Die DS-GVO und ihre praktische Umsetzung

DS-GVO in der Unternehmenspraxis

IHK

Inhalt

1. Datenschutz – ein Grundrecht

”Jeder Mensch hat grundsätzlich das Recht, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.”

BVerfG, u.a. ”Volkszählungsurteil” vom 15. Dezember 1983

Grundrecht → Informationelle Selbstbestimmung

DS-GVO (Art. 1 DS-GVO)

Schützt die Grundrechte und Grundfreiheiten natürlicher Personen bei Verarbeitung personenbezogener Daten

BDSG-neu: 25.05.2018

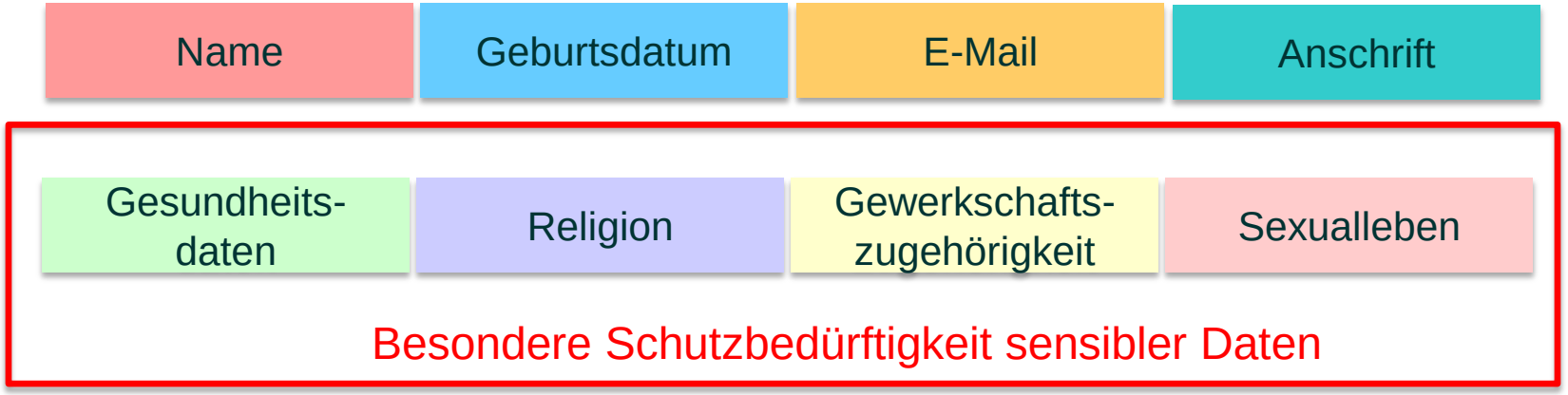
Inkrafttreten:	25.05.2016
Anwendbarkeit:	25.05.2018

2. Anwendungsbereich der DS-GVO

- **Personenbezogene Daten (pbD)**
  = alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen lassen.

- **Verarbeitung (sehr umfangreiche Definition)**
  = ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit pbD

Beispiele pbD:



2. Anwendungsbereich der DS-GVO

Identifizierbare personenbezogene Daten

- Dynamische IP-Adresse
- Akteneinsicht in Strafverfahren
- Werturteile (Zeugnisse etc.)
- Bestellverlauf (Onlineshop)

EuGH Urt. v. 19.10.2016 – C 582/14
Dynamische IP-Adresse – pbD

Begründung: nicht alle zur Identifikation notwendigen Mittel müssen in einer Hand sein.
Es genügt, dass der Website-Betreiber (Verantwortlicher) potenziell legale Möglichkeiten hat, an die Identifizierungsmerkmale heranzukommen.

pbD → weit zu fassender Begriff

3. Grundprinzipien: Rechtmäßigkeit, Treu und Glauben, Transparenz

Rechtmäßigkeit: Jede Verarbeitung pbD bedarf einer **Rechtsgrundlage** oder Einwilligung (Art. 6 Abs.1 DS-GVO)

