Datenschutz-Management im Unternehmen nach DSGVO

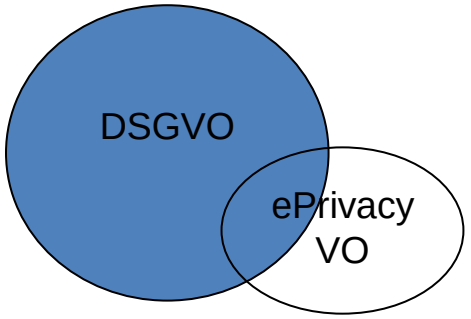
IHK-Fachforum

München, 12. März 2018

Rechtsanwältin, Fachanwältin für IT-Recht Isabell Conrad

Entwicklung im Datenschutzrecht

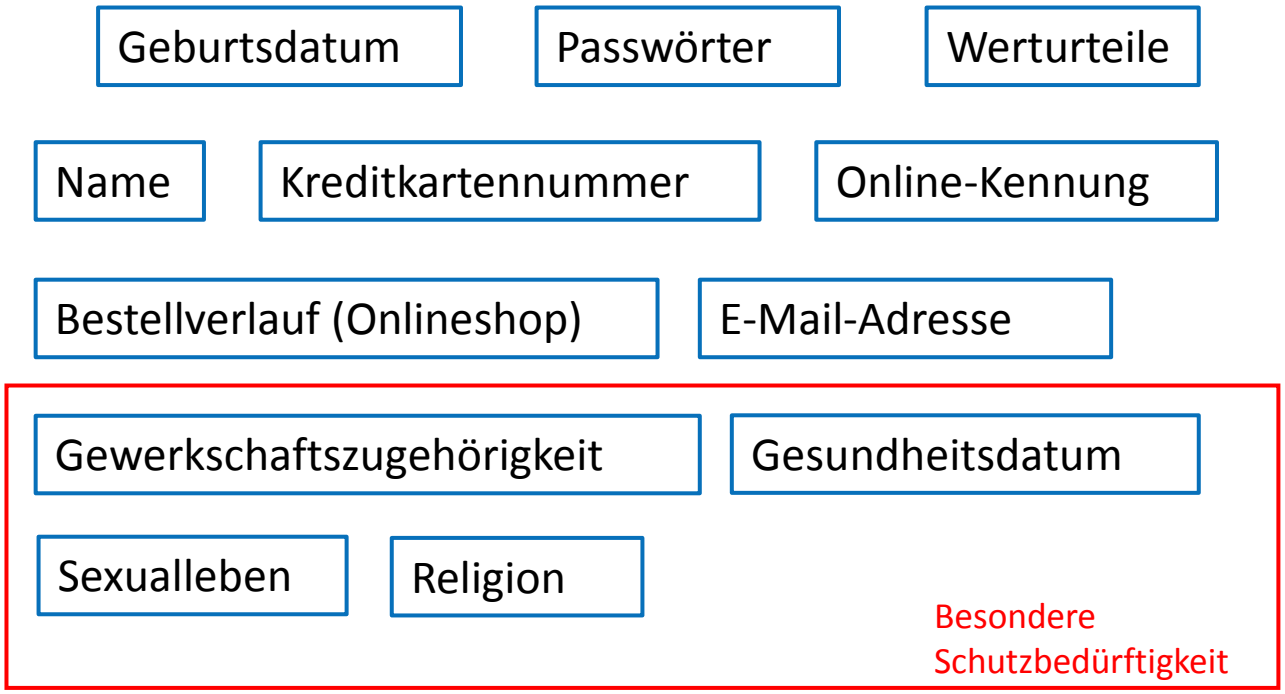
- **Inkrafttreten der DSGVO** und **RL 2016/680 am 25.5.2016**
- **Anwendbarkeit der DSGVO** ab 25.5.2018
- Bußgelder von bis zu **20 Mio. €** bzw. bis zu **4 % des gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist
- **Neues BDSG bereits verabschiedet;** gilt ebenfalls ab 25.5.2018
- Achtung: seit 2017 § 203 StGB n.F. zur Strafbarkeit „mitwirkender Personen“ (kann auch IT-Dienstleister von Ärzten, RAen etc. treffen)
- Entwurf einer **E-Privacy-Verordnung (ePrivacy-VO)** v. 10.1.2017 – Start des Trilogverfahrens Ende 2018
- Erwartungsgemäß höhere Kontrolldichte der Datenschutzaufsichtsbehörden
- Datenschutz kann aber ein Wettbewerbsvorteil sein



Was sind „personenbezogene Daten“?

Art. 4 Nr. 1 DSGVO: **Alle Angaben**, die sich auf eine identifizierte oder **identifizierbare** natürliche Person beziehen.

⇒ Das betrifft nicht nur private Angaben, sondern **auch berufliche** und sonstige Informationen über einen Menschen.

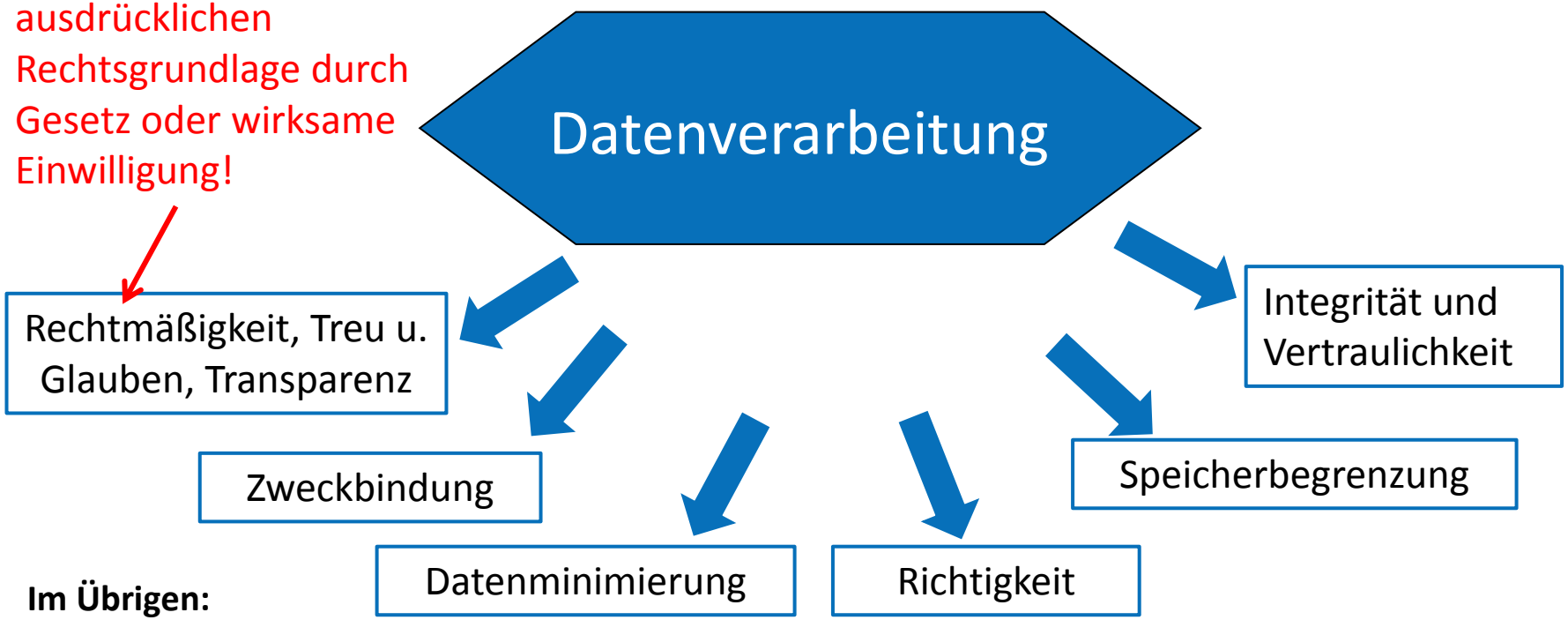


Welche Daten führen zur „Identifizierbarkeit“?

