Datenschutzmanagement

Sicherstellung und Überwachung der Einhaltung
der Datenschutz-Grundverordnung (DS-GVO)

Markus Gierschmann, atprivacy consulting
BvD-Herbstkonferenz 2018, Stuttgart

Agenda

1. **Paradigmenwechsel im Datenschutz**

2. Sicherstellung der Compliance durch ein Managementsystem

3. Ansätze und Gestaltung eines Datenschutz-Managementsystems

Paradigmenwechsel im Datenschutz durch DS-GVO

Datenschutz-Grundverordnung (DS-GVO)

1. EU-Grundverordnung (nicht nur Richtlinie!)
2. Rechenschafts- und Nachweispflicht
3. Risikobasierter Ansatz
4. Wirksamkeitsüberprüfung
5. Zertifikate / Verhaltensregeln

→ **Paradigmen-wechsel**

Rechenschaftspflicht (Accountability)

Art. 5: Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) … auf rechtmäßige Weise … („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“)

b) … für festgelegte, eindeutige und legitime Zwecke … („Zweckbindung“)

c) … auf das notwendige Maß beschränkt … („Datenminimierung“)

d) … sachlich richtig … („Richtigkeit“)

e) … erforderlich … („Speicherbegrenzung“) [und mit]

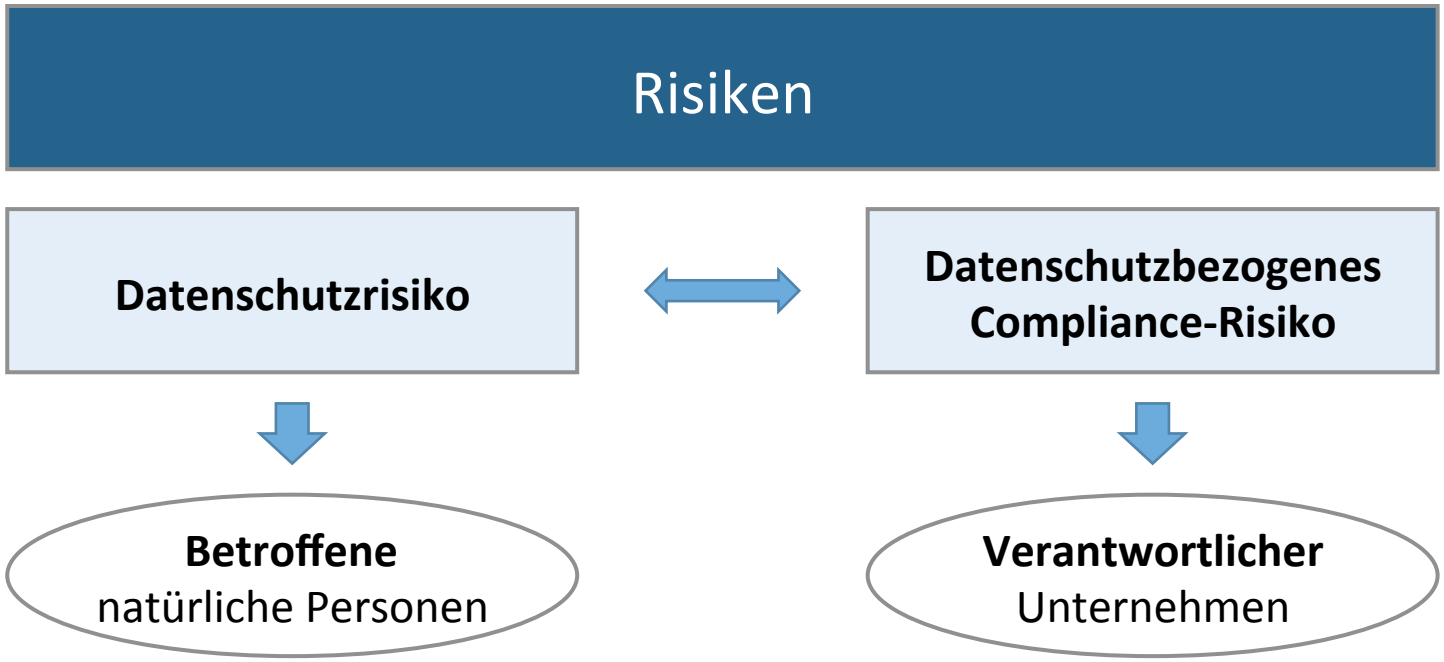
f) … angemessener Sicherheit … („Integrität und Vertraulichkeit“) [verarbeitet werden.]

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

Art. 24: Verantwortung des für die Verarbeitung Verantwortlichen

(1) Der **Verantwortliche** setzt … geeignete TOMs um, um sicherzustellen und den Nachweis erbringen zu können, das …

