlüsse bleiben in Kraft

Geeignete Garantien + durchsetzbare Rechte + wirksame Rechtsbehelfe

Genehmigungsfrei: BCR; Standard-verträge; Verhaltensregeln (Art. 40); Zertifizierung (Art. 42)
Genehmigungspflichtig: Vertragsklauseln; Kohärenzverfahren; bestehende Genehmigungen bleiben in Kraft

Ausnahmen für Sonderfälle (ohne Angemessenheitsbe-schluss / Garantien)

Insbes. Einwilligung, Vertrag / vorvertragl. Maßnahmen auf Antrag des Betroffenen; Vertrag im Interesse des Betroffenen; Rechtsansprüche; lebenswichtige Interessen; Übermittlung aus einem öffentlichem Register

Ausnahmen von Ausnahmen und vom angemessenen Schutzniveau

Beurteilung und Garantien erforderlich; genehmigungsfrei aber Information der Aufsicht und (zusätzlich zu Art. 13/14) Information der Betroffenen

Beliebte Mechanismen der Unternehmen

- Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DS-GVO)
  - Für die Datenweitergabe an **Auftragsdatenverarbeiter** (2010/87/EU)
  - Für die Datenübermittlung an eine **verantwortliche Stelle** (2004/915/EG und 2001/497/EG)
- Angemessenheitsentscheidungen der Kommission (Art. 45 DS-GVO)
- Binding Corporate Rules (BCR) (Art. 47 DS-GVO)
  - Für Unternehmen
  - Für Auftragsverarbeiter
- EU-U.S. Privacy Shield

Die Mechanismen sind nicht unumstritten!

© pressmaster / fotolia.com

Die ungewisse Zukunft der Standardvertragsklauseln

Um Daten aus Europa in die USA zu übermitteln bedarf es einer Rechtsgrundlage. Zurzeit können die Daten auf Grundlage von Standardvertragsklauseln oder auf Grundlage des EU-US-Privacy-Shields (welches derzeit überprüft wird) in die USA übermittelt werden.

Nun werden auch die EU-Standardvertragsklauseln durch den Europäischen Gerichtshof (EuGH) überprüft.

News

Newsticker Foren

IT Mobiles Entertainment Wissen Netzpolitik Wirtschaft Jo

Topthemen: Windows 10 Firefox iPhone 8 iOS 11 Fritzbox Alexa Google Pixel

heise online > News > 11/2016 > Bürgerrechtsorganisationen klagen gegen den "EU-US Privacy Shield"

Bürgerrechtsorganisationen klagen gegen den "EU-US Privacy Shield"

01.11.2016 13:25 Uhr – Christiane Schulzki-Haddouti vorlesen

Irische und französische Bürgerrechtsorganisationen haben gegen den "EU-US Privacy Shield" Nichtigkeitsklagen eingereicht. Ob sie zugelassen werden, hat das Gericht der Europäischen Union noch nicht entschieden.

KLAGE UM FACEBOOK-DATEN

EuGH erklärt Safe Harbor für ungültig

Erfolg für Max Schrems: Der Europäische Gerichtshof hat das Safe-Harbor-Abkommen zwischen der EU und den USA für ungültig erklärt. Das Urteil könnte vor allem für kleine und mittelständische Unternehmen in der EU Probleme verursachen.

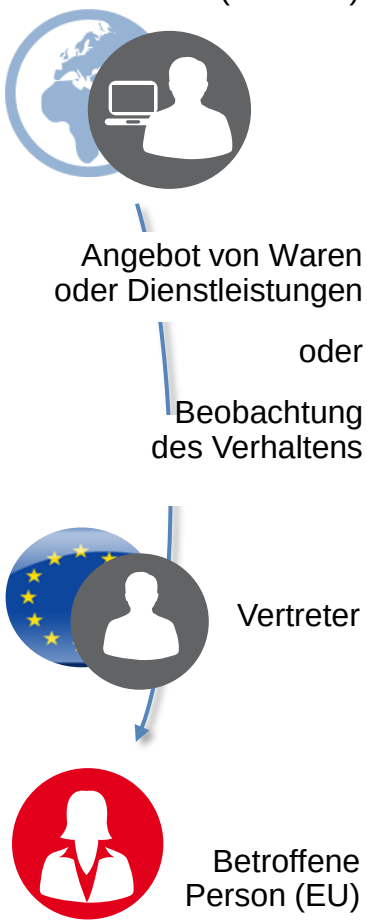
Von Hauke Gierow

Gesetzeslage zum Datenschutz in den USA (Exkurs):

- Kein umfassendes Gesetz zum Schutz personen-bezogener Daten vorhanden
- Sektorspezifische Regelungen existieren (Federal, Trade Commission Act, Children's Online Privacy Protection Act (COPPA), Health Insurance Portability and Accountability Act, Fair Credit Reporting Act etc. [Bundesebene], Security breach notification laws auf Bundesstaatenebene etc.)

Vertreter

Art. 27 DS-GVO



Marktortprinzip

Verpflichtung für Verantwortliche / Auftragsverarbeiter in Drittstaaten zur Benennung eines „Vertreters“

Ausnahme:
- „gelegentliche“ Verarbeitung „nicht-sensitiver“ Daten
- Behörden / öffentliche Stellen

- Der Vertreter ist zu beauftragen
- In einem EU-Staat, in dem die Handlung erfolgt
- Zusätzliche Stelle insbes. für Aufsichtsbehörden und Betroffene bei sämtlichen Fragen im Zusammenhang mit der Verarbeitung zur Gewährleistung der Einhaltung der DS-GVO

Art. 4 Nr. 17:
„Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;

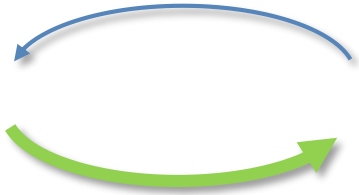
2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO
2.2.9 Datenverarbeitung für Werbezwecke

Lehrveranstaltung Datenschutz

Ausgangslage

Betroffene Person / Kunde / Interessent



Verantwortlicher

Zwecke

Vertrag	Kundenbetreuung / Kundenbindung	Werbung
• Anbahnung • Durchführung • Beendigung …	• CRM • Datenanalyse • Befragung …	• für eigene Zwecke • für Dritte …

Ansprache

Brief

Telefon

Fax

E-Mail

(Sonstige) Nachrichten

Personenbezogene Werbung unterliegt neben der DS-GVO zusätzlichen (engeren!) Voraussetzungen insbesondere nach § 7 UWG (Kommunikationswege):

Werbung ist

„jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen, einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen zu fördern."

Art. 2a) der Richtlinie über vergleichende und irreführende Werbung (2006/114/EG)

Abgrenzung:

- Werbung
- Information im laufenden Vertragsverhältnis
- Kundenbetreuung / Geschäftsbeziehung
- Markt-/ Meinungsforschung

Zulässigkeit der Werbung

Vertrags-durchführung:

Kundenbetreuung, insbes.
- **Bestell-/ Lieferprozess**
- **Beschwerde-management**

Kompatible Weiterverarbeitung:
- **z. B. Weitergabe bei Leistungs-störung (Rechtsanwalt, Inkasso)**

Interessens-abwägung:
- **insbes. Werbung**

Zur Zulässigkeit der Werbung:
- Interessensabwägung (Art. 6 Abs. 1 lit. f DS-GVO)
- Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO)
- Kompatible Weiterverarbeitung (Art. 6 Abs. 4 DS-GVO)

Zu beachten:
- Informationspflichten
- Werbewiderspruch
- Einzelauswertung / Profiling

Einzelne Werbeformen

- Die DS-GVO sieht Werbung als „berechtigtes Interesse“ (EG 47)
- Es besteht eine Pflicht zur Berücksichtigung der „reasonable expectations“ (EG 47) des Adressatenkreises (Betroffene)
  - Besondere Bedeutung der Informationspflichten nach Art. 13, 14 DS-GVO
- Die Eigenwerbung gegenüber Bestandskunden ist möglich
- Die Nutzung von eigenen Datenbeständen für Werbezwecke Dritter ist möglich
- Datenübermittlungen für Werbezwecke ist grds. möglich
- Eine Beschränkung auf bestimmte Datenarten ist grds. nicht vorgesehen
- Bei einer nachträglichen Entscheidung zur werblichen Datenverarbeitung ist der „Kompatibilitätstest“ (Art. 6 Abs. 4) durchzuführen

Umsetzung Werbewiderspruch

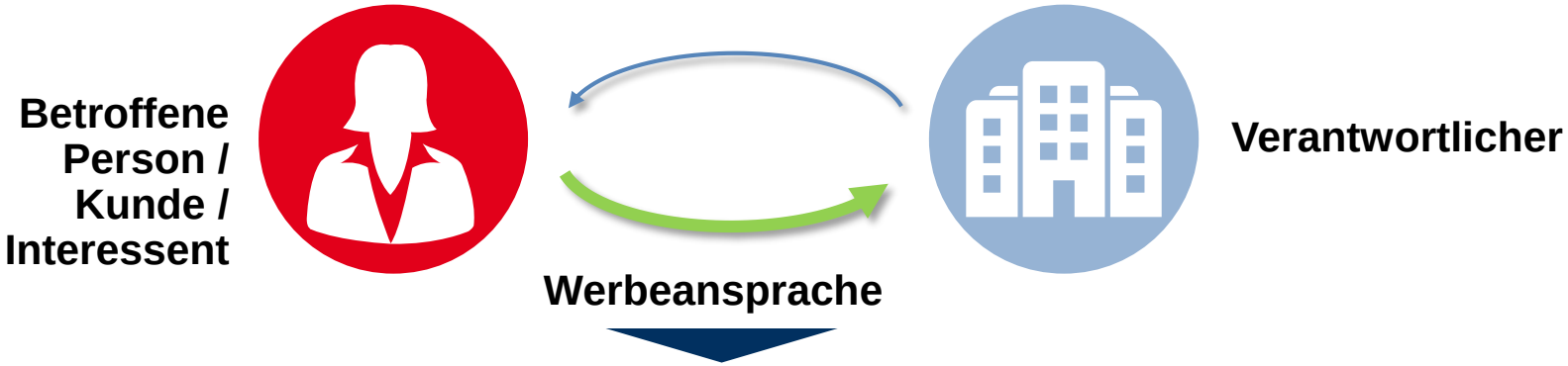
Beispiel Werbewidersruch

„Sofern Sie keine an Ihren Interessen orientierte Werbung mehr erhalten möchten, können Sie hiergegen jederzeit kostenfrei und mit Wirkung für die Zukunft Widerspruch einlegen. Hierfür genügt eine E-Mail an xxx@yy.zz.“

