3. Risikobasierter Ansatz nach der DS-GVO

Risiko (vgl. Erwägungsgründe 75-77)

Worst-Case-Szenarien

Beispiele:

Was könnte passieren, wenn die Liste der Beschäftigten missbräuchlich veröffentlicht würde?

Wie könnten die in der Mieterverwaltung gespeicherten Daten missbraucht werden?

Kategorie	Schadenspotenzial	Eintrittsplausibilität
Sehr hoch	Existenzbedrohend: Der Fortbestand der verantwortlichen Stelle ist gefährdet.	Ein plausbiles Szenario für einen Schadenseintritt ist beschreibbar.
Hoch	Schwerwiegende Auswirkungen sind zu erwarten.	Ein Eintritt ist prinzipiell denkbar, aber unwahrscheinlich.
Mittel	Spürbare, aber (insb. finanziell) tragbare Auswirkungen.	Eintritt nur durch Verkettung unglücklicher Umstände denkbar.
Niedrig	Vernachlässigbare Auswirkungen	Kein Eintrittsszenario erkennbar.

BSI (IT-Grundschutzkatalog)

- Normal

  Die Schadensauswirkungen sind begrenzt und überschaubar.

  Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.

- Hoch

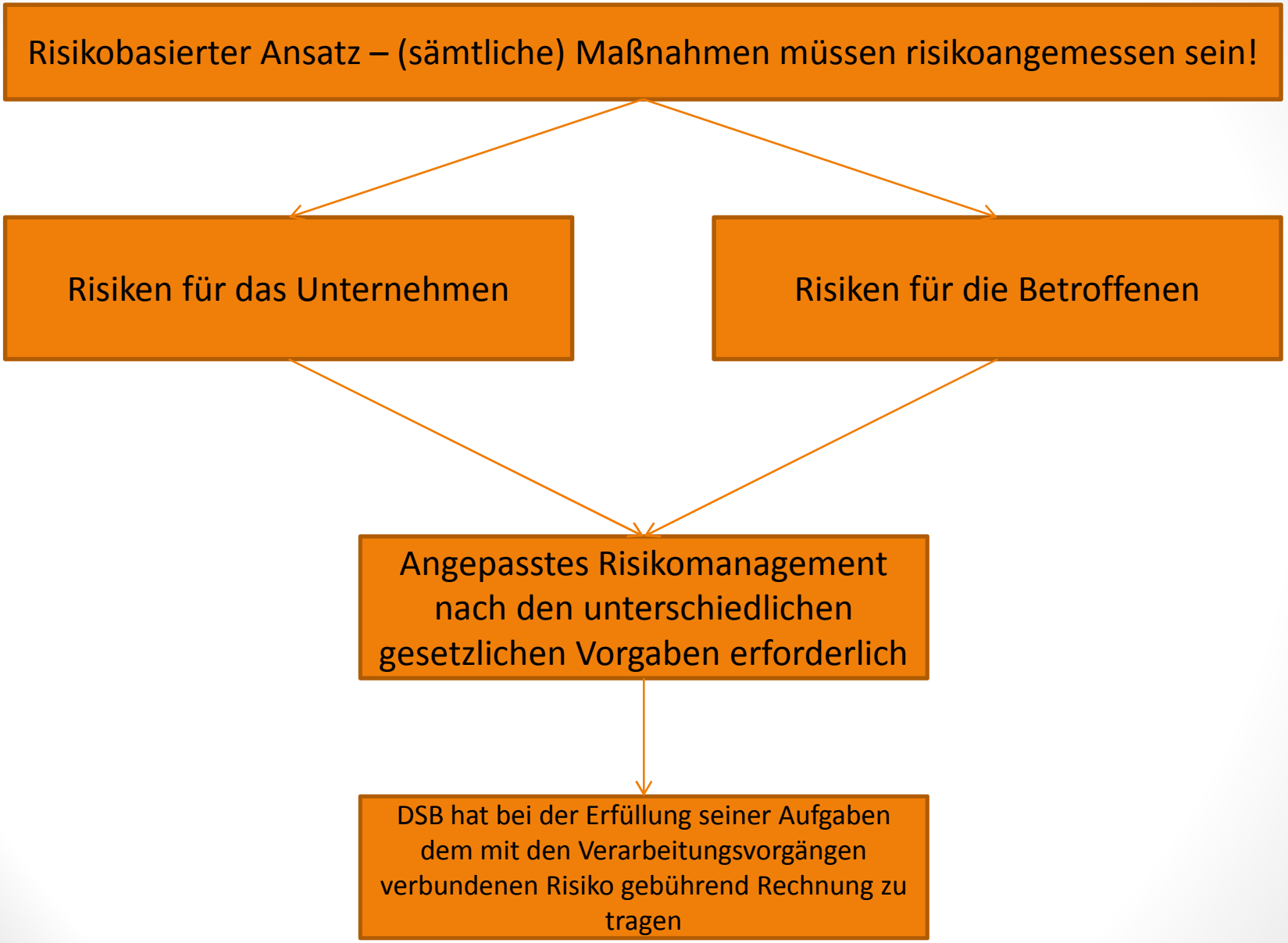
  Die Schadensauswirkungen können beträchtlich sein.

  Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen **erheblich** beeinträchtigt werden kann

- Sehr hoch

  Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen. Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine **Gefahr für Leib und Leben oder die persönliche Freiheit** des Betroffenen gegeben ist.

Risikobasierter Ansatz nach der DS-GVO



4. Das Verzeichnis der Verarbeitungstätigkeiten (VVT)

Bisher: Verfahrensverzeichnis bzw. Verarbeitungsübersicht (§§ 4e, g BDSG)

„Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis **aller Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen." (Art. 30 Abs. 1 DSGVO)

- Neu: keine Begrenzung mehr auf automatisierte Verarbeitungsvorgänge
- Neu: keine Veröffentlichung oder Einsichtnahme mehr erforderlich
- Neu: Führung durch den Verantwortlichen
- Neu: auch durch Auftragsverarbeiter zu erstellen und zu führen

Beispiele für Verfahren

- Kunden-, Personal- oder Lieferantenverwaltung
- Zeiterfassung
- Zugangskontrollsystem
- Videoüberwachung
- E-Mail-System/Outlook
- Telefondatenerfassung
- Reisekostenabrechnung
- Elektronische Bewerberdatenbank
- Online-Shop

...

Ausnahmen

Für Stellen mit weniger als 250 Mitarbeitern, es sei denn:

1. es besteht ein **Risiko** für Rechte und Freiheiten der betroffenen Personen (z.B. Scoring)
2. oder: die Verarbeitung erfolgt **nicht nur gelegentlich**
3. oder: die Verarbeitung betrifft **besondere Datenkategorien** gemäß Art. 9 Abs. 1 DS-GVO oder Daten über strafrechtliche Verurteilungen und Straftaten

Zweck

- Werkzeug des DSB zur Aufgabenerfüllung in Form der Gesetzmäßigkeit der Überwachung
- Interne Übersicht über die Datenverarbeitungen
  - Prüfung und Sicherstellung der Erfüllung datenschutzrechtlicher Anforderungen
  - Übersicht über aktuelle Datenverarbeitungsvorgänge für den betrieblichen Datenschutzbeauftragten
    - → bessere Beratung
  - Effektive Information und Beauskunftung der Betroffenen
- Gegenüber Aufsichtsbehörden: Nachweis der Einhaltung der Verordnung (EG 82)
  - Aufsichtsbehörde kann die Vorlage des Verzeichnisses zur Durchführung Ihrer Kontrolle verlangen
  - **Effektives Mittel zur Sicherstellung der Rechenschaftspflicht**

Inhalt gemäß Art. 30 Abs. 1 DS-GVO

(1) **Name** und Kontaktdaten
   a. des Verantwortlichen
   b. ggf. des gemeinsam mit ihm Verantwortlichen
   c. ggf. des Vertreters in der EU
   d. ggf. des betrieblichen Datenschutzbeauftragten

(2) **Zwecke der Verarbeitung** (ggf. Beschreibung)

(3) Kategorien **betroffener Personen**

(4) Kategorien personenbezogener **Daten**

(5) Kategorien von **Empfängern** (ggf. auch zukünftige)

(6) Ggf. Übermittlungen an ein **Drittland** oder eine internationale Organisation

(7) (Wenn möglich) **Fristen für die Löschung** der verschiedenen Datenkategorien

(8) (Wenn möglich) allgemeine Beschreibung der **technisch und organisatorischen Maßnahmen** (Art. 32 Abs. 1 DS-GVO)