Risikobasierter Ansatz

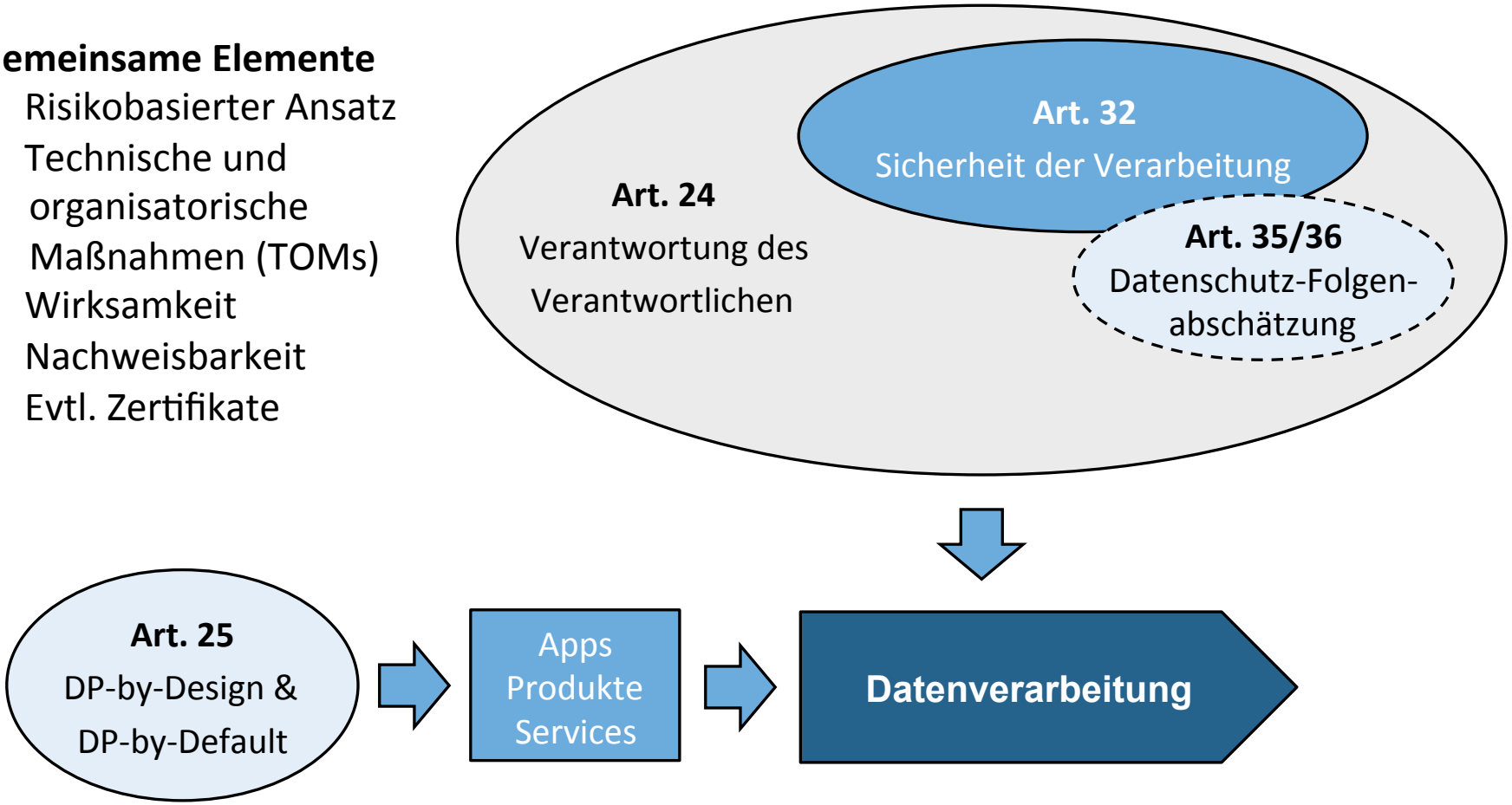


DS-GVO betrachtet nur die Risiken für die Rechte und Freiheiten natürlicher Personen (Betroffener); Nicht-Einhaltung der Vorschriften ist Compliance-Risiko des Verantwortlichen.

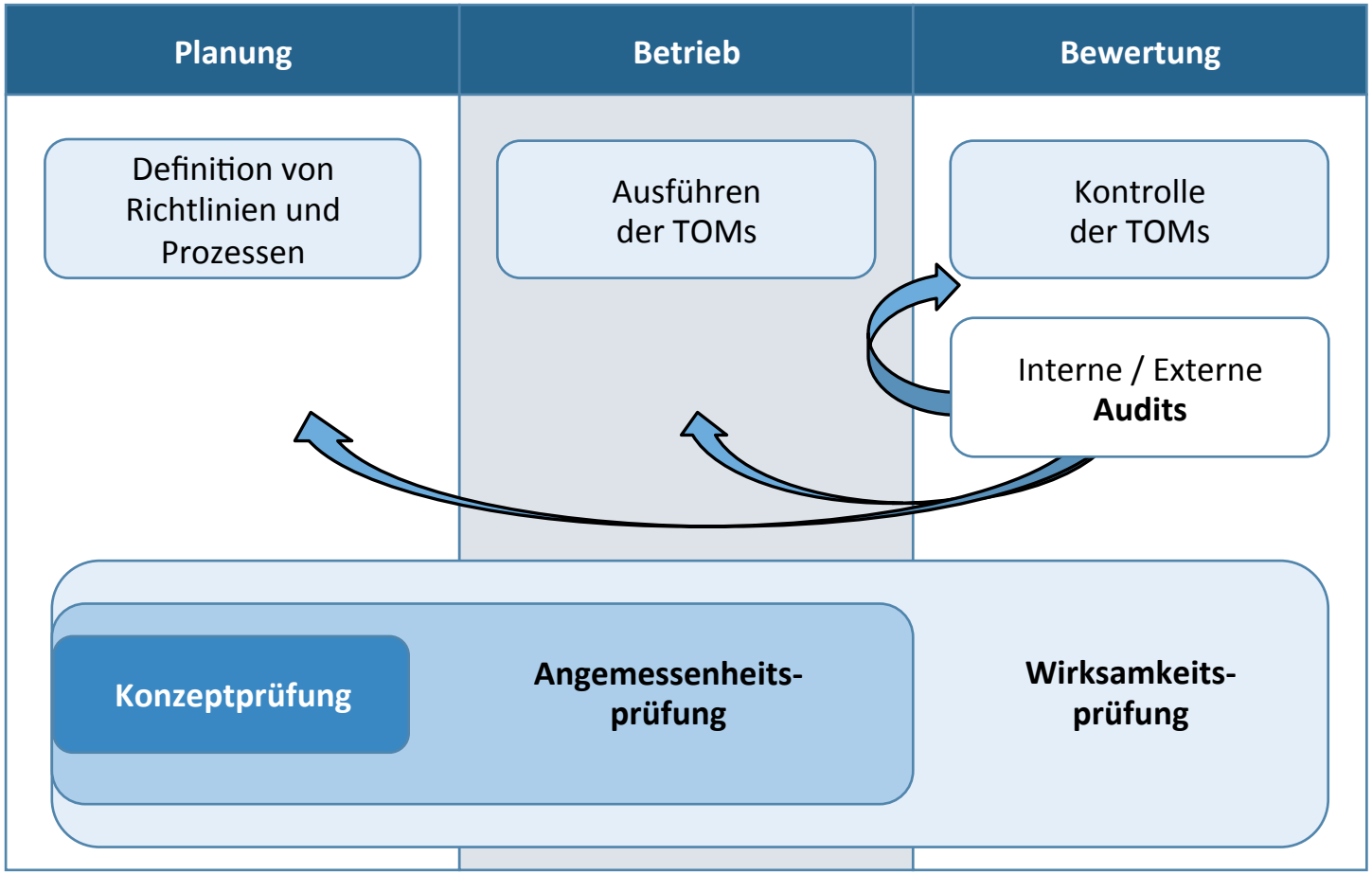
Pflichten des Verantwortlichen

Gemeinsame Elemente

- Risikobasierter Ansatz
- Technische und organisatorische Maßnahmen (TOMs)
- Wirksamkeit
- Nachweisbarkeit
- Evtl. Zertifikate



Überprüfung der Wirksamkeit der TOMs



... stärkere Prozessorientierung

Datenschutz-konforme Verarbeitung

- **Umfangreiche Anforderungen** im Umgang mit personenbezogenen Daten, u.a. Rechtmäßigkeit, Sicherheit, Risikobeurteilung, DSFA
- Berücksichtigung von **Privacy by design & default** (Art. 25)
- Ggfs. **Management von Auftragsverarbeitern**