GDD-Ratgeber Werbung nach DS-GVO

- Widerspruch bei nicht personenbezogener Werbung durch Briefkastenaufkleber (anderer Ansicht: OLG München, Urteil vom 05.12.2013 - 29 U 2881/13 sowie LG Lüneburg, Urteil vom 04.11.2011 - 4 S 44/11)
- Schutz gegen Werbung auf Basis einer Einwilligung: Widerruf der Einwilligung

Werbeansprache vs. UWG



Grundsatz zur Ansprache (nach Art der Kontaktaufnahme):

- Schutz der „Marktteilnehmer“ (Verbraucher und sonstige „Marktteilnehmer“) vor unzumutbarer Belästigung durch Werbung.
- Ansprache zur Werbung ist abhängig vom (erklärten) Willen des Marktteilnehmers

§ 7 Abs. 2 UWG

Eine unzumutbare Belästigung ist stets anzunehmen
1. bei Werbung unter Verwendung eines [...] für den Fernabsatz geeigneten Mittels der kommerziellen Kommunikation, durch die ein Verbraucher **hartnäckig** angesprochen wird, obwohl er dies **erkennbar nicht wünscht**;
2. bei Werbung mit einem **Telefonanruf** gegenüber einem Verbraucher ohne dessen vorherige ausdrückliche Einwilligung oder gegenüber einem sonstigen Marktteilnehmer ohne dessen zumindest mutmaßliche Einwilligung,
3. bei Werbung unter Verwendung einer automatischen **Anrufmaschine**, eines **Fax**gerätes oder **elektronischer Post**, ohne dass eine vorherige ausdrückliche Einwilligung des Adressaten vorliegt, oder
4. bei Werbung mit einer Nachricht,
a) bei der die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird oder
b) bei der gegen § 6 Absatz 1 des Telemediengesetzes verstoßen wird oder in der der Empfänger aufgefordert wird, eine Website aufzurufen, die gegen diese Vorschrift verstößt, oder
c) bei der keine gültige Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

Ansprache per Brief

Brief

UWG

Zulässig soweit kein hartnäckiges Ansprechen, obwohl dies erkennbar nicht erwünscht ist

Datenschutzrecht

Zulässigkeit nach den datenschutzrechtlichen Vorschriften ist gegeben

Ansprache per Telefon

(§ 7 Abs. 2 Nr. 2 UWG)

Differenzierung zwischen Verbrauchern und sonstigen Marktteilnehmern

Telefon

Verbraucher

vorherige ausdrückliche Einwilligung

B2B

auch mutmaßliche Einwilligung genügt

⇒ Nach der Rspr. ist nötig, dass „*auf Grund konkreter Umstände ein sachliches Interesse des Anzurufenden*“ erwartet werden kann

E-Mail Werbung

(§ 7 Abs. 2 Nr. 3 UWG)

Grundsatz:

Vorherige ausdrückliche Einwilligung des Adressaten erforderlich

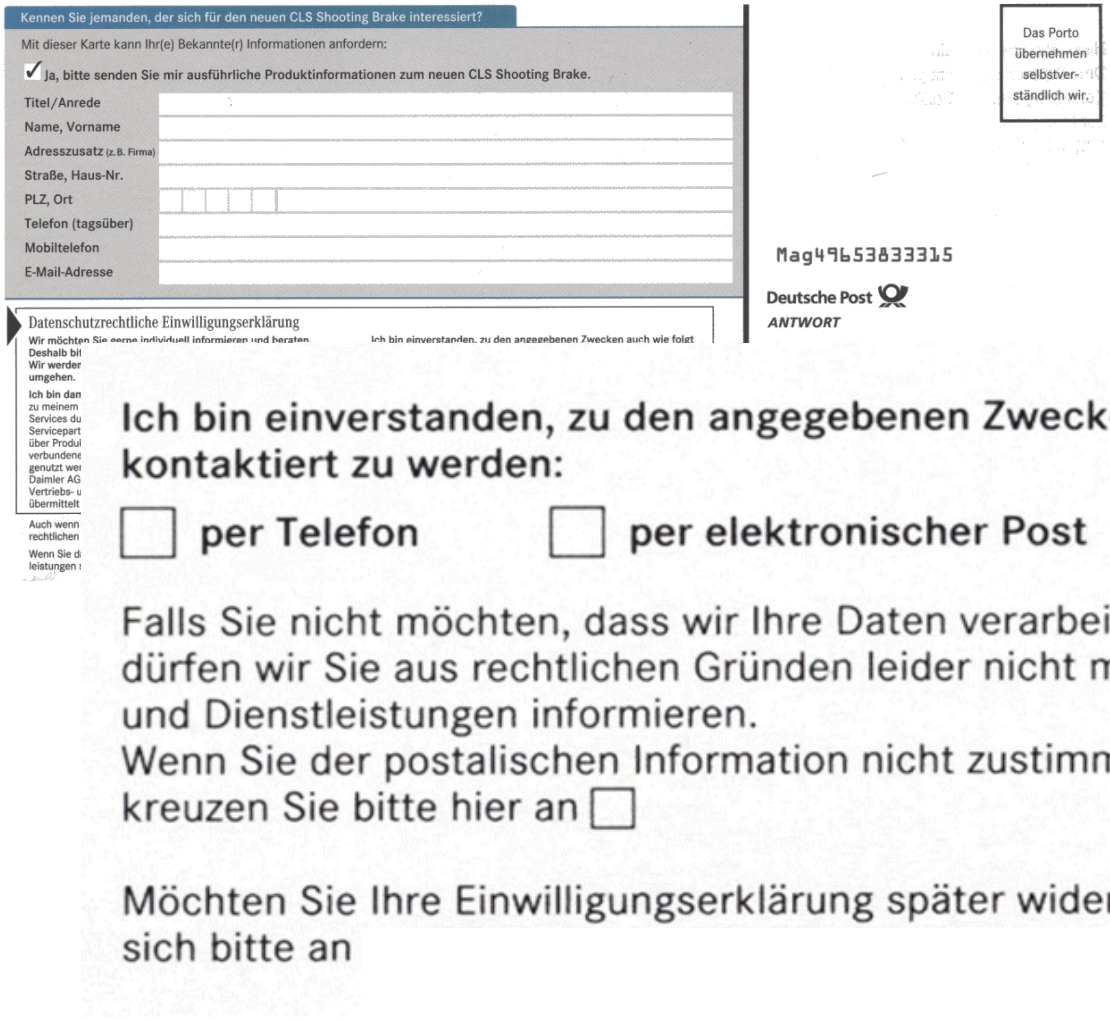
⇒ Keine Differenzierung zwischen Verbrauchern und sonstigen Marktteilnehmern!

Ausnahme:

Die Einwilligung des Beworbenen ist entbehrlich, wenn sämtliche (!) Voraussetzungen des § 7 Abs. 3 UWG vorliegen

1. *Erhalt der elektronischen Postadresse vom Kunden im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung.*
2. *Verwendung der Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen.*
3. *Der Kunde hat der Verwendung nicht widersprochen.*
4. *Der Kunde wird bei der Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.*

Gebündelte Werbung



Kennen Sie jemanden, der sich für den neuen CLS Shooting Brake interessiert?

Mit dieser Karte kann Ihr(e) Bekannte(r) Informationen anfordern:

☑ Ja, bitte senden Sie mir ausführliche Produktinformationen zum neuen CLS Shooting Brake.

Titel/Anrede
Name, Vorname
Adresszusatz (z. B. Firma)
Straße, Haus-Nr.
PLZ, Ort
Telefon (tagsüber)
Mobiltelefon
E-Mail-Adresse

Datenschutzrechtliche Einwilligungserklärung

Wir möchten Sie gerne individuell informieren und beraten. Ich bin einverstanden, zu den angegebenen Zwecken auch wie folgt

Deshalb bi
Wir werder
umgehen.

Ich bin dan
zu meinem
Services du
Servicepart
über Produl
verbundene
genutzt wer
Daimler AG
Vertriebs- u
übermittelt

Auch wenn
rechtlichen

Wenn Sie di
leistungen

Das Porto übernehmen selbstverständlich wir.

Mag496538333l5

Deutsche Post
ANTWORT

Ich bin einverstanden, zu den angegebenen Zwecken auch wie folgt kontaktiert zu werden:

☐ per Telefon ☐ per elektronischer Post

Falls Sie nicht möchten, dass wir Ihre Daten verarbeiten und nutzen, dürfen wir Sie aus rechtlichen Gründen leider nicht mehr über Produkte und Dienstleistungen informieren.
Wenn Sie der postalischen Information nicht zustimmen wollen, kreuzen Sie bitte hier an ☐

Möchten Sie Ihre Einwilligungserklärung später widerrufen, wenden Sie sich bitte an

Zwischenfall: Beipackwerbung

Die A GmbH verschickt ihre Elektronik-Kataloge auf Bestellung per Post. In der Sendung sind auch Wertgutscheine für den Weinhandel der B-GmbH enthalten.
Rechtmäßigkeit?

Lösungsskizze

Fragestellung: Ist die Datenverarbeitung zulässig?

- Versenden der Kataloge an die Postadresse?
  - Vertragserfüllung, Art. 6 Abs. 1 lit. b (+/-)
  - Einwilligung, Art. 6 Abs. 1 lit. a (+/-)
  - Interessenabwägung, Art. 6 Abs.1 lit. f (+)
- Versenden der Gutscheine?
  - Zweckänderung, Art. 6 Abs. 4 (+/-)
  - Interessenabwägung, Art. 6 Abs.1 lit. f (+)

ERGEBNIS: Datenverarbeitung wohl zulässig..