- Erfüllung eines Vertrages oder vorvertraglicher Maßnahmen
- Lebenswichtige Interessen der Betroffenen oder einer anderen natürlichen Person
- Erfüllung rechtlicher Verpflichtung
- Wahrnehmung einer Aufgabe im öffentlichen Interesse
- berechtigte Interessen des Verantwortlichen oder eines Dritten und keine entgegenstehenden Interessen der betroffenen Personen → Interessenabwägung

3. Grundprinzipien

- Zweckbindung

  → pbD dürfen nur zum angegebenen Zweck verarbeitet werden

- Datenminimierung

  → nur benötigte Daten erheben

- Richtigkeit

  → auf die Richtigkeit der Daten ist zu achten

- Speicherbegrenzung

  → nicht benötigte Daten müssen gelöscht werden

- Integrität und Vertraulichkeit

  → Daten müssen vor Zugriff Dritter geschützt werden

Marktortprinzip:
DS-GVO anwendbar, wenn pbD einer Person verarbeitet werden, die sich in der EU befindet.

1. Benennungspflicht des Datenschutzbeauftragten

- Benennungspflicht des Datenschutzbeauftragten entspricht grundsätzlich dem derzeitigen Recht (Art. 37 Abs. 1 DS-GVO i.V.m. § 38 Abs. 1 BDSG-neu):

  → Ab 10 Personen, die ständig mit der automatisierten personenbezogenen Datenverarbeitung beschäftigt sind

  → Kerntätigkeit: umfangreiche und systematische Überwachung von Betroffenen oder die Verarbeitung sensibler Daten i.S.d. Art. 9 oder 10 DS-GVO

  → Unabhängig von der Anzahl der Personen, wenn Verarbeitungen pbD vorliegen, die einer Datenschutz-Folgeabschätzung unterliegen

2. Überblick über personenbezogene Daten verschaffen

1. Welche pbD werden verarbeitet?
   - Mitarbeiterdaten (Name, Anschrift, Geburtstag, etc.)
   - Kundendaten (Rechnung, Anschrift, E-Mail etc.)
   - Systemwartung, Einzelgesprächsnachweise etc.
2. Wo werden die pbD verarbeitet?
   - Personalabteilung
   - Vertrieb, Buchhaltung
   - IT-Abteilung
3. Wie werden die pbD verarbeitet?
   - Bewerberverwaltung, etc.
   - Rechnungsstellung, Newsletter-Versand etc.
   - Wartung etc.

Grundlage für: Betroffenenrechte, Erstellung von Verzeichnissen von Verfahrenstätigkeiten, Meldung von Datenpannen, Erfüllung von Dokumentationspflichten etc.

3. Verzeichnis von Verarbeitungstätigkeiten (VvV) – Art. 30 DS-GVO

1. Welche pbD werden verarbeitet?
2. Wo werden die pbD verarbeitet?
3. Wie werden die pbD verarbeitet (zu welchen Zweck)?
4. An wen werden die pbD übermittelt?
5. Welches Risiko birgt die Verarbeitung (Datenschutz-Folgeabschätzung)?

Kein VvV gemäß Art. 30 Abs. 5 DS-GVO notwendig (greift jedoch in der Regel nicht → siehe Punkt 4), wenn:

- Weniger als 250 MA
- Kein Risiko für Rechte und Freiheiten Betroffener
- Keine Verarbeitung sensibler pbD nach Art. 9 oder 10 DS-GVO
- Gelegentliche Verarbeitung

3. Verzeichnis von Verarbeitungstätigkeiten (VvV) – Art. 30 DS-GVO

Verzeichnis von Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	*Mustermann GmbH*
Ggf. gemeinsamer Verantwortlicher	*(Name, Anschrift)*
Gesetzlicher Vertreter (= Geschäftsführung)	*(Name, Kontaktdaten)*
Datenschutzbeauftragter (soweit benannt)	*(Name, Kontaktdaten)*

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Bezeichnung der Verarbeitungstätigkeit:	*Werbung via E-Mail*
Zweckbestimmung:	*Werbung*
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	• *Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7)*
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	*Risikobewertung ergab:*