Sicherstellung der Betroffenenrechte

- **Umfangreiche Rechte der Betroffenen** (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch)
- Verantwortliche muss **Prozesse implementieren**, um eine fristgerechte und korrekte Bearbeitung der Anträge zu gewährleisten

Handhabung von Datenschutz-verletzungen

- **Absenkung der Meldeschwelle in Abhängigkeit des Risikos** und Einhaltung von engen Zeitvorgaben (72h)
- **Vorbereitet sein**, um Datenschutzvorfälle zu identifizieren und angemessen reagieren zu können (Art. 33, 34, ErwGr. 87)

Datenschutz-Zertifikate sind ein wichtiges Instrument zur Nachweiserbringung

- Erhöhte Nachfrage nach Zertifikaten durch **Nachweispflichten.**

- Umfangreiche **Zertifizierungsgegenstände** nach DS-GVO möglich, u.a.
  - Datenschutzkonforme Verarbeitung, Art. 24
  - Datenschutz durch Technik, Art. 25 Abs.1
  - Datenschutzfreundliche Voreinstellung, Art. 25 Abs. 2
  - Auftragsverarbeitung, Art. 28
  - Sicherheit der Verarbeitung, Art. 32

- Anforderungen an die **Qualität und Transparenz** steigen!
  - Akkreditierung der Zertifizierungsstellen
  - Billigung der Zertifizierungskriterien durch Aufsichtsbehörden
  - Überprüfung der Zertifizierungen durch Aufsichtsbehörden

Bußgelder

- Bei **unzureichender oder Nicht-Erfüllung der Vorschriften** der DS-GVO drohen den Unternehmen u.a. Geldbußen (Non-Compliance).

- Die Aufsichtsbehörde soll dabei sicherstellen, dass die Verhängung der Geldbuße in jedem Einzelfall **wirksam, verhältnismäßig und abschreckend** ist, Art. 83 Abs. 1 DS-GVO.

- Geldbußen können in einer Höhe von **bis zu 20 Mio. EUR oder bis 4 % des gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahres verhängt werden, je nachdem welcher Betrag höher ist.

Management "attention"

Agenda

1. Paradigmenwechsel im Datenschutz

2. **Sicherstellung der Compliance durch ein Managementsystem**

3. Ansätze und Gestaltung eines Datenschutz-Managementsystems

Rechenschaftspflicht = Beweislastumkehr?

Produkthaftung
in der Fertigung

Qualitätsbegriff
= wahrnehmbare Zustandsform

Prozessorientierung
zur repetitiven Qualitätssicherung
→ PDCA

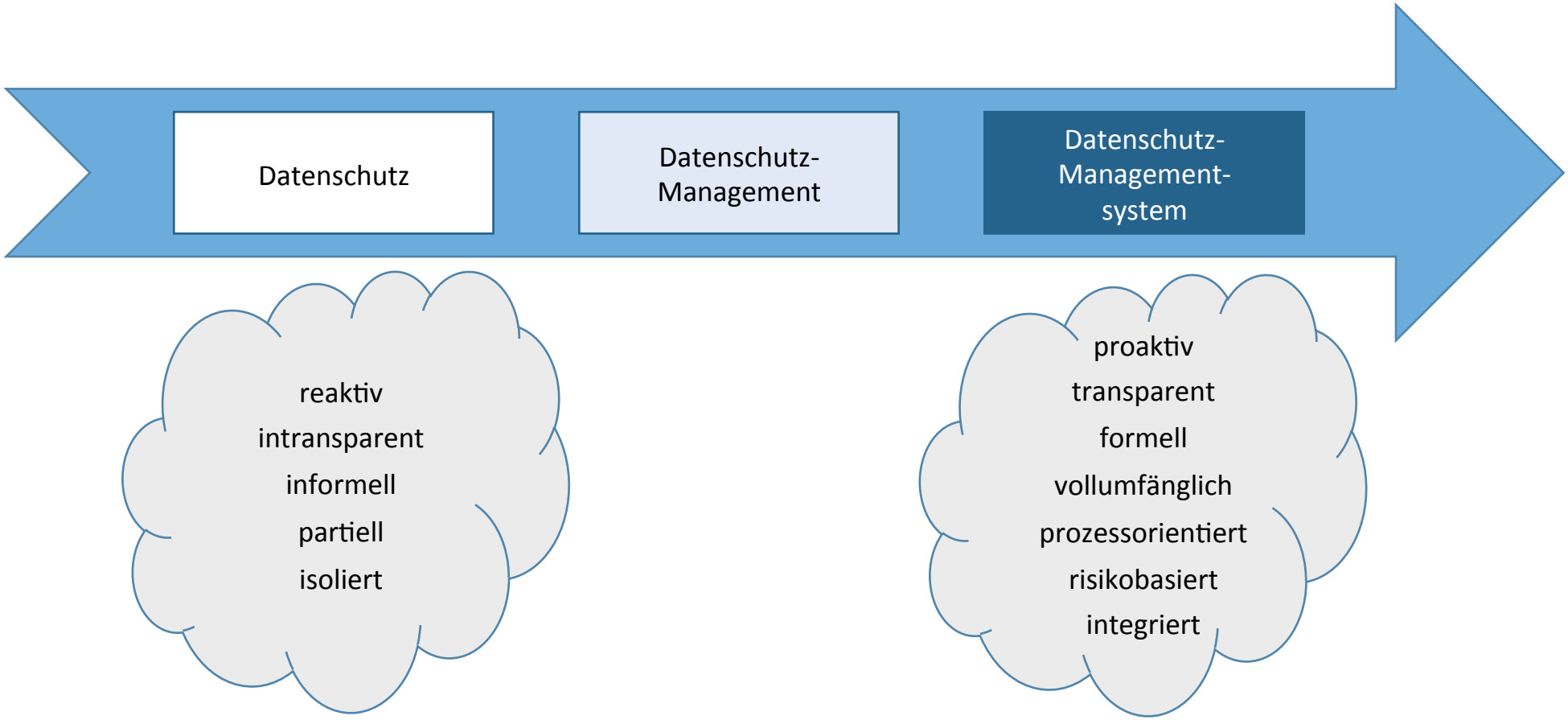
Qualitäts-Managementsystem
QMS nach ISO 9001

