interflex

Aus Daten werden Werte

Datenschutz in einem internationalen Unternehmen

Referat für den AK Sicherheit eco Verband, im Rahmen der it-sa, 2010 in Nürnberg

20.10.2010, Heinz Schumacher

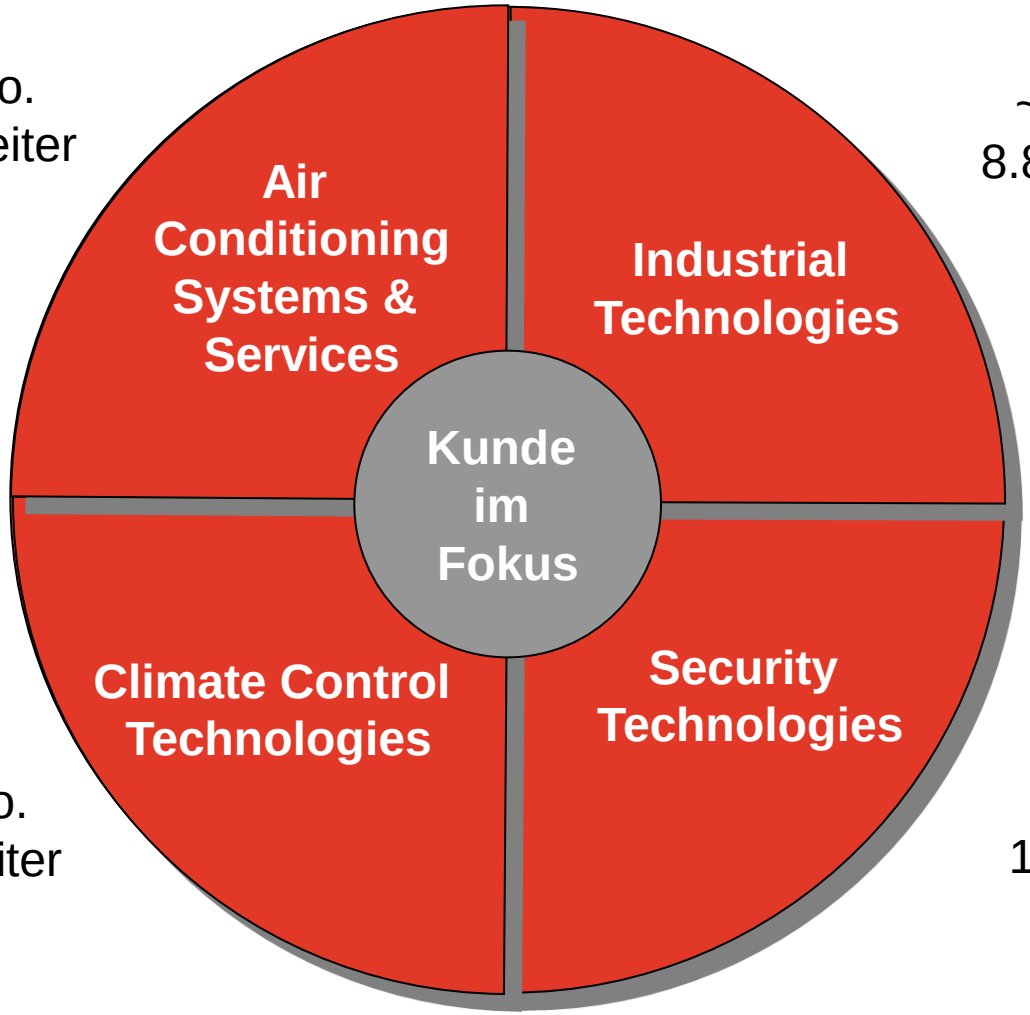
Ingersoll Rand
Security Technologies

Interflex und Ingersoll Rand

Wir sind Teil einer der größten und traditionsreichsten Industriemischkonzerne der Welt.