Zwischenfall: Kaufabbrecher

Ein Kunde klickt sich durch einen Online-Shop, bei dem er angemeldet ist. Er deponiert diverse Waren in seinem Warenkorb, bricht dann jedoch den Bestellvorgang ab und loggt sich aus.
Einige Stunden später meldet sich ein Shop-Mitarbeiter telephonisch, was er für den Kunden tun könne, damit die Bestellung doch noch erfolgt.
Rechtmäßigkeit?

Lösungsskizze

Fragestellung: Ist die telefonische Ansprache zulässig?

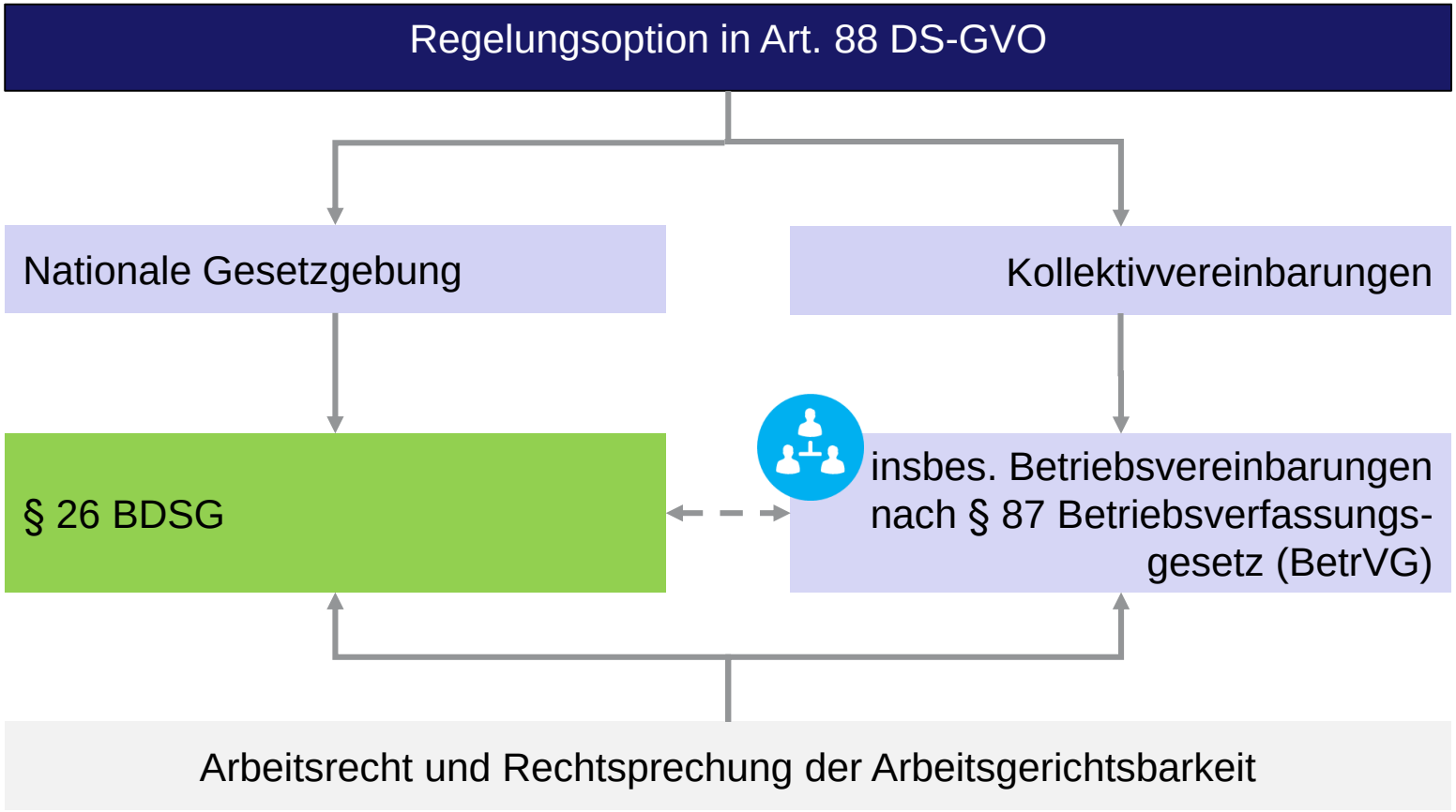
- Speicherung des Bestellverlaufs?
  - Art. 6 Abs. 1 lit. b (+)
- Speicherung nach Abbruch des Kaufs?
  - Art. 6 Abs. 1 lit. a/b/f (-)
- Ggf. separate Speicheroption anbieten?
- Kontaktaufnahme
  - § 7 Abs. 2 Nr. 2 UWG

ERGEBNIS: Die telefonische Kontaktaufnahme war ohne Einwilligung des Betroffenen unzulässig.

2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO
2.2.10 Beschäftigtendatenschutz

Regelung des Beschäftigtendatenschutzes



Definition „Beschäftigte“

(§ 26 BDSG)

- Arbeitnehmerinnen und Arbeitnehmer (einschließlich Leiharbeitnehmer/-innen im Verhältnis zum Entleiher),
- zu ihrer Berufsbildung Beschäftigte,
- Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
- in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
- Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten,
- Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
- Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende Bewerberinnen,
- Bewerber für ein Beschäftigungsverhältnis,
- Personen, deren Beschäftigungsverhältnis beendet ist.

Lehrveranstaltung Datenschutz

Datenumgang für Zwecke des Beschäftigungsverhältnisses

§ 26 Abs. 1 S. 1 BDSG

Verarbeitung durch den Betriebsrat

§ 26 Abs. 1 S. 1 BDSG

Aufdeckung von Straftaten

§ 26 Abs. 1 S. 2 BDSG

Einwilligung im Beschäftigungsverhältnis

§ 26 Abs. 2 BDSG

Betriebsvereinbarungen

§ 26 Abs. 4, 6 BDSG

Umgang mit besonderen Datenarten i. S. d. Art. 9, § 26 Abs. 1 S. 1 BDSG

§ 26 Abs. 3 BDSG

§ 26 Abs. 1 - 6 BDSG gelten auch für pb Beschäftigtendaten, wenn sie nicht in einem Dateisystem gespeichert werden (sollen)

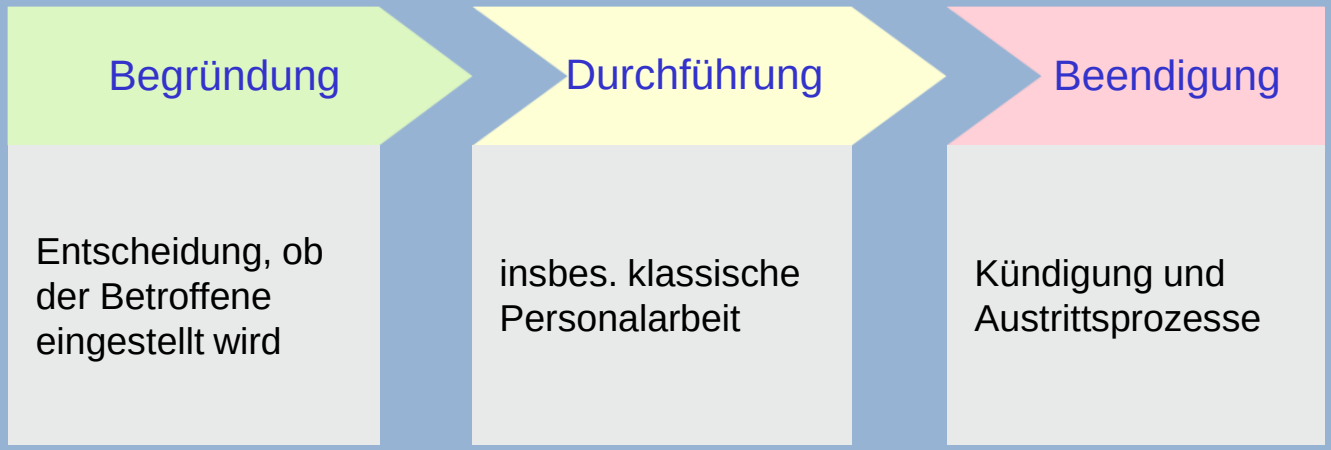
§ 26 Abs. 7 BDSG

Für den **nicht-automatisierten Umgang** (Personalakten etc.) gelten ebenfalls die allgemeinen arbeitsrechtlichen Grundsätze, z. B. BetrVG, arbeitsrechtliche Rechtsprechung zum Personalaktenrecht, Videoüberwachung etc.

Achtung: § 26 Abs. 1 S. 1 i.V.m. Abs. 5 BDSG gilt als Umsetzung zu Art. 10 DS-GVO

Allgemeiner Zulässigkeitsrahmen – Konkretisierung der Zweckbestimmung des Beschäftigungsverhältnisses (§ 26 Abs. 1 S. 1 BDSG)

Personenbezogene Daten eines Beschäftigten dürfen erhoben, verarbeitet und genutzt werden, wenn dies erforderlich ist für das Beschäftigungsverhältnis zu seiner



Anknüpfung: (Arbeits-)Vertrag

Vorbehalt: abweichende Kollektivvereinbarungen

Verarbeitung von Beschäftigtendaten außerhalb von § 26 BDSG

Art. 6 DS-GVO, insbes. Abs. 1 lit. f) - Interessenabwägung – und Abs. 4 – kompatible Weiterverarbeitung - bleiben neben § 26 BDSG anwendbar.