Erhebung der Daten	
Kreis der betroffenen Personengruppen	*Kunden ,Interessenten*
Art der gespeicherten Daten bzw. Datenkategorien:	*Beispiele:* • *Name/Vorname/Anrede/Titel* • *E-Mail Adresse*
Herkunft der Daten:	*Vom Betroffenen selbst*

Zugriffsberechtigte Personen	
Zugriffsberechtigte Personen	*Marketing Abteilung*

Auftragsverarbeitung als Auftraggeber (optionale Angabe)
Mustermann GmbH

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	*Mustermann Gmbh in USA*
Angemessenes Datenschutzniveau durch:	*z.B.* • *Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO* • *Garantien gem. Art. 46 DSGVO* - *Verbindliche interne Datenschutzvorschriften (BCR)* - *EU-Standardvertrag* - *(USA: Privacy Shield)* *Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren (Art 49 Abs. 1. Abs. 2 DSGVO)*

Speicherdauer
Bis zur Abmeldung vom Newsletter. *Löschung innerhalb der 24 Stunden nach Abmeldung*

Stellungnahme des Datenschutzbeauftragten
Der Datenschutzbeauftragter hat das Verfahren freigegeben/ nicht freigegeben. *Begründung:…*

Prüfung durch die Geschäftsführung	
Geprüft und freigegeben	
Datum, Unterschrift	

2

Beispiel

Viele sehr gute Muster online verfügbar.
In der Suchmaschine Begriffe wie z.B. „Muster Verzeichnis von Verarbeitungstätigkeit“ eingeben.

3. Verzeichnis von Verarbeitungstätigkeiten (VvV) – Art. 30 DS-GVO

Neu: Verantwortlicher/Auftraggeber

- Verantwortlicher:

  Außen: Geschäftsführung

  Innen: Abteilungsleitung
- Datenschutzbeauftragter (sofern bestellt) nur Überwachungspflicht
  → Pflicht zur Vorab-Einbindung
  → und Möglichkeit der StN
- Risikobewertung und ggf. DS-FA

Neu: Auftragsverarbeiter

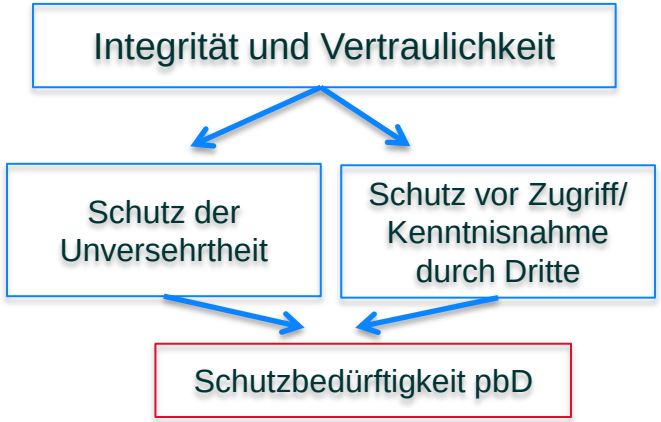
- Pflicht zur Führung des VvV
- Verantwortlicher:

  Außen: Geschäftsführung

  Innen: Abteilungsleitung
- Risikobewertung und ggf. DS-FA
- Verantwortung für die Sicherheit der Verarbeitung nach Art. 32 DS-GVO, Art. 5 Abs. 1 f DS-GVO