Aufbau

Empfehlung 3-stufiger Aufbau

(1) Angaben zum Verantwortlichen

(2) Allgemeingültige Angaben

(Angaben, die für die überwiegenden Verarbeitungen zutreffend sind), bspw. zuständige Aufsichtsbehörde, allg. Beschreibung der technischen und organisatorischen Maßnahmen

(3) Angaben zu den einzelnen Verfahren (Einzelangaben nach Art. 30 DS-GVO)

- Zwecke
- Betroffene
- Daten
- Empfänger
- Löschfristen
- Spezielle technische und organisatorische Maßnahmen

Neu: Auftragsverarbeiter müssen Verzeichnis bzgl. ihrer Dienstleistung führen

- **Zweck:** Übersicht, welche Leistungen für welchen Auftraggeber erbracht werden

- **Aufbau:** Orientierung an Standardleistungen (Produkten)
  - Ableitung von „Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden“

Inhalt, Art. 30 Abs. 2 DS-GVO

(1) **Name** und Kontaktdaten
   a. des Auftragsverarbeiters bzw. der Auftragsverarbeiter
   b. jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist
   c. ggf. des Vertreters des Verantwortlichen
   d. ggf. des Vertreters des Auftragsverarbeiters
   e. ggf. des betrieblichen Datenschutzbeauftragten des Auftragsverarbeiters

(2) Kategorien von **Verarbeitungen**, die im Auftrag jedes Verantwortlichen durchgeführt werden

(3) Ggf. Übermittlungen an ein **Drittland** oder eine internationale Organisation

(4) Vorgesehene **Fristen für die Löschung** der verschiedenen Datenkategorien

(5) (Wenn möglich) allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen** (Art. 32 Abs. 1 DS-GVO)

Aufbau

Empfehlung 3-stufiger Aufbau

(1) Angaben zum Auftragsverarbeiter
- Name und Anschrift
- Datenschutzbeauftragter

(2) Angaben zu Dienstleistungen
- a) Allg. Beschreibungen der techn. und org. Maßnahmen
- b) Datenweitergabe in Drittland
- c) Kategorien der Dienstleistungen

(3) Angaben zu den Kunden
- a) Verantwortlicher und sein Vertreter
- b) Gebuchte Dienstleistungen

5. Die Datenschutz-Folgenabschätzung (DSFA)

„Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.“ (Art. 35 DS-GVO)

- Bisher Vorabkontrolle und allgemeine Meldepflicht – jetzt: erhöhte Anforderungen, vorher und im weiteren Verlauf Wiederholung (ca. aller 3 Jahre) - auch für Altverfahren
- Frühzeitige Einbeziehung des betrieblichen Datenschutzbeauftragten
- Aufsichtsbehörde veröffentlicht Listen zur Orientierung, wann eine Folgenabschätzung durchzuführen ist
- Insoweit keine Folgenabschätzung vorgenommen wird, ist die Begründung ggf. für eine nachträgliche Prüfung zu dokumentieren
- Ggf. vorherige Konsultation der Aufsichtsbehörde, wenn Risiken nicht ausreichend eingedämmt werden können
- Vgl. Erwägungsgründe 84, 89 - 93

Im Zweifel: Folgenabschätzung durchführen!

Einschlägige Erwägungsgründe:

- 84, 89 bis 93 und 95

- Datenschutz-Folgenabschätzung soll die nach Einschätzung der EU nicht gelungene Vorabkontrolle und Meldepflicht ablösen (zwingender Wegfall entsprechender nationaler Bestimmungen)

- Bußgeld: Artikel 83 Abs. 4 lit. a DS-GVO; bis zu EUR 10 Mio. oder bei Unternehmen bis zu 2 % des Weltjahresumsatzes

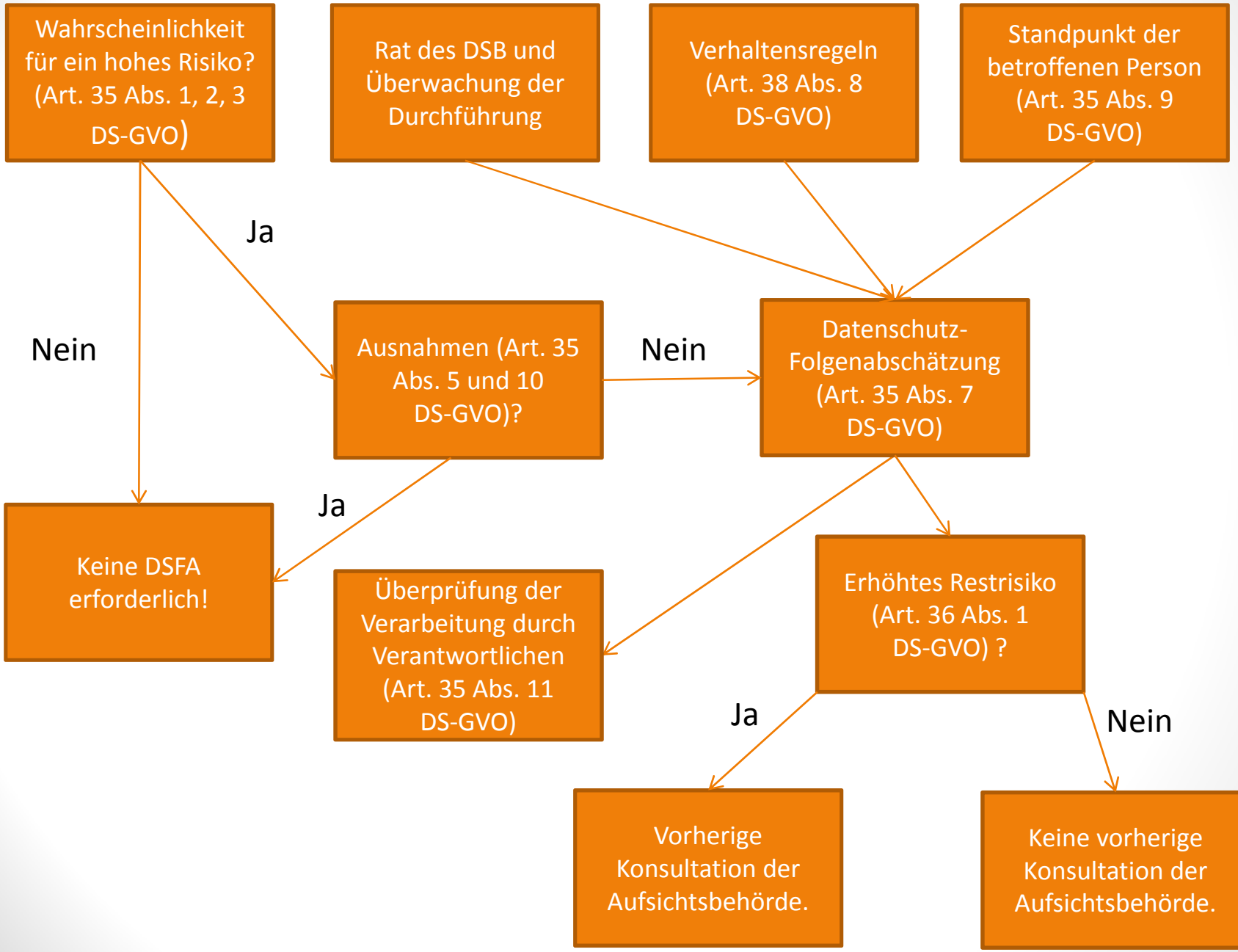
Erforderlichkeit einer Datenschutz-Folgenabschätzung

Planung der Einführung neuer Verfahren

- **Grundsatz:**
  Datenschutz-Folgenabschätzung 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 und 10 DS-GVO
  - Weiträumige 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
- **Keine Ausnahmen**

Die Grundprinzipien

Die Datenschutz-Folgenabschätzung (DSFA)



Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein ULD):