Beispiele für die Anwendung des Art. 6 DS-GVO:

- Mitteilung an Strafverfolgungsbehörden ohne gesetzliche Verpflichtung
- Versand von arbeitsplatzbezogener Werbung (Jahreswagen) oder einer Arbeitgeberzeitschrift
- Veröffentlichung von Verbesserungsvorschlägen u.ä.
- Auskunft an Gläubiger oder Inkassofirma bei Forderungstitel
- Due-Dilligence Prüfung

Einwilligung im Beschäftigungsverhältnis

Besonderheit der datenschutzrechtlichen Einwilligung zur Datenverarbeitung im Beschäftigungsverhältnis: Freiwilligkeit

Inhalt des § 26 Abs. 2 BDSG:

- Freiwilligkeit ist aufgrund des Abhängigkeitsverhältnisses fragwürdig
- Freiwilligkeit kann insbesondere vorliegen bei
  - reinem rechtlichen oder wirtschaftlichen Vorteil für Beschäftigten oder
  - gleichgelagerten Interessen zwischen Arbeitgeber und Beschäftigtem
- Informationspflichten (Zweck der Datenverarbeitung und Widerrufsrecht – Art. 7 Abs. 3) des Arbeitgebers und grundsätzliches Schriftformerfordernis der Einwilligung

Bewerbungsverfahren

Konkretisierung im Bewerbungsverhältnis (§ 26 Abs. 1 S. 1 BDSG):
Personenbezogene Daten eines Beschäftigten dürfen verarbeitet werden, wenn dies erforderlich ist für die Entscheidung, ob der Betroffene eingestellt wird

- Fragerecht und Offenbarungspflicht
- Persönlichkeitsrechtschutz und Diskriminierungsverbot (AGG)
  - Objektives Informationsinteresse für fundierte Einstellungsentscheidung unter Beachtung der Interessenabwägung und des Verhältnismäßigkeitsprinzips, z. B. bei:
    - Gesundheitsdaten
    - Schwerbehinderung
    - Vermögensverhältnissen
    - Religionszugehörigkeit
    - Schwangerschaft
    - …….
  - Konkretisiert durch die Rechtsprechung

Erhoben werden und mitzuteilen sind Daten,

1. die erforderlich sind zur Entscheidung über die Begründung des Beschäftigungs-verhältnisses
2. und nicht diskriminieren

Allgemeines Gleichbehandlungsgesetz (AGG)

Benachteiligungen

- aus Gründen der Rasse oder wegen der ethnischen Herkunft,
- der Religion oder Weltanschauung,
- des Alters,
- des Geschlechts,
- einer Behinderung
- oder der sexuellen Identität

sollen verhindert oder beseitigt werden.

Folge:
Diese Daten dürfen zur Begründung des Beschäftigungsverhältnisses grundsätzlich nicht erhoben werden

Aber:

Nicht jede Ungleichbehandlung verstößt gegen das Benachteiligungsverbot.

Zulässig können unter bestimmten Voraussetzungen (Eigenschaften) unterschiedliche Behandlungen sein wegen

- beruflicher Anforderungen (§ 8 AGG),
- der Religion und Weltanschauung (§ 9 AGG)
- des Alters (§ 10 AGG)

wenn die Eigenschaft eine wesentliche und entscheidende berufliche Anforderung darstellt

Offenbarungspflicht bei der Bewerbung

Der Bewerber ist zur **ungefragten Mitteilung** von Tatsachen verpflichtet, von denen er annehmen muss, dass sie für den Arbeitgeber für die Einstellungsentscheidung maßgebend sind.
(gesundheitliche Handikaps etc.)

Anfechtung wegen Täuschung wegen arglistiger Täuschung bei der Einstellung
= LAG Frankfurt vom 21.9.2011- 8 Sa 109/11-

Wenn ein Arbeitnehmer den Arbeitgeber bei Abschluss des Arbeitsvertrages bewusst über persönliche Eigenschaften, die für das Arbeitsverhältnis von Bedeutung sind, (hier: gesundheitliche Eignung zur Tätigkeit als Frachtabfertiger in Nacht- und Wechselschicht) täuscht, rechtfertigt dies die Anfechtung des Arbeitsvertrages, der damit sofort beendet ist.

Zwischenfall: Du bekommst heute leider keine Anstellung bei mir.

Dietrich Kernig, Inhaber des Grafikbüros „An.alog“ hat seine Luschenbande satt. Bewerber für die Tätigkeit als Grafiker in seinem Betrieb sollen zumindest einmal Zeit hinter schwedischen Gardinen verbracht haben. Insofern sieht der neue Papier-Bewerberfragebogen besagte Abfrage vor. Kernig ist der Meinung, als Inhaber dürfe ihm niemand in die Gewerbefreiheit nach Art. 14 GG hineinreden.

a. Zu Recht?

b. Ändert sich die Einschätzung, wenn Kernig eine Bank betreibt?

Lösungsskizze

Frage: Ist die Datenverarbeitung zulässig?

Anwendbarkeit der DS-GVO (-), Art. 2 Abs. 1 DS-GVO: Keine ganz oder teilweise automatisierte Verarbeitung. Fragebogen beinhaltet keine Dateistruktur
ABER: § 26 Abs. 7 BDSG: Beschäftigtendatenschutz gilt auch bei nicht-automatisierten Verarbeitungen außerhalb einer Dateistruktur.
Keine private/familiäre Tätigkeit im Sinne von Art. 2 Abs. 2 lit. c DS-GVO.

Personenbezug (+), Art. 4 Nr. 1 DS-GVO
Verarbeitung (+), Art. 4 Nr. 2 DS-GVO: Erhebung

Zu a.
Zulässigkeit für die Begründung des Beschäftigungsverhältnisses, § 26 Abs. 1 S. 1 BDSG?
Erforderlichkeit (-); Qualifikation als Grafiker steht in keinem Zusammenhang mit der Frage nach einer Haft

Zu b.
Erforderlichkeit der allgemeinen Frage nach einer Haft (-); anders wäre zu urteilen, wenn es um die Frage nach Vorstrafen im Bereich der Vermögensdelikte ginge

Arbeitsverhältnis

Konkretisierung im Arbeitsverhältnis (§ 26 Abs. 1 S. 1 BDSG):
Personenbezogene Daten eines Beschäftigten dürfen verarbeitet werden, wenn dies erforderlich ist Durchführung des Beschäftigungsverhältnisses (insbes. klassische Personalarbeit)

Erforderliche Verarbeitung zur Durchführung des Beschäftigungsverhältnisses insbes.

- wenn sie unmittelbar aus dem Arbeitsvertrag abgeleitet werden kann
  (Bsp.: Nutzung von Personaldaten zur Abrechnung)

- bei Herleitung aus den Arbeitsvertrag ausfüllenden, ggf. ungeschriebenen Rechten und Pflichten
  (Bsp.: IT-Leiter soll für Notfälle eine private Kontaktnummer hinterlassen)

Wichtig:
Ergibt sich die Zulässigkeit nicht unmittelbar aus dem Arbeitsvertrag, bedingt die „Erforderlichkeit“ eine Interessenabwägung unter Beachtung des Verhältnismäßigkeits prinzips

Beispiel - Unternehmensverkauf

- Umstrukturierungen erfordern oft die Offenbarung von Mitarbeiterdaten gegenüber potenziellen Erwerbern

Rechtsgrundlagen:

- Art. 6 Abs. 1 lit. f) / Abs. 4 DS-GVO (Veräußerungsinteresse / Vertraulichkeitsinteresse)
- Nur jeweils erforderliche Daten
- Datensicherheit gewährleisten (z. B. sicherer Data-Room)
- Möglichst anonymisiert

Beispiel – Übermittlung an Matrix-Vorgesetzte

- Vorgesetzte nicht nur im Beschäftigungs- sondern auch in anderen Konzernunternehmen (Übermittlung)

Rechtsgrundlagen:

- § 24 Abs. 1 S. 1 oder Art. 6 Abs. 1 lit. f) / Abs. 4 DS-GVO
  - Konzerndimensionales Arbeitsverhältnis (kann sich auch nachträglich konkretisieren)
  - Überwiegende organisatorische Interessen
  - Auch keine entgegenstehenden Interessen beim Drittlandtransfer, wenn zweckgebundene Verwendung sichergestellt

Beispiel – Kontrolle Internet / E-Mail Nutzung

Dienstliche Nutzung

- Im Rahmen des zur Ablauf der Arbeit und dem Betrieb der Kommunikationstechnik Erforderlichen
- dienstliche E-Mails sind Dienstpost

▲

Kontrolle der E-Mail- und Internetnutzung

▼

Private Nutzung

- Es gilt das Fernmeldegeheimnis
- Der Arbeitgeber ist Diensteanbieter (er ist zum Zeitpunkt Diensteanbieter gem. § 3 Nr. 6 TKG)
- Kenntnisnahme nur wenn TKG es gestattet oder mit Einwilligung

Zwischenfall: Happy birthday.

Sie sind betriebliche/r Datenschutzbeauftragte/r in einem mittelständischen Unternehmen. Die Personalabteilung gratuliert in der Werkszeitung zu Betriebsjubiläen und Geburtstagen. Die Veröffentlichung erfolgt ohne Zustimmung der Mitarbeiter.

Ist das Vorgehen zulässig?

Lösung

Fragestellung: Ist die Datenverarbeitung rechtmäßig im Sinne von Art. 5 Abs. 1 lit. a DS-GVO?

- Anwendbarkeit der DS-GVO (+), Art. 2 Abs. 1 DS-GVO: ganz oder teilweise automatisierte Verarbeitung.
- Keine private/familiäre Tätigkeit im Sinne von Art. 2 Abs. 2 lit. c DS-GVO.
- Personenbezug (+), Art. 4 Nr. 1 DS-GVO
- Verarbeitung (+), Art. 4 Nr. 2 DS-GVO: Erhebung & Übermittlung
- Rechtfertigung durch Erlaubnistatbestand?

- Art. 9 DS-GVO bzw. § 26 Abs. 3 BDSG gelten nicht, Alter ist kein Gesundheitsdatum
- § 26 Abs. 1 BDSG gilt ebenfalls nicht, da eher kein Zweck des Beschäftigungsverhältnisses, sondern darüber hinausgehende Gute-Laune-Aktion.
- Betriebsjubiläen lassen sich nach Art. 6 Abs. 1 lit. f DS-GVO rechtfertigen, da der Arbeitgeber ein berechtigtes Interesse daran hat, das Betriebsklima zu fördern. Schutzwürdiges Interesse der Betroffenen steht bei dieser Datenkategorie zurück.
- Geburtstage lassen sich hingegen nicht nach Art. 6 Abs. 1 lit. f DS-GVO rechtfertigen. Berechtigtes Interesse des Arbeitgebers ist nicht ersichtlich, jedenfalls aber überwiegt das Interesse der Betroffenen.