Rechenschaftspflicht
im Datenschutz

Nachweis erbringen können
wie Verantwortung <u>überprüfbar</u>
wahrgenommen wird

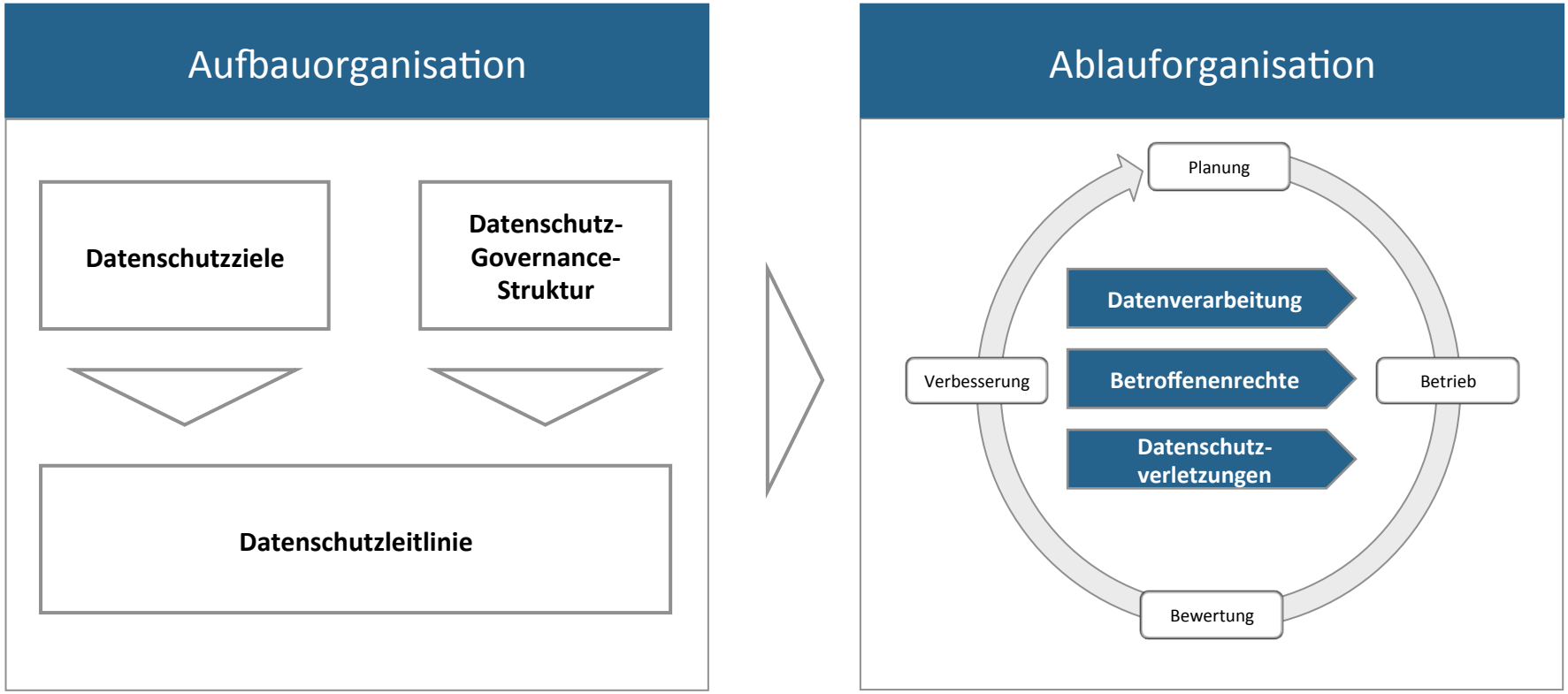
„Compliance-Programme"
(Art. 29-Gruppe, WP 173, 2010)

Evolution im Datenschutz



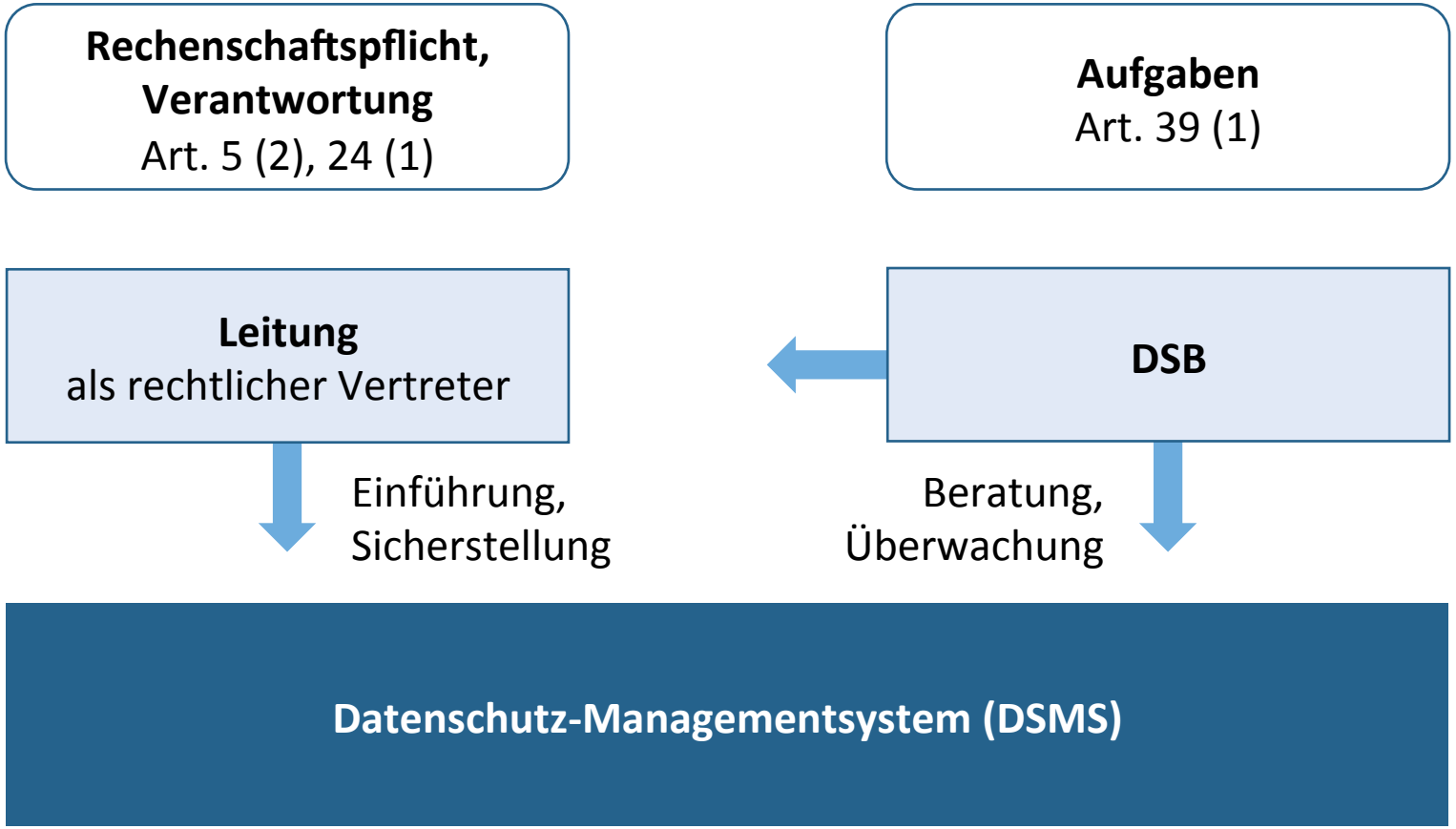
Entwicklung des Datenschutzes hin zu einem effektiven Compliance-Management-System