4. Datenschutz-Folgeabschätzung (DS-FA) - Art. 35 DS-GVO

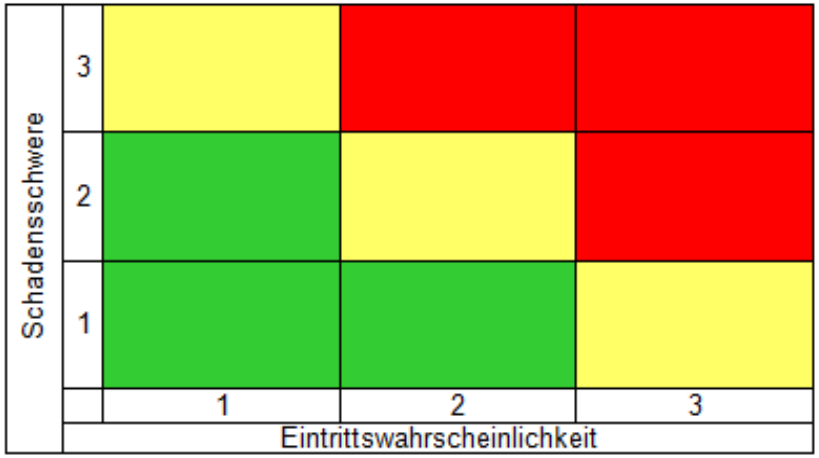
aus der Sicht des Betroffenen



1. Schritt: Risikobewertung

Feststellung des Risikos

→ z.B.: normales, hohes oder sehr hohes



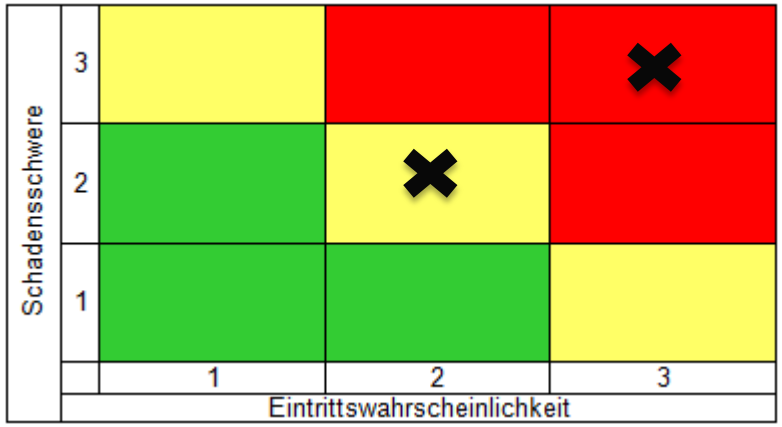
Normales Risiko → tolerable Beeinträchtigung, geringfügige Auswirkung

Hohes Risiko → erhebliche, nicht tolerable Beeinträchtigung, breite Beeinträchtigung des Ansehens oder Vertrauens

Sehr hohes Risiko → besonders bedeutende Beeinträchtigung wie gesellschaftlicher oder wirtschaftlicher Ruin, Gefahr für Leib und Seele