- Patrick Breyer (Piratenpartei) rief Websites von **Einrichtungen des Bundes** ab.
- Um Angriffe abzuwehren und die strafrechtliche Verfolgung von Angreifern zu ermöglichen, werden bei den Websites **alle Zugriffe, insb. die IP-Adresse in Protokolldateien** festgehalten.
- Allerdings speichert der Website-Betreiber die IP-Adressen **ohne** für die Identifizierung **erforderliche Zusatzinformationen.**
- **Personenbezug ?** EuGH Urt. v. 19.10.2016 – C 582/14 (dynam IP-Adressen)
  - ❖ Ja, denn nicht alle zur Identifikation notwendigen Mittel müssen **in einer Hand** sein.
  - ❖ Es genügt, dass der Website-Betreiber potentiell **legale Möglichkeiten** hat, an die Identifizierungsmerkmale heranzukommen (etwa Akteneinsicht im Strafverfahren)

Grundprinzipien des Datenschutzrechts

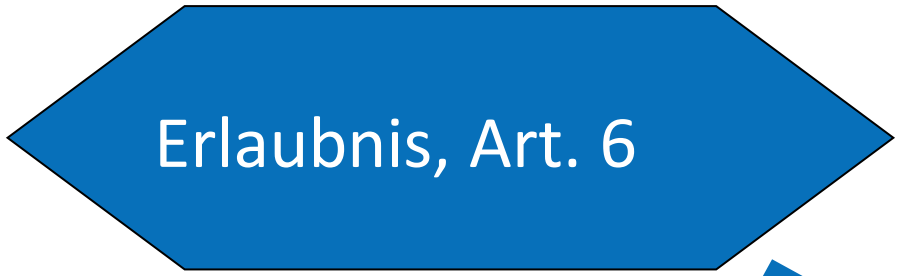
Jede Verarbeitung personenbez. Bedarf einer ausdrücklichen Rechtsgrundlage durch Gesetz oder wirksame Einwilligung!



Im Übrigen:

1. **Kein Konzernprivileg**
2. **Kontrolle** (intern/extern), **Bußgeld, Schadensersatz**

Erlaubnistatbestände nach DSGVO



Einwilligung

Erfüllung eines Vertrags mit Betroffenem

Erfüllung rechtliche Verpflichtung

Lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person

Wahrnehmung einer Aufgabe im öffentlichen Interesse

Art. 6 Abs. 1 f) DSGVO:
berechtigten Interessen des Verantwortlichen oder eines Dritten und keine entgegen-stehenden Interessen der betroffenen Personen

Achtung:
Sondernorm Art. 9 für besondere Kategorien personenbezogener Daten (z.B. Gesundheitsdaten; Art. 6 Ab. 1 f) DSGVO gilt **nicht**!

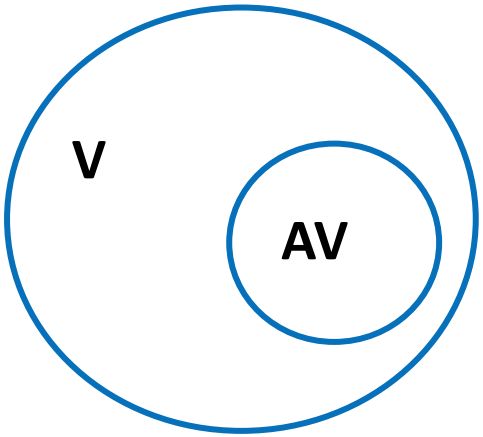
Weitergabe personenbezogener Daten

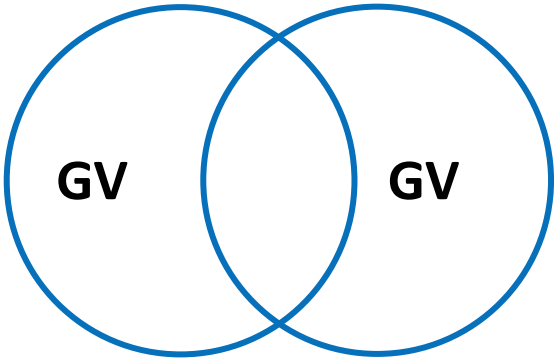
Zusätzlich zur erforderlichen Erlaubnis zu beachten:

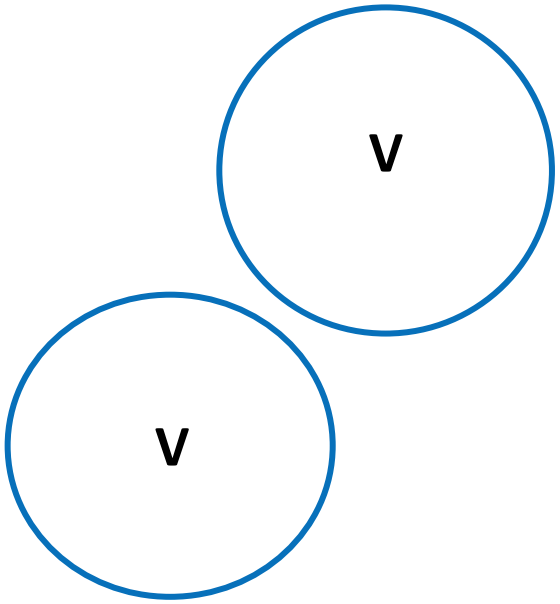
Zwingend:
Auftrags-verarbeitungsvertrag Art. 28 DSGVO **(AVV)**

Zwingend:
Joint Control-Vertrag Art. 26 DSGVO

Übermittlung an Dritten ohne gemeinsame Verantwortlichkeit







V = Verantwortlicher
GV = Gemeinsam Verantwortliche (Joint Controller)
AV = Auftragsverarbeiter

Erkennungsmerkmale der Auftragsverarbeitung

- Verarbeitung der Daten des Auftraggebers nur im Auftrag und nur für den Auftraggeber
- keine Nutzung der Daten zu eigenen Zwecken (z.B. Marketing) des Auftragnehmers
- keine Ermessensspielräume des Auftragnehmers bei Zwecken und Mitteln der Datenverarbeitung (inkl. Art und Umfang der Datenverarbeitung und bei Sicherheitsmaßnahmen)
- weisungsgebundene Unterstützung
- keine (vertragliche) Beziehung des Auftragnehmers zu den Betroffenen [daher z.B. bei Factoring Auftragsverarbeitung ausgeschlossen]
- Art. 28 Abs. 10 DSGVO: Auftragsverarbeitung (-), wenn der Auftragnehmer *„Zwecke und Mittel der Verarbeitung mitbestimmt“.* Noch unklar was gilt, wenn der Auftragnehmer zwar nicht die Zwecke, aber die Mittel mitbestimmt.