10 Schritte für die Umsetzung

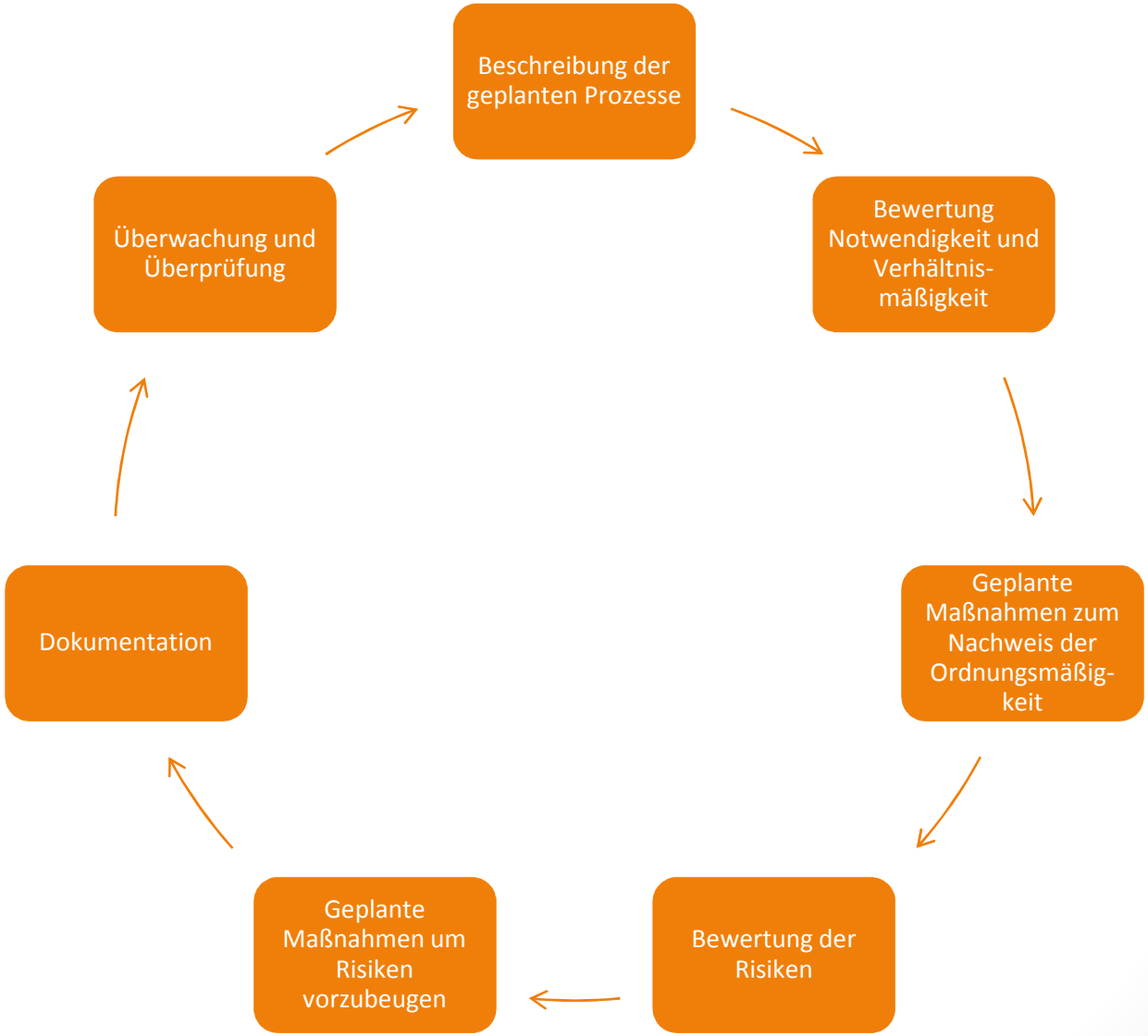
1. In Betracht kommende Verfahren erfassen
2. Erforderliche Kenntnisse bzw. Personen ermitteln
3. Gegenstand der Betrachtung festlegen / abgrenzen
4. Schutzziele beachten (Grundsätze Artikel 5)
5. Objekte der Datenverarbeitung bestimmen
6. Schutzstufen definieren und festlegen
7. Gefährdungen identifizieren
8. Risiko bewerten
9. Maßnahmen festlegen und umsetzen
10. Bericht für die Verantwortlichen erstellen

Regelbeispiele nach WP 248 der Art. 29-Gruppe

1. Bewertung (Profiling) oder Scoring
2. Automatisierte Entscheidungsfindung mit rechtlicher oder ähnlicher erheblicher Wirkung
3. Systematische Überwachung
4. Sensible Daten oder höchstpersönliche Daten (Art. 9 und 10 DS-GVO)
5. Datenverarbeitung in großem Umfang
6. Datensätze werden abgeglichen oder kombiniert
7. Daten über „schutzbedürftige“ Personen (EG 75)
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
9. Die Verarbeitung an sich „verhindert, dass die betroffenen Personen ein Recht ausüben oder eine Dienstleistung oder einen Vertrag ausüben“ (vgl. Art. 22 DS-GVO und EG 91)

Liegen ein oder mehrere Regelbeispiele vor, ist regelmäßig von einer DSFA auszugehen.

Durchführung der Datenschutz-Folgenabschätzung



(Mindest-) Inhalte einer Folgenabschätzung

(1) Systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Verarbeitungszwecke (ggf. einschließlich berechtigter Interessen)

(2) Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck

(3) Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Person („Risikoanalyse/-bewertung“)

(4) Geplante Maßnahmen zur Bewältigung der Risiken (einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren unter Beachtung der Rechenschaftspflicht und Berücksichtigung der Betroffenenrechte)

Die Durchführung einer Datenschutz-Folgenabschätzung ist Aufgabe des Verantwortlichen, nicht des Datenschutzbeauftragten!

Der Verantwortliche sollte den Rat des DSB zu folgenden Fragen einholen:

- Ob eine DSFA durchzuführen ist?
- Mit welcher Methodik soll bei der Durchführung einer DSFA vorgegangen werden?
- Soll eine DSFA intern durchgeführt werden oder extern vergeben werden?
- Welche Garantien sind anzuwenden, um das Risiko für die Rechte der betroffenen Person zu mindern?
- Ist die DSFA ordnungsgemäß durchgeführt worden? Ist die Durchführung im Einklang mit der DS-GVO erfolgt?

Es finden sich zu allen Dingen Grundsätze, allein dabei muss es nicht verbleiben, sondern man muss sich bemühen, über diese Sache selbst zu denken, auch sie fleißig üben, um in diesen Grundsätzen geschickt und geläufig zu werden.

Friedrich II., „der Große“

Agenda 14.06.2018

V. Das Datenschutz-Management nach der DS-GVO
   1. Das Prinzip der Accountability
   2. Die Rolle des Datenschutzbeauftragten nach der DS-GVO
   3. Entwicklung und wesentliche Elemente eines Datenschutz-Managementsystems
   4. Verfahrensgestaltung (data protection by design and by default)
   5. Sicherstellung von Betroffenenrechten

1. Das Prinzip der Accountability

„Beweislastumkehr“

Art. 5 DS-GVO

Grundsätze des Absatz 1

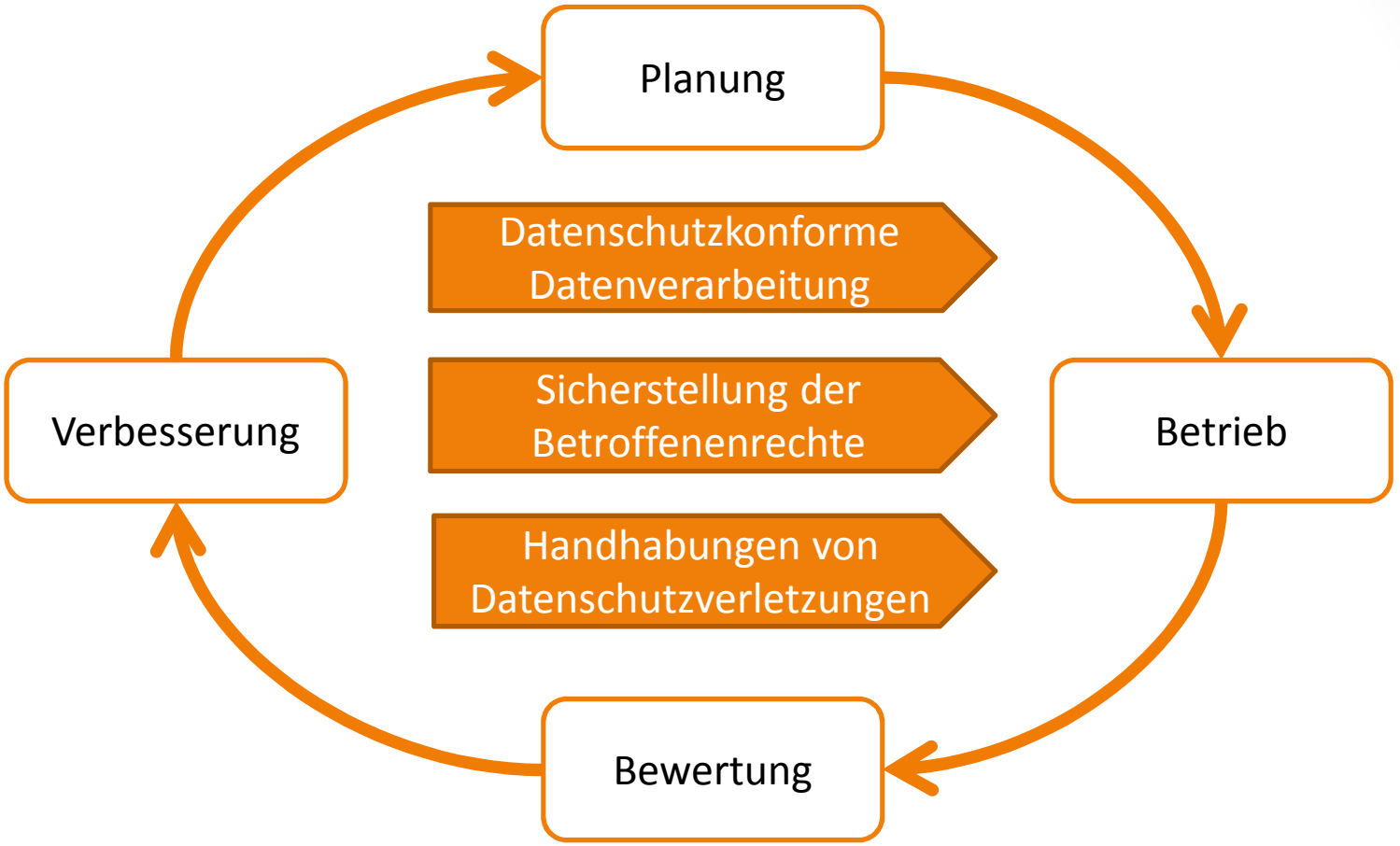
- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

„Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung **nachweisen können** („Rechenschaftspflicht“).“ (Abs. 2)

Art. 24 DS-GVO

„Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maß-nahmen um, um sicherzustellen und **den Nachweis dafür erbringen zu können**, dass die Verarbeitung gemäß dieser Verordnung erfolgt.“ (Abs. 1 Satz 1)

Das Prinzip der Accountability



„Allgemein gesagt drückt er [der Begriff „Accountability“] … aus, **wie Verantwortung überprüfbar wahrgenommen wird**. Verantwortung und Rechenschaftspflicht sind zwei Seiten einer Medallie und wesentliche Bestandteile der GOOD Governance.“

Artikel-29-Gruppe, WP 173

*PDCA-Modell

Exkurs: Verpflichtung auf das Datengeheimnis

Rechtslage bisher: § 5 BDSG (alt)

- Den bei der Datenverarbeitung beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, verarbeiten oder zu nutzen (Datengeheimnis).
- Die Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten

Neu:

- Vergleichbar klare und eindeutige **Regelung in DS-GVO nicht enthalten**
- Im Rahmen Dokumentations- und Nachweispflicht gem. Art. 5 Abs. 2 DS-GVO ist Verpflichtung probates Mittel, um Einhaltung datenschutzrechtlicher Vorschriften zu gewährleisten
- Verpflichtung auf Vertraulichkeit zumindest beim Dienstleister ausdrücklich geregelt, vgl. Art. 28 Abs. 3 lit. b DS-GVO
- Denkbar **Verpflichtung auf die Vertraulichkeit (Art. 5 Abs. 1 lit. f DS-GVO)** und damit auf
  - Angemessene Sicherheit personenbezogener Daten
  - Schutz vor unbefugter oder unrechtmäßiger Verarbeitung
  - Schutz vor unbeabsichtigten Verlust
  - Schutz vor unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung

2. Die Rolle des Datenschutzbeauftragten nach der DS-GVO

DS-GVO
- Art. 37 – 39
- Bestellpflicht
- Stellung
- Aufgaben

BDSG
- §§ 5 – 7 für den öffentlichen Bereich
- § 38 für nicht-öffentliche Stellen

Art. 29-Gruppe, WP 243
- Bestellung
- Stellung
- Aufgaben

Anforderungen an den Datenschutzbeauftragten

Benennung
(aus Nachweisgründen Textform)

Kein Interessenskonflikt
(z.B. Geschäftsführer, IT-Abt. bzw. andere Person, die aufgrund ihrer Aufgaben im Unternehmen die Zwecke der Datenverarbeitung beeinflussen kann)

Zuverlässigkeit und Erreichbarkeit

Veröffentlichung der Kontaktdaten und Mitteilung an Aufsichtsbehörde

Fachwissen und laufende Fortbildung

Bestellpflichten Datenschutzbeauftragter

- Regelungen in § 38 BDSG (neu) und Art. 37 DS-GVO
- Verpflichtende Bestellung für Öffentliche Stellen
- Freiwillige Bestellung nach Art. 37 DS-GVO

Hinweis:
Alle datenschutzrechtlichen Regelungen sind auch dann einzuhalten, wenn kein DSB bestellt werden muss!

- Kleinunternehmen mit weniger als 10 Angestellten sollten prüfen, ob sie in die Kategorien des Art. 37 Abs. 1 DS-GVO fallen

- ✓ Hauptaktivität des Unternehmens ist dem Umfang oder seinem Zweck nach die massenhafte, regelmäßige und systematische Beobachtung von Betroffenen
- ✓ Kerngeschäft besteht in der massenhaften Verarbeitung sensibler Daten

Art. 37 DS-GVO
„… falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie [der Verantwortliche oder der Auftragsverarbeiter] einen solchen [Datenschutzbeauftragten] benennen."

§ 38 BDSG (neu)
(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

- Verantwortliche und Auftragsverarbeiter sollten die interne Prüfung dokumentieren, ob eine Bestellpflicht eines Datenschutzbeauftragten besteht
- Wird ein DSB freiwillig bestellt gelten gleichwohl die Anforderungen der Art. 37 – 39 DS-GVO
- Bei der Bestellung – freiwillig und obligatorisch - kann eine interne oder eine externe Lösung gewählt werden
- Die Benennung des DSB erfolgt durch den Verantwortlichen
- Die Kontaktdaten werden veröffentlicht und an die Aufsichtsbehörde gemeldet
- Name und Kontaktdaten des DSB sind in das Verzeichnis der Verarbeitungstätigkeiten aufzunehmen (VVT)

Wichtig: Kontaktdaten müssen nicht den Namen des DSB beinhalten, es genügt eine postalische Anschrift oder eine speziell eingerichtete Telefonnummer bzw. E-Mail-Adresse

Interessenkonflikt

Art. 38 DS-GVO

…

(6) Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

- Keine Interessenkonflikte sind Voraussetzung für **unabhängige Aufgabenerfüllung**
- „Der Datenschutzbeauftragte darf keine Position innerhalb der Organisation innehaben, die ihn dazu veranlasst, die Zwecke und Mittel der Datenverarbeitung festzulegen“

  Art. 29-Gruppe, WP 243
- Beispiele für Interessenkonflikt: Geschäftsführung, IT-Administrator

Aufgaben des Datenschutzbeauftragten

- **Der DSB dient der Beratung und Überwachung im Unternehmen**
- Beratung und Unterrichtung hinsichtlich Daten-schutzpflichten für Geschäftsführung, Mitarbeiter und Auftragsverarbeiter - Ansprechpartner
- Beratung Betroffener bzgl. datenschutzrechtlicher Fragen
- Beratung bei der Datenschutz-Folgenabschätzung
- Wirkt auf die Einhaltung des Datenschutzrechts hin
- Zusammenarbeit mit und Ansprechpartner für Aufsichtsbehörde

Beratungsauftrag des DSB

Beratung der Geschäftsführung

- Etablierung eines Datenschutz-Managements
- Direkte Unterstellung
- Intensive Kommunikation zw. DSB und Geschäftsführung
- Beratung hinsichtlich der Pflichten nach der DS-GVO
- Einhaltung und Umsetzung des Datenschutzes
- **Schwerpunkt: Beratung in Fragen der Strategie**

Beratung der Beschäftigten

- Sensibilisierung der MA
- Prozesse für Rechte der Betroffenen
- Dokumentation, Nachweise und Meldepflichten
- Beratung hinsichtlich der Pflichten nach der DS-GVO
- Einhaltung und Umsetzung des Datenschutzes
- **Schwerpunkt: Beratung in operativen Fragen**