4. Datenschutz-Folgeabschätzung (DS-FA) - Art. 35 DS-GVO

aus der Sicht des Betroffenen



2. Schritt: DS-FA (beim hohen/ sehr hohen Risiko)

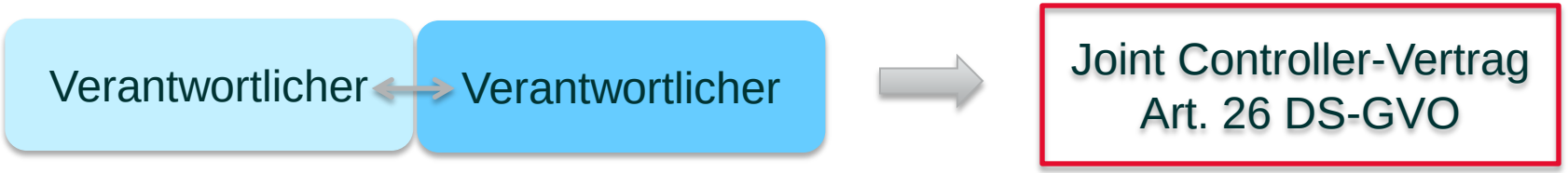
Abmilderung des Risikos soweit möglich

Falls möglich → keine DS-FA
Falls nicht möglich → DS-FA

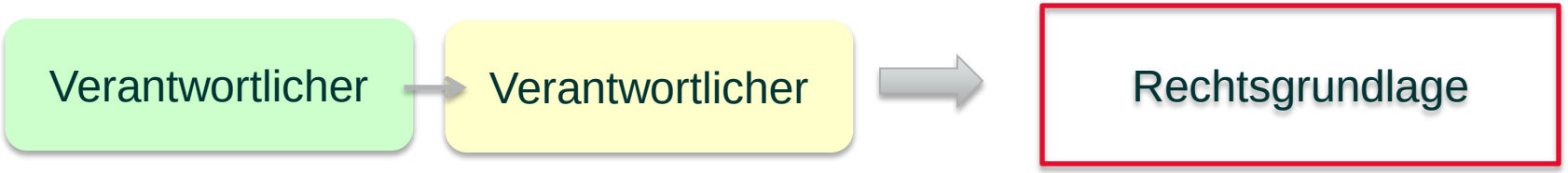
Black/ White List der Datenschutzaufsichtsbehörden: kommt nicht zum 25.05.2018

5. Übermittlung pbD: Verantwortliche und Auftragsverarbeitung

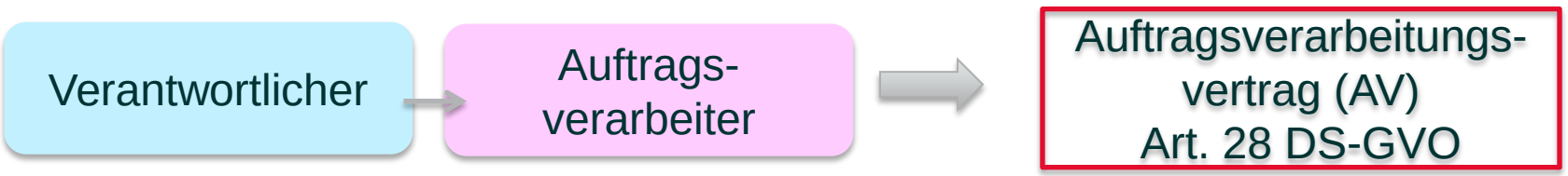
1. Konstellation: gemeinsam Verantwortliche



2. Konstellation: keine gemeinsamen Verantwortlichen



3. Konstellation: Auftragsverarbeitung



5. Übermittlung der pbD

Innerhalb der EU

- Rechtsgrundlagen für die Übermittlung

Außerhalb der EU (Drittländer)

- Gewährleistung des angemessenen Datenschutzniveaus:
  - Angemessenheitsbeschluss der EU - Kommission gem. Art. 45 Abs. 3 DSGVO
  - Garantien gem. Art. 46 DSGVO
  - Verbindliche interne Datenschutzvorschriften (BCR)
  - EU-Standardvertragsklauseln
  - USA: Privacy Shield

Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren (Art. 49 Abs. 1. Abs. 2 DSGVO)

- Rechtsgrundlage für die Übermittlung

6. Auftragsverarbeitung - Art. 28 ff. DS-GVO

- Auftragsverarbeitung: Weisungsgebundes Outsourcing einer personenbezogenen Datenverarbeitung
- Kein Konzernprivileg

  → entweder Rechtsgrundlage wie z.B. berechtigtes Interesse (Art. 6 Abs. 1 f) DS-GVO) oder gemeinsame Verantwortliche
- Wartungsfälle: Auftragsverarbeitungsvertrag notwendig, da der Zugriff auf pbD nicht ausgeschlossen werden kann
- Pflicht zum sorgfältigen Auswählen des Auftragsverarbeiters
- Haftung des Auftragsverarbeiters und Subunternehmers

  → nur für den jeweiligen Bereich der Datenverarbeitung

6. Auftragsverarbeitung - Art. 28 ff. DS-GVO

- Abschluss des Auftragsverarbeitungsvertrages schriftlich oder in elektronischer Form