ERGEBNIS: Datenverarbeitung gemäß Art. 5 Abs. 1 lit. a DS-GVO hinsichtlich der Geburtstage unrechtmäßig.

Straftaten im Beschäftigungsverhältnis

Aufdeckung von Straftaten im Arbeitsverhältnis (§ 26 Abs. 1 S. 2 BDSG):
Personenbezogene Daten eines Beschäftigten dürfen nur dann verarbeitet werden, wenn dies erforderlich ist für die Aufdeckung von Straftaten

Die Verarbeitung nur in engen Grenzen zulässig:

- es muss ein **tatsächlicher Anhaltspunkt** bestehen, nicht eine bloße Vermutung, dass der Beschäftigte eine Straftat begangen hat (ein Massenscreening ist ausgeschlossen) und
- der Anhaltspunkt ist zu **dokumentieren** und
- die Datenerhebung muss **erforderlich** sein, um den Sachverhalt aufzuklären **und**
- das **schutzwürdige Interesse** des Betroffenen überwiegt nicht, insbesondere darf die Verarbeitung **nicht unverhältnismäßig** sein

2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO

2.2.11 Videoüberwachung

Lehrveranstaltung Datenschutz

Öffentlicher Raum

z. B. Straßen, Verkehrsflächen, Versammlungsplätze, öffentliche Parks

Polizei- und Ordnungsrecht

Öffentlich zugänglicher Raum

z. B. Private Parkplätze, Verkaufsflächen

Öffentlich zugänglicher „Sonderraum“

- großflächigen Anlagen, z. B.:
- Sport-, Versammlungs-, Vergnügungsstätten, Einkaufszentren oder Parkplätze,
- öffentlicher Schienen-, Schiffs- und Busverkehr (Fahrzeuge und seine großflächigen Einrichtungen)

Datenschutzrecht für den öffentlichen Bereich

(z. B. § 4 BDSG)

DS-GVO

BDSG

(BAG-)Recht-sprechung

BetrVerfG

Nicht-öffentlich zugänglicher Raum

z. B. Fabrikgelände, Büroräume

DS-GVO

(BAG-)Recht-sprechung

BetrVerfG

Privatbereich

Umkleiden, Sozialräume

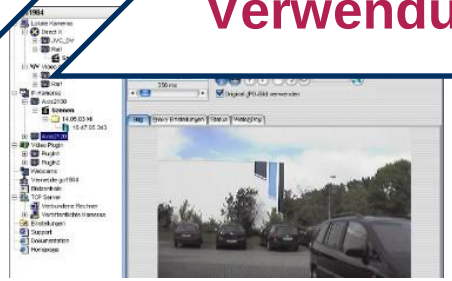
unzulässig

Phasen der Videoüberwachung

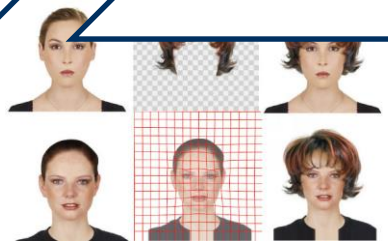
(§ 4 BDSG)

Beobachtung

Aufzeichnung (Speicherung/ Verwendung)



Personen-bezogene Auswertung



Kennzeichnungspflicht – Beispiele alte Rechtslage

Kennzeichnungspflicht:

Der Umstand der Videoüberwachung und der Verantwortliche sind durch geeignete Maßnahmen erkennbar zu machen (§§ 4 Abs. 2).

Kennzeichnungspflicht – neue Rechtslage

Beispiel für ein vorgelagertes Hinweisschild nach Art. 13 der Datenschutz-Grundverordnung bei Videoüberwachung[1]

Weitere Informationen erhalten Sie:
- per Aushang (wo genau?)
- an unserer Kundeninformation / Rezeption / Kasse im Erdgeschoss
- (ggf.) zusätzlich im Internet unter ...

Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters:

Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden):

Zwecke und Rechtsgrundlage der Datenverarbeitung:

berechtigte Interessen, die verfolgt werden:

Speicherdauer oder Kriterien für die Festlegung der Dauer:

[1] *Hinweis: Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. Art. 12 DSGVO). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A4 erfolgen.*

Lehrveranstaltung Datenschutz

(§ 4 Abs. 1 BDSG)

Beobachtung

Zulässig im Rahmen einer Interessensabwägung

Berechtigte Interessen im öffentlich zugänglichen Raum:

- Erforderlich zur Aufgabenerfüllung öffentlicher Stellen,
- Erforderlich zur Wahrnehmung des Hausrechts oder
- Erforderlich zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

Besonders wichtiges Interesse im öffentlich zugänglichen „Sonderraum“:

- Der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen

+

„Gegeninteressen“ der Betroffenen:

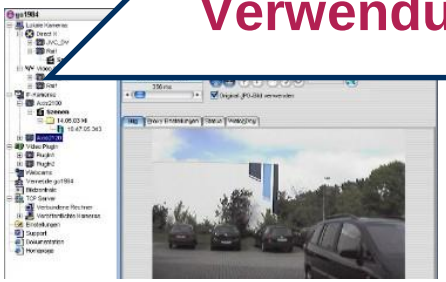
- Es bestehen keine Anhaltspunkte, dass schutzwürdige Interessen der Betroffenen überwiegen

Für andere Fallgestaltungen gilt Art. 6 Abs. 1 lit. f) als allgemeine Rechtsgrundlage

Lehrveranstaltung Datenschutz

(§ 4 Abs. 3, 5 BDSG)

Aufzeichnung (Speicherung/ Verwendung)



Zulässig im Rahmen einer Interessensabwägung

Zulässige Beobachtung

+

Berechtigte Interessen:

- Erforderlich zum Erreichen des verfolgten Zwecks im öffentlich zugänglichen Raum oder
- Erforderlich zum Erreichen des verfolgten Zwecks im öffentlich zugänglichen „Sonderraum“

+

„Gegeninteressen“ der Betroffenen:

- Es bestehen keine Anhaltspunkte, dass schutzwürdige Interessen der Betroffenen überwiegen (Interessen des „Sonderraums“)

Zweckänderung:

Nur zulässig, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

Unverzügliche Löschung:

- Die Daten sind zur Zweckerreichung nicht mehr erforderlich
- Schutzwürdige Interessen der Betroffenen stehen einer weiteren Speicherung entgegen

Lehrveranstaltung Datenschutz

(§ 4 Abs. 4, 5 BDSG)

Personen-bezogene Auswertung

Bei Zuordnung zu einer Person

Information der betroffenen Person über die Verarbeitung gemäß Art. 13, 14

+

Keine Ausnahmeregelung einschlägig nach

- Art. 13
- Art. 14
- § 32 BDSG

Unverzügliche Löschung:

- Die Daten sind zur Zweckerreichung nicht mehr erforderlich
- Schutzwürdige Interessen der Betroffenen stehen einer weiteren Speicherung entgegen

Zwischenfall: Antanzen

Der Betreiber des Hamburger Kiezclubs „Angenehm & Ungefährlich“ möchte den nicht umzäunten Parkplatzbereich seiner Diskothek mit Videokameras ausstatten, nachdem es in der letzten Zeit häufig zum sog. „Antänzer-Trick“ und damit verbundener Taschendiebstähle gekommen war.

Beurteilen Sie die Zulässigkeit einer solchen Videoüberwachung.

Lösungsskizze

Frage: Ist die *Beobachtung* zulässig?

Mögliche Rechtsgrundlage: § 4 BDSG – Videoüberwachung öffentlich-zugänglicher Räume
=> Parkplatz öffentlich zugänglich

§ 4 Abs. 1 S. 1 Nr. 1 BDSG (-): Keine Aufgabenerfüllung einer öffentlichen Stelle
§ 4 Abs. 1 S. 1 Nr. 2 BDSG (-): Zweck der Videoüberwachung ist nicht der Schutz des Objekts oder die Abwehr unbefugten Betretens, sondern dient der Aufdeckung von Diebstählen auf dem Gelände
§ 6b Abs. 1 S. 1Nr. 3 BDSG (+/-): Hier wäre eine umfassende Interessensabwägung vorzunehmen, die die Interessen der von der Videoüberwachung Betroffenen adäquat berücksichtigt. Es sprechen hier gute Gründe gegen eine Zulässigkeit der Videoüberwachung auf Basis von § 4 Abs. 1 S.1 Nr. 3 BDSG, da der Zweck der Überwachung nicht eigenen Eigentumsinteressen des Clubbetreibers dient, sondern fremde Eigentumsinteressen der Besucher gewahrt werden sollen. Hier wären aber mildere Mittel in Erwägung zu ziehen, so beispielsweise das Aussprechen eines Hausverbots mit dessen Durchsetzung durch das angestellte Sicherheitspersonal.
§ 4 Abs. 1 S. 2 Nrn. 1 u . 2 (-): Leben, Gesundheit oder Freiheit sollen nicht geschützt werden

Lösungsskizze

Frage: Ist die *Speicherung* zulässig?

- Die Speicherung ist grundsätzlich eingriffsintensiver als die reine Beobachtung und muss zur Zweckerreichung erforderlich sein. Private Stellen sollten sich nicht als Gehilfen der Polizei ansehen. Je nach Ausgang der Zulässigkeit der Beobachtung müsste hier u.U. wieder eine Interessensabwägung stattfinden.

– Kommt der Bearbeiter/die Bearbeiter/in zu dem Ergebnis, dass eine Überwachung gem. § 4 Abs. 1 S. 1 Nr. 3 BDSG zulässig ist, sollten die weiteren Anforderungen des § 4 Abs. 2-5 BDSG thematisiert werden.

