it.sec
security for your information

Informationstechnik & Datenschutz
– Ein spannendes Verhältnis

Ringvorlesung zur Technikfolgenabschätzung
an der Universität Stuttgart am 8. Mai 2012

Bernhard C. Witt (it.sec GmbH & Co. KG)

Bernhard C. Witt

- **Senior Consultant für Datenschutz & Informations-sicherheit** bei der it.sec GmbH & Co. KG verantwortlich für die Geschäftsfelder
  ° Datenschutz
  ° IT Governance, Risk & Compliance Management
- Industriekaufmann, Diplom-Informatiker
- geprüfter fachkundiger Datenschutzbeauftragter (UDIS)
- zertifizierter ISO/IEC 27001 Lead Auditor (BSi)
- CRISC (ISACA)
- **Lehrbeauftragter** für Datenschutz und IT-Sicherheit an der Universität Ulm (seit 2005)
- **Autor** der Bücher „IT-Sicherheit kompakt und verständlich“ und „Datenschutz kompakt und verständlich“
- **Sprecher** der GI-Fachgruppe Management von Informationssicherheit (seit 2009)
- Mitglied im Leitungsgremium des GI-Fachbereichs Sicherheit – Schutz und Zuverlässigkeit
- Mitglied im Leitungsgremium der GI-Fachgruppe Datenschutzfördernde Technik (PET)
- Mitglied im DIN-Arbeitsausschuss „IT-Sicherheitsverfahren“ (Normierung zur Informationssicherheit)

it.sec
security for your information

it.sec GmbH & Co. KG

- **beratend** tätig zu:
  - ° Informationssicherheitsmanagement (ISMS), z.B. ISO/IEC 27001
  - ° IT-Risikomanagement, z.B. ISO/IEC 27005
  - ° Business Continuity Management (BCM), z.B. BS 25999
  - ° externer Datenschutzbeauftragter bzw. Datenschutzberatung
  - ° Penetrationstests zu Infrastruktur und Web-Applikationen
  - ° Firewall-Audits
  - ° IT-Forensik
  - ° SCADA Security
  - ° Planung, Integration und Management von Sicherheitssystemen
  - → **Dienstleister ganzheitlicher Informationssicherheit**
- seit 1996 am Markt; mit Standorten in Ulm und München
- bundesweit (mit Schwerpunkt im Süden) beauftragt von: IT-Dienstleister, Industrie, Banken- und Finanzsektor, Kanzleien, Stadtwerken, Gesundheitswesen, Krankenkassen, u.v.a.m.
- immer **auf der Suche nach neuen Mitarbeitern** (sowohl Technik als auch Management), inkl. Praktikanten, Masteranten / Diplomanden, Trainees (Berufsanfänger) und Senior Consultants

→ nähere Informationen zu it.sec zu finden unter www.it-sec.de

Agenda

1. Was ist Datenschutz?
2. Verhältnis von Datenschutz zu Informationssicherheit
3. Folgen der IT auf den Datenschutz
4. Folgen des Datenschutzes auf die IT
5. Fazit zum spannenden Verhältnis

Was ist Datenschutz?

Was ist Datenschutz? (1)

Datenschutz =

Schutz des Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts beim Umgang mit seinen personenbezogenen Daten (nach § 1 Abs. 1 BDSG)

→ Schutz des Individuums (= natürliche Person)

→ Beschränkung auf personenbezogene Daten:

- **unmittelbar personenbezogen**: Identifikationsdaten (z.B. Name oder Foto → Person bestimmt)
- **personenbeziehbar** (→ Person bestimmbar):
  - leichte Zuordnung (z.B. Matrikel-Nr., User-ID)
  - Verknüpfung mit Identifikationsdaten (z.B. Konto)

→ Maßgeblich: Persönlichkeitsrecht des Betroffenen

Was ist Datenschutz? (2)

Informationelles Selbstbestimmungsrecht =

Grundrecht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (nach BVerfGE 65, 1 [43])

→ **Grundrecht** resultiert aus persönlicher Handlungsfreiheit & Menschenwürde (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG):

Art. 2 Abs. 1 GG

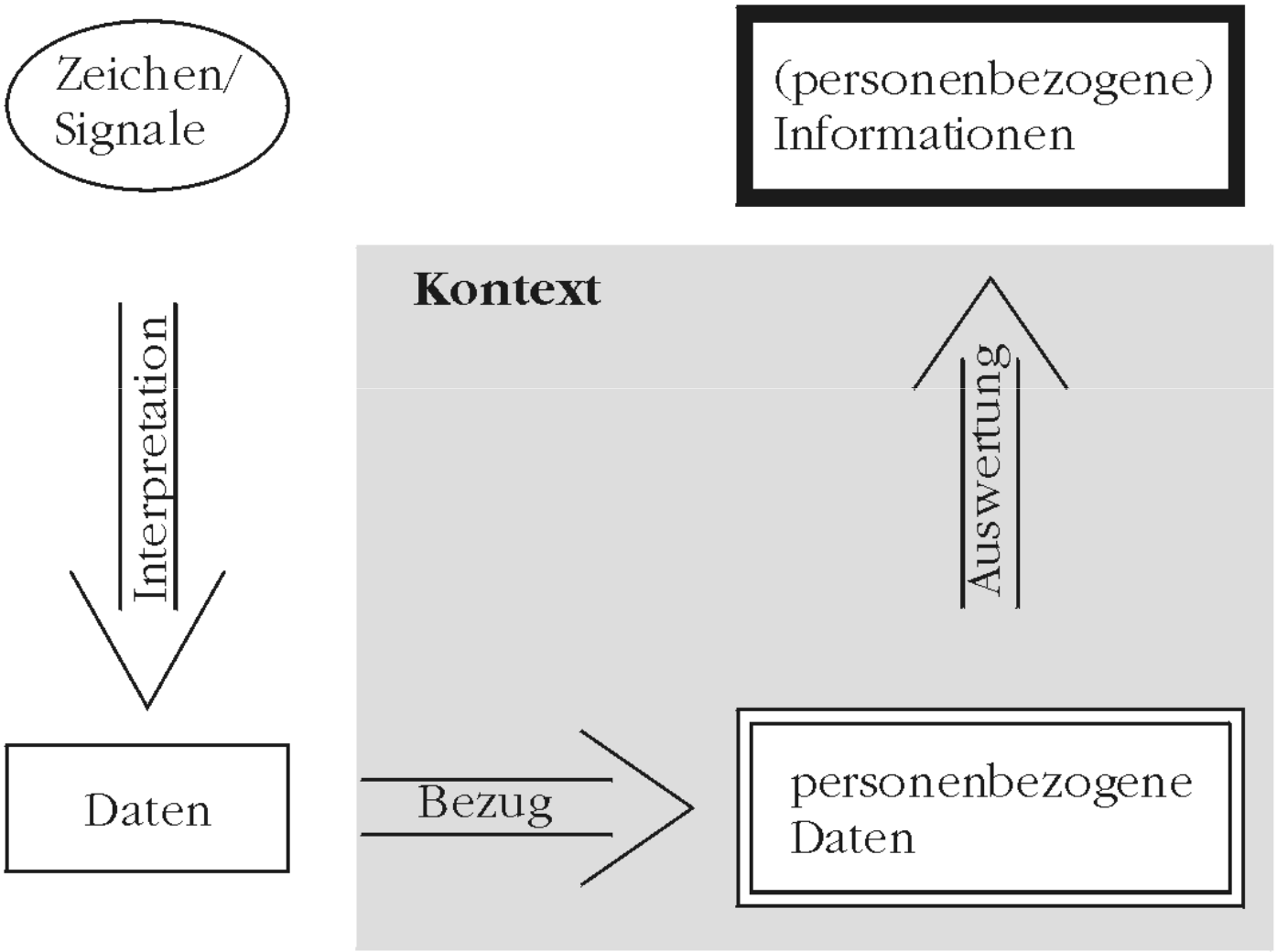
Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