  → Signatur oder Unterschrift nicht notwendig

  Bei bestehenden Auftragsdatenverarbeitungsverträgen

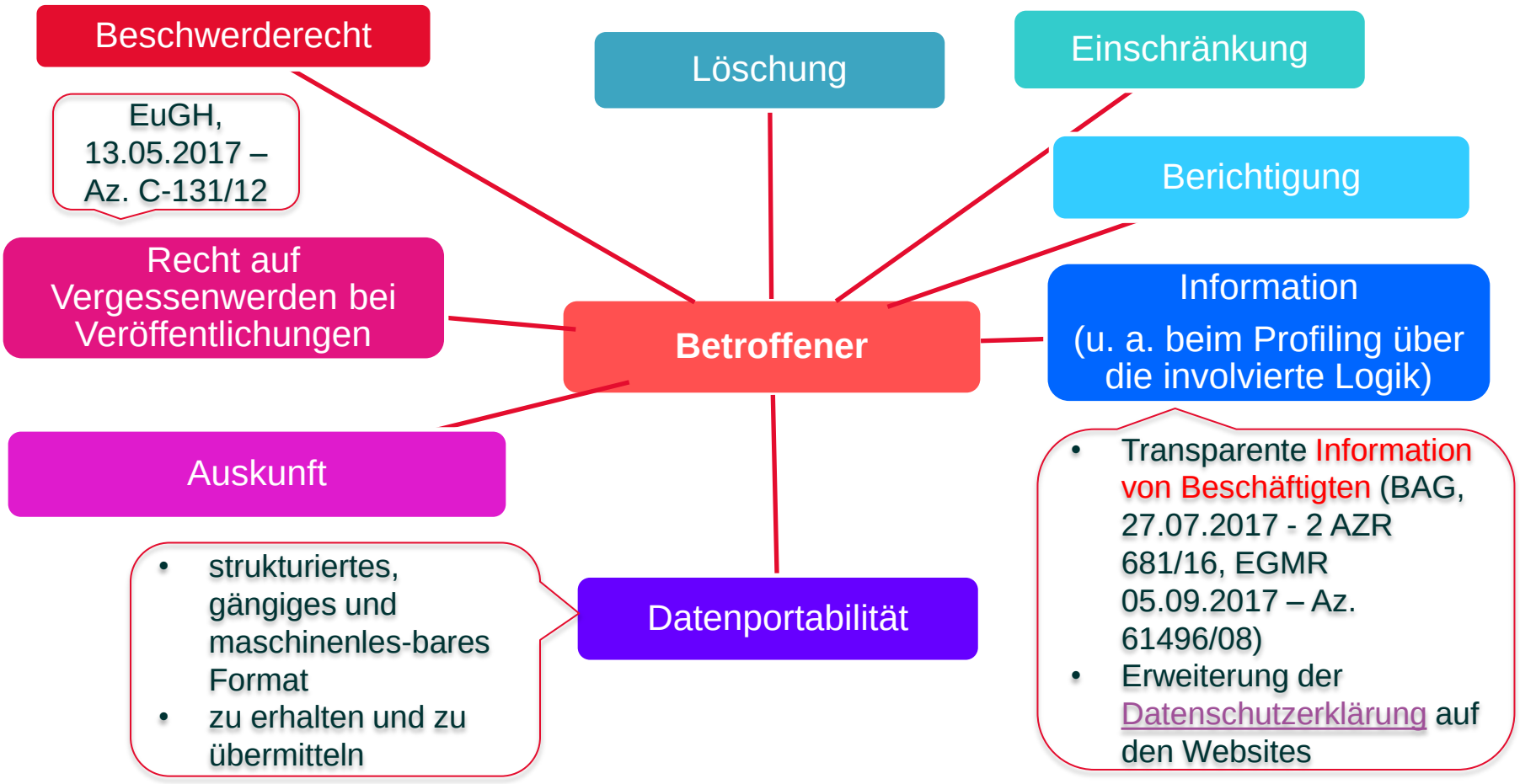
  → Neuerstellung, da gesetzliche Mindestinhalte sich geändert haben

  → online sehr gute Muster verfügbar

- Sitz nicht in der EU: Benennung eines Repräsentanten in der EU

Art. 28 Abs. 10 DS-GVO
Bestimmt der Auftragsverarbeiter die Zwecke und Mittel der Verarbeitung pbD wird er zu Verantwortlichen
Hinweispflicht im Auftragsverarbeitungsvertrag