Beratung von Betroffenen

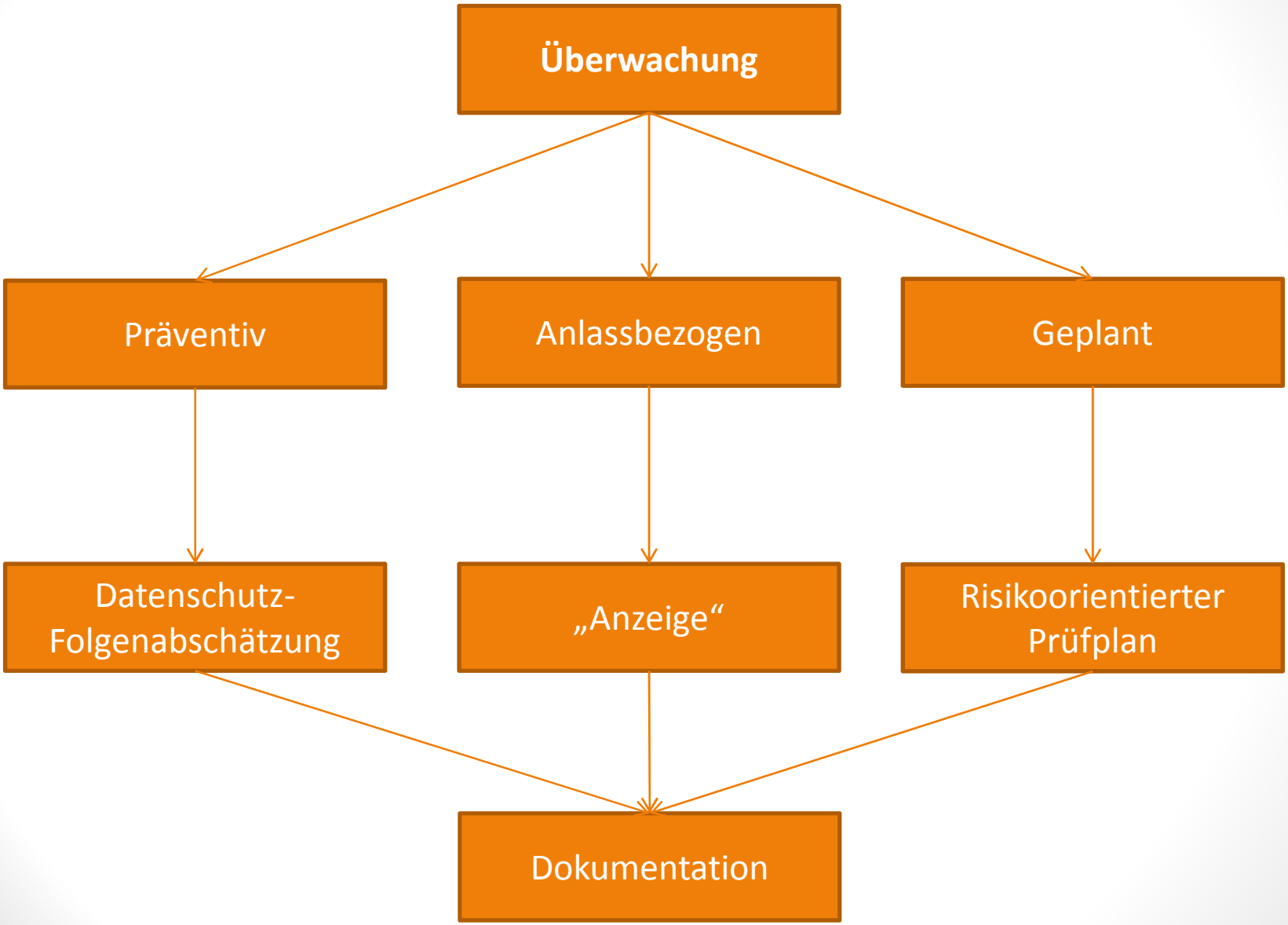
„Betroffene Personen können den Datenschutzbeauftragten **zu allen mit der Verarbeitung ihrer personenbezogenen Daten** und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung **im Zusammenhang stehenden Fragen zu Rate ziehen**."
(Art. 38 Abs. 4 DS-GVO)

Überwachungsauftrag des DSB

- Die Überwachung bedeutet nicht, dass der DSB im Falle eines Verstoßes verantwortlich ist
- Ebenso Verantwortliche und nicht der DSB für die technisch-organisatorischen Maßnahmen und den Nachweis der Rechtmäßigkeit verpflichtet

Einhaltung des Datenschutzes liegt in der Verantwortung des Unternehmens und nicht des DSB!

- Die Überwachung beinhaltet:
  - Etablierung eines Datenschutzmanagements
  - Umsetzung der Prozessgestaltung, der Datenschutzfolgenabschätzung, Prozesse zur Sicherstellung von Betroffenenrechten, Meldepflichten usw.
  - Unterstützung der technischen Umsetzung von Datenschutzvorgaben
- Als Teil der Überwachung darf der DSB insbesondere:
  - Informationen sammeln, um Verarbeitungsaktivitäten zu identifizieren
  - Gesetzmäßigkeit von Verarbeitungsvorgängen analysieren
  - Verantwortlichen/Auftragsverarbeiter informieren und Empfehlungen aussprechen

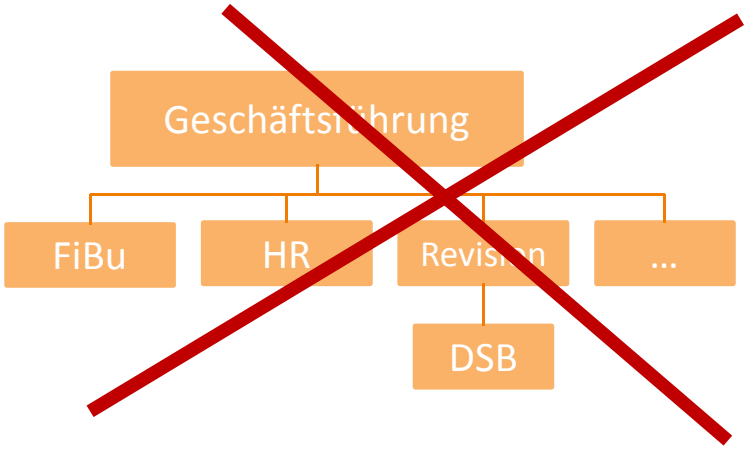

Überwachung
Präventiv
Anlassbezogen
Geplant
Datenschutz-Folgenabschätzung
„Anzeige“
Risikoorientierter Prüfplan
Dokumentation

Stellung des Datenschutzbeauftragten

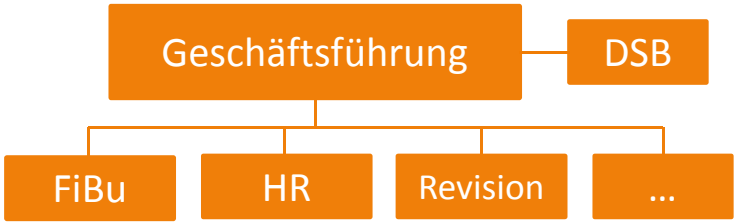
- Fachkunde und Zuverlässigkeit
  - Berufliche Qualifikation, insb. Fachwissen im Bereich Datenschutzrecht und –praxis
  - Fähigkeit zur Erfüllung Aufgaben aus Art. 39 DS-GVO
- Untersteht direkt der Geschäftsführung
- Arbeitet (doppelt) weisungsfrei (Art. 39 DS-GVO)
- Beratende Einbindung bei der Datenschutz-Folgenabschätzung
- Frühzeitige Konsultation bei datenschutzrechtlichen Fragen
- Abberufungsschutz und Benachteiligungsverbot
- Kündigungsschutz (§ 38 Abs. 2 i.V.m. § 6 Abs. 4 BDSG [neu])
- Unterliegt der Verschwiegenheitspflicht nach nationalem Recht (§ 38 Abs. 2 i.V.m. § 6 Abs. 5 S. 2 und Abs. 6 BDSG [neu], § 203 Abs. 2a StGB)
- Mittel zur Selbstkontrolle
- Kontaktstelle zur Zusammenarbeit mit der Aufsichtsbehörde

Organisatorische Einbindung des DSB

FALSCH



RICHTIG



Bereitstellung von Ressourcen

DSB sind effektiv und mit ausreichend Ressourcen für die auszuführenden Verarbeitungen auszustatten:

- Aktive Unterstützung durch das obere Management (bspw. relevante Informationen zeitnah zur Verfügung stellen)
- Regelmäßige Treffen
- Ausreichend Zeitbudget des DSB zur Aufgabenerfüllung
- Angemessene Unterstützung mit Ressourcen (finanzielle Mittel, Räumlichkeiten, Einrichtungen, Ausstattung, Personal)
- Kommunikation der Bestellung an die Beschäftigten
- Sicherstellung der notwendigen Zugänge
- Regelmäßige Fortbildung
- Ggf. Einrichtung eines DSB-Teams

„Konzerndatenschutzbeauftragter“

- Bestellung eines DSB für juristische Person, d.h. einzelnes Konzernmitglied (Art. 37 Abs. 2 DS-GVO)
- Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.
- Innerhalb von Behörden oder öffentlichen Stellen kann für mehrere Behörden bzw. Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden
- Stellung als Beschäftigter oder Abschluss Dienstleistungsvertrag
- Bei einem Dienstleistungsvertrag:
  - Klare Zuweisung von Aufgaben
  - Jedes Mitglied muss Umsetzung und Schutz der DS-GVO betreiben
  - Jedes Mitglied muss die Anforderungen durch DS-GVO erfüllen

Grundsatz: Ein Unternehmen (Legal-Einheit) ein Datenschutzbeauftragter

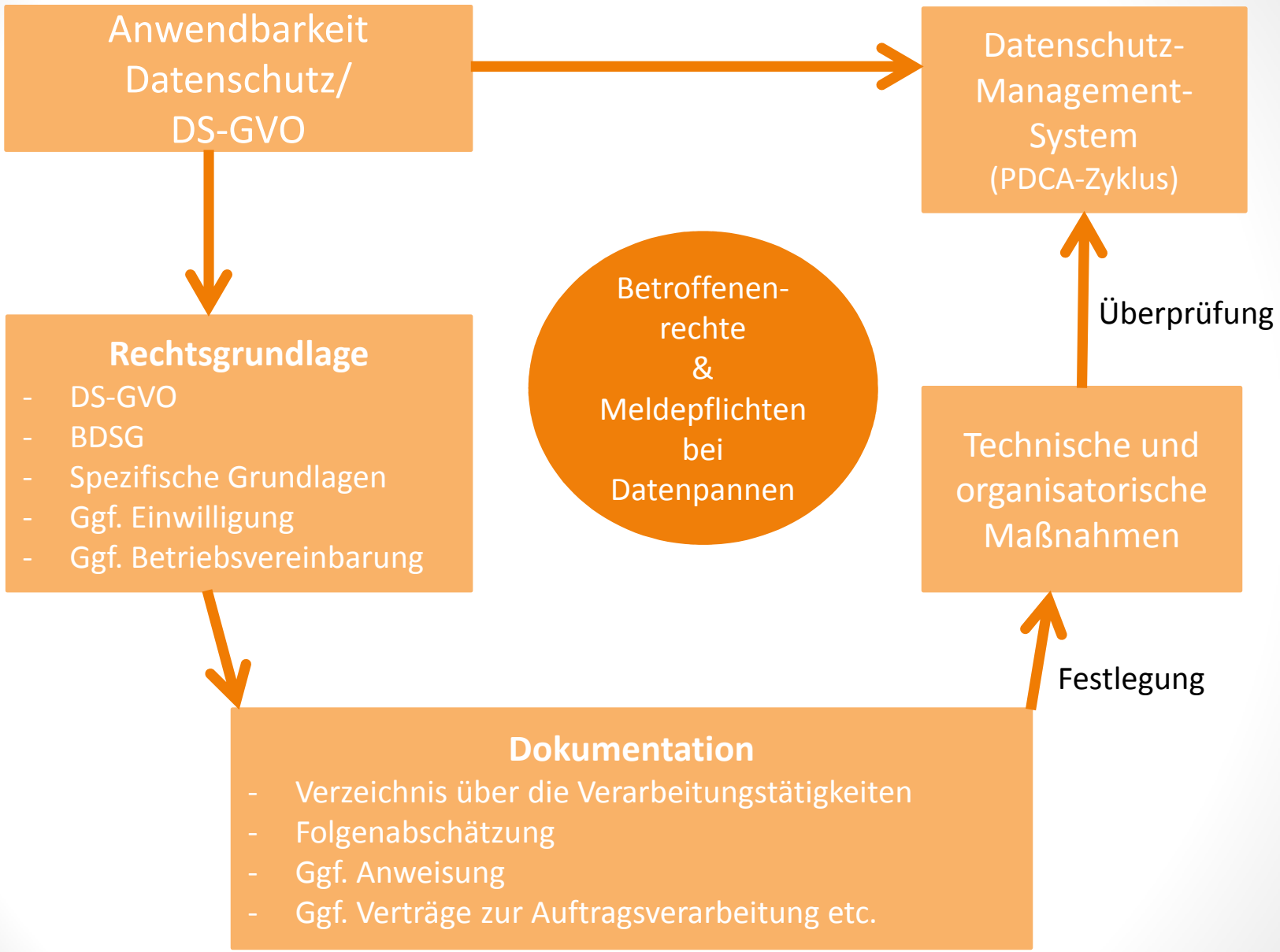
3. Entwicklung und wesentliche Elemente eines Datenschutz-Managementsystems

1. **Die DS-GVO erfordert ein Managementsystem**
   - Definition komplexer Handlungsanforderungen
   - Überbrückung von Organisationsgrenzen
   - Nachweisfähigkeit zur Erfüllung gesetzlicher Anforderungen
   - Rechtmäßige Verarbeitung personenbezogener Daten als Ziel

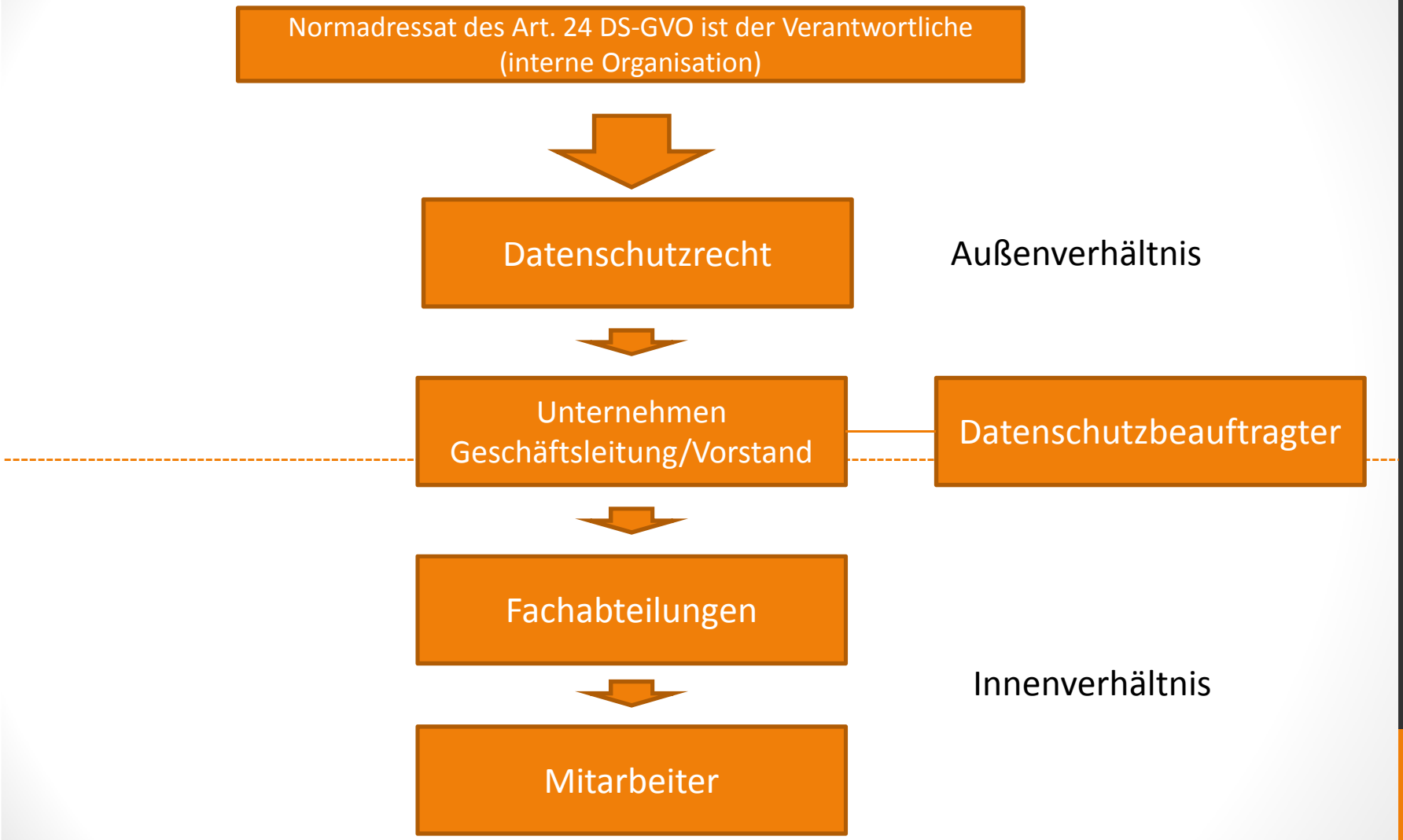
2. **Zur Umsetzung bedient sich die DS-GVO etablierter Systeme**
   - Verwendung etablierter Instrumente
   - Orientierung am „Stand der Technik“
   - Kontinuierlicher Verbesserungsprozess