i. V. m.

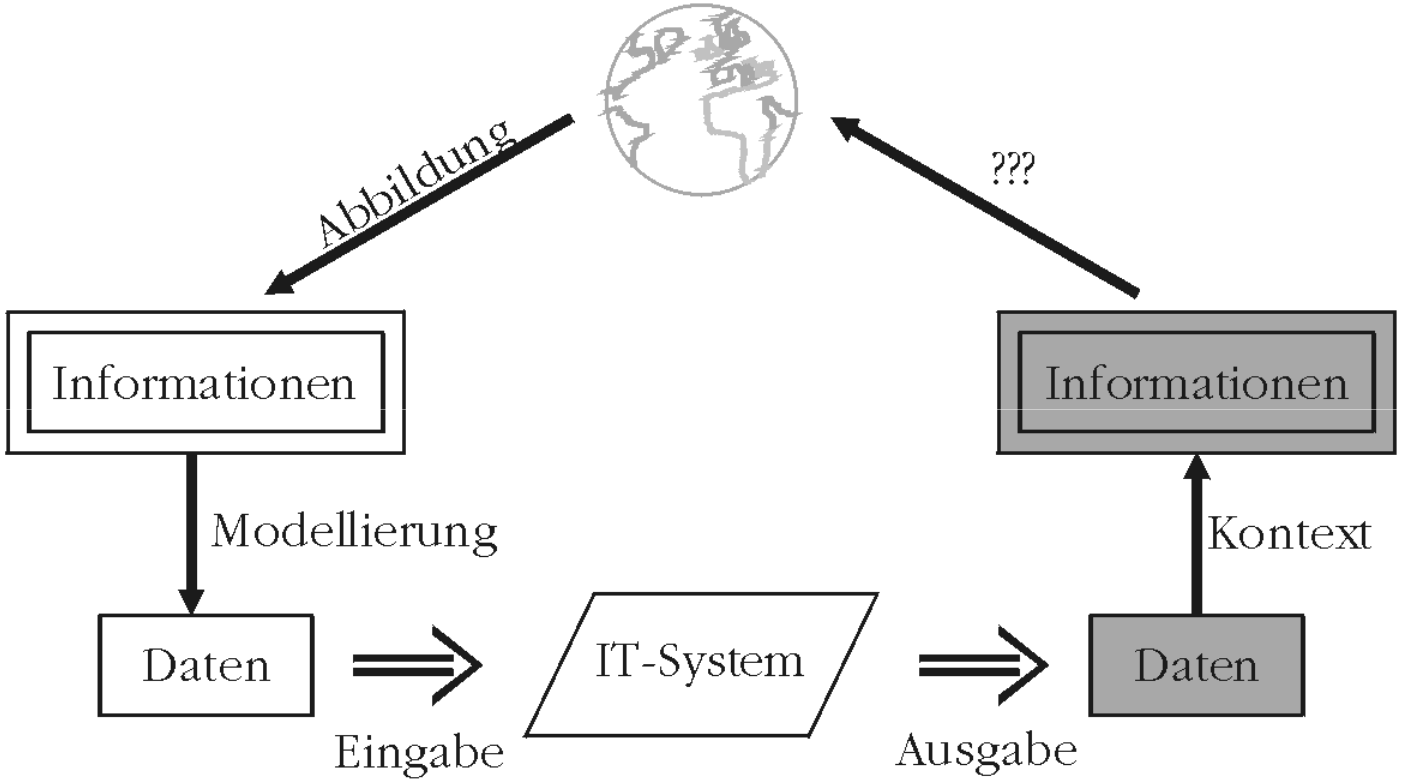
Art. 1 Abs. 1 GG

Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Was ist Datenschutz? (3)



Was ist Datenschutz? (4)



Was ist Datenschutz? (5)

Schutzbedarf der Daten am Beispiel von Unternehmen:

- **Sehr hoch**: Besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG & § 4d Abs. 5 BDSG & § 42a BDSG)
  - ° Gesundheitsdaten, z.B. Krankmeldungen
  - ° Gesichtstyp & Hautfarbe, z.B. Foto
- **Hoch**: Persönlichkeitsprofile (§ 4d Abs. 5 BDSG)
  - ° Fähigkeitsbewertung, z.B. Zeugnisse
  - ° Leistungsbewertung (mitbestimmungspflichtig!), z.B. Prämien
  - ° Verhaltensbewertung (mitbestimmungspflichtig!), z.B. Arbeitszeit
- **Hoch**: Berufsgeheimnisbezogene Daten (§ 42a BDSG)
  - ° Aufzeichnungen von Rechtsanwälten, Wirtschaftsprüfern, Betriebsräte, Sicherheitsbeauftragte, Datenschutzbeauftragter, etc.
- **Hoch**: Bank- & Kreditkartenkontendaten (§ 42a BDSG)
- **Niedrig**: (Faktisch) Anonymisierte Daten
- **Mittel**: Rest (→ Großteil!)

→ **Je höher der Schutzbedarf, desto mehr Maßnahmen sind nötig!**

Was ist Datenschutz? (6)

- Datenschutz = **Schutz des Persönlichkeitsrechts** der Betroffenen beim Umgang mit deren Daten
- Datenschutz = **Schutz vor unerwünschten Verfahren**
- Verwendung der Daten ausschlaggebend für Zweck-bindung und Informationsgehalt der Daten
  → Datenschutz = **Informationsschutz**
- Datenschutz abhängig vom Schutzgrad der Daten und damit von deren Kontext
- Die Entwicklung des Datenschutzes ist aber nicht unab-hängig von der Entwicklung der Informationstechnik!