Die Ingersoll Rand Sektoren

Umsatz:
~ $ 8.000 Mio.
32.000 Mitarbeiter
weltweit

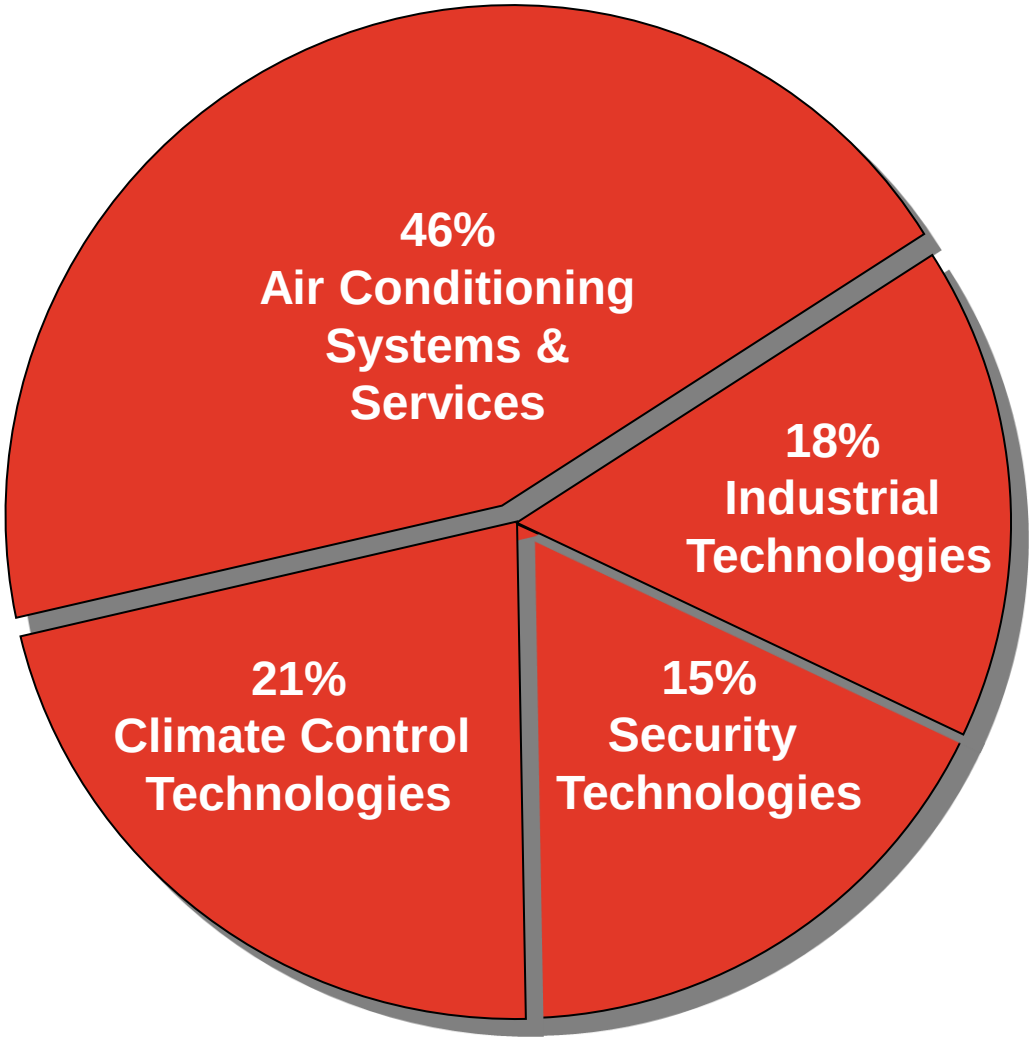


Umsatz:
~ $ 3.000 Mio.
8.800 Mitarbeiter
weltweit

Umsatz:
~ $ 3.000 Mio.
10.000 Mitarbeiter
weltweit

Umsatz:
~ $ 3.000 Mio.
11.400 Mitarbeiter
weltweit

Anteile Sektoren am Gesamtumsatz



Security Technologies

Technologien für Sicherheit

Produkte und Komplett-Lösungen zur Sicherung von Gebäuden und Anlagen sowie für Zeiterfassung und Personaleinsatzplanung

interflex

BRICARD

Normbau

CISA

Ingersoll Rand
Security Technologies

Unsere Daten

Interflex

Gründung: 1976

Mitarbeiter: 499 (Europa)

Hauptsitz: Stuttgart / Deutschland

Umsatz 09: 75 Mio. € (Europa)

Unsere Geschäftsfelder

Themeninhalte

- Einleitung Datenschutz (nur als hand out)
- Elemente eines Unternehmens
- Management- und Unterstützungsprozesse
- Typische Konzerninteressen
- Konzernorganisation, Theorie und Praxis
- Technische und organisatorische Maßnahmen
- Externe Datenverarbeitung
- Unterscheidung Datenübermittlung und ADV
- Fallbeispiel

Einleitung Datenschutz

Der Schutz personenbezogener Daten ist ein Grundrecht

- Jeder soll **selbst** über die Preisgabe und Verwendung seiner persönlichen Daten **bestimmen** (Informationelle Selbstbestimmung)

- Es gilt das Verbot mit Erlaubnisvorbehalt durch das BDSG, andere gültige Rechtsvorschriften oder die freiwillige Einwilligung des Betroffenen

Einleitung Datenschutz

Der Umgang mit personenbezogenen Daten wird durch das Datenschutzrecht geregelt.

- Es kommt zur Anwendung, wenn Daten, die **einem Menschen zugeordnet** werden können, erhoben, verarbeitet oder genutzt werden.
- Daten von **juristischen Personen**, Vereinen, Verbänden etc. sind durch das BDSG nicht geschützt.

Einleitung Datenschutz

Personenbezogene Daten

Einige Beispiele:

- Name, Vorname
- Geburtsdatum
- Anschrift
- Wohnverhältnisse
- Bankverbindungsdaten, Kreditkartennummer
- Vermögensverhältnisse
- Telefonnummer

Einleitung Datenschutz

Personenbezogene Daten

Zu den persönlichen Daten/ personenbezogenen Daten zählen auch:

- das gesprochene Wort,
- verfasste, persönliche Texte (Briefe etc.),
- das eigene Bild (Photo/ Video),
- soziale Daten,
- Diagnosedaten

Einleitung Datenschutz

Besondere Arten personenbezogener Daten

sind Angaben über:

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder philosophische Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit oder Sexualleben

Einwilligung: Form und Inhalt

Der Betroffene muss ausreichend informiert sein

Die Einwilligung

- muss schriftlich erfolgen
- muss optisch deutlich erkennbar sein, wenn sie zusammen mit anderen Erklärungen erfolgen soll
- muss besondere Arten personenbezogener Daten gesondert ausweisen

Bei der Erstellung solcher Vereinbarungen stets Ihren DSB einschalten.