3. **Die DS-GVO definiert die Verantwortung im PDCA-Zyklus**
   - Organisationsverantwortung gemäß Art. 24 DS-GVO

Entwicklung und wesentliche Elemente eines Datenschutz-Managementsystems



Klärung von Verantwortlichkeiten



Entwicklung und wesentliche Elemente eines Datenschutz-Managementsystems

Unternehmen

(durch Führungskräfte)

Mitarbeiter

(inkl. Aushilfen, Auszubildende und Praktikanten)

- Einhaltung der gesetzlichen und internen Regelungen

Schaffung der Voraussetzungen für einen ausreichenden Schutz von personenbezogenen Daten

Unternehmen trägt als „verantwortliche Stelle“ die Gesamtverantwortung.

Information an Führungskraft und/oder den betrieblichen Datenschutzbeauftragten bei Kenntnis von Missbrauch, Verlust oder Manipulation

Entwicklung und wesentliche Elemente eines Datenschutz-Managementsystems

- Einführung eines Datenschutz-Managementsystems, insbesondere zur Gewährleistung der Accountability (Art. 24 DS-GVO)
  - Risikobasierter Ansatz
  - Überprüfung
  - Nachweis durch Zertifizierung

- Operative Datenverarbeitung:
  - Weitreichende Dokumentations- und Nachweispflichten für alle Verarbeitungsvorgänge (Verzeichnis der Verarbeitungstätigkeiten)
  - IT-Sicherheit nach dem Stand der Technik
  - Einsatz „datenschutzfreundlicher“ Technologien
  - Implementierung und Durchführung einer Datenschutz-Folgenabschätzung
  - Konsultationspflicht der Aufsichtsbehörde

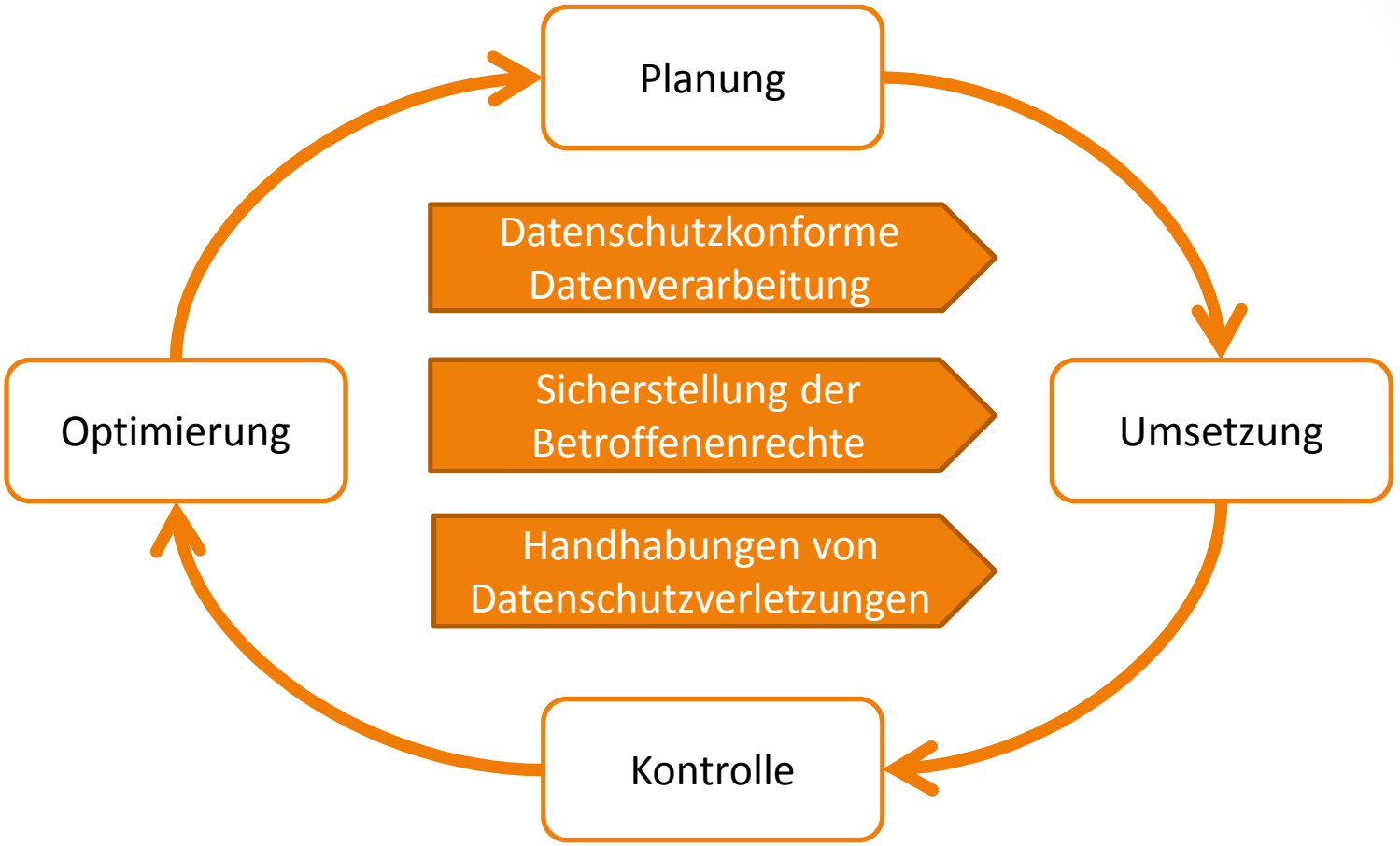
Konsequenzen

Unternehmen müssen in der Lage sein:

- jederzeit detailliert Auskunft (vgl. Informationspflichten) über die bei Ihnen laufenden Datenverarbeitungsvorgänge zu geben und ggf. die Einhaltung datenschutzrechtlicher Anforderungen nachweisen zu können
- auf Anfrage personenbezogene Daten, die der Betroffene selbst bereitgestellt hat, in einem gängigen elektronischen Format dem Betroffenen bereitzustellen
- eine unverzügliche Meldung und Dokumentation aller Datenschutzverstöße zu gewährleisten (Mindest-anforderungen Art. 33 Abs. 3 DS-GVO)

Klar geregelte Prozesse erforderlich!

Entwicklung und wesentliche Elemente eines Datenschutz-Managementsystems



*PDCA-Modell

Datenschutz-Organisation

1. **Planung**
   - Thematik erkennen und herausarbeiten
   - Probleme abgrenzen
   - Ursachen identifizieren
   - Ziele festlegen
   - Umsetzung planen

2. **Umsetzung**
   - Koordinierung der Umsetzung
   - Dokumentation der Ergebnisse

3. **Kontrolle**
   - Auswertung der Ergebnisse

4. **Optimierung**
   - Verbesserungen analysieren und initiieren

Umsetzung und Implementierung des Managementsystems

Bestandsaufnahme

- Aktuelle Prozesse (z.B. anhand bestehender Dokumentationen)
- Bestimmung und Dokumentation der Rechtsgrundlagen
- (schriftliche) Festlegung von Abläufen und Zuständigkeiten
  - ✓ Planung und Umsetzung der Datenverarbeitung
  - ✓ Einhaltung datenschutzrechtlicher Anforderungen
  - ✓ Erstellung datenschutzrechtlicher Dokumentationen
  - ✓ Prüfung bzw. Erstellung von Betriebsvereinbarungen
  - ✓ Umsetzung der Betroffenenrechte
  - ✓ Reaktionsmechanismus bei Datenpannen
- Dienstleistungsbeziehungen (Vertragsprüfung)

Regelmäßige Schulung/Sensibilisierung der Mitarbeiter

- Z.B. durch DSB oder externen Dienstleister
- Empfehlung: in sensiblen Bereichen alle 2 Jahre, ansonsten mindestens alle 5 Jahre

  Problem: Einstellungen während des Zyklus bzw. häufige Fluktuation
- Hinweise und interne Anordnungen ggf. als Reaktion auf Entwicklungen, Verstöße von Mitarbeitern o.ä.
- Sensibilisierung im Umgang mit Betroffenen und Aufsichtsbehörde!