Verhältnis Datenschutz : Informationssicherheit

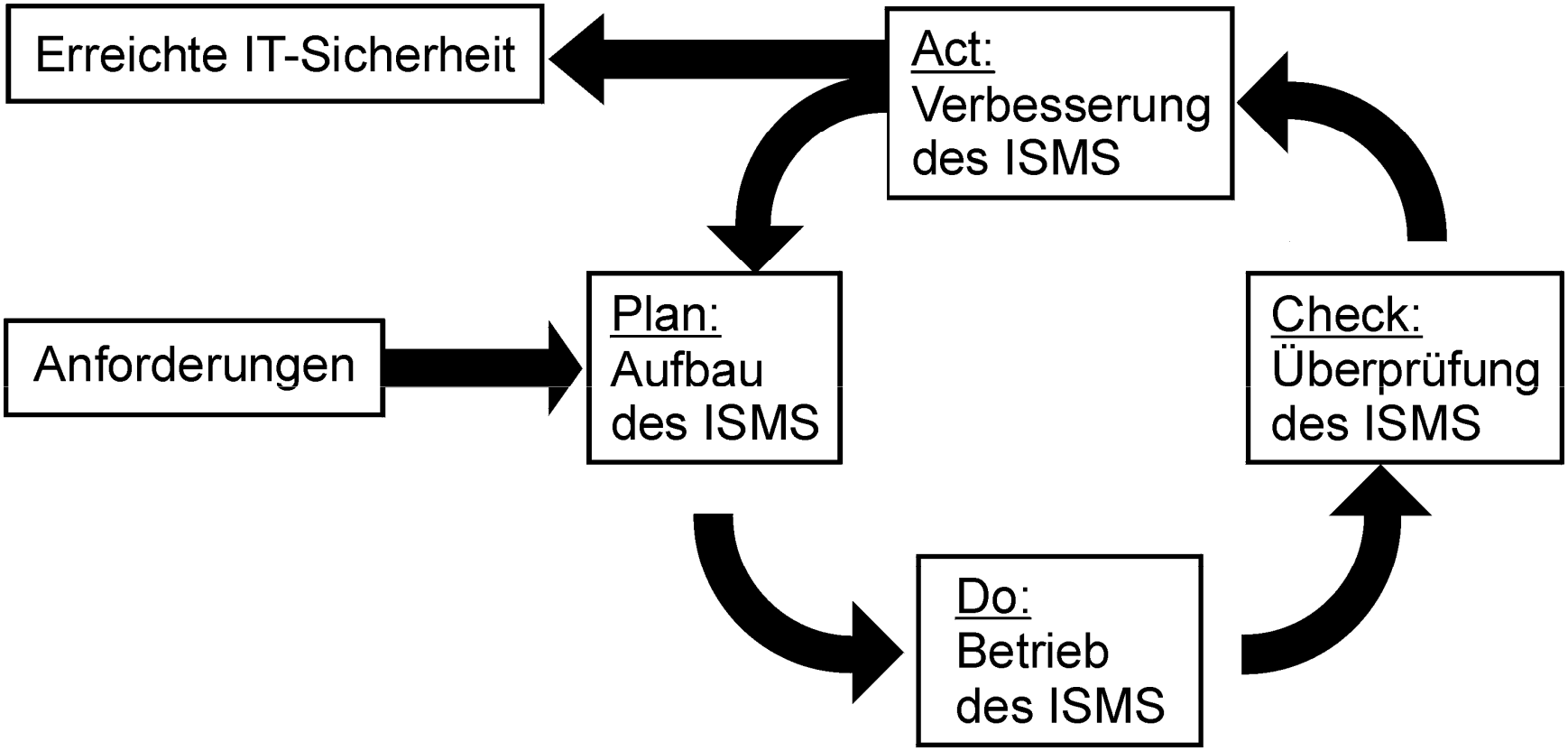
Informationssicherheit (1)

Informationssicherheit =

Schutz der Verfügbarkeit, Integrität und Vertraulichkeit (und ggf. weiterer Eigenschaften) von Informationen
(nach ISO/IEC 27001)

- → Gewährleistung von **Schutzzielen** (Verfügbarkeit, Integrität & Vertraulichkeit & ggf. weiterer Ziele)
- → betrifft alle Informationen eines Unternehmens: **Geschäftsgeheimnisse und Datengeheimnis**
- → **umfassender** als Datenschutz!
- → Information ist ein **hoher Vermögenswert**
- → verknüpft mit **IT-Risiko-Management**
- → Informationssicherheit ist Aufgabe des **Managements**

Informationssicherheit (2)



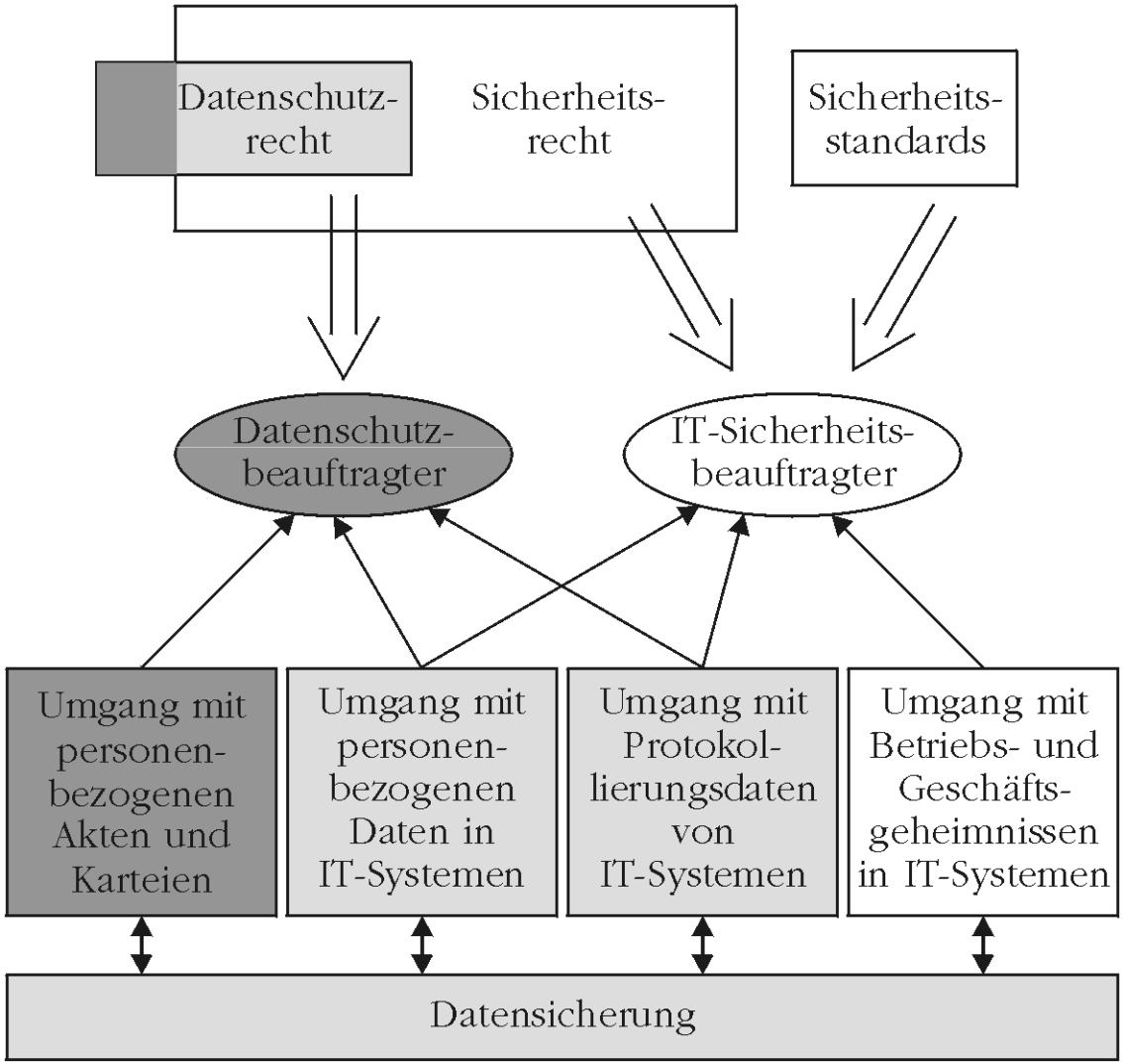
ISMS = Informationssicherheitsmanagementsystem