Managementsystem für Datenschutz-Compliance



Rechenschaftspflicht, Verantwortung des Verantwortlichen (Art. 5 Abs. 2, Art. 24)

Verantwortung für ein datenschutzorientiertes Compliance-Managementsystem



Aufgaben des Verantwortlichen vs. „originäre“ Aufgaben des Datenschutzbeauftragter

Verantwortlicher	Datenschutzbeauftragter
Bestellung des DSB, Art. 37 **Stellung des DSB, Art. 38** **Sicherstellung der Einhaltung der DS-GVO, insbesondere Art. 5 Abs. 2, Art. 24** **Datenschutzmanager (!)**	**Aufgaben des DSB, Art. 39** – Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten – **Überwachung der Einhaltung der DS-GVO** – Beratung und Überwachung der DSFA gem. Art. 35 (auf Anfrage!) – Zusammenarbeit mit und Anlaufstelle für AB

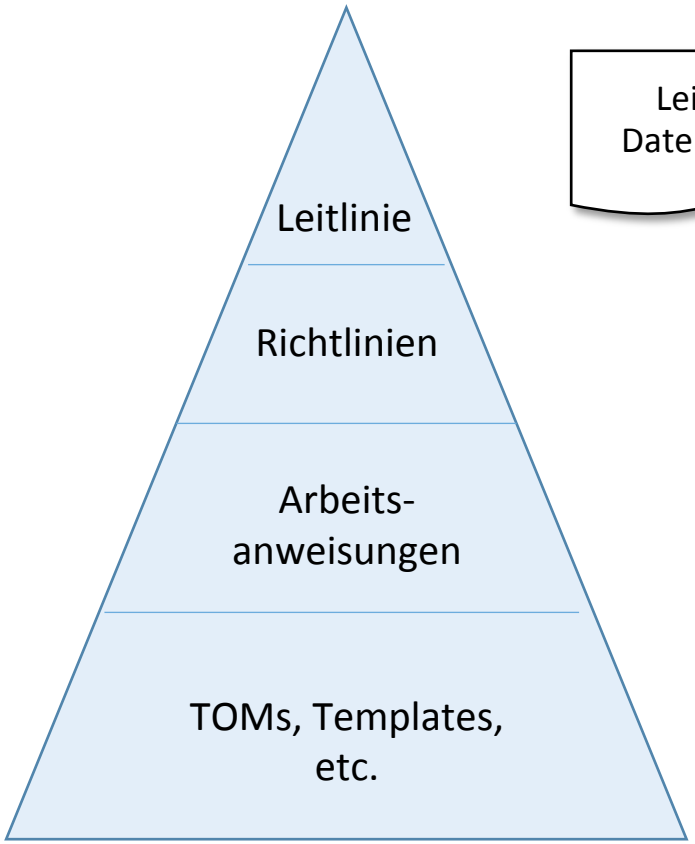
Verantwortliche natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung entscheidet, Art. 4 Nr. 7 → Juristische Person vertreten durch GF

Paradigmenwechsel in der Datenschutz-Kultur

Verantwortlichkeiten der DS-GVO erfordern ein Umdenken und Wandel der Datenschutz-Kultur auf vielen Ebenen einer Organisation, z.B. bei …

- **Geschäftsleitung**
  - Datenschutz ist ein Compliance Thema;
  - Verantwortung für die Sicherstellung liegt bei der Geschäftsleitung und muss delegiert werden (Etablierung der erforderlichen Strukturen und Prozesse → Kommunikation).
- **Fachbereiche / Mitarbeiter**
  - Jeder Bereichs- und Prozessverantwortliche ist innerhalb seines Zuständigkeitsbereichs für die Sicherstellung verantwortlich (d.h. Konkretisierung, Umsetzung und Einhaltung);
  - Jeder Mitarbeiter muss sich der Vorgaben bewusst sein und entsprechend handeln.
- **Datenschutzmanager**
  - Handelt im Auftrag der Geschäftsleitung und koordiniert das Datenschutzmanagement.
- **Datenschutzbeauftragter**
  - Berät und überwacht weisungsfrei.

Mehrstufige Datenschutzpolitik



Wesentliche Dokumente

Leitlinie Datenschutz

Rollen / Verantwortlichkeiten → Governance Struktur

RL datenschutz-konforme Verarb.