Einleitung Datenschutz

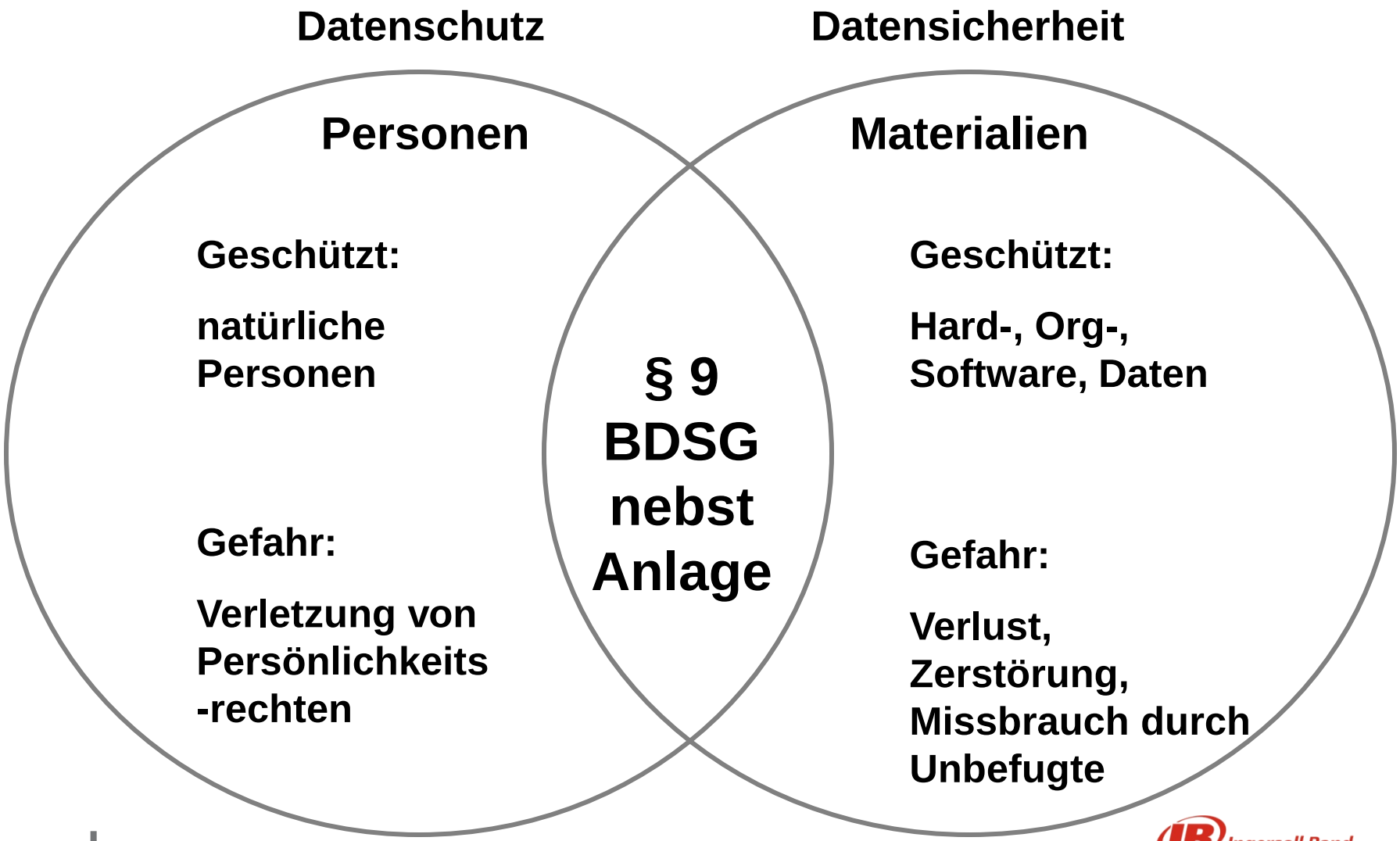
Erlaubnisbeispiele

Erlaubt ist u.a. das Erheben, Verarbeiten oder Nutzen, wenn

- die Daten aus öffentlichen und frei zugänglichen Quellen stammen (z.B. Telefonbuch)
- dies der Begründung/ Erfüllung eines Vertrags dient (Arbeits-, Kauf- oder Mietvertrag, Versicherungen)
- es zur Wahrung berechtigter Interessen erforderlich ist, ohne dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegt.
- eine gesetzliche Vorschrift die Verarbeitung der Daten fordert (Konfession wegen Besteuerung)
- eine schriftliche, freiwillige Einwilligung des umfassend informierten Betroffenen vorliegt

Einleitung Datenschutz

Abgrenzung zwischen Datenschutz und Datensicherheit



Einleitung Datenschutz

§ 9 BDSG: Auszug Technisch organisatorische Maßnahmen (TOM)

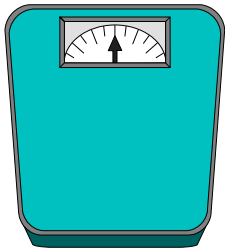
Werden personenbezogene Daten….
Dabei sind insbesondere Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind. Insbesondere sind dies:

Zutrittskontrolle,	Gebäude- Raumzugang
Zugangskontrolle,	Netz- Rechnerzugang
Zugriffskontrolle,	Zugriff auf einzelnen Datensatz
Weitergabekontrolle,	Schutz auf Transportweg
Eingabekontrolle,	Was, wann, von wem verändert
Auftragskontrolle,	Ext. DV regeln/ überwachen
Verfügbarkeitskontrolle,	Ausfall, Maßnahmen wie Raid
Trennungsgebot,	pro Zweck getrennte Ausgaben

Personenbezogene Daten und Datengeheimnis

- Was fällt unter das Datengeheimnis?

- Sachliche oder persönliche Verhältnisse einer natürlichen Person (z.B. Gewicht, Geburtsdatum, Sparbuch, Attest etc.)

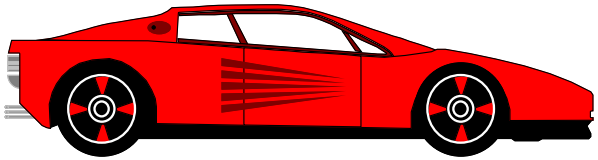


§ 3 Abs. 1 BDSG:
Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener).

Personenbezogene Daten und Datengeheimnis

- Was fällt nicht unter das Datengeheimnis?

- Sichtbare sachliche Verhältnisse
  (z.B. wer hat welches Auto ?)



- Sachliche Verhältnisse einer juristischen Person
  (z.B. Veröffentlichte Firmenergebnisse einer AG)

Einleitung Datenschutz

Datenschutzrechtliches Grundproblem Nr. 1:

- **Erfahrungsfreies Wissen**
  Der Betroffene hat kein informationelles (Mit-) Entscheidungsrecht. Er weiß nicht was an welcher Stelle über ihn gespeichert und wie es genutzt und verknüpft wird.

- Entweder Regelung per Gesetz (Geheimdienst) oder Betroffene **müssen** informiert werden.

Einleitung Datenschutz

Datenschutzrechtliches Grundproblem Nr. 2:

- Entscheidungsabläufe können durch

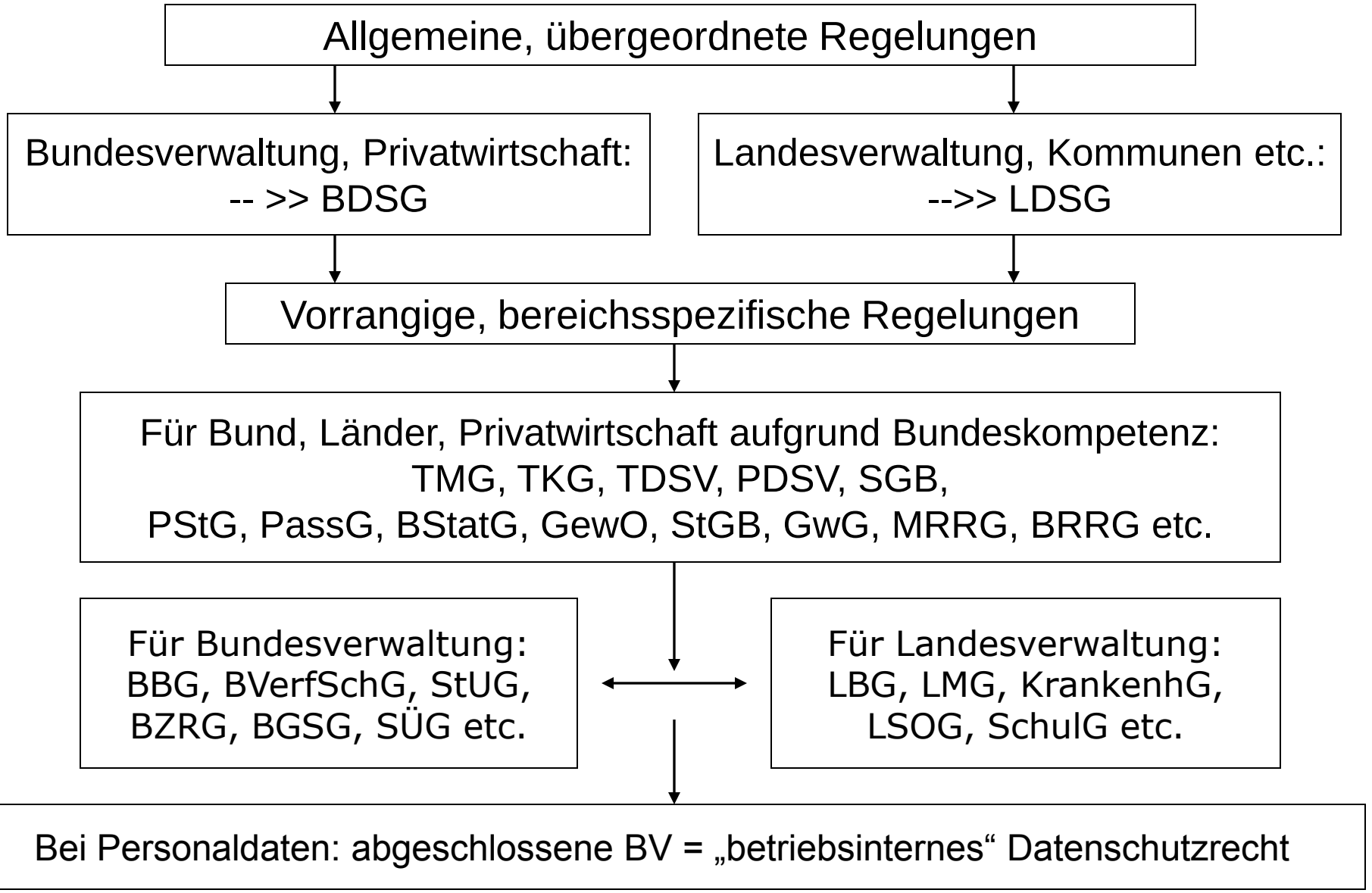
  verkürzte Nutzung von Daten

  oder durch

  falsche, unzulässige Verknüpfung von Daten

  negativ für den Betroffenen beeinflusst werden

Einleitung Datenschutzrecht + Zuständigkeiten



Elemente eines Unternehmens

- Geschäftsidee/ Geschäftsmodell

  Produkte → Fertigung und/ oder Handel

- Interessenten/ Kundengewinnung

  Werbung, Akquise, Beratung, Vertrag

- Kundenservice

  Service, Vertragsverwaltung, Bestandsverwaltung und Mahnwesen

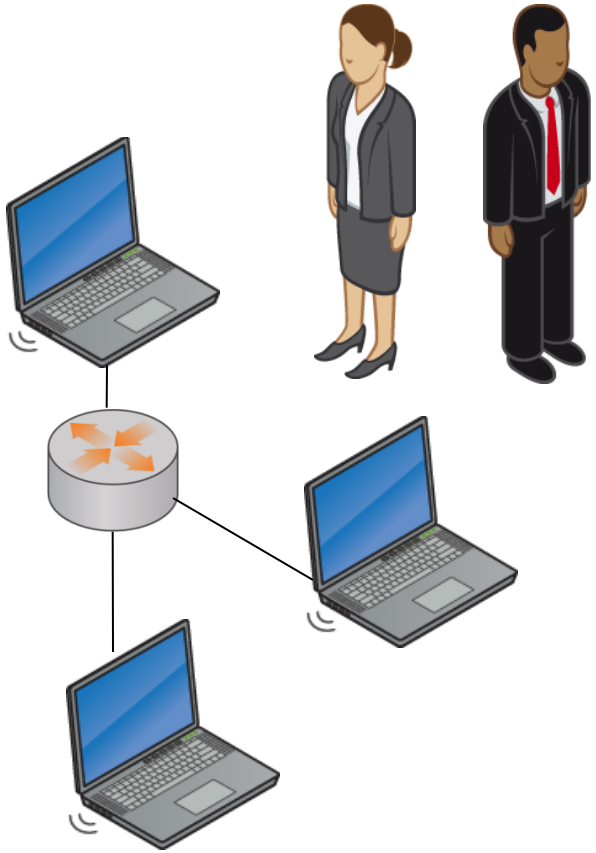
Management Prozesse

Personal und Daten für:

- Steuerung →
  Prozess-, Projekt- und Organisationsmanagement
- Planung →
  Personal-, Wirtschafts- und Finanzplanung
- Controlling →
  Risikomanagement und Finanzcontrolling
- Überwachung →
  Compliance, Datenschutz und Revision

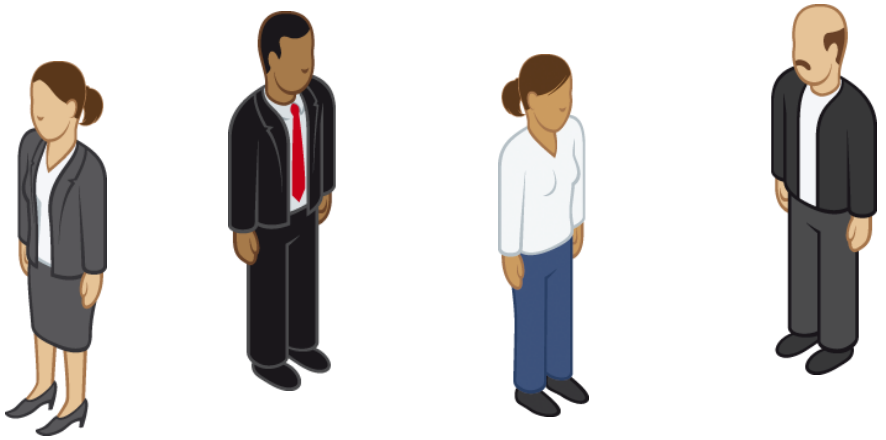
Unterstützungsprozesse

- Personalverwaltung, Personalentwicklung
- Verkaufsförderung, Vertriebsunterstützung, Provisionsabrechnung
- Warenwirtschaft, Beschaffung
- Rechnungserstellung
- Buchhaltung
- Druck- und Formularwesen
- Information, Kommunikation
- Postwesen
- Aktenverwaltung, Archivierung