Informationssicherheit (3)

Zu treffende Regelungen zum ISMS in der Leitlinie (in Anlehnung an die ISO/IEC 27002):

- Festlegung der **Ziele** der umzusetzenden Informationssicherheit & deren **Bedeutung** für das Unternehmen (inkl. Aussage des Managements zur Priorisierung)
- **Geltungsbereich** der Leitlinie
- Beschreibung der **Anforderungen**
  - ° gesetzliche Vorgaben
  - ° anzuwendende Standards
  - ° zu beachtende Prinzipien
  - ° relevante Vorgaben durch vertragliche Vereinbarungen / SLAs
- Festlegung zentraler **Methoden**
  - ° IT Risk Assessment (zentral für die konkrete Planung der Maßnahmen!)
  - ° Business Impact Analysis (zentral zur Schutzbedarfsfeststellung!)
- Festlegung der **Verantwortlichkeiten**
- **Kommunikation**skonzept (inkl. zur Awareness)
- **Konsequenzen** für Nichtbeachtung der Vorgaben zur Informationssicherheit
- Auflistung des kompletten **Regelwerk**s zur Durchsetzung der Leitlinie (inkl. Konzepte, Verfahrensbeschreibungen, Dienstanweisungen, etc.), in denen die jeweiligen Einzelmaßnahmen zur Informationssicherheit festgelegt werden

Verschiedene Blickwinkel



Datenschutz versus Informationssicherheit?

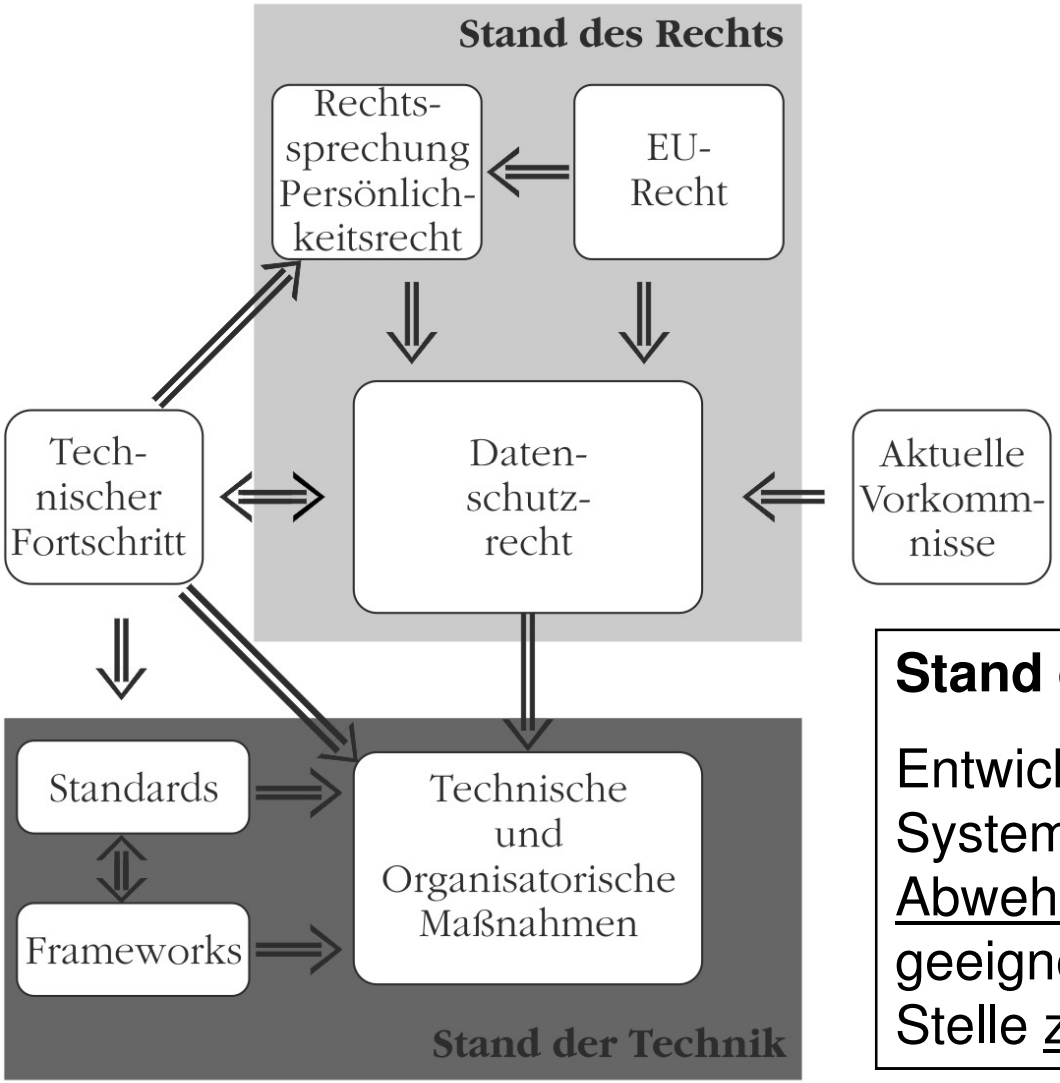
Auflösung folgender Zielkonflikte nötig:

- Datenschutz: Grundsatz der Datensparsamkeit
  IT-Sicherheit: Redundante Datensicherung zur Ausfallsicherheit
- Datenschutz: Informationelles Selbstbestimmungsrecht
  IT-Sicherheit: Nachvollziehbarkeit und Überwachung von Aktionen
- Datenschutz: Transparenz der Verfahren
  IT-Sicherheit: Geheimhaltung von Schutzmechanismen und Informationen
- Datenschutz: Inhaltsebene der Daten im Vordergrund
  IT-Sicherheit: Transportebene der Daten im Vordergrund
- Datenschutz: Vertraulichkeit zentral
  IT-Sicherheit: Vertraulichkeit nur ein Ziel unter vielen
- Datenschutz: Ausgangspunkt = Interesse von Betroffenen
  IT-Sicherheit: Ausgangspunkt = Interesse von Systembetreibern

→ Ausgleich möglich durch Konstruktion von IT-Systemen unter Beachtung des privacy by design principles

= Konstruktion eines IT-Systems, so dass dieses datenschutzrechtliche Anforderungen von sich aus bereits erfüllen kann

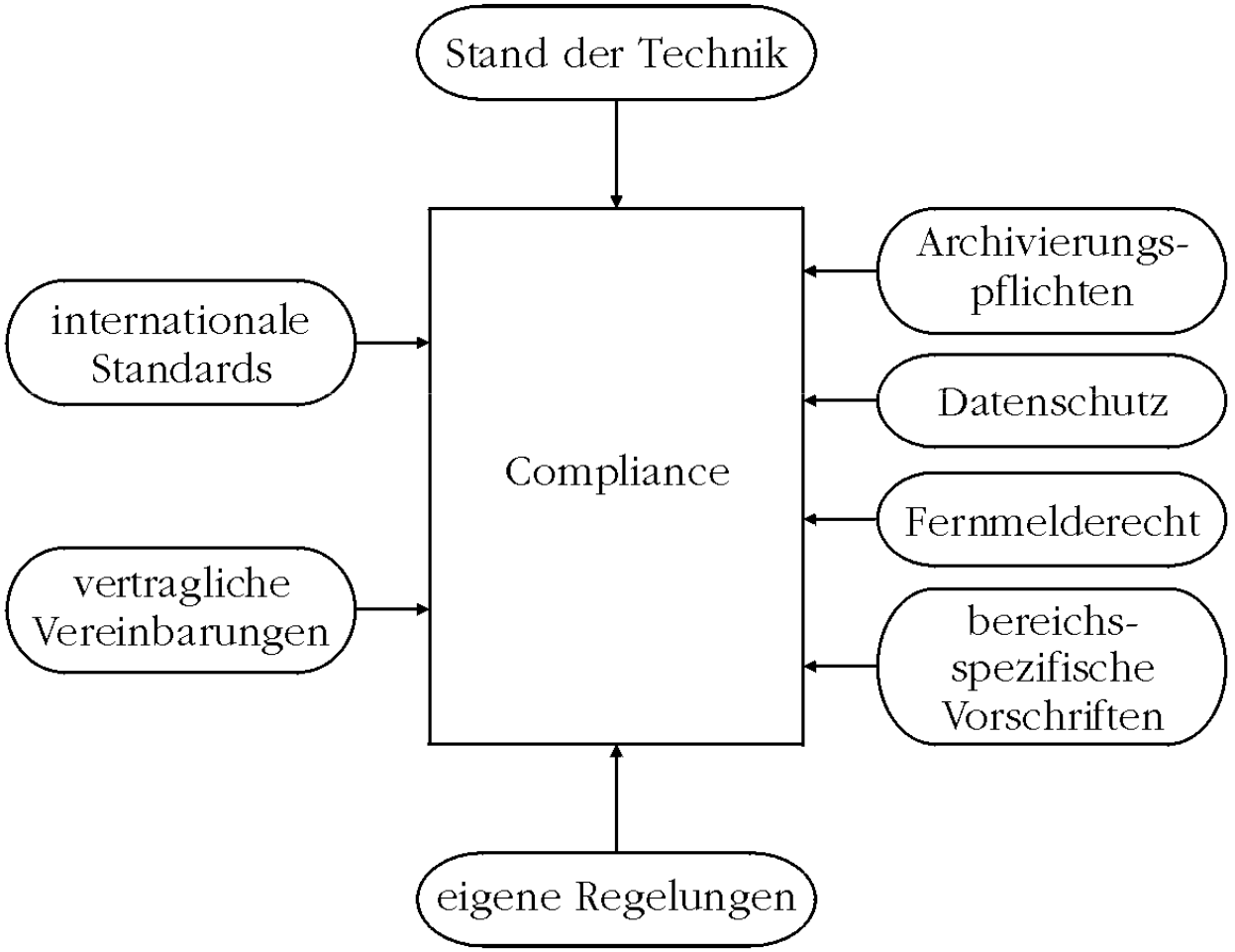
Verhältnis Datenschutz & Stand der Technik