  Bsp.: Business Process Outsourcing mit weitgehend selbständiger Auftragsausführung

Beispiele Auftragsverarbeitung

- Lohnabrechnung durch ein Dienstleistungszentrum
- Einscannen des schriftlichen Posteingangs durch einen Dienstleister
- Werbeadressenpflege und -ausdruck sowie Werbepostversand durch einen Lettershop
- Kontaktdatenerhebung durch ein Callcenter (abhängig von der Gestaltung)
- Fernzugriff von IT-Dienstleistern auf eigene IT-Infrastruktur zu **Wartung**szwecken
- **Aktenvernichtung**, Entsorgung von Datenträgern
- Auslagerung IT-Infrastruktur an **konzernangehöriges Unternehmen**

Art. 28 DSGVO wohl bereits dann zu beachten, wenn Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann (z.B. bei Wartung, Pflege von IT-Systemen, Tests) – noch strittig, da in Art. 28 DSGVO eine Vorschrift entsprechend § 11 Abs. 5 BDSG fehlt

Kein Konzernprivileg im Datenschutzrecht (auch nach DSGVO), aber im Einzelfall ggf. Erlaubnis nach Art. 6 Abs. 1 lit. f DSGVO; erlaubnispflichtige Übermittlung grds. bereits bei **zentralen Datenbanken im Konzern** **§ 26 DSGVO (Gemeinsame Verantwortlichkeit)**

Auftragsverarbeitung Art. 28 DSGVO

Zahlreiche neue Pflichten des Auftragnehmers (Auftragsverarbeiters), die zu einer wesentlich stärkeren Mitverantwortung führen als nach BDSG-alt:

- Bestellung eines **EU-Repräsentanten** bei Sitz im EU-Ausland
- **Verarbeitungsverzeichnis** hins. Auftragsverarbeitung
- **Zusammenarbeit mit der Datenschutzaufsicht** (allerdings Klarstellung, dass die Informationspflicht über Datenpannen nur den Auftraggeber trifft)
- Bestellung eines **Datenschutzbeauftragten** hins. Auftragsverarbeitung (sofern nicht ohnehin Bestellpflicht)
- Mitverantwortung für die risikobasierten technische und organisatorische Maßnahmen (TOMs, auch Schutzbedarfsfeststellung und Risikoanalyse!)
- Mitverantwortung für die Beschränkungen des **Datentransfer in Drittländer**
- Haftung für die Subunternehmer / Unterauftragsverarbeiter!
- Erlaubt der Auftraggeber allgemein den Einsatz von Subunternehmer, muss ich, der Auftragnehmer vor jeder Änderung ein **Widerspruchrecht** geben
- Erleichterung durch Möglichkeit eines elektronischen Vertragsschlusses

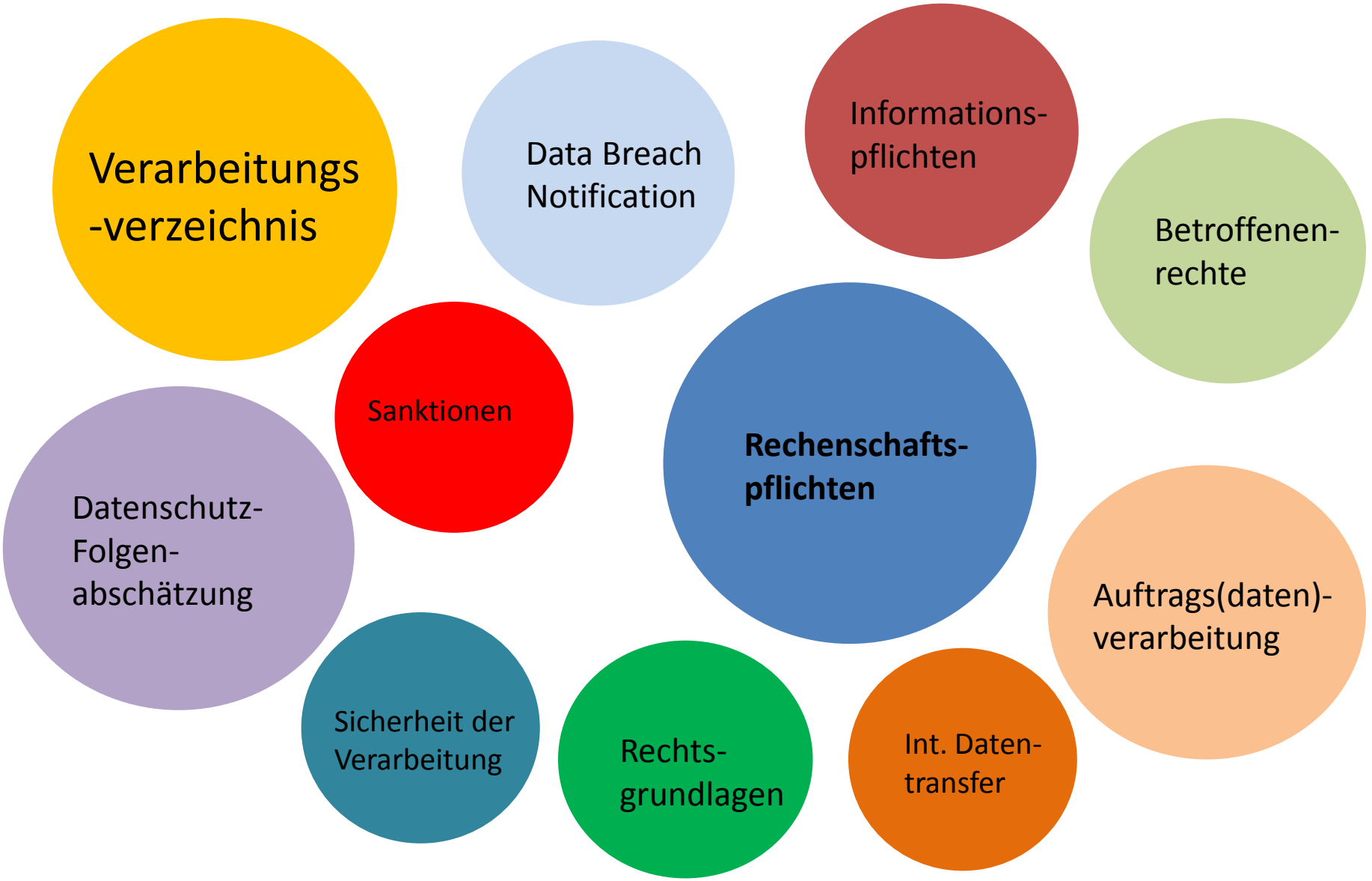
Mindestinhalte eines AVV

1. Gegenstand und Dauer der Verarbeitung,
2. Art und Zweck der Verarbeitung,
3. Art der personenbezogenen Daten,
4. Kategorien betroffener Personen
5. Pflichten und Rechte des Verantwortlichen
6. Weisungsgebundenheit des Auftragnehmers
7. Vertraulichkeitsverpflichtung des Personals des Auftragsverarbeiters
8. Festlegung der risikobasierten TOMs
9. Bedingungen für Einsatz von Unterauftragsverarbeitern;
10. Unterstützungspflicht hins. Rechten der betroffenen Personen
11. Unterstützung des Auftraggebers bei der Einhaltung der TOMs, Meldepflichten bei Datenpannen und Datenschutzfolgeabschätzung (DSFA)
12. Datenlöschung / -rückgabe bei Auftragsende
13. Nachweispflicht ggü. dem Auftraggeber bzgl. Einhaltung Art. 28 DSGVO inkl. Inspektionsrecht für Auftraggeber und von diesem beauftragten Prüfer

Accountability-Prinzip

- Für Unternehmen gilt nach der DSGVO die **Nachweis- und Rechenschaftspflicht** (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO):
- Sehr **kurze Fristen** z.B. für die Erfüllung von **Auskunftsansprüchen** von betroffenen Personen (Art. 12 Abs. 3, 15 ff. DSGVO)
- **Das erfordert eine umfassende Dokumentation der Verarbeitungstätigkeiten, insb.**
  - Verarbeitungsverzeichnis Art. 30 DSGVO
  - Datenschutzfolgenabschätzung (DSFA), Art. 35 f. DSGVO
  - Sicherheit der Verarbeitung, Art. 32 DSGVO