7. Betroffenenrechte



8. Dokumentationspflichten

- Art. 5 Abs. 2, Art. 24 Abs. 1 DS-GVO: Unternehmen haben die Nachweis- und Rechenschaftflicht (Accountability-Prinzip)

  → Unternehmen müssen nachweisen, dass sie die pbD datenschutzkonform verarbeitet haben

- Sehr kurze Fristen, z.B. für die Erfüllung von Auskunftsansprüchen von Betroffenen nur 1 Monat (Art. 12 Abs. 3, 15 ff. DS-GVO)
- Daher: umfassende Dokumentation der Verarbeitungstätigkeiten notwendig

  → Verzeichnis von Verarbeitungstätigkeiten

  → Risikobewertung und Datenschutz-Folgenabschätzung

  → Sicherheit der Verarbeitung

Implementierung Datenschutz-Management- System

9. Datenpannen – Art. 33 DS-GVO

- Datenpanne: liegt bei Verletzung des Schutzes pbD vor

  → z. B. Verlust von Hardware (mobile Endgeräte), gezielter Angriffe von außen oder versehentlich durch einen Mitarbeiter, unsachgemäße Verschrottung von Datenträgern, unrechtmäßige Übermittlung pbD etc.

- Meldepflicht: sobald jede Verletzung des Schutzes der pbD festgestellt wurde; nicht erst bei Schäden
- Meldeberechtigt: die zuständige Datenschutzaufsichtsbehörde

  → für Unternehmen in Bayern ist Bayerisches Landesamt für Datenschutzaufsicht (BayLDA) zuständig (Online Tool)

- Zeitrahmen: unverzüglich, d.h. innerhalb von 72 Stunden
- Bei hohen Risiken für die Betroffenen: Meldung an die Betroffenen

10. Weitere Regelungen

- Überarbeitung von Einwilligungen aufgrund neuer Formvorschriften und Begriffsänderungen