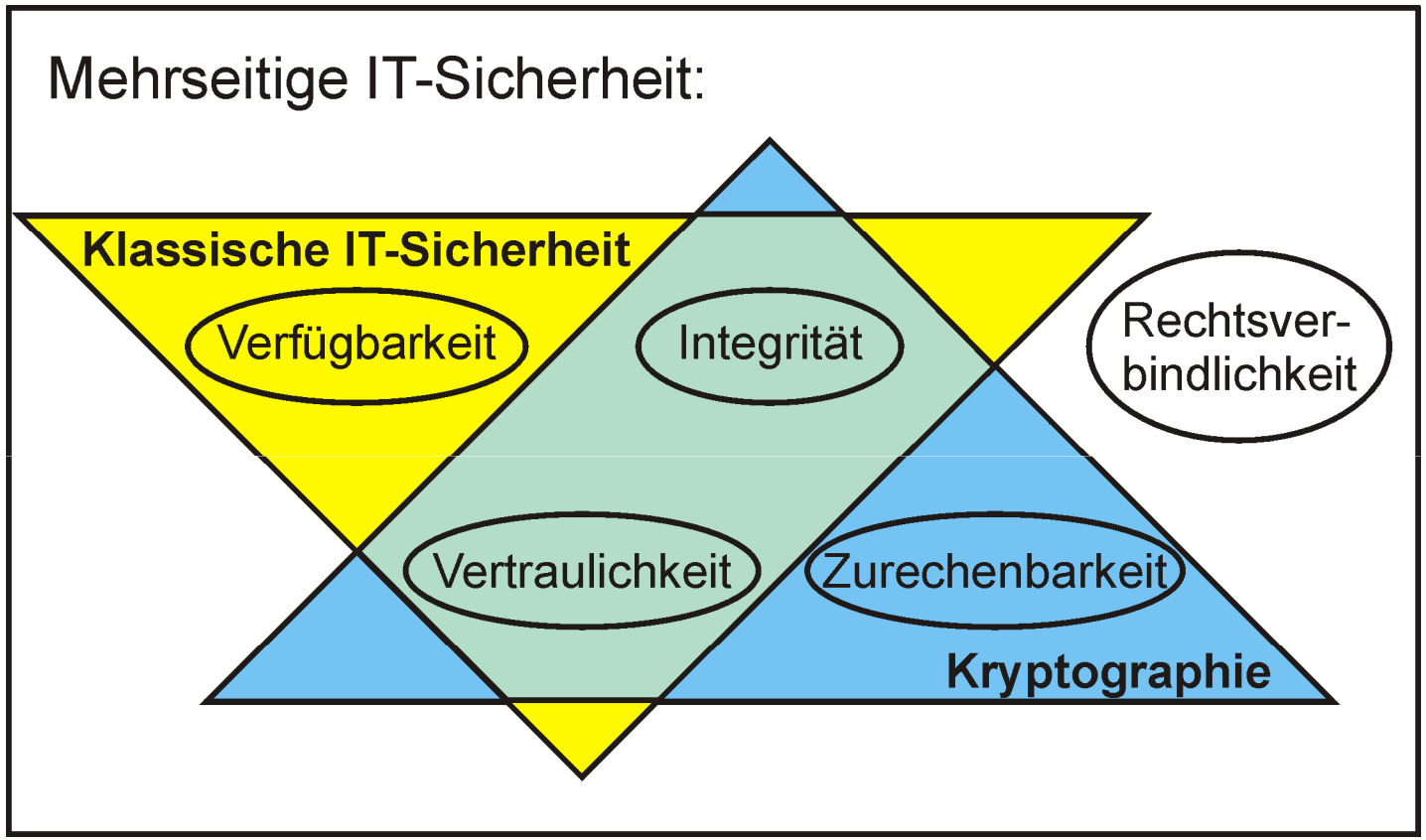
Stand der Technik =

Entwicklungsstand technischer Systeme, der zur vorsorgenden Abwehr spezifischer Gefahren geeignet und der verantwortlichen Stelle zumutbar ist

Anforderungen zur Compliance



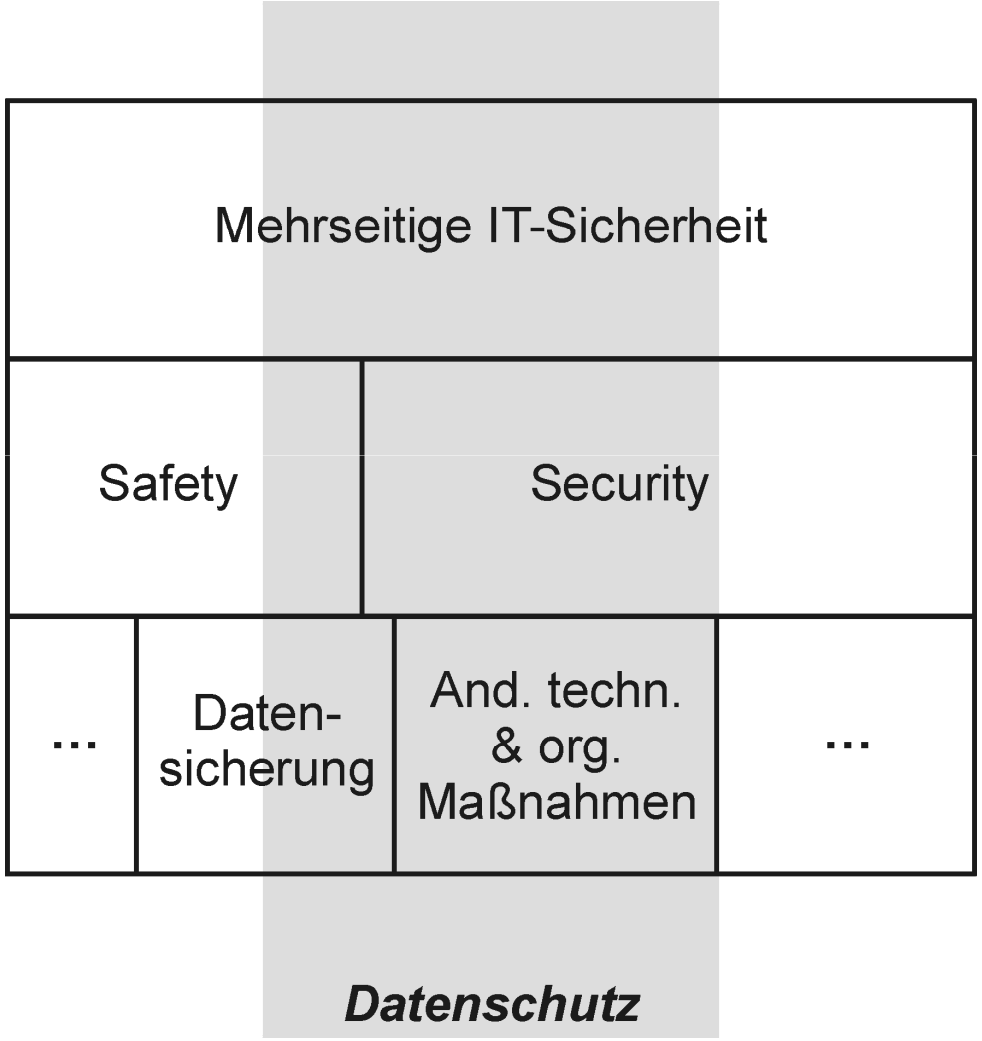
Information Security (1)