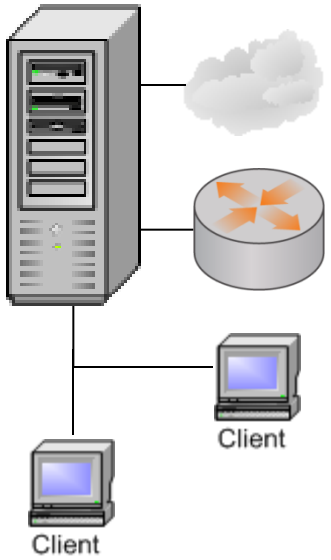
Datenkategorien im Unternehmen

- Arbeitnehmerdaten
- Lieferantendaten
- Interessentendaten
- Kundendaten
- Vertragsdaten



- Technische Daten
- Wirtschaftsdaten
- Finanzdaten

IT- Konzept, IT- System



IT - Komponenten

Ein internationales Unternehmen

- entsteht durch eigene Expansion mittels Gründung ausländischer Filialen/ Büros, Vertretungen, Produktionsstätten
  oder
  durch Zukauf fremder Firmen im Ausland, einschließlich deren Übernahme/ Fusion.

- Ein Konzern entsteht immer durch Zukauf von rechtlich selbstständigen Firmen im Inland und/ oder Ausland. Dabei hält die Konzernmutter die Mehrheit der Anteile.

Datenschutz im internationalen Konzern

- Datenschutzrechtlich komplexer ist in jedem Fall ein internationaler Konzern

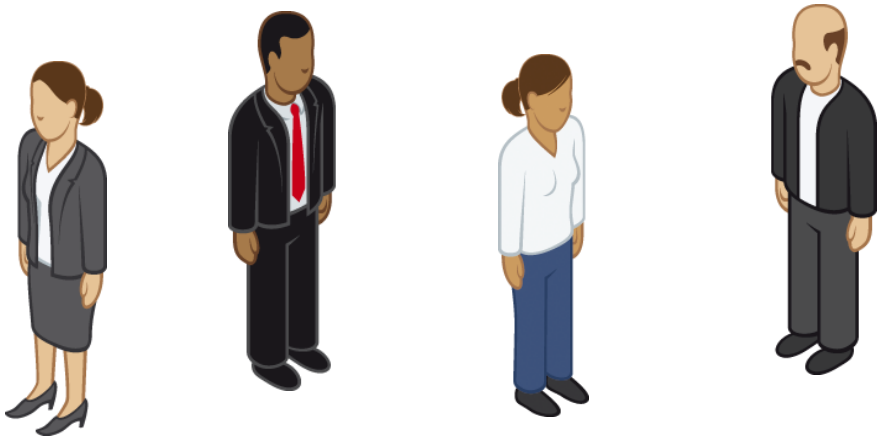
  Grund  :

  - Datentransfer zwischen rechtlich selbstständigen Firmen, der Konzernmutter und unterschiedlichen Ländern

  - Das deutsche Datenschutzrecht kennt kein Konzernprivileg

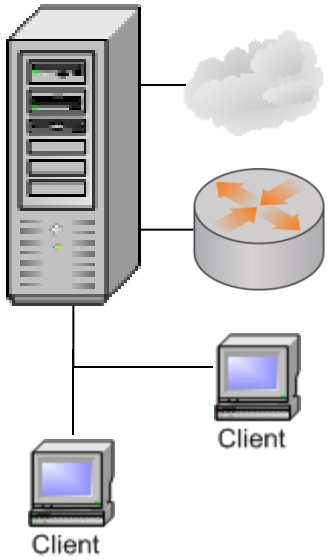
Datenkategorien in Tochter 1 - n

- Arbeitnehmerdaten
- Lieferantendaten
- Interessentendaten
- Kundendaten
- Vertragsdaten



- Technische Daten
- Wirtschaftsdaten
- Finanzdaten

IT- Konzept, IT- System



IT - Komponenten

Typische Konzerninteressen

- Vereinheitlichung sowie Zentralsierung der Prozesse und Hilfsmittel zum Zwecke aktueller, abrufbarer Informationen statistisch und detailliert, wie z.B. für Personal, Personalkosten, IT, Wirtschaftsdaten, Finanzen, etc.
  - Zentrales Personalverwaltungssystem
  - Zentrales Bildungswesen mittels elektronischer Universität
  - Zentrales Zielvorgabe- und Beurteilungssystem
  - Zentrales Reisekostenmanagement
  - Zentrale IT
  - Einkauf und Lieferantenmanagement
  - Zentrales Buchhaltungssystem, Kreditoren, Debitoren, Mahnwesen
  - Zentrale Überwachung von CoC und Ethikrichtlinien