2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO
2.2.12 Datenschutzorganisation

Schutzkonzept

Überwachung durch den Datenschutzbeauftragten
(Art. 37-39 DS-GVO)

Standards und Zertifizierung
(Art. 40-43 DS-GVO)

Organisatorische Absicherung
(Art. 24-31, 35-36 DS-GVO – Datenschutzmanagement)

Dokumentation und Nachweise
(Verschiedene Stellen der DS-GVO)

Technische Absicherung
(Art. 25, 32 DS-GVO – IT-Sicherheitsmanagement)

Schutz natürlicher Personen bei der Verarbeitung personen-bezogener Daten

Lehrveranstaltung Datenschutz

Basis

- Datenschutzmanagementsystem, insbes. zur Gewährleistung der Accountability
  (geeignete Datenschutz-„Vorkehrungen“ – engl.: approriate data protection policies), Art. 24 DS-GVO
  - Risikobasierter Ansatz
  - Überprüfung
  - Nachweis durch Zertifizierung möglich

Ergänzung

- Weitere Vorgaben zur operativen Datenverarbeitung insbesondere:
  - Einsatz „datenschutzfreundlicher“ Technologien
  - IT-Sicherheit nach dem „Stand der Technik“
  - Weitrechende Dokumentationspflichten, u. a. aller Verarbeitungsvorgänge
  - Weitreichende Nachweispflichten insbes. nach dem Prinzip der Rechenschaftspflicht [accountability]
  - „Datenschutzfolgenabschätzung“
  - Konsultationspflicht der Aufsichtsbehörde

Normadressat ist der Verantwortliche (interne Organisation)

Lehrveranstaltung Datenschutz

Haupt-Aufgaben des **Unternehmens** 	**Etablierung:** ▪ Datenschutz-Management (insbes. im Hinblick auf „Accountability“/Nachweise) ▪ IT-Sicherheitsmanagement
Haupt-Aufgaben der **Fachabteilung, Mitarbeiter** 	**Umsetzung:** ▪ Prozessgestaltung (Privacy by design/default) ▪ Datenschutzfolgenabschätzung/PIA ▪ Dokumentationen/Nachweise/Meldepflichten ▪ Prozesse für Rechte der Betroffenen
Haupt-Aufgaben der **IT** 	**Umsetzung:** ▪ Vorgaben des IT-Sicherheitsmanagements **Unterstützung:** ▪ Technische Umsetzung der Datenschutzvorgaben in den Prozessen
Haupt-Aufgaben des **DSB** 	**Beratung:** ▪ Abstimmung bei „Strategien“ und – vorgegebenen – Einzelfällen **„Überwachung“:** ▪ Umsetzung, risikoorientiert

Exkurs: Der Datenschutzbeauftragte - Aufgaben

Sicherstellungsauftrag

(§ 29 Abs. 1 BDSG 1977 / § 37 Abs. 1 BDSG 1990)

Hinwirkungsauftrag

(§ 4g Abs. 1 BDSG 2001)

Überwachungsauftrag

(Art 38 Abs. 1 DS-GVO 2016)

Exkurs: Der Datenschutzbeauftragte - Aufgaben

Beratung

- Unterrichtung und Beratung hinsichtlich der Datenschutzpflichten (Verantwortlicher, Auftragsverarbeiter, Beschäftigte)
- Beratung Betroffener hinsichtlich der Datenschutzfragen/-rechte
- Beratung bei der Datenschutzfolgeabschätzung (auf Anfrage)
  (Pflicht des Verantwortlichen zur Konsultation gemäß Art. 35 Abs. 2 DS-GVO)

Zielsetzung:

Wirksame Umsetzung der DS-GVO in

- der Organisation
- Prozessen
- Systemen

Exkurs: Der Datenschutzbeauftragte - Stellung

- Ordnungsgemäße und frühzeitige Einbindung „ in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen”
- Unterstützungspflicht durch das Unternehmen
  - Erforderliche Ressourcen
  - Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen
  - Erhalt der Fachkenntnisse
- Ratgeber für Betroffene
- Verschwiegenheitspflicht nach nationalem Recht
- Weisungsfreiheit bzgl. der Aufgaben
- Abberufungsschutzschutz und Benachteiligungsverbot
- Unmittelbarer Bericht an die höchste Managementebene
- Weitere Aufgaben möglich, soweit hierdurch kein Interessenskonflikt entsteht

Exkurs: Der Datenschutzbeauftragte - Bestellpflicht

Verpflichtend

- Nationale Öffnungsklausel:
  § 38 BDSG

- Alle öffentliche Stellen
- Unternehmen
  - → *Kerntätigkeit besteht aus Verarbeitungs-vorgängen, welche auf Grund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen*
  - → *Verantwortliche / Auftragsverarbeiter, deren Kerntätigkeit aus der Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 und 10 der DS-GVO in großem Umfang besteht*

Exkurs: Der Datenschutzbeauftragte - Bestellpflicht

Automatisierte DV *§ 38 BDSG*

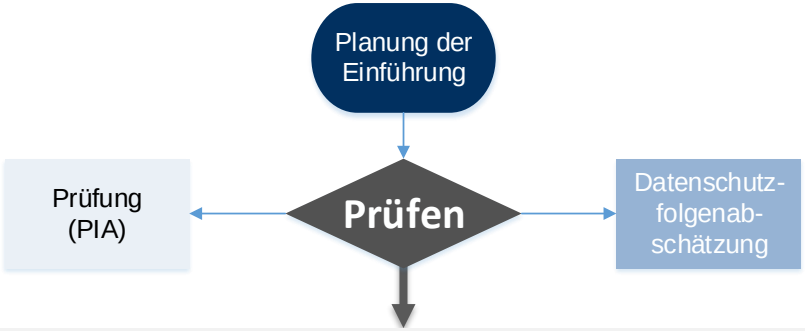
1)

- DV zum Zwecke der Übermittlung → DSB-Pflicht!
- DV zum Zwecke der anonymisierten Übermittlung → DSB-Pflicht!
- Markt- u. Meinungsforschung → DSB-Pflicht!

2)

- >9 AN ständig mit pb DV befasst → DSB-Pflicht!
- <10 AN mit automatisierter DV befasst → Keine DSB-Pflicht!

Datenschutz-Folgenabschätzung



Grundsatz:
DSFA bei Verarbeitungen, die voraussichtlich ein *hohes Risiko* für den Betroffenen aufweisen

- Gesetzliche Regelbeispiele:
  - Systematische und umfassende Auswertung persönlicher Aspekte
  - Umfangreiche Verarbeitung besonderer Daten nach Art. 9, 10
  - Weiträumiger Überwachung öffentlich zugänglicher Bereiche
- Hohes Risiko insbesondere durch
  - die Verwendung neuer Technologien,
  - die Art der Verarbeitung
  - den Umfang der Verarbeitung
  - die Umstände der Verarbeitung
  - die Zwecke der Verarbeitung
- Es gibt keine Ausnahmen

Erforderlich:

Risikobewertung durch den Verantwortlichen

Datenschutz-Folgenabschätzung

Regelbeispiele* (nach WP 248, Art. 29-Gruppe)

1. Bewertung (Profiling) oder Scoring,
2. Automatisierte Entscheidungsfindung mit rechtlicher oder ähnlicher erheblicher Wirkung
3. Systematische Überwachung
4. Sensible Daten (s. insbes. Art. 9,10)
5. Datenverarbeitung in großem Umfang
6. Datensätze (insbes. Aus verschiedenen Prozessen) werden abgeglichen („match“) oder kombiniert
7. Daten zu schutzbedürftigen Personen
8. Innovative Nutzung oder Anwendung technologischer oder organisatorischer Lösungen
9. Grenzüberschreitende Datenübertragung außerhalb der Europäischen Union
10. Die Verarbeitung an sich "verhindert, dass die betroffenen Personen ein Recht ausüben oder eine Dienstleistung oder einen Vertrag ausüben"

Liegen zwei oder mehr Regelbeispiele vor, ist regelmäßig eine DSFA durchzuführen

**** Die Regelbeispiele werden im WP 248 näher erläutert***

Art. 29 Gruppe, WP 248

Datenschutz-Folgenabschätzung

Die Datenschutzfolgeabschätzung enthält zumindest Folgendes

- Zwecke der Verarbeitung, ggf. einschließlich der von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen
- systematische Beschreibung der geplanten Verarbeitungsvorgänge
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen (Risikonanalyse)
- zur Bewältigung der Risiken geplante Abhilfe(-/Sicherheits)maßnahmen, einschließlich
  - Garantien,
  - Sicherheitsvorkehrungen
  - Verfahren,
- Maßnahmen, durch die der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden (IKS)

Dokumentations- und Nachweispflichten

Allgemeine Dokumentations-pflichten
(Art. 5 Abs. 2, Art. 24 Abs. 1 DS-GVO)

Erfüllen der Rechenschaftspflicht per Dokumentation
Verstoß ist bußgeldbewehrt (unter anderem Art. 83 Abs. 5 lit. a DS-GVO)

Spezielle Dokumentations-pflichten
(Art. 7 Abs. 1, Art. 12 ff., Art. 30, Art. 34 Abs. 2, Art. 35, Art. 49 Abs. 6 DS-GVO)

Speziell für Auftragsverarbeiter insbesondere:

- Dokumentation der Weisungen
- Dokumentation der Weisungen für Drittlandstransfers
- Verzeichnis der Verarbeitungen nach Art. 30 Abs. 2