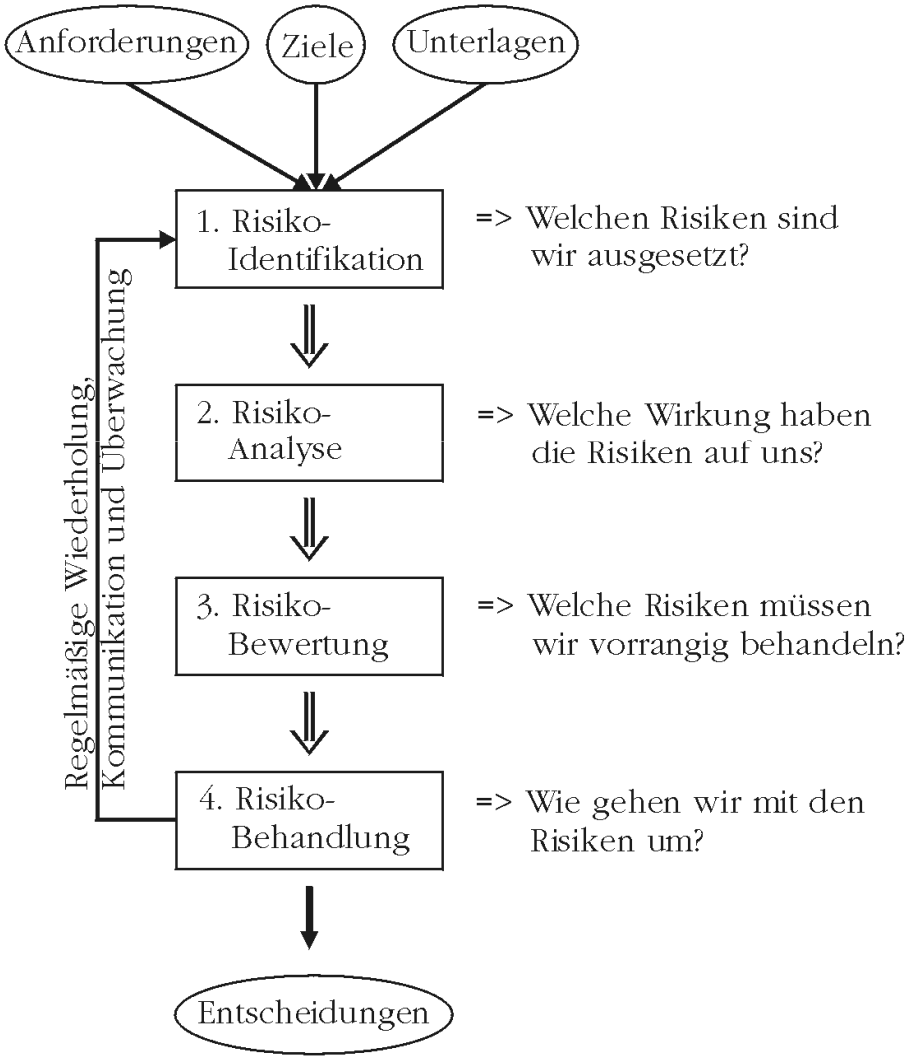
Ziel <u>Klassischer</u> IT-Sicherheit:
Verlässlichkeit der IT-Systeme

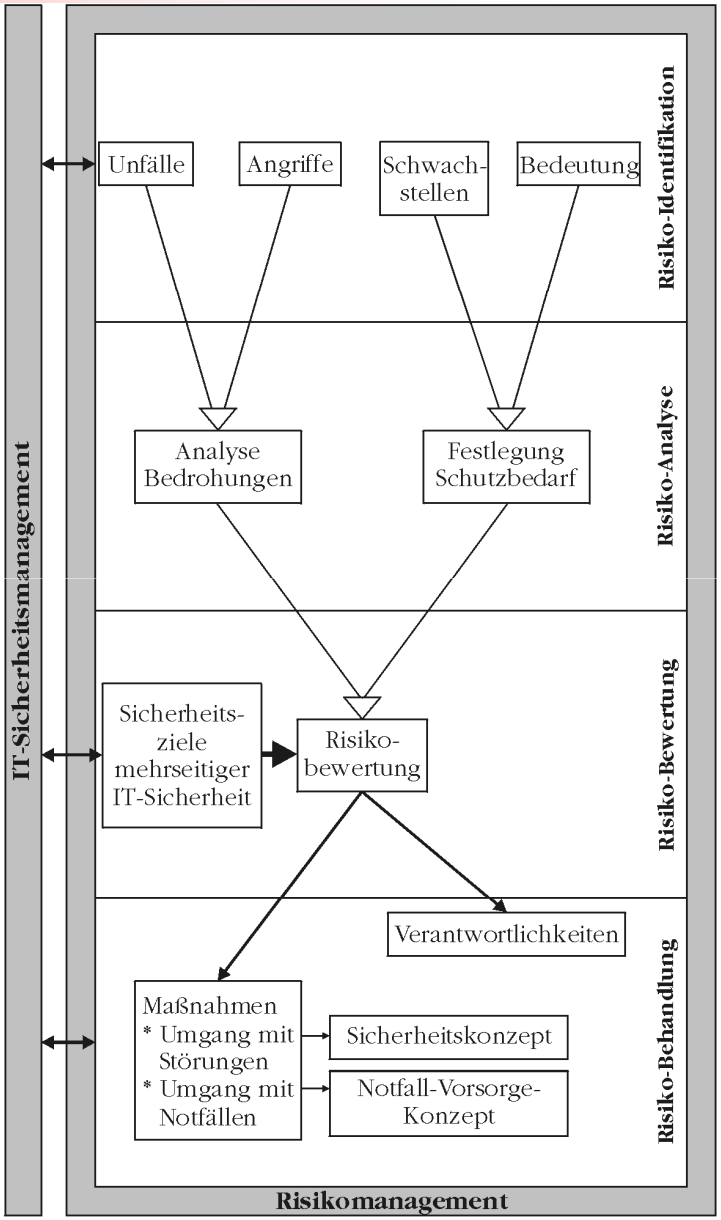
Ziel <u>Mehrseitiger</u> IT-Sicherheit:
Verlässlichkeit <u>und</u> Beherrschbarkeit der IT-Systeme

Information Security (2)