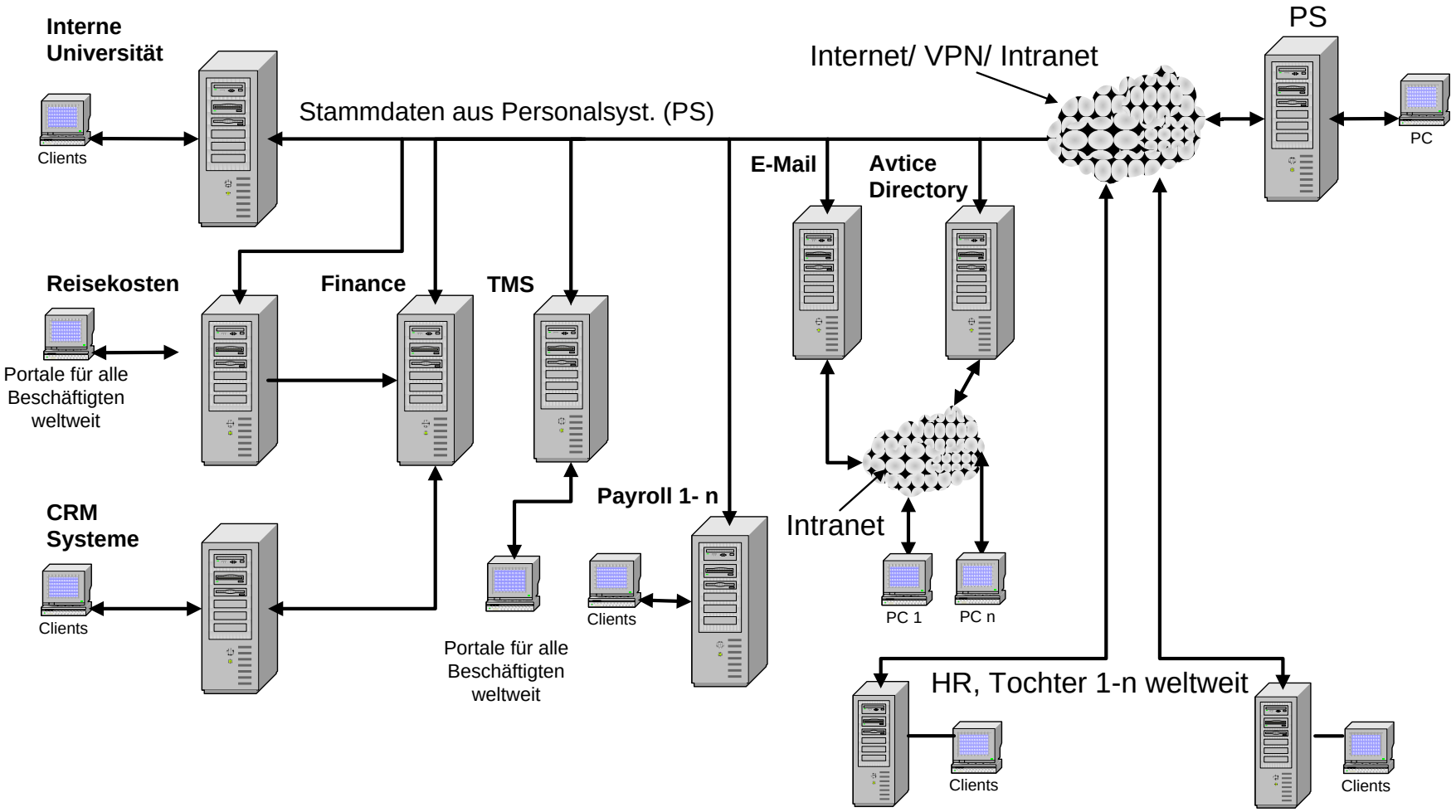
Verbreitete Konzernorganisation

Pro Tochter, da unterschiedlich

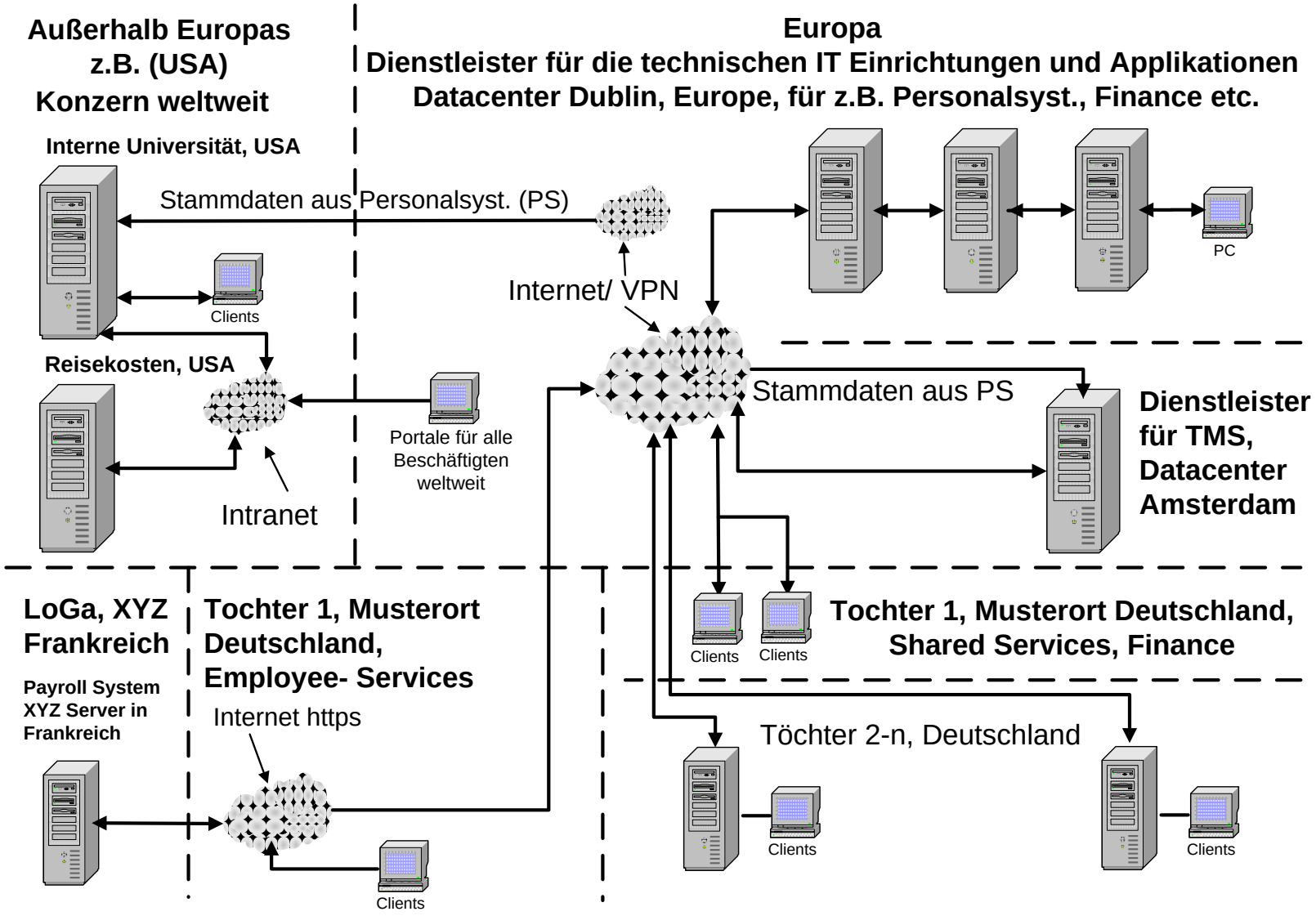
Shared Services, zentrale Elemente, gemeinsam für alle Töchter

Beispiel einer Konzernorganisation (1)

Führendes System im weltweiten Konzern = Personalverwaltungssystem (PS)



Beispiel einer Konzernorganisation (2)