RL Betroffenen-rechte

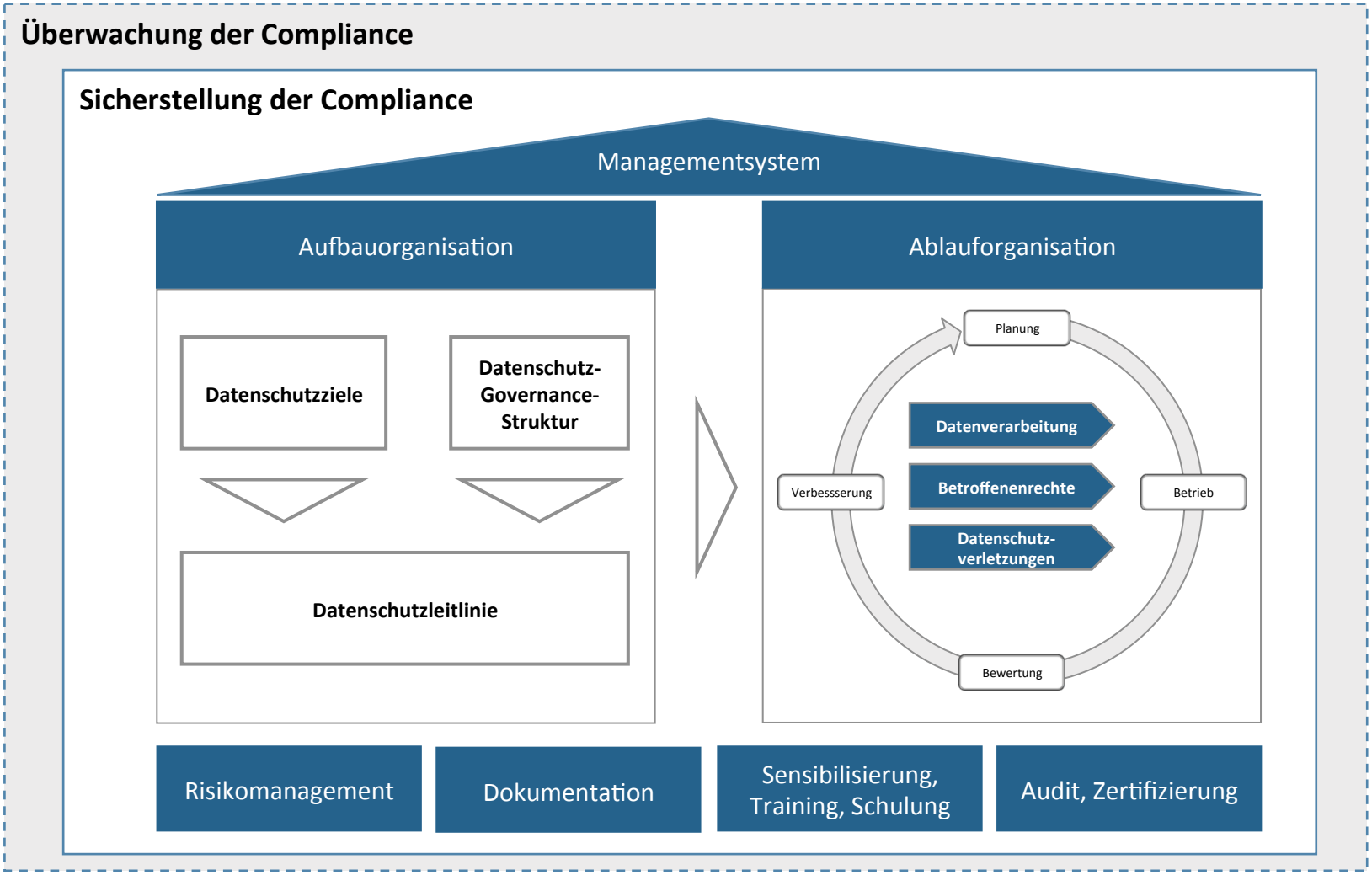
RL Datenschutz-verletzungen

Kontroll- und Überwachungs-konzept

Bewertung → Audits

… und weitere, z.B.
- Sicherheitskonzept,
- Lösch- und Sperrkonzept

Sicherstellung und Überwachung der Compliance



Agenda

1. Paradigmenwechsel im Datenschutz

2. Sicherstellung der Compliance durch ein Managementsystem

3. **Ansätze und Gestaltung eines Datenschutz-Managementsystems**

Nutzen eines DSMS-Standards

... für **Unternehmen** (als Verantwortlicher bzw. Auftragsverarbeiter)

- Umsetzung der Compliance durch Orientierung, Best Practices, Knowledge Sharing
- Auswahl und Management von Auftragsverarbeitern
- Nachweis der Compliance durch Zertifizierung (Art. 40) → Exkulpation

... für **Aufsichtsbehörden** und Europ. Datenschutzausschuss (EDPB)

- Höhere Transparenz der Unternehmen gegenüber der AB, dadurch
  - effizientere und effektivere Überwachung
  - z.T. Reduktion der Überwachung
- Vereinfachtere Überprüfung von Datenschutzverletzungen und Beschwerden

... für **Betroffene** (u.a. als Kunden, Mitarbeiter)

- Transparenz und Selbstverpflichtung des Unternehmens
- Vertrauen in die Zertifizierungsstelle

Ansätze für ein Datenschutz-Managementsystem

Stand-alone DSMS	Entwicklung eines **eigenständigen Systems** zum Management vom Datenschutz	Fokus auf Datenschutzrisiken
Nutzung eines vorhandenen Managementsystem	z.B. Qualitätsmanagementsystem (**QMS**), Compliance-Managementsystem (**CMS**) oder Informationssicherheitsmanagement-system (**ISMS**)	Problematisch: z.T. andere Zielsetzung
Integriertes DSMS	z.B. **Erweiterung eines ISMS nach ISO/IEC 27001** durch ein eigenes Anforderungswerk und Controls	Kombination von Datenschutz- und Unternehmensrisiken

Arten von Managementsystemen

Qualitäts-managementsystem QMS	– **ISO 9001**, etabliert und weit verbreitet – Methodisch übertragbar (u.a. PDCA, Support) – ABER: Inhaltlich keine Überschneidung
Compliance-Managementsystem CMS	– **ISO 19600, IDS PS 980**, teilweise verbreitet – Compliance-Ansatz auf Datenschutz anwendbar – ABER: Datenschutzspezifische Ausprägung notwendig → s. PH
Informationssicherheits-Managementsystem ISMS	– **ISO 27001**, etabliert, aber wenig verbreitet – Überschneidung zum technischen Datenschutz – ABER: Security controls auf Unternehmensrisiken ausgerichtet
Datenschutz-Managementsystem DSMS	– Bisher nur ein nationaler Standard (UK **BSI 10012:2017**, PIMS) – Entwicklung eines ISO-Standards als Erweiterung eines ISMS nach ISO 27001 (***ISO DIS 27552***, *Extension to ISO 27001 and ISO 27002 for privacy information management*)

Quality Management System (QMS)

- **Qualitätsmanagementsystem (QMS)**
  - Methode der Unternehmensführung;
  - Ziel ist ein systematisches Qualitätsmanagement:
    Sicherstellen, dass die **System-, Prozess- und Produktqualität** in einer Organisation geprüft und verbessert wird;
  - Dauerhafte Verbesserung der Unternehmensleistung.

- **Qualitätsmanagementnormen**
  - **Anforderungen**, die ein Managementsystem genügen muss, um einem bestimmten Standard bei der Umsetzung des Qualitätsmanagements zu entsprechen;
  - Nachweis wird durch einen **Zertifizierungsprozess** mit zeitlich befristeten Zertifikat durch unabhängige Zertifizierungsstellen erbracht;
  - Kann als **Nachweis** der Umsetzung bestimmter Standards dienen.

  - QMS nach **ISO 9001:2015** und branchenspezifische Normen

Compliance Management System (CMS)

- **Compliance Management System (CMS)**
  - Gesamtheit der in einer Organisation eingerichteten Strukturen, Prozesse und Maßnahmen, zur Sicherstellung einer **Regelkonformität** (u.a. rechtliche und interne Regeln);
  - Sicherstellen, dass Risiken für wesentliche **Regelverstöße** rechtzeitig erkannt, kommuniziert, darauf angemessen reagiert und zukünftig verhindert werden;
  - Schaffung und Erhaltung einer **nachhaltigen Compliance-Kultur**.
- **Compliance Management Normen**
  - CMS nach **ISO 19600:2014**, auch als DIN-Norm, keine Zertifizierung vorgesehen;
  - CMS nach **IDW PS 980**, Zertifizierung möglich; **IDW PH 9.860.1** für Prüfungen nach der DSGVO und dem BDSG.