Accountability-Prinzip



Verzeichnis der Verarbeitungstätigkeiten

1. Stufe: Wo fallen personenbezogene Daten überhaupt an?

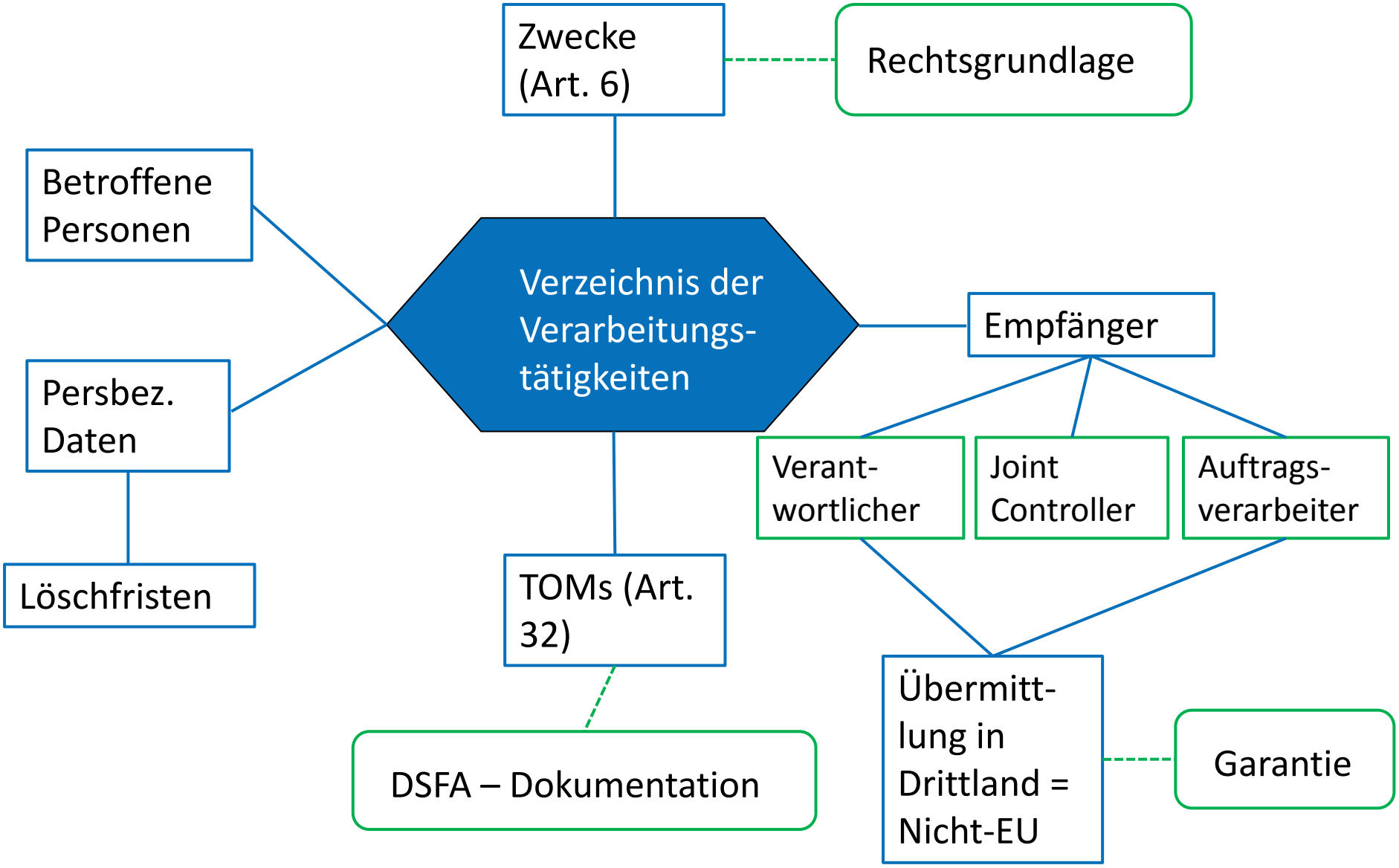
Bsp.:

Datenkategorien	Abteilung/Fachbereich
Mitarbeiterdaten (Name, Geburtsdatum, etc.)	Personalverwaltung
Telefon-Verbindungsdaten in Einzelgesprächsnachweisen	IT-Abteilung
Kundendaten	Vertrieb, Marketing

2. Stufe: Wie werden in den Abteilungen solche Daten verarbeitet?

Bsp.:

Personalabteilung	Abwesenheitsverwaltung
	Betriebliche Altersvorsorge
	Einweisung neuer Mitarbeiter
	Empfang-/Besucherverwaltung
	Bewerberdatenverwaltung



Quelle (aber ergänzt): *Kranig/Sachs/Gierschmann*, Datenschutz-Compliance, 2017, S. 47

Datenschutz-Folgenabschätzung

Grundsatz: zwingende DSFA
Art. 35 Abs. 1 DSGVO

Voraussichtlich hohes Risiko für die Rechte des Betroffenen

Regelbeispiele
Art. 35 Abs. 1 DSGVO

Automatisierte Einzelentscheidung

Besondere Kategorien personenbezogener Daten

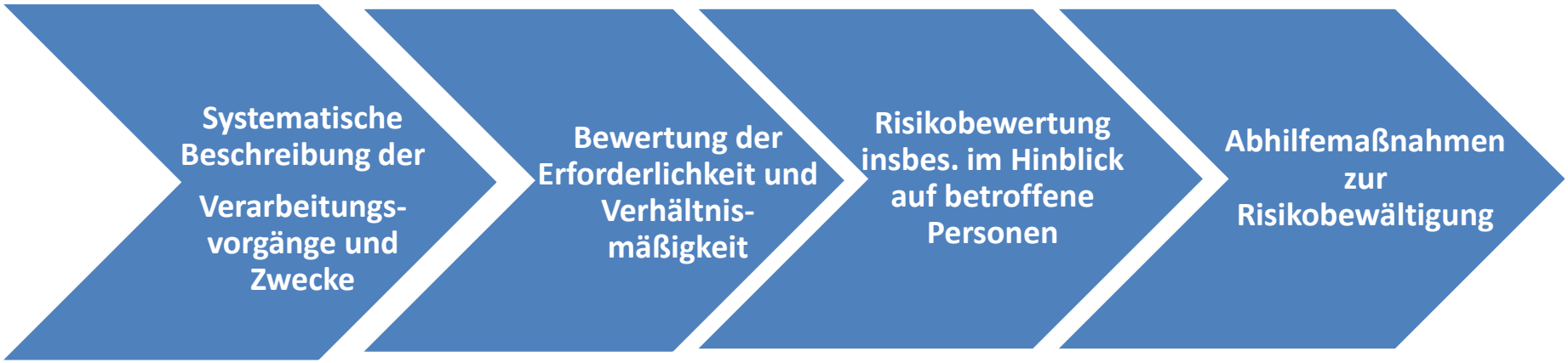
Systematische Überwachung öffentlich zugänglicher Bereiche

Listen der Aufsichtsbehörden
Art. 35 Abs. 4, 5 DSGVO

<u>Positivliste:</u>
Liste für Verarbeitungs-vorgänge, für die DSFA erforderlich ist