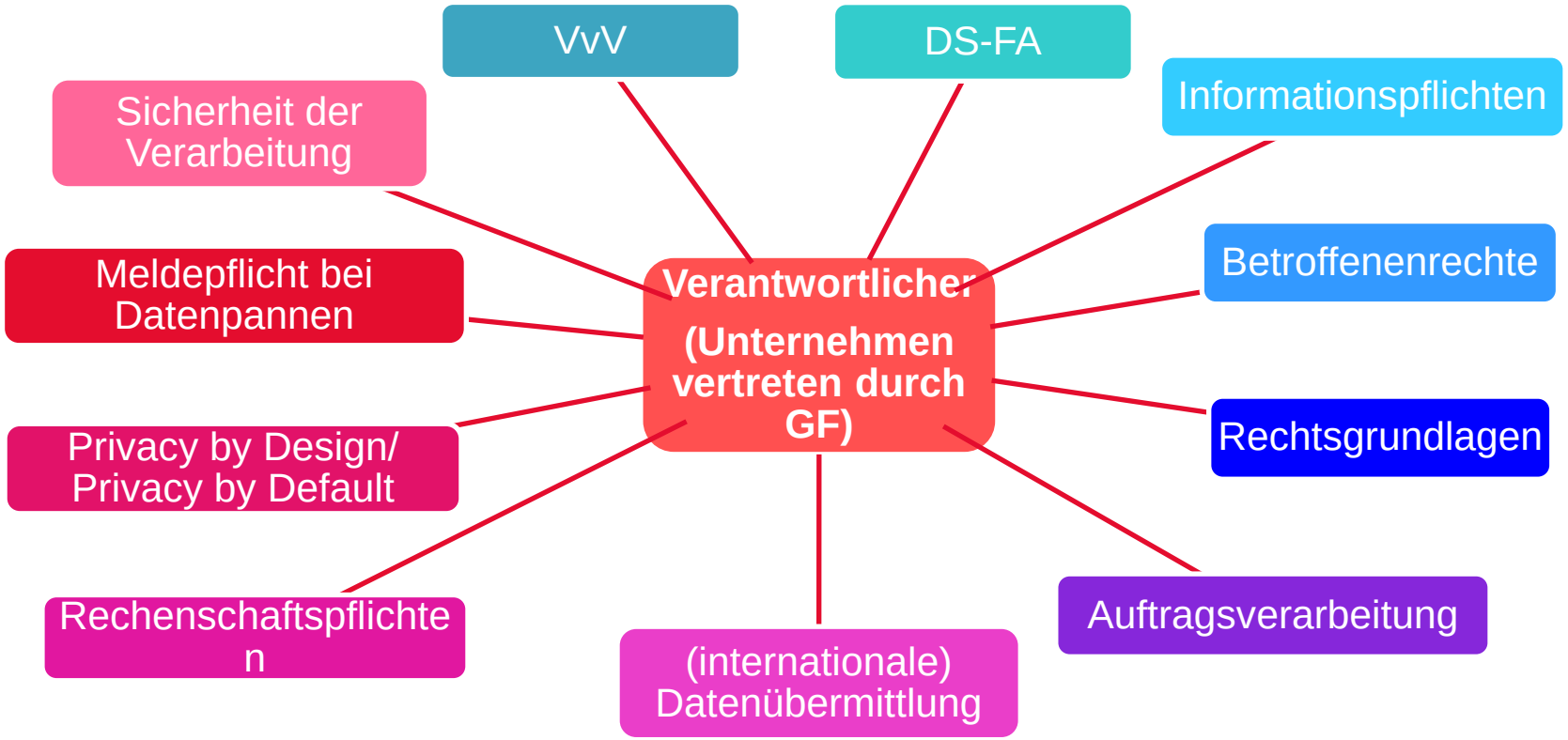
- Privacy by Design/ Privacy by Default

  → Datenschutz durch Technikgestaltung/ datenschutzfreundliche Voreinstellungen (z.B. durch Pseudonymisierung oder Anonymisierung)

- Beschäftigtendatenschutz beachten, z.B. bei Einwilligungen, Übermittlung von pbD etc.

- Überarbeitung der Datenschutzerklärung auf der Website

Aufgabenfelder: Verantwortlicher



Vorteil:
Wettbewerbsfähigkeit

3 wichtigste Fragen der DS-GVO

1. Welche personenbezogenen Daten werden verarbeitet?

2. Wo werden diese verarbeitet?

3. Wie werden diese verarbeitet?

Datenschutzerklärung, Verzeichnis von Verarbeitungstätigkeiten (samt Risikobewertung), Übermittlung pbD (Auftragsverarbeitung)

Empfehlenswerte Informationen zur DS-GVO

- IHK München und Oberbayern: www.ihk-muenchen.de/datenschutz oder www.ihk-muenchen.de/datenschutz-kmu
- Broschüre "Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine - Das Sofortmaßnahmen-Paket“ (Hrsg. Bayerische Landesamt für Datenschutzaufsicht, C. H. Beck Verlag, Kosten: 5,50€)
- BayLDA Homepage: https://www.lda.bayern.de/de/datenschutz_eu.html
- Datenschutzaufsicht in Niedersachsen Checkliste zur Anpassung an die DS-GVO: https://www.lfd.niedersachsen.de/startseite/dsgvo/fragen_zur_vorbereitung_auf_dsgvo/nur-noch-6-monate-bis-zur-anwendung-der-datenschutz-grundverordnung-159273.html
- Praxishilfen GDD: https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo
- Bitkom: https://www.bitkom.org/Themen/Datenschutz-Sicherheit/DSGVO.html

FRAGEN?

Datenschutz – IHK-Ansprechpartner

Rita Bottler

Datenschutzbeauftragte der IHK für München und Oberbayern und des BIHK e.V.

rita.bottler@muenchen.ihk.de, 089-5116-1683
dsb_bihk_ev@muenchen.ihk.de

Julia Franz

Referentin für Datenschutzrecht

franzj@muenchen.ihk.de, 089-5116-2065