IDW PH 9.860.1: *Prüfung der Grundsätze, Verfahren und Maßnahmen nach DS-GVO und BDSG* → konkretisiert die Anwendung der Grundsätze des *IDW PS 860* in Bezug auf datenschutzspezifische Prüfungen

Grundelemente der IDW PS 980

1. Kultur
2. Ziele
3. Risiken
4. Programm
5. Organisation
6. Kommunikation und Information
7. Überwachung und Verbesserung

Information Security Management System (ISMS)

- **Informationssicherheitsmanagementsystem (ISMS)**
  - Aufstellung von **Verfahren und Regeln** innerhalb einer Organisation, welche dazu dienen, die **Informationssicherheit** dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern;
  - Informationssicherheit ist grundsätzlich eine **Aufgabe der Leitung** einer Organisation.

- **Informationssicherheitsnormen**
  - ISMS nach **ISO/IEC 27001:2013**, zertifizierungsfähig;
  - **IT-Grundschutz** vom BSI angepasst an ISO/IEC 27001,
    ISO/IEC 27001-Zertifikat auf Basis von IT-Grundschutz,
    derzeit in Überarbeitung → IT-Grundschutz-Kompendium;

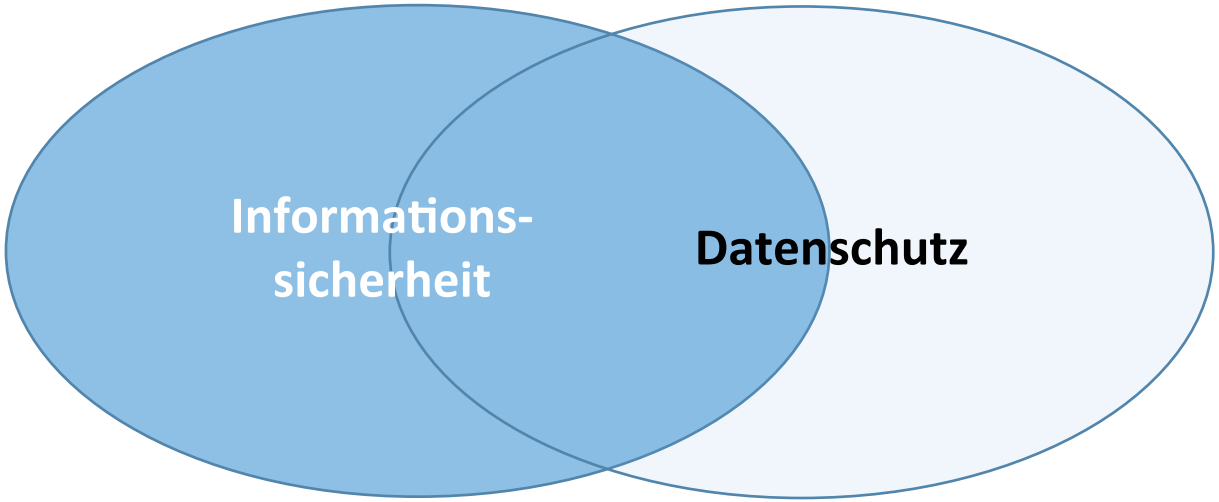
  - KMU: auf Basis von ISO/IEC 27001 und IT-Grundschutz **ISIS12**, **VdS 3473**

Datenschutz-Managementsystem (DSMS)

- **Datenschutz-Managementsysteme (DSMS)**
  - Datenschutzmanagement ist eine Managementmethode, um die gesetzlichen und betrieblichen **Anforderungen des Datenschutzes** systematisch zu planen, zu organisieren, zu steuern und zu kontrollieren (Datenschutzrisiken);
  - Ein **systematisches Datenschutzmanagement** ist wichtig, um im Fall von aufsichtsbehördlichen Verfahren, die Bußgelder und weiteren Sanktionen zur Folge haben können, den Vorwurf des fahrlässiges Handelns abschwächen zu können (Compliance-Risiken).

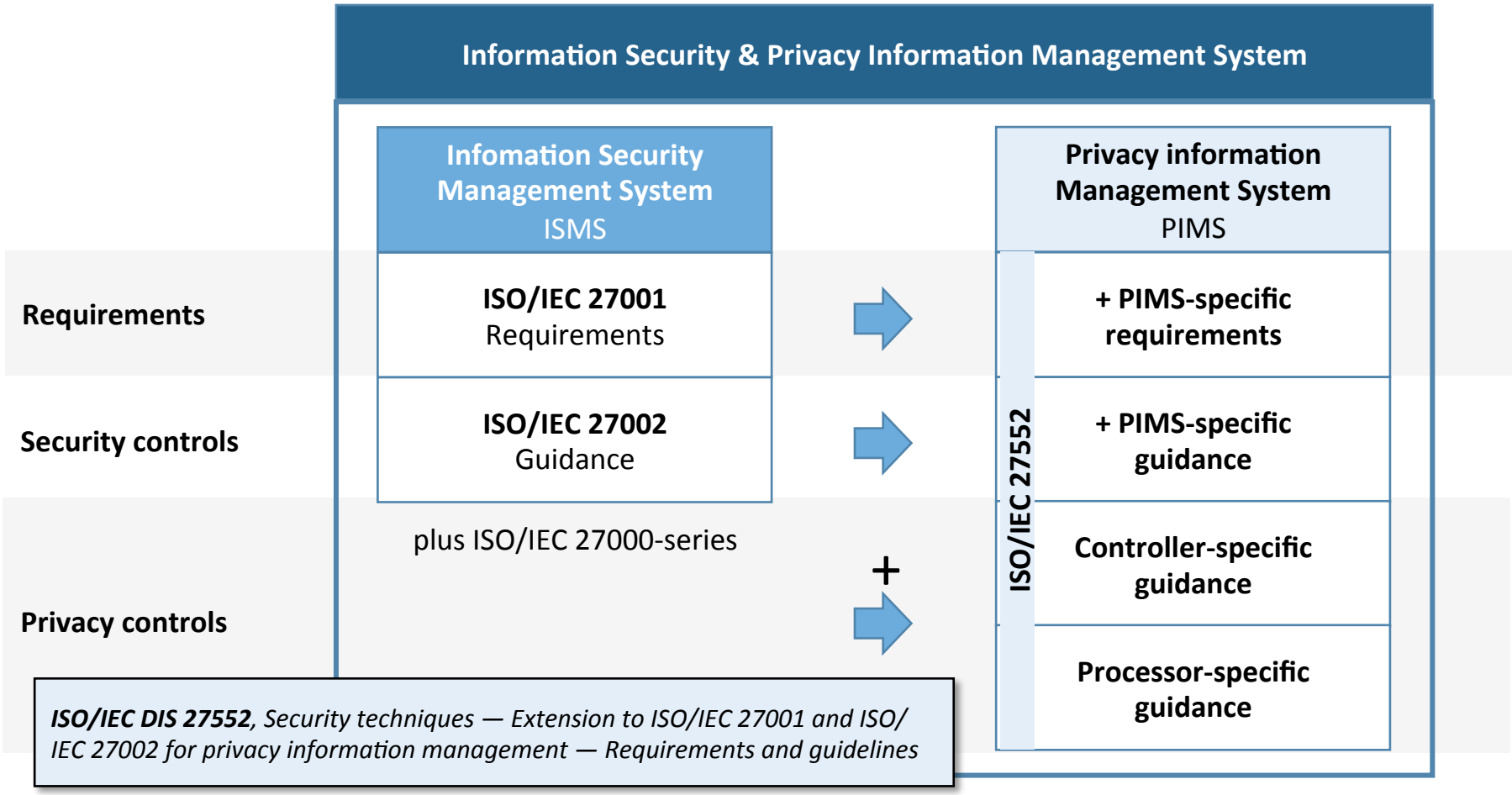
- **Datenschutzmanagementnormen**
  - **BS 10012:2017**, Personal Information Management System & GDPR Regulation Compliance, zertifizierungsfähig durch BSI (The British Standards Institut);
  - **ISO/IEC DIS 27552**, Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidance.