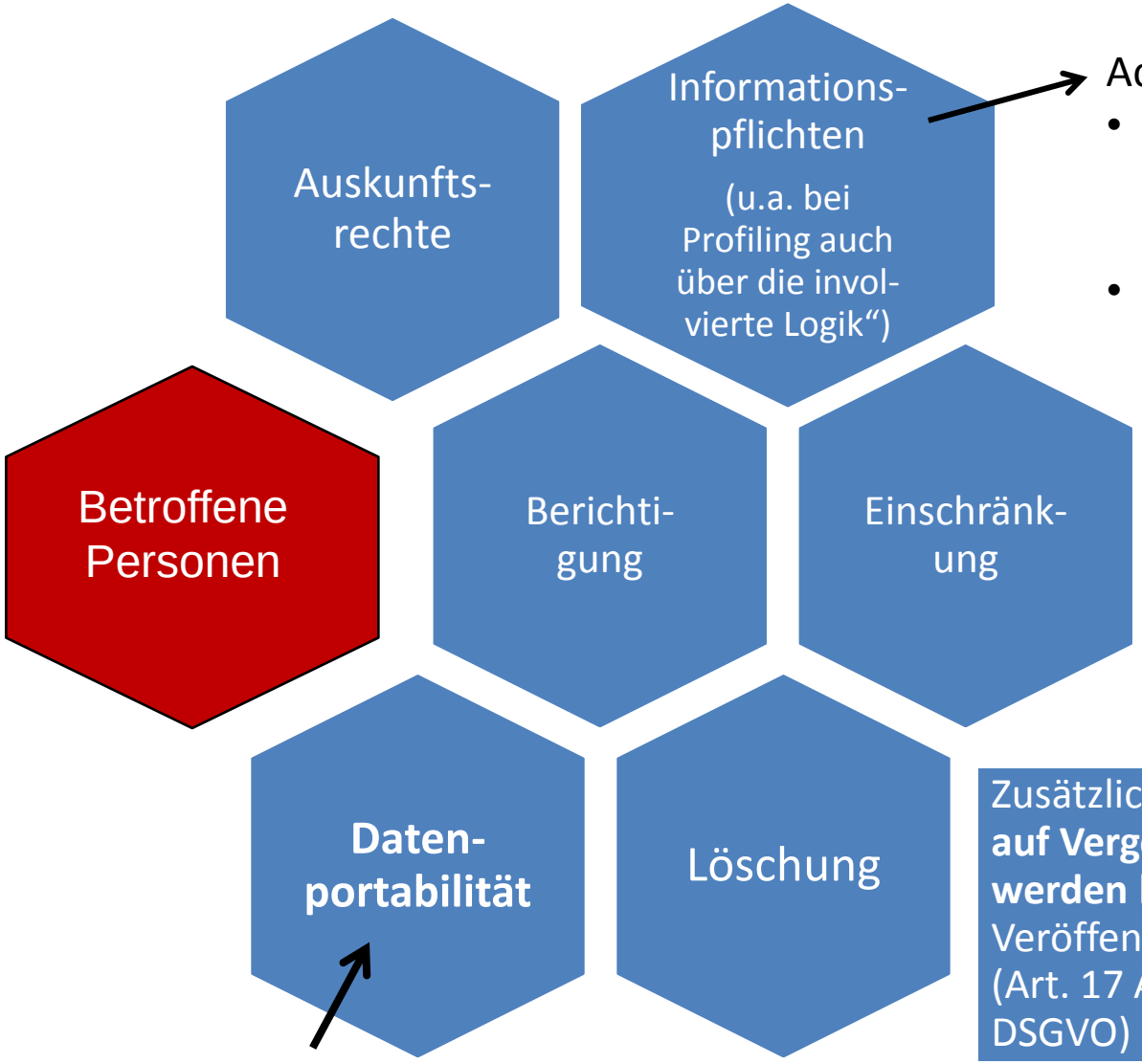
<u>Negativliste:</u>
Liste der Verarbeitungs-vorgänge, die keine DSFA erfordern

Datenschutz-Folgenabschätzung



Falls keine Risikobewältigung: Pflicht zur Konsultation der Datenschutzbehörde (Art. 36 DSGVO)

Betroffenenrechte



Achtung:

- Transparente Information von Beschäftigten
- Erweiterung der Datenschutz-erklärung auf Websites

Zusätzlich: **sog. Recht auf Vergessen-werden** bei Veröffentlichung (Art. 17 Abs. 2 DSGVO)

Zulässigkeit + Information bei betriebl. Überwachung

BAG, Urt. vom 27.7.2017 - 2 AZR 681/16:

Bei Überwachungsmaßnahmen des Arbeitgebers mittels Keylogger
Beweisverwertungsverbot

EGMR Urt. v. 5.9.2017 – Az. 61496/08 (1)

- Ein rumänischer Ingenieur hatte auf Anweisung seines Arbeitgebers ein dienstliches Yahoo-Messenger-Konto eingerichtet, das er zur Kommunikation mit Kunden nutzen sollte.
- Jedoch führte er hierüber auch private Chats mit seinem Bruder und teilweise intime Unterhaltungen mit seiner Verlobten.
- Der Arbeitgeber überwachte den Inhalt der Chats und kündigte dem Ingenieur. Denn die Nutzung dienstlicher Ressourcen für private Zwecke war im Betrieb verboten.
- Der rumänische Arbeitgeber hatte den Ingenieur nicht ausdrücklich darüber informiert, dass er die Chats mitliest.
- Die rumänischen Arbeitsgerichte gaben dem Arbeitgeber recht und bestätigten die Kündigung.

Zulässigkeit + Information bei betriebl. Überwachung

EGMR Urt. v. 5.9.2017 – Az. 61496/08 (2):

- Der Gerichtshof für Menschenrechte (EGMR) entschied, dass dies das Recht des Ingenieurs auf Achtung des Privatlebens (Art. 8 EMRK) verletze
- Arbeitgeber müssen Arbeitnehmer vorab ausdrücklich und in transparenter Weise informieren, wenn und wie weitgehend der Arbeitgeber etwa die E-Mail-Korrespondenz kontrolliert. Das gilt auch, wenn die Privatnutzung ausdrücklich ausgeschlossen ist.
- Wenn sich der Arbeitgeber nur Sender und Empfänger einer E-Mail ansieht, ist das Recht auf Privatleben weniger stark berührt, als wenn er auch den Inhalt liest. Der Arbeitnehmer muss also genau wissen, wie stark er vom Arbeitgeber überwacht wird.
- Das Gericht sprach dem Kläger einen Kostenerstattungsanspruch von 1.365 EUR zu, lehnte aber eine Zahlung von immateriellen Schäden ab. Die Feststellung der Rechtswidrigkeit sei ausreichende Kompensation.

Konsequenz für die Vertragsgestaltung:

- Nicht nur durch die DSGVO, sondern auch aufgrund EGMR sehr hohe Transparenzanforderungen an Regelungen zu ITK-Kontrollen in Arbeitsverträgen, IT-Richtlinien, Einwilligungen und Betriebsvereinbarungen!
- FAQ als probates Mittel?

Datenschutzerklärung auf Websites (1)

§ 13 Abs. 1 S. 1 TMG	Art. 13 Abs. 1, Abs. 2 DSGVO [→ ePrivacy-Verordnung / TMG-neu ??]
[1]Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über • Art, • Umfang und • Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die • Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG […] in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. *[**Speicherdauer** wohl auch nach TMG-alt (+)]*	Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:
	Namen und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters;
	ggf. **Kontaktdaten des Datenschutzbeauftragten**;
	Zwecke sowie die **Rechtsgrundlage** für die Verarbeitung;
	wenn die Verarbeitung auf **Art. 6 Abs. 1 lit. f DSGVO** beruht, die **berechtigten Interessen**, die vom Verantwortlichen oder Dritten verfolgt werden;
	ggf. die **Empfänger / Kategorien von Empfängern** der personenbezogenen Daten *[gilt wohl auch hins. Datenweitergabe an **Auftragsverarbeiter**]*
	ggf. Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das **Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses** der Kommission oder im Falle von Übermittlungen gemäß Art. 46, 47, 49 DSGVO einen Verweis auf die **geeigneten oder angemessenen Garantien** und die Möglichkeit, wie eine **Kopie** von ihnen zu erhalten ist, oder wo sie verfügbar sind.
	Dauer der Speicherung oder die **Kriterien für die Dauer** der Aufbewahrung