Verzeichnis von Verarbeitungsaktivitäten

Art. 30 Abs. 1 DS-GVO

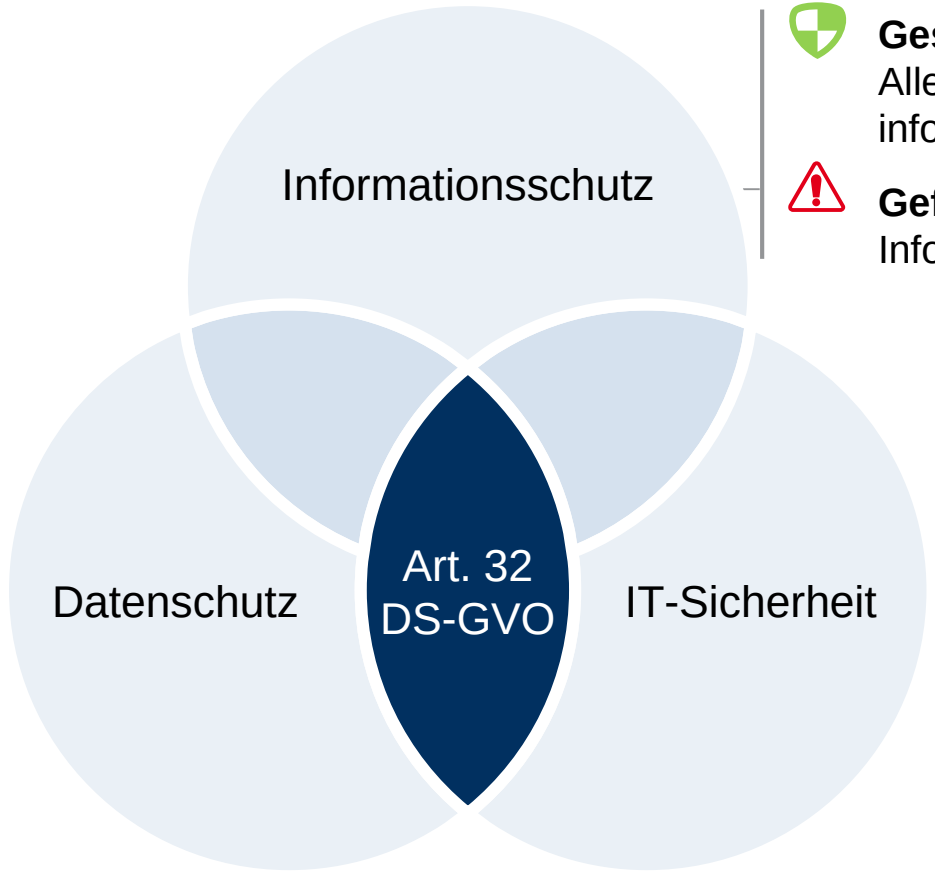
- „Verzeichnis aller Verarbeitungstätigkeiten”
- Nicht öffentlich / Einsicht für Aufsichtsbehörden
- Dokumentation ähnlich Verfahrensverzeichnis
- Beurteilung und Garantien bei Drittlandsübermittlungen gemäß Art. 49 Abs. 1 (g)

Ausnahmen für Einrichtungen unter 250 MA
– häufig nicht einschlägig

2. Die Datenschutzgesetzgebung in Europa und Deutschland

2.2 Die wesentlichen Inhalte der DS-GVO
2.2.12 Datensicherheit aus rechtlicher Sicht

Abgrenzung Datenschutz/IT-Sicherheit



Geschützt
Alle Unternehmens-informationen

Gefahr
Informationsabfluss

Geschützt
Natürliche Personen und deren Recht auf Schutz personen-bezogener Daten

Gefahr
Verletzung der Grundrechte und Grund-freiheiten

Geschützt
- Hardware
- Software
- Daten

Gefahr
- Verlust
- Zerstörung
- Missbrauch durch Unbefugte

Sicherheit der Verarbeitung

Sicherheit der Verarbeitung (Art. 32 DS-GVO)	Verantwortlich:	Unternehmen, sonstige Stelle – IT-Sicherheitsmanagement wird unterstellt
Vorgaben	Angemessen:	Beachtung insbes. des „Stands der Technik“
	Risikoorientiert:	insbes. im Hinblick auf den Betroffenen

Fokussierung auf die IT-Sicherheitsziele:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit

Berücksichtigung von

- Pseudonymisierung / Verschlüsselung
- Notfallplanung
- Wirksamkeitstests

Sicherheit nach der alten Rechtslage

- Zutrittskontrolle (Zutritt zu Datenverarbeitungsanlagen)
- Zugangskontrolle (Nutzung von Datenverarbeitungsanlagen)
- Zugriffskontrolle (Berechtigungskonzept, kein unbefugtes Lesen oder Verändern)
- Weitergabekontrolle (kein unbefugtes Lesen oder Verändern beim
- Transfer)
- Eingabekontrolle (wer hat befugtermaßen eingeben und verändert)
- Auftragskontrolle (Weisungen nach § 11 BDSG)
- Verfügbarkeitskontrolle (Schutz gegen zufällige Zerstörung oder Verlust)
- Trennungsgebot (Unterschiedliche Zwecke bedingen getrennte
- Verarbeitung)
- [Verschlüsselung]

Passwort 2017

DIE TOP TEN DEUTSCHER PASSWÖRTER

22.12.2017

Pressemitteilung

Die Top Ten deutscher Passwörter

Ein Blick auf die Top Ten der in Deutschland meistgenutzten Passwörter zeigt: Die Ziffernfolge „123456" belegt erneut den Spitzenplatz. Am beliebtesten sind weiterhin schwache und unsichere Zahlenreihen.

Das Hasso-Plattner-Institut (HPI) veröffentlicht jedes Jahr die meistgenutzten Passwörter der Deutschen – Datengrundlage sind 12,9 Millionen E-Mail-Adressen, die als .de-Domain registriert sind.

Top Ten deutscher Passwörter

1. 123456	6. hallo
2. 123456789	7. passwort
3. 1234	8. 1234567
4. 12345	9. 111111
5. 12345678	10. hallo123

Sichere Passwörter

- Es sollte mindestens acht Zeichen lang sein, je länger desto besser. (Ausnahme: Bei Verschlüsselungsverfahren wie zum Beispiel WPA und WPA2 für WLAN sollte das
- Passwort mindestens 20 Zeichen lang sein. Hier sind so genannte Offline-Attacken möglich, die auch ohne stehende Netzverbindung funktionieren - das geht zum Beispiel beim Hacken von Online-Accounts nicht.)
- Es sollte aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern (?!%+…) bestehen.
- Tabu sind Namen von Familienmitgliedern, des Haustieres, des besten Freundes, des Lieblingsstars oder deren Geburtsdaten und so weiter.
- Wenn möglich sollte es nicht in Wörterbüchern vorkommen.
- Es soll nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern bestehen, also nicht asdfgh oder 1234abcd und so weiter.
- Einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen $! ? #, am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen ist auch nicht empfehlenswert.
- Bitte beachten Sie: Wenn Ihr System Umlaute zuläßt, bedenken Sie bei Reisen ins Ausland, dass auf landestypischen Tastaturen diese evtl. nicht eingegeben werden können.

https://www.bsi-fuerbuerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

2. Die Datenschutzgesetzgebung in Europa und Deutschland

3. Einzelne bereichsspezifische Normen

3.1 Ärztliche Schweigepflicht

Ärzte Schweigepflicht

§ 9 Berufsordnung: Schweigepflicht

(1) Ärztinnen und Ärzte haben über das, was ihnen in ihrer Eigenschaft als Ärztin oder Arzt anvertraut oder bekannt geworden ist – auch über den Tod der Patientin oder des Patienten hinaus – zu schweigen.

(2) Ärztinnen und Ärzte sind zur Offenbarung befugt, soweit sie von der Schweigepflicht entbunden worden sind, soweit eine gesetzliche Vorschrift dies vorsieht oder soweit die Offenbarung zum Schutze eines höherwertigen Rechtsgutes erforderlich ist. Soweit gesetzliche Vorschriften die Schweigepflicht der Ärztin oder des Arztes einschränken, soll die Ärztin oder der Arzt die Patientin oder den Patienten darüber unterrichten.

(3) Mitarbeiterinnen und Mitarbeiter sowie die Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen, sind über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und zur Einhaltung zu verpflichten

Ärzte Schweigepflicht

§ 203 StGB

(1) Wer **unbefugt** ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, **offenbart**, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert, […]

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. […]

(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse **den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen** zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber **sonstigen Personen** offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, **soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist**; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken. […]

Ärzte Schweigepflicht

Offenbarungsbefugnis?

1. Art. 28 DS-GVO (Auftragsverarbeitung): (-)

2. Wirksame Einwilligung des Geheimnisgeschützten, Entbindung von der Schweigepflicht (Fischer, StGB, § 203 Rn. 32 ff.)

a) Ausdrückliche und konkludente Einwilligung

b) Fähigkeit, die Bedeutung der Erklärung zu verstehen, sodass auch Minderjährige – auch gegen den gesetzlichen Vertreter – die Einwilligung wirksam erklären kann.

c) Grds. keine Formerfordernisse, sodass auch eine konkludente Einwilligung möglich ist, beispielsweise wenn der Betroffene an Abläufen mitwirkt, die ihrer Natur nach das Offenbaren von Geheimnissen voraussetzen (z. B. Überweisung an Facharzt zur Klärung eines Verdachts) oder ohne Offenbarung ihren Sinn verlieren würden (z. B. Mitteilung der fachärztlichen Feststellungen an den überweisenden Hausarzt).

3. Mutmaßliche Einwilligung

a) Jede – auch konkludente – Erklärung des Berechtigten fehlt oder ist unmöglich, beispielsweise wegen Unerreichbarkeit, krankheitsbedingter Unfähigkeit oder Tod.

b) 2. Offensichtliches Interesse des Betroffenen.

2. Die Datenschutzgesetzgebung in Europa und Deutschland

3. Einzelne bereichsspezifische Normen

3.2 KUG

Anfertigung von Bildnissen

Rubrik: #GDPRFAIL

Anfertigung von Bildnissen

LDA Brandenburg:

[…] Bei einer öffentlichen bzw. größeren Veranstaltung auf Einladung dürfte die Erwartungshaltung der Gäste und der an der Durchführung Beteiligten regelmäßig dahingehen, dass eine Dokumentation in Form von Fotografien stattfinden wird. […]

Art. 6 Abs. lit. f DS-GVO (+)
[Art. 13 GrCh - Freiheit der Kunst und der Wissenschaft
Kunst und Forschung sind frei. Die akademische Freiheit wird geachtet.]
Ausnahmen: Foto die Intimsphäre des Betroffenen erfasst oder jemanden in einer Situation darstellt, die diskreditierende sein kann oder die Gefahr einer Diskriminierung birgt oder bei Bildnissen von Kindern
+ **Transparenz** der Anfertigung

Veröffentlichung von Bildnissen

Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KUG)

§ 22

Bildnisse dürfen nur mit **Einwilligung** des Abgebildeten **verbreitet** oder **öffentlich zur Schau** gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, daß er sich abbilden ließ, eine Entlohnung erhielt. Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Abgebildeten und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Abgebildeten.