Informationssicherheit und Datenschutz

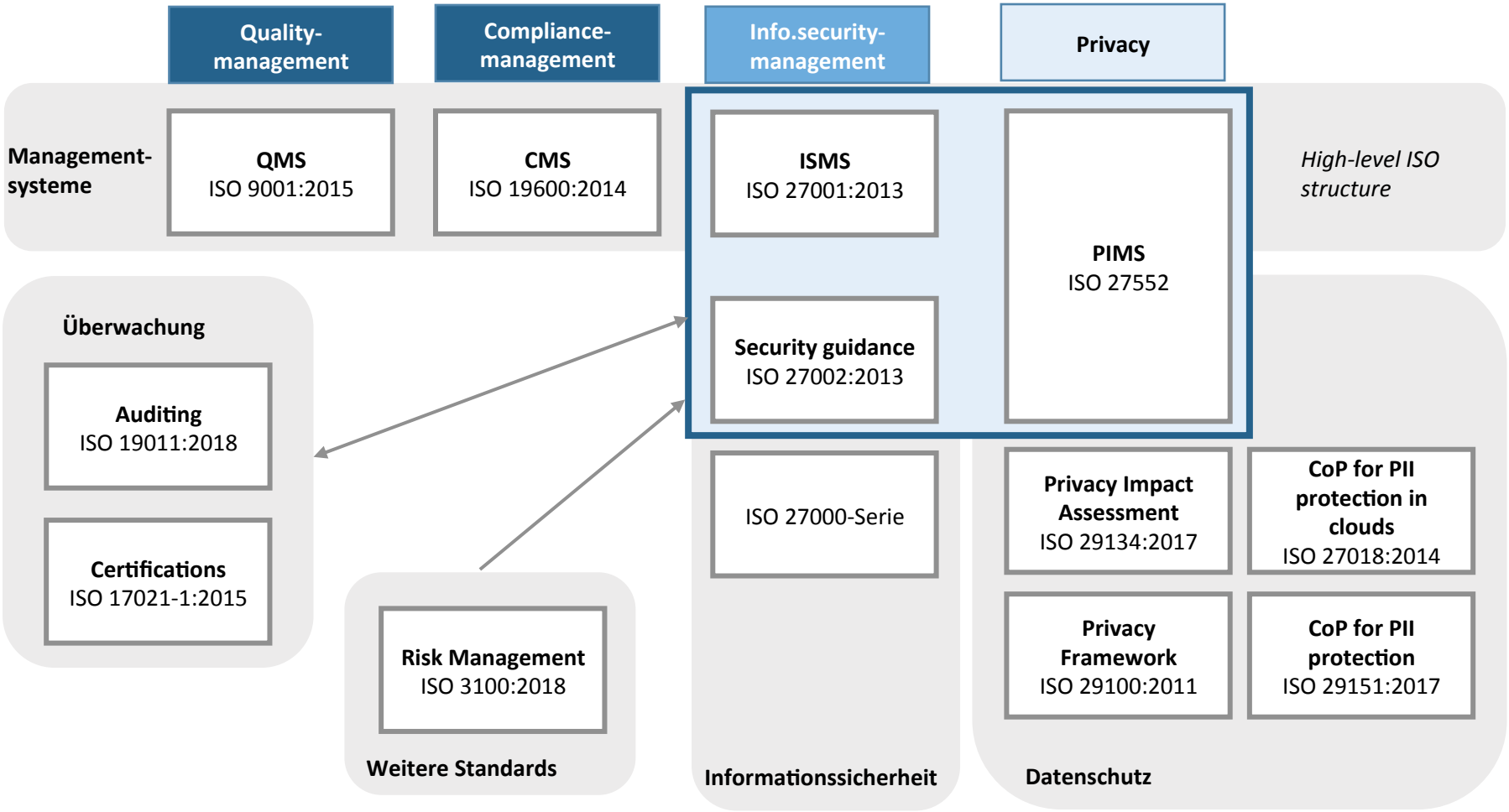


Abgrenzung	Informationssicherheit	Datenschutz
Ziel	Schutz der **Organisation**	Schutz der **Betroffenen**
Umfang / Gegenstand	**Alle Informationen**, einschl. pbD Geschäftsprozesse	**Personenbezogene Daten** Datenverarbeitung
Folgen für:	**Unternehmensrisiken**, einschl. Compliance- und Finanzrisiken	**Datenschutzrisiken** und Folgen für Betroffene

Extension to ISO/IEC 27001 & 27002 for privacy information management (ISO/IEC 27552)



Ausblick auf ein integriertes Informationssicherheits- und Datenschutz-Managementsystem



Kontaktdaten

Markus Gierschmann

Dipl.-Ing. oec, Finanzökonom (ebs)
Datenschutzbeauftragter (udis, TÜV)
Datenschutzauditor (TÜV)
CIPP/E, CIPM

Markus Gierschmann I atprivacy consulting
Tel +49 89 500 77 270, Mobil + 49 175 5961 553
m.gierschmann@atprivacy.de

www.atprivacy.de

Thomas Kranig / Andreas Sachs / Markus Gierschmann:
Datenschutz-Compliance nach der DS-GVO
Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden

Bundesanzeiger Verlag, 2017

ISBN (Print): 978-3-8462-0760-4
ISBN (E-Book): 978-3-8462-0773-4
www.bundesanzeigerverlag.de

Anmerkungen, Anregungen, Kritik:
feedback@datenschutz-compliance-buch.de

Aktuelle Prüffragen:
www.lda.bayern.de