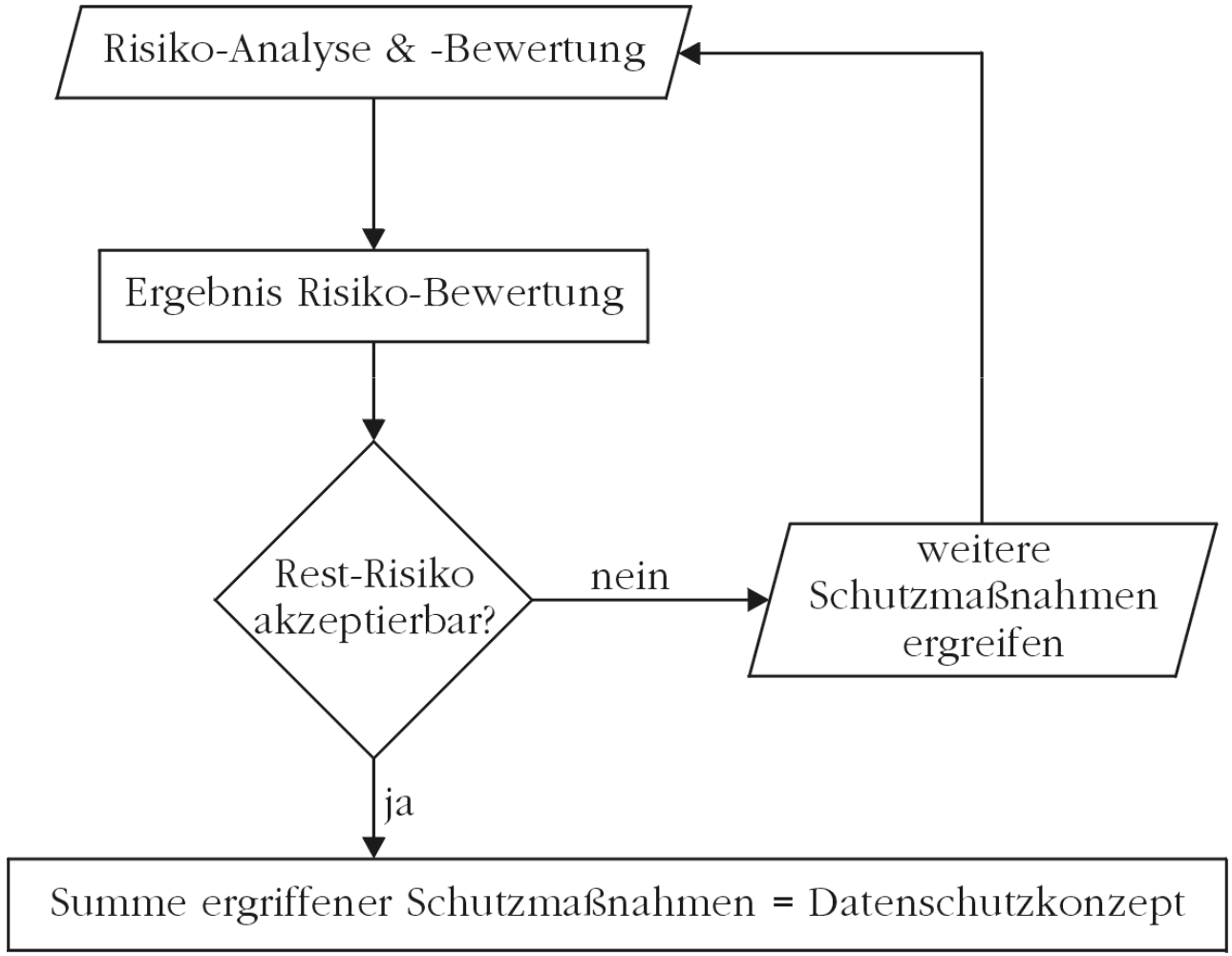


Information Security (3)





Information Security (4)



Folgen der IT auf das Datenschutzrecht

Zentrale Rolle der Informationstechnik

Informationen stellen einen besonderen „Rohstoff“ dar:

- Informationen sind **immateriell**
- **Wert** von Informationen **mal exponentiell**, **mal subtrahierend**
- Informationen sind **manipulierbar**
- Informationen auch **unbewusst oder ungewünscht übertragbar**
- **Zugang** zu **und Bewertung** von Informationen **entscheidet Zukunft**

→ „Rohstoff“ der IT setzt neue Maßstäbe! (auch für rechtliche Regelungen!)

Rasche Fortentwicklung der Informationstechnik:

- schnelle Fortentwicklung von IT-Systemen: **Verdoppelung** der Datenspeicherkapazitäten & Arbeitsgeschwindigkeit ca. **alle 2 Jahre**
- hohe **Komplexität** der i.d.R. vernetzten IT-Systeme
- **stark anwachsender** Sektor Informationswirtschaft
- **hohe Abhängigkeit** von IT-Systemen & Informationen
- **Allgegenwart** der Datenverarbeitung
- **Ambivalenz** technischer Entwicklungen

→ Technik der IT führt fortlaufend zu neuen Herausforderungen!

Folgen der IT auf das Datenschutzrecht

- Erst die automatisierte Verarbeitung mit ihren variablen Verknüpfungsmöglichkeiten führte zur Ausprägung des informationellen Selbstbestimmungsrechts!
- Datenschutzrecht muss sich auf rasche Fortentwicklung der IT fortlaufend neu einstellen
  → Regeln aus der Zeit zentraler RZs nicht mehr zeitgemäß
  → **Steuerung über Ziele** zeitgemäßer als über Kontrollbereiche
  → neue Technik erfordert Technikfolgenabschätzung (= **IT-Risiko-Management** im Rahmen der Vorabkontrolle)
  → **Schutzbedarf** der Daten (abhängig vom Zweck) maßgeblich für zu treffende Schutzmaßnahmen

Folgen des Datenschutzes auf die IT

Folgen des Datenschutzes auf die IT

- Es gibt zahlreiche Verfahren, bei denen personenbezogene Daten mittels IT-Systemen automatisiert verarbeitet werden
  → Datenschutz stellt wichtige Rahmenbedingung dar
- Zunehmende Internationalisierung & Arbeitsteilung zur Nutzung von IT-Systemen erfordert intelligente Systeme, die Datenschutz erfüllen können (→ **privacy by design**)
  → Datenschutz ist ein Entwicklungs-Treiber
- IT muss verschiedene Anforderungen erfüllen, zunehmend im Zusammenhang mit Datenschutz
  → Datenschutz ist **wichtiger Kern für Compliance**
  → IT wird so gesteuert, dass sie compliant ist
- Sorge vor Datenpannen führt zunehmend zur Implementierung von **Sicherheitsfunktionen** in IT-Systemen

Datenschutzfördernde Technik

Datensparsamkeit & Systemdatenschutz

- je weniger personenbezogene Daten herausgegeben werden (müssen), desto leichter lassen sich entsprechende Techniken anwenden

→ nur erforderliche Daten verarbeiten

→ frühestmögliche Anonymisierung

→ frühestmögliche Löschung

→ Verschlüsselung bei Kommunikation

Selbstdatenschutz & Transparenz

- Selbstbestimmung und Steuerung durch Nutzer

→ Nutzer entscheidet selbst, wie anonym er Dienste in Anspruch nimmt

→ Verarbeitung wird verständlich offengelegt (Verfahrensverzeichnis) und ist nachprüfbar (→ Identitätsmanagement)

→ Formulierung eigener Schutzziele

→ Nutzung vertrauenswürdiger Institutionen (Trust Center)

→ Unterstützung durch Anwendung der Betroffenenrechte

Fazit zum spannenden Verhältnis

IT & Datenschutz bieten ein spannendes Verhältnis

- Beide beeinflussen sich wechselseitig
- Datenschutz muss aktuelle IT-Entwicklung berücksichtigen
  → fortwährender Anpassungsbedarf
- IT muss Datenschutzkonformität unterstützen
  → Implementation des privacy by design principles
- Datenschutz ist wichtiger Bestandteil zur Compliance
- Steuerung der IT erfolgt über Informationssicherheit
- Informationssicherheit ist aber umfassender als Datenschutz
  → Management von Datenschutz als Teil des Managements von Informationssicherheit betrachten

it.sec GmbH & Co. KG
Einsteinstr. 55
D-89077 Ulm

USt Id Nr.: DE 225547544
Steuernummer: 88012/53709
Amtsgericht Ulm: HRA 3129

vertreten durch den **Geschäftsführer Dipl. Ing. (FH) Holger Heimann**

Haftender Komplementär:
it.sec Verwaltungs GmbH
Amtsgericht Ulm: HRB 4593
Einsteinstr. 55
D-89077 Ulm