Veröffentlichung von Bildnissen

§23 KUG

(1) **Ohne** die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:

1. Bildnisse aus dem Bereiche der Zeitgeschichte;
2. Bilder, auf denen die Personen nur als **Beiwerk** neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
3. Bilder von **Versammlungen, Aufzügen und ähnlichen Vorgängen**, an denen die dargestellten Personen teilgenommen haben;
4. Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.

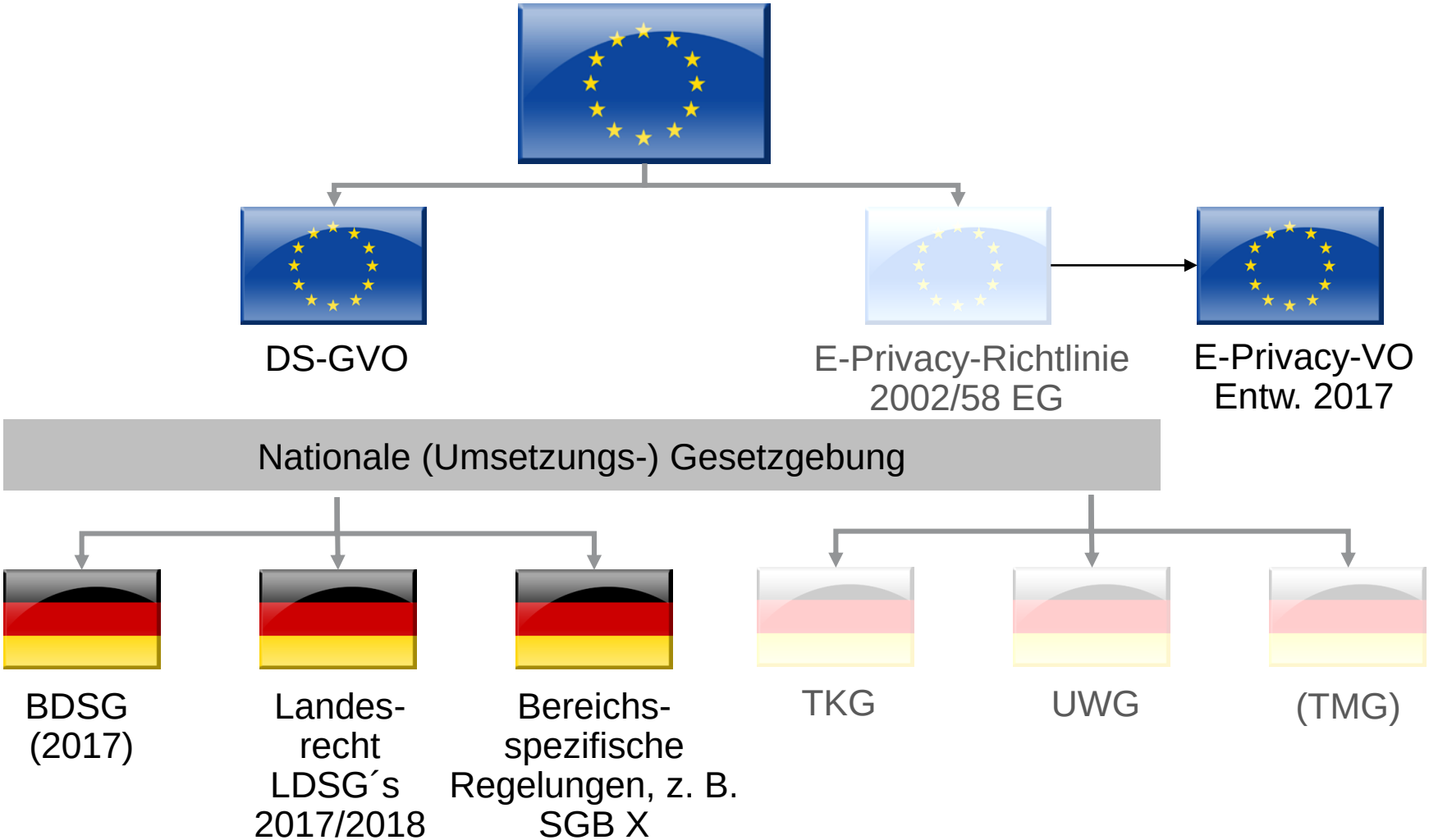
(2) Die Befugnis erstreckt sich jedoch nicht auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten oder, falls dieser verstorben ist, seiner Angehörigen verletzt wird.

2. Die Datenschutzgesetzgebung in Europa und Deutschland

3. Einzelne bereichsspezifische Normen

3.3 ePrivacy

Datenschutz



Lehrveranstaltung Datenschutz

E-Privacy-VO
Entw. v. 10.01.2017

Zielsetzung

- Aufhebung der E-Privacy-Rili und der „Cookie-Richtlinie“
- Lex specialis zur DS-GVO

- Datenschutz im TMG wird ersetzt
- § 7 UWG wird (teilweise) ersetzt
- Geltung zeitgleich mit der DS-GVO ab dem 25.05.2018 nicht realisert worden

Regelungsinhalte

- Nutzung elektronischer Kommunikationsdienste

- Erfassung der gesamten Online-Branche
- Herkömmliche Telekommunikationsdienste
  - Over-the-top-Dienste (OTT)
  - Maschine-zu-Maschine-Kommunikation / Internet-of-Things (IOT)

Web-Tracking

Zulässigkeit vor dem 25.05.2018:

§ 15 Abs. 3 Telemediengesetz (TMG)

(3) Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

Umstrittene Rechtslage: Cookie Banner nicht nötig, § 15 TMG
Praxis heute : Cookies mit Opt-Out (Cookie Banner)

Web-Tracking

DSK DATENSCHUTZKONFERENZ

Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 26. April 2018

1. Im Verhältnis zum nationalen Recht kommt ab dem 25. Mai 2018 die DSGVO für sämtliche automatisierte Verarbeitungen personenbezogener Daten vorrangig zur Anwendung, es sei denn nationale Vorschriften sind aufgrund einer Kollisionsregel, eines Umsetzungsauftrages oder einer Öffnungsklausel der DSGVO vorrangig anwendbar.

4. Damit können die §§ 12, 13, 15 TMG bei der Beurteilung der Rechtmäßigkeit der Reichweitenmessung und des Einsatzes von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen, ab dem 25. Mai 2018 nicht mehr angewendet werden.

Web-Tracking

DSK
DATENSCHUTZKONFERENZ

Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 26. April 2018

6. Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Diensteanbieter von Telemedien kommt folglich nur Artikel 6 Absatz 1, insbesondere Buchstaben a), b) und f) DSGVO in Betracht. Darüber hinaus sind die allgemeinen Grundsätze aus Artikel 5 Absatz 1 DSGVO, sowie die besonderen Vorgaben z. B. aus Artikel 25 Absatz 2 DSGVO einzuhalten.

9. Es bedarf jedenfalls einer vorherigen Einwilligung beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und bei der Erstellung von Nutzerprofilen. Das bedeutet, dass eine informierte Einwilligung i. S. d. DSGVO[8], in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung vor der Datenverarbeitung eingeholt werden muss, d. h. z. B. bevor Cookies platziert werden bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.

Web-Tracking vs. ePrivacyVO

Art. 8 ePrivacyVO (Entwurf)

(1) Jede vom betreffenden Endnutzer nicht selbst vorgenommene Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer, auch über deren Software und Hardware, ist **untersagt**, außer sie erfolgt aus folgenden Gründen:

d) sie ist für die Messung des Webpublikums nötig, sofern der Betreiber des vom Endnutzer gewünschten Dienstes der Informationsgesellschaft diese Messung durchführt.

=> Messung des Webpublikums, sofern Betreiber Messung durchführt zulässig mittels
(1) Webanalysetools auf eignem Webservern, z.B. Piwik oder
(2) AuftragsDV, z.B. Google Analytics, ansonsten: **Einwilligung**

Web-Tracking vs. ePrivacyVO

Art. 9 ePrivacyVO (Entwurf) - Web-Tracking mit Einwilligung

- Voraussetzungen der Art. 4 Nr. 11 und Art. 7 DS-GVO

- Anforderungen an rechtwirksame Einwilligung

- Einwilligung durch passende **technische Einstellung der Software**
- Einwilligung wird auf Anbieter von Zugangssoftware verschoben (Browser, Apps): „Gate Keeper“
- ErwG. 23: Einstellungsmöglichkeiten vom höheren Schutz (z. B. „Cookies niemals annehmen“) über einen mittleren Schutz (z. B. „Cookies von Drittanbietern zurückweisen“ oder „Nur Cookies von Erstanbietern annehmen“) bis zum niedrigeren Schutz (z. B. „Cookies immer annehmen“)

Web-Tracking vs. ePrivacyVO

Art. 10 ePrivacy-VO - Einstellungsmöglichkeiten in Software

- Einwilligung durch passende **technische Einstellung der Software**
- ErwG. 23: Es gilt Art. 25 DS-GVO (Datenschutzfreundliche Voreinstellung): keine Standardeinstellung „Alle Cookies annehmen“.
- Software ist so zu konfigurieren, dass sie die Möglichkeit bietet zu verhindern, dass Dritte Informationen in der Endeinrichtung speichern; diese Einstellung wird häufig als „Cookies von Drittanbietern zurückweisen“
- Kritik: Bei Ausschaltung von 3rd-party Cookies nur eingeschränktes Netzangebot; Webseiten mit eigenen 1st-party-Angeboten profitieren