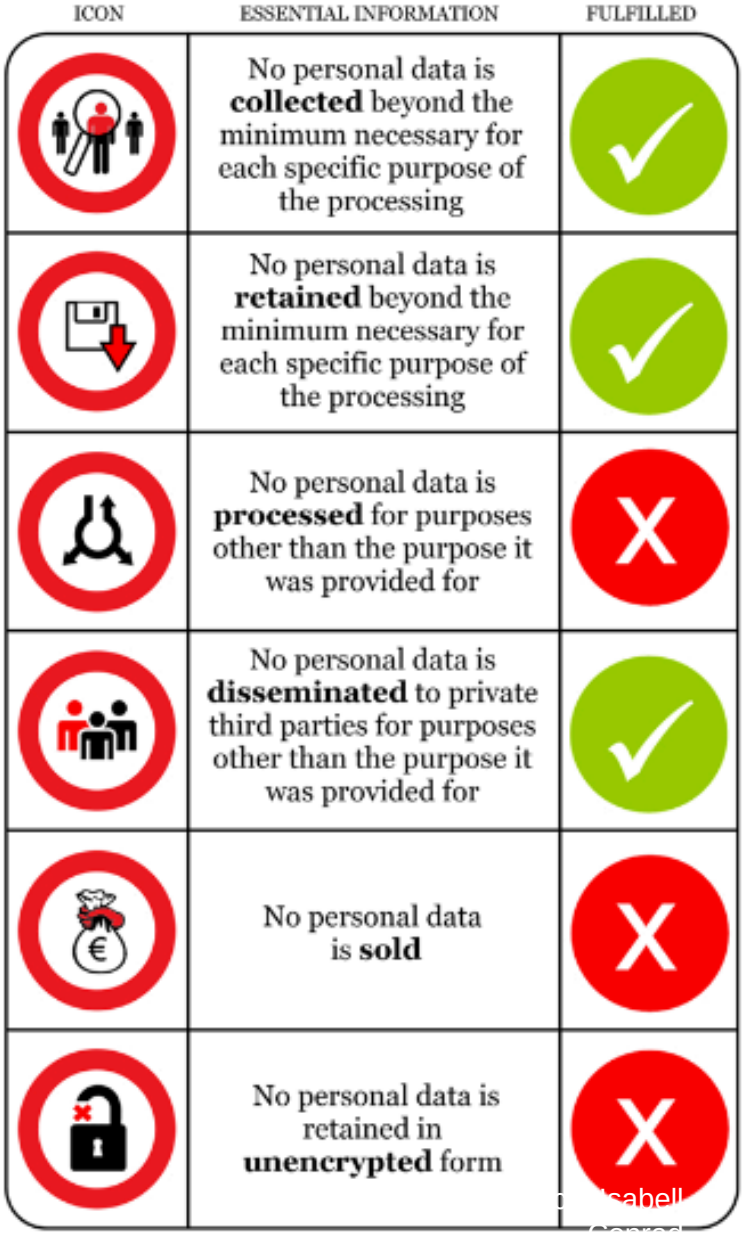
Datenschutzerklärung auf Websites (2)

§ 13 Abs. 1 S. 1 TMG	Art. 13 Abs. 1, Abs. 2 DSGVO [→ ePrivacy-Verordnung / TMG-neu ??]
(-)	Information über Rechte der betroffenen Person (Auskunft, Berichtigung, Löschung inkl. **Recht auf Vergessenwerden**, Einschränkung, Widerspruch, **Datenportabilität**)
	wenn die Verarbeitung auf einer Einwilligung beruht, Information über das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, **ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird**; *[das muss aber nicht in der Datenschutzunterrichtung/Datenschutzerklärung erfolgen, sondern üblicherweise im Rahmen der Einholung der Einwilligungserklärung]*
	Bestehen eines **Beschwerderechts bei einer Aufsichtsbehörde**;
	ob die Bereitstellung der personenbezogenen Daten **gesetzlich oder vertraglich vorgeschrieben** oder **für einen Vertragsabschluss erforderlich** ist, **ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte**; *[insoweit wohl auch erforderlich klare Differenzierung zwischen beim Betroffenen oder bei Dritten erhobenen Daten]*
	das Bestehen einer **automatisierten Entscheidungsfindung** einschließlich **Profiling** und – zumindest in diesen Fällen – aussagekräftige Informationen **über die involvierte Logik** *[BGH zu Schufa-Scoring hatte 2014 verneint, das es eine Informationspflicht/Auskunsftanspruch zur Score-Formel gibt, weil diese Geschäftsgeheimnis der Schufa sei]* sowie die **Tragweite** und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Informationspflichten

- Faire und vergleichbare Informationspolitik
- Ausreichende und verständliche Information der betroffenen Personen über Datenverarbeitungen (Vermeidung eines Information Overkills)
- „**Kombination mit standardisierten Bildsymbolen**“ möglich
- Allerdings evtl. Konflikt mit Datenschutzhinweisen und Einwilligungserklärungen, wenn diese im Detail abweichen oder andere/weitere Verarbeitungsvorgänge vorsehen!

Rechts: Beispiel aus Alexander Alvaro, Lifecycle Data Protection Management, 2012, S. 5



Google Analytics

Bisherige Anforderungen der Datenschutzbehörden:

- Einsatz von Google Analytics ausschließlich zur Erstellung pseudonymer Nutzerprofile
- Informationspflichten in der Datenschutzunterrichtung des Website-Betreibers über den Einsatz von Google Analytics nach einem von der Hamburgischen Datenschutzaufsichtsbehörde angestimmten Text https://www.datenschutzbeauftragter-info.de/fachbeitraege/google-analytics-datenschutzkonform-einsetzen/
- Abschluss eine Auftragsdatenverarbeitungsvertrags (ADV) mit Google Inc. ist erforderlich. ACHTUNG: Muster von Google basiert bislang auf BDSG-alt https://static.googleusercontent.com/media/www.google.de/de/de/analytics/terms/de.pdf

BayLDA, TB 2015/2016 (Seite 49) https://www.lda.bayern.de/media/baylda_report_07.pdf):

„Auch künftig ist es nicht erforderlich, dass der ADV-Vertrag einen Hinweis enthält, auf welche Rechtsgrundlage die Datenübermittlung an Drittländer gestützt wird.“

„Seit 26. September 2016 ist Google nach dem Privacy Shield zertifiziert, sodass die materiellen Voraussetzungen für eine rechtmäßige Übermittlung in die USA vorliegen.“

„Dies entbindet den Verantwortlichen jedoch nicht von der allgemeinen Pflicht gem. Art. 5 Abs. 2 DS-GVO nachzuweisen zu können, dass der Einsatz von Analysetools zur Reichweiten-messung die Anforderungen der DS-GVO erfüllt.“

- Es bleibt also auch abzuwarten und nachzuprüfen, ob Google Inc. ein aktualisiertes AVV-Muster gemäß DSGVO zur Verfügung stellt.

Onlinemarketing (Datenschutz und Unlauter Wettbewerb)

- Onlinemarketing umfasst insb.
  - E-Mail-Werbung (auch an Bestandskunden)
  - Tracking (Web-Analyse) und Targeting (bspw. Geo-Targeting)
- Werbemaßnahmen können zukünftig nur gerechtfertigt sein
  - **bei berechtigten Interesse**n (Art. 6 Abs. 1 lit. f) DSGVO) unter Einbeziehung allg. Grundsätze (Art. 5 Abs. 1 DSGVO:
    - Faire Verfahrensweise
    - Dem Zweck angemessen
    - Kein umfangreiches Interessenprofil
    - In einer für die betroffene Person nachvollziehbaren Weise (insb. Nennung der Quellen)
  - aufgrund einer **Einwilligung** des Betroffenen (Art. 6 lit. a) DSGVO)
- **Einwilligung**
  - Freiwilligkeit (Kopplungsverbot!) Informiertheit des Betroffenen über die Tragweite!
  - jederzeitiges freies Widerrufsrecht
  - Kein klares Ungleichgewicht zwischen Einwilligendem und dem Datenverarbeiter
  - Gesonderte Einwilligungserteilungen bei mehreren Verarbeitungen
- Werbe-Maßnahmen außerdem an § 7 UWG zu messen