Datenschutz (technisch), Einrichtungen

- **Technische** und organisatorische zentrale Maßnahmen zum Schutz von Daten jeglicher Art:
  - Firewall
  - Antivirensoftware mit automatischen Updates
  - Emailfilterung mit Sperrung verdächtiger Anhänge
  - Gesicherte Übertragungsmechanismen im Intranet
  - Active Directory für Berechtigungen und Zugang zum Intranet
  - Automatische Erfassung/ Meldung installierter Programme auf lokalen Systemen
  - CSA Security Agent
  - SCCM für automatische Softwareupdates
  - Redundante gesicherte Datacenter
  - Passwortpolicies mit automatischer Überwachung

Datenschutz (organisatorisch), Personal

- Technische und **organisatorische** Maßnahmen zum Schutz von Daten jeglicher Art beim Beschäftigten:
  - Jährliche CB-Trainings Code of Conduct mit Verpflichtung
  - Regelmäßige Datenschutzunterweisungen
  - Schutz lokaler Rechner/ geeignete, geheime Passwörter
  - Bildschirmschoner mit Passwortschutz aktivieren
  - Emailanhänge mit Zip Programm und 256 Bit Verschlüsselung passwortgeschützt versenden
  - Daten auf Servern mit automatischer Backupfunktion ablegen
  - Regelmäßige verschlüsselte Backups lokaler Daten auf externe Laufwerke
  - Daten lokal in verschlüsselten Containern verarbeiten
  - USB- Sticks nur mit verschlüsselten Containern verwenden

Datenschutz (rechtlich) im Konzern

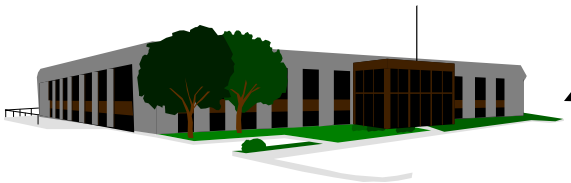
- Einhalten der datenschutzrechtlichen Vorschriften:
  - Prüfen der Rechtmäßigkeit von Datenerhebung, Verarbeitung und Nutzung
  - Detaillierte Vorabkontrollen durchführen
  - Prüfung der Zweckbestimmung und der Datenempfänger zur Entscheidung, welche Vertragsarten zu verwenden sind.
  - In Zweifelsfällen „Sachfrage mit beratender Stellungnahme“ an die zuständige Landesaufsichtsbehörde für Datenschutz und Informationsfreiheit senden
    → dringend zu empfehlen, da höhere Rechtssicherheit und in dem angefragten Fall keine Überraschungen bei Kontrolle seitens der Behörde zu erwarten sind.
    Meine Erfahrung:
    Zusammenarbeit sehr sinnvoll und hat sich bestens bewährt.

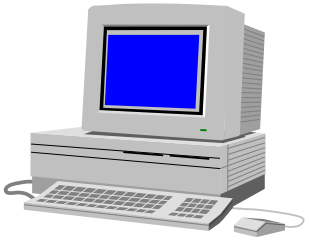
Externe Datenverarbeitung 1

Funktionsübertragung

Auftraggeber

Auftragsdatenverarbeitung





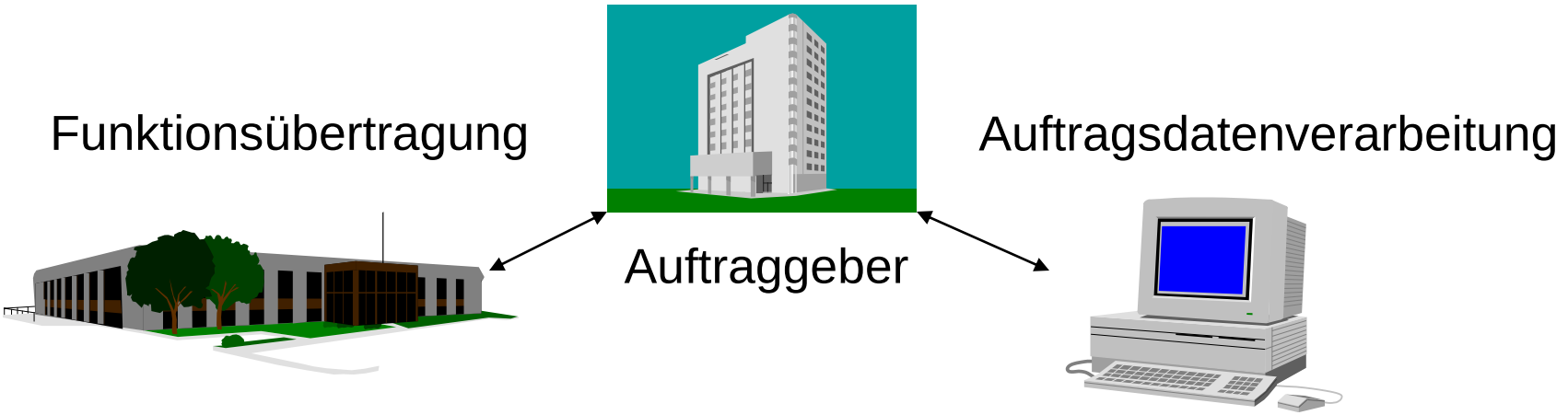
Dritter,
der eigenverantwortlich mit DV beauftragt wird.

Daten werden übermittelt.

Auftragnehmer (kein Dritter)
Erhebung, Verarbeitung, Nutzung personenbezogener Daten nach Weisung (§11)

Serviceunternehmen für Hard- und Software bzgl. des Zugriffs auf personenbezogene Daten

Externe Datenverarbeitung 2



Kriterien für Funktionsübertragung:

- die Nutzung der Daten für eigene Zwecke des Funktionsnehmers
- eine Dienstleistung, die über die praktisch technische DV hinausgeht
- das Fehlen der Möglichkeit des Funktionsgebers, auf die einzelnen Phasen der DV Einfluss zu nehmen

Kriterien für Auftragsdatenverarbeitung:

- keine Entscheidungsbefugnis über die Daten beim Auftragnehmer
- ein Auftragsschwerpunkt, der auf die praktisch technische Durchführung der DV gerichtet ist
- das Fehlen einer eigenständigen rechtlichen Beziehung des Auftragnehmers zum Betroffenen

Datenschutzrechtlicher Unterschied

Funktionsübertragung/ Datenübermittlung:

- sie muss rechtmäßig sein (§ 28 BDSG) → im Konzern meistens Interessenabwägung, BV/ Einwilligung
- ist eine Datenübermittlung, der Datenimporteur verwendet die Daten für eigene Zwecke
  - Personalverwaltung, Systeme für Personalentwicklung
  - Zentrales Bildungswesen
  - Zentraler Einkauf
  - Zentrale Buchhaltung
- Vertrag zwischen Datenexporteur und Datenimporteur, bei Drittstaaten EU Standardvertrag mit Originalklauseln
- Wichtig: Benachrichtigung der Betroffenen

Datenschutzrechtlicher Unterschied

Auftragsdatenverarbeitung:

- Erfordert Vertrag gemäß § 11 BDSG, bei Drittstaaten EU Standardvertrag mit Originalklauseln (Bußgeld).
- Vorgabe und regelmäßige Kontrollen der Datenverarbeitung sowie der technischen und organisatorischen Maßnahmen durch den Auftraggeber.
- Beispiele der Auftragsdatenverarbeitung:
  - Externe Datacenter (z.B. ACS, Microsoft etc.)
  - Gehaltsabrechnung
  - Lettershop
  - Systeme für Emailmassenversand
  - IT – Dienstleistungen und Wartungsverträge
- Wichtig: Benachrichtigung der Betroffenen

Die Rechte des Betroffenen

Bei der Auftragsdatenverarbeitung und/ oder Datenübermittlung müssen die Rechte des Betroffenen in jedem Falle gewahrt bleiben:

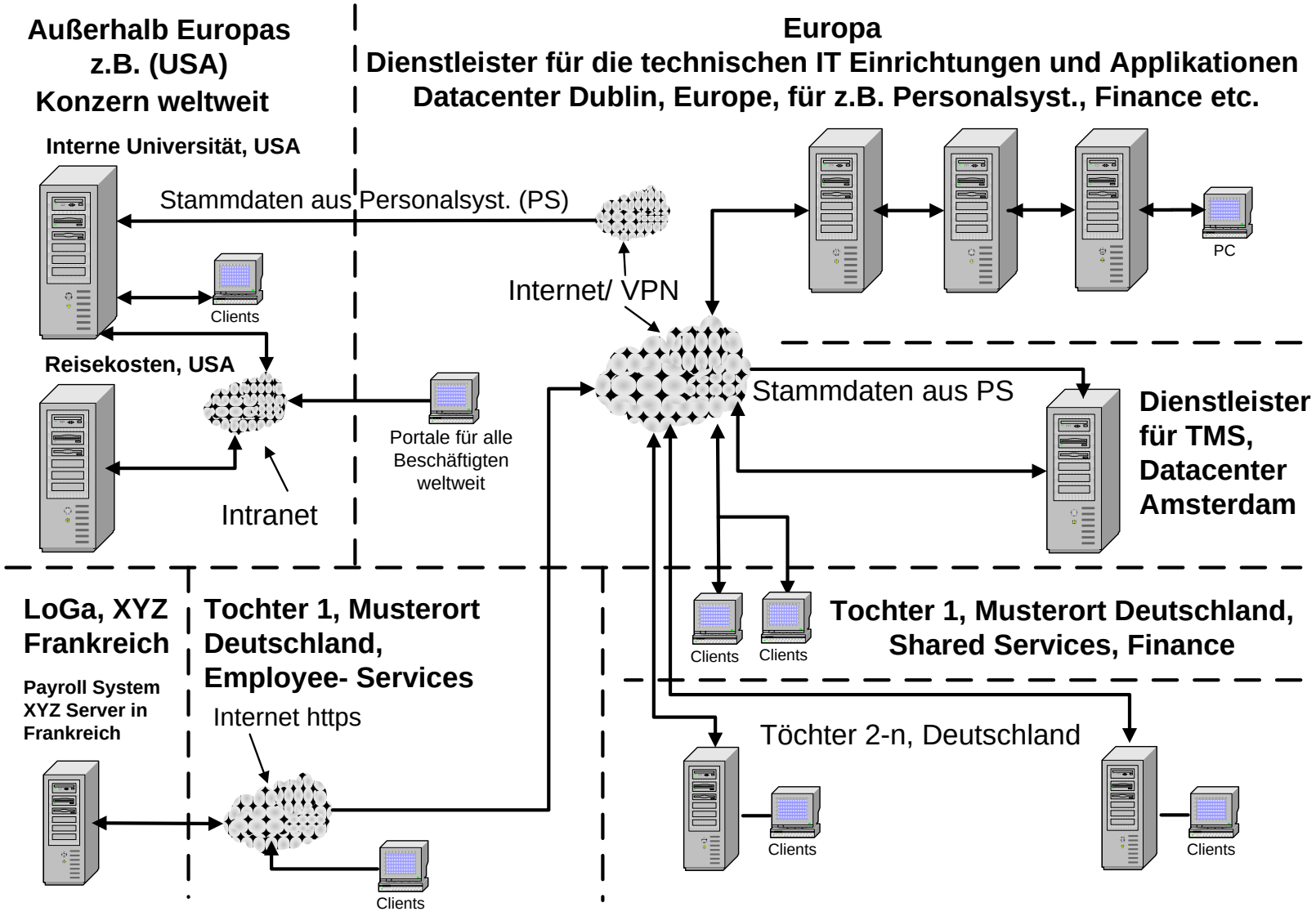
- Information bei Erhebung oder Benachrichtigung bei erstmaliger Speicherung
- Auskunftsrecht:
  welche Daten, Herkunft und Datenempfänger
- Berichtigungsanspruch
- Löschungsanspruch
- Sperrungsanspruch

Warum Datenschutzverträge?

Die verantwortliche Stelle (Datenexporteur) haftet **immer** gegenüber Beschäftigten/ Betroffenen. Deshalb auch stets einen Datenschutzvertrag bei der Datenübermittlung abschließen, der u. a. die Rechte des Betroffenen gewährleistet:

- Benachrichtigung
- Auskunftsrecht
- Berichtigungsanspruch
- Löschungsanspruch
- Sperrungsanspruch

Beispiel einer Konzernorganisation (2)



Was tun bei gemischten Anwendungen?

Bei gemischten Anwendungen, die sowohl Tätigkeiten im Sinne einer Auftragsdatenverarbeitung als auch Tätigkeiten im Sinne einer Funktionsübertragung/ Datenübermittlung beinhalten, ist es empfehlenswert, vertragsmäßig die Funktionsübertragung mit präziser Definition der Zweckbestimmung einzusetzen.