Auditierung/Zertifizierung

Vertrauen ist gut - Kontrolle ist besser!

- Förderung durch EU - Ziel: Rechtssicherheit und damit Stärkung des Marktes
- Freiwillig und transparent (Kriterien, Notifikation, Registrierung)
- EU-Kommission legt Standards fest, ggf. Datenschutzsiegel
- Zertifizierung von Verarbeitungsvorgängen (nicht für gesamte verantwortliche Stelle bzw. IT-Produkt eines Herstellers)
- Kriterien der Zertifizierungsstelle benötigen Anerkennung der Aufsichtsbehörde (bei grenzüberschreitenden Zertifizierungs-verfahren des Ausschusses gemäß Art. 63 ff. DS-GVO)
  - Angemessene Berücksichtigung der besonderen Bedürfnisse kleinster, kleiner und mittelständischer Unternehmen

Exkurs: Datenschutz im Konzern

Definition Unternehmensgruppe

Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht

Erwägungsgrund 37

Eine Unternehmensgruppe sollte aus einem **herrschenden Unternehmen und den von diesem abhängigen Unternehmen** bestehen, wobei das herrschende Unternehmen dasjenige sein sollte, das zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen **beherrschenden Einfluss** auf die übrigen Unternehmen ausüben kann. **Ein Unternehmen, das die Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert**, sollte zusammen mit diesen als eine „Unternehmensgruppe“ betrachtet werden.

Auftragsdatenverarbeitung
- Vertrag
- DV nur auf Weisung
- Zwecke und Mittel bestimmt der Auftraggeber (Verantwortlicher)

Erforderlichkeit für **berechtigtes Interesse & Interessenabwägung**

Konzern-übermittlung

Einwilligung in Datenübermittlung

Vertrag mit <u>erforderlicher</u> Datenübermittlung

„Kleines Konzernprivileg“

Verantwortliche, die **Teil einer Unternehmensgruppe** oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind **können ein berechtigtes Interesse** haben, personenbezogene Daten innerhalb der Unternehmensgruppe **für interne Verwaltungszwecke**, einschließlich der Verarbeitung personenbezogener **Daten von Kunden und Beschäftigten**, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein **Unternehmen in einem Drittland bleiben unberührt**.

4. Verfahrensgestaltung

NEU: „data protection by design“ und „[…] by default“

Datenschutz durch Technik

Datenschutz und Datensicherheit müssen bereits in der Planung und Entwicklung von IT-Systemen berücksichtigt werden.

Grund: keine teuren, zeitintensiven Zusatzprogrammierungen

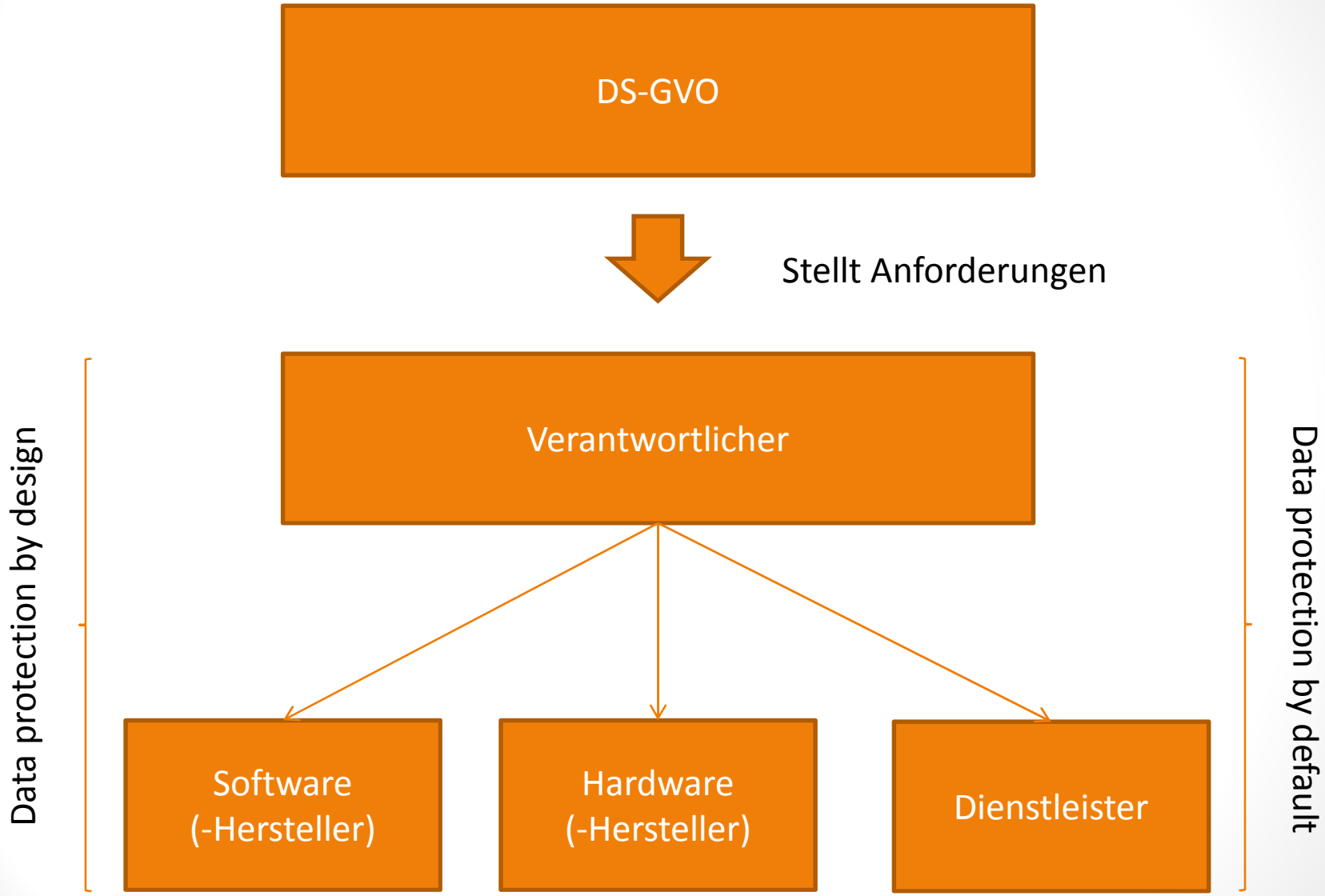
Maßnahmen: “Sparsamkeit“ bei Funktionalitäten, Anonymisierung/ Pseudonymisierung, Authentisierung (Nachweis der Person, z.B. Passwort, Personalausweis) und Authentifizierung (Prüfung der behaupteten Authentisierung durch den Prüfer/ Server), detaillierte Berechtigungsvergabe, Verschlüsselung etc.

Datenschutzfreundliche Voreinstellungen

Voreinstellungen stellen sicher, dass nur die für den Zweck erforderlichen Daten erhoben werden. Dem Nutzer müssen außerdem Funktionalitäten zum Schutz bereitgestellt werden (z.B. Verschlüsselung).

Grund: Nutzer verfügen häufig nicht über ausreichende IT-Kenntnisse und können daher keine Einstellungen zu ihrem Schutz wahrnehmen

Maßnahmen: Häkchen für Datenübertragungen dürfen nicht bereits gesetzt sein. Hinweise zu Programmdownloads oder bereitgestellten Funktionalitäten etc.


DS-GVO
Stellt Anforderungen
Verantwortlicher
Data protection by design
Data protection by default
Software
(-Hersteller)
Hardware
(-Hersteller)
Dienstleister

5. Sicherstellung der Betroffenenrechte

Rechtlich

Die Ausübung der Rechte des Betroffenen muss im Einklang mit den einschlägigen Datenschutzvor-schriften stehen

Technisch

Eingesetzte Ver-fahren müssen so gestaltet sein, dass Rechte des Betroffenen umgesetzt werden können

Organisatorisch

Mitarbeiter müssen wissen, wie sie sich zu verhalten haben (bspw. Handeln bei einem Auskunftsersuchen)