Einwilligung

- Freiwilligkeit (Kopplungsverbot!)
- Vorherige Information der betroffenen Person über die Tragweite der Einwilligung (Datenkategorien, Zwecke, Datenempfänger)
- „in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“
- jederzeitiges freies Widerrufsrecht
- Kein klares Ungleichgewicht zwischen Einwilligendem und dem Datenverarbeiter
- Gesonderte Einwilligungserteilungen bei mehreren Verarbeitungen

Vorwirkung der DSGVO / Löschpflichten

VG Karlsruhe v. 6.7.2017, 10 K 7698/16:

- Eine aufsichtsbehördliche Maßnahme (§ 38 Abs. 5 S. 1 BDSG-alt) ist nicht erst dann zulässig, wenn die betreffende Datenverarbeitung ins Werk gesetzt ist. Insbesondere bei besonders sensiblen und sogar strafrechtlich geschützten Daten kann die Aufsichtsbehörde Anordnungen bereits treffen, wenn die unzulässige Datenverarbeitung durch ein Vertragswerk schon deutlich vorgezeichnet ist und dieses Vertragswerk in Kraft getreten ist.
- Die Datenschutzgrundverordnung enthält über den Erforderlichkeitsgrundsatz (vgl. Art. 5 Abs. 1 Buchst. e EU-DSGVO) hinaus **keine konkreten Vorgaben zu den Prüf- und Löschfristen**. Ihr ist lediglich – unter anderem in Erwägungsgrund 39 – zu entnehmen, dass der Verantwortliche die Dauer seiner Datenverarbeitung unabhängig von einem entsprechenden Verlangen des Betroffenen nach Art. 17 EU-DSGVO („Recht auf Vergessenwerden“) regelmäßig zu überprüfen hat. Hierbei kann auf **typisierte Regelprüffristen** für wiederkehrende Vorgänge zurückgegriffen werden, da es gerade Unternehmen, die in großem Umfang Daten verarbeiten – wie etwa Auskunfteien – **nicht zuzumuten ist, jeden Einzelfall gesondert zu bewerten**.
- Eine **Überprüfung kann in bestimmten Intervallen** erfolgen, so wie es beispielsweise bislang nach § 35 Abs. 2 S. 2 Nr. 4 BDSG möglich und zulässig war.

Vorwirkung der DSGVO / Terrorlistenabgleich

Finanzgericht (FG) Düsseldorf (Beschluss v. 9.8.2017 – 4 K 1404/17)

Das FG Düsseldorf behandelte einen Fall zum Terrorlisten-Abgleich:

Die Zollbehörden hatten einem Unternehmen das Zertifikat als Acknowledged Economic Operator (AEO) nicht erteilt, weil das Unternehmen (aus Datenschutzgründen: mangelnde Erforderlichkeit) das Durchführung von Terrorlisten-Screenings seiner Mitarbeiter verweigerte.

Aus Sicht des FG Düsseldorf verstößt das verhalten der Zollbehörden gegen die DSGVO.

Risikobasierter Ansatz

- Datenschutzfragen sollen künftig anhand einer „**Risikoorientierung**“ entschieden werden.
- Das betrifft bspw.
  - die Sicherheit der Verarbeitung (technische und organisatorische Maßnahmen),
  - die Datenschutzfolgenabschätzung und
  - die Data Breach Notification (Meldepflicht).
- Bietet Flexibilität, birgt aber zunächst Rechtsunsicherheit
- erheblich gesteigerten Haftungsrisiken für den Verantwortlichen
- erheblicher Aufwand

Sicherheit der Verarbeitung

Risikoanalyse: Risikobewertungskriterien zur Festlegung von Sicherheitsmaßnahmen
Art der Datenverarbeitung (insb. Kategorien v. Daten)
Kategorien v. betroffenen **Personen** (bsp. Kinder)
Umfang der Datenverarbeitung)
Zweck der Datenverarbeitung (soweit gesetzl. zu präzisieren)
Konkrete **Bedrohung** bspw. durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. unbefugten Zugang zu pD Daten
Implementierungs**kosten** (Berücksichtigung ökonomischer Aspekte)
Stand der Technik
Eintrittswahrscheinlichkeit (vergangenheitsbezogen als statistischer Erfahrungswert oder zukunftsorientiert geschätzt)
Schaden für den Betroffenen: alle physischen, materiellen oder immateriellen Schäden) wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit, erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene Person.
Schaden für den Verantwortlichen

Pressemitteilung des BayLDA v. 21.2.2017

„Unverschlossene Aktenschränke mit Patientenakten im öffentlich zugänglichen Treppenhaus geht gar nicht“

- **Mehrfamilien**haus mit einer Zahn**arzt**praxis und einer Bankfiliale
- Im einem Kellergang **unverschlossene** Aktenschränke
- Akten und anderes Material mit personenbezogenen Daten aus der Zahnarztpraxis

Verstoß gegen Datensicherheit → Bußgeldbewehrt

Datenpannen: Schnelle Reaktion

- **Wann melden?**
  - **Jede Verletzung der Sicherheit, unabhängig von Datenarten, nicht erst bei Schäden**
  - **Mögliche Fälle** unrechtmäßiger Kenntniserlangung:
    - Hacking
    - unsachgemäße Verschrottung von Datenträgern
    - Verlust und Diebstahl von Datenträgern (Laptop, Smartphone, etc.)
    - (Heimlicher) Weiterverkauf von Daten durch Mitarbeiter
    - Fehlübermittlung von E-Mails
    - Achtung: False Positives möglich (*wichtige Kunden-E-Mail im Spam-Ordner ohne Grund*)
  - **Unverzüglich**, **grundätzlich innerhalb 72 Stunden!?** (Art. 33 DSGVO)
- **An wen melden?**
  - An die zuständige Datenschutzaufsichtsbehörde (für Unternehmen in Bayern: Bayerisches Landesamt für Datenschutzaufsicht)
  - Zwingend vorher: Einbeziehung der Geschäftsleitung und des Datenschutzbeauftragten
  - **bei hohen Risiken** für die betroffenen Personen: Auch Meldung an die Betroffenen (Art. 34 DSGVO)

Datenschutzbeauftragter - Benennpflicht (1)

Artikel 37 DSGVO

(1) Der **Verantwortliche und** der **Auftragsverarbeiter** benennen **auf jeden Fall** einen Datenschutzbeauftragten, wenn

[…]

b) die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche regelmäßige und systematische Überwachung** von betroffenen Personen erforderlich machen, oder

c) die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung **besonderer Kategorien von Daten** gemäß Artikel 9 oder von personenbezogenen Daten über **strafrechtliche** Verurteilungen und Straftaten gemäß Artikel 10 besteht.

(2) Gemeinsamer Datenschutzbeauftragter bei Unternehmensgruppe möglich

Datenschutzbeauftragter – Benennpflicht (2)

Öffnungsklausel für die Mitgliedstaaten in Art. 37 Abs. 4 DSGVO:

§ 38 BDSG 2018: Zusätzlich Benennpflicht, wenn

- *„in der Regel mindestens 10 Personen ständig mit automatisierter [Datenverarbeitung] beschäftigt“* oder unabhängig von der Personenzahl:
- und/oder Datenverarbeitung unterliegt einer DSFA oder
- geschäftsmäßige Datenübermittlung /anonymisierte Übermittlung / Markt- und Meinungsforschung

Mindestaufgaben des Datenschutzbeauftragten

- Unterrichtung/Beratung des Verantwortlichen
- Überwachung der Einhaltung von Datenschutz-Vorschriften und DS-Strategien
- **neue Aufgaben** infolge des risikobasierten Ansatzes
- **Beratung** bei DSFA auf Anfrage (anders als bei BDSG-alt ist nicht mehr der Datenschutzbeauftragte für die „Vorabkontrolle“ zuständig)
- **Überwachung** der Durchführung der DSFA
- Zusammenarbeit mit Aufsichtsbehörden
- str. ob Begriff der „Überwachung“ beim Datenschutzbeauftragten zu einer Risikoerweiterung ggü. Hinwirkungspflicht nach BDSG-alt führt (Garantenstellung?)

§ 38 Abs. 2 i.V.m. § 6 Abs. 4 BDSG 2018: **Kündigungsschutz** bei internem Datenschutzbeauftragten, wenn Benennpflicht besteht

Notfallplan zur Umsetzung DSGVO-Implementierung

Prioritäre Maßnahmen: bereits jetzt zu beginnen

- Update/Erstellung des Verzeichnis von Verarbeitungstätigkeiten
- GAP-Analyse:
  - Wo liegt für Verarbeitungen eine gesetzliche Erlaubnis vor?
  - Wo liegen wirksame Einwilligungen vor?
  - Wo gibt es ein „Gap“?
- Sensibilisierung für Risiko-Klassifikation und IT-Sicherheit (v.a. Verschlüsselung!)
- Update/Erstellen von interner Richtlinien für Auditprozesse und DSFA
- Anpassung von Auftragsverarbeitungsvertägen (evtl. Joint Control)
- Vorbereitung auf Betroffenenrechte
  - neue Auskunft, Recht auf Vergessenwerden, Datenübertragbarkeit
  - Erweiterte Informationspflichten: etwa bei der Datenschutzerklärung auf Websites
- Prozess für Benachrichtigungen bei Datenschutzverletzungen

Hilfestellung

Leitfäden / Formulare / Literatur u.ä.

- IHK München: https://www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Datenschutz/Die-EU-Datenschutz-Grundverordnung/
- BayLDA: https://www.lda.bayern.de/de/datenschutz_eu.html
- BITKOM: https://www.bitkom.org/Themen/Datenschutz-Sicherheit/DSGVO.html
- GDD: https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo
- Siehe auch z.B. Musterauftragsverarbeitungsvertrag für das Gesundheitswesen von BvD u.a.
- Fachzeitschriften: ZD (Zeitschrift für Datenschutz), DuD, RDV etc.
- Kommentarliteratur:

  Gola, DS-GVO, 2017

  Ehmann/Selmayr; DSGVO, 2017

  Kühling/Buchner, DSGVO, 2017

  Paal/Pauly, DSGVO, 2017

  Piltz, BDSG, 2018

Datenschutz als Managementaufgabe

Meldung der Süddeutschen Zeitung v. 6.10.2016, 18:50 Uhr:

„Datenschutz für Manager

Ein EU-Gesetz zwingt Unternehmen zu mehr Daten-Sicherheit ab Mai 2018 - sonst drohen hohe Strafen. Trotzdem freuen sie sich.

Daimler-Datenschützer Rieß: ‚Da verändert sich richtig was in den Unternehmenskulturen', sagte er. **Datenschutz sei in Zukunft eine echte Managementaufgabe.“**

Quelle: *http://www.sueddeutsche.de/wirtschaft/recht-datenschutz-fuer-manager-1.3193109*

Privacy by Design / by Default

Privacy baked in ?

EG 4 DSGVO: „Die Verarbeitung personenbezogener Daten sollte **im Dienste der Menschheit stehen. […]“**

Systemgestaltung mit Datenschutz

Minimum	Für „Optimum“ zusätzlich
• Defensive Interpretation der gesetzlichen Regelungen	• Proaktiv agieren
• Dokumentation von internen Strategien und Maßnahmen	• Lösungsraum kennen und Erweitern
• Kommende Anforderungen der Aufsichtsbehörden abwarten und darauf reagieren	• Zertifizierung anstreben
• Klare Verantwortlichkeit	• Datenschutz-Management-System für gesamten Lebenszyklus einsetzen
	• Mit anderen Akteuren und Disziplinen interagieren: Technik und Prozesse

Quelle: Hansen, LfD Schleswig-Holstein, 5. DFN-Konferenz, 29.11.2016

Privacy by Design

- betrifft Designstandards und Standardeinstellungen in allen Geschäftsmodellen und -sektoren
- Verantwortliche haben die Datenschutz-Einstellungen der betroffenen Personen zu berücksichtigen
- Anforderungen an **Hersteller/Produkte**: z.B.
  - granulare Löschfunktionen
  - granulares Berechtigungskonzept
  - Report-Funktionalität: anonyme Reports
  - **Datenportabilität** (z.B. „Kontoumzugsfunktion“ für Bankkunden)
  - Aktualisierungsfunktion für Datei-Eigenschaften (Datenschutz-Default-Einstellungen), evtl. kombiniert mit Signatur
  - Funktionen zur Protokollierung, Abrufbarkeit und Widerrufbarkeit von elektronischen Einwilligungen

Privacy by Design: Folgen für die IT-Beschaffung

1. **Mangel einer Software, wenn sie (im Standard) nicht datenschutzkonform eingesetzt werden kann?**

- je nach Art der Software-Überlassung (Kauf, Miete, Werkvertrag?)
- Mangel in Folge "vereinbarter Beschaffenheit" → spezifische Funktionalitäten in positiver / negativer Beschaffenheitsvereinbarung vereinbart?
- Mangel in Folge "vorausgesetzter Verwendung" → Positive Kenntnis des Herstellers, dass Software zur Verarbeitung personenbez. Daten verwendet wird
- Mangel in Folge "gewöhnliche Verwendung" → Wem und was dient die Software? Der Verarbeitung personenbez. Daten?
- Einzelfallprüfung → **Pflichtenheft!!**

2. **Anforderungen an Software-Hersteller / IT-Zulieferer**

- Softwarehersteller sind grds. nicht Adressaten von Datenschutzvorschriften
- Anforderungen (ggf. unter Einbindung des DSB) für Lieferanten festlegen, d.h., welche Funktionalitäten aus datenschutzrechtlicher Sicht erforderlich sind (Ausgangspunkt sind (Produkt-)Spezifikationen & Projektbeschreibungen)

Zusammenfassung zur DSGVO

- Territorialer Anwendungsbereich ausgeweitet: **Marktortprinzip** statt Sitzlandprinzip
- **Rechenschaftspflicht (Accountability):** Dokumentationspflicht als neues Prinzip
- **strenges Verbotsprinzip** bei besonderen Datenarten (Gesundheit, Religion etc.)
- „**Recht auf Vergessenwerden**“ und „**Einschränkung**“ (die Unklarheit, wann z.B. Altkundendaten konkret gelöscht werden müssen, bleibt); besonders relevant die **Mitteilungspflichten** im Zusammenhang mit Löschung und Sperrung
- **Datenportabilität** (Fremdkörper im Datenschutzrecht, Reichweite der Pflicht für den Altanbieter unklar)
- **Automatisierte Generierung von Einzelentscheidungen einschließlich Profiling:** neu ist die Pflicht zur Information über die „**involvierte Logik**“, also über den Algorithmus (anders als noch bei BGH zu SCHUFA-Formel 2014!)
- **Privacy by Design / Default + risikobasierter Ansatz**: Entwicklung technischer Verfahren, die sicherstellen, dass „privacy impact“ im Rahmen der Datenverarbeitung möglichst gering ist.
- **Erweiterte** Pflichten für **Auftragsverarbeiter**
- **Datenschutzfolgenabschätzung** (Erweiterung der Vorabkontrolle nach BDSG)
- **Zertifizierung**
- **Meldepflicht bei Datenschutzverstößen**

SSW Schneider Schiffer Weihermüller

Rechtsanwälte Steuerberater Wirtschaftsprüfer

Beethovenstraße 6 80336 München
Tel. 089/54349-100 Fax 089/54349-111

isabell.conrad@ssw-muc.de

Homepage: www.ssw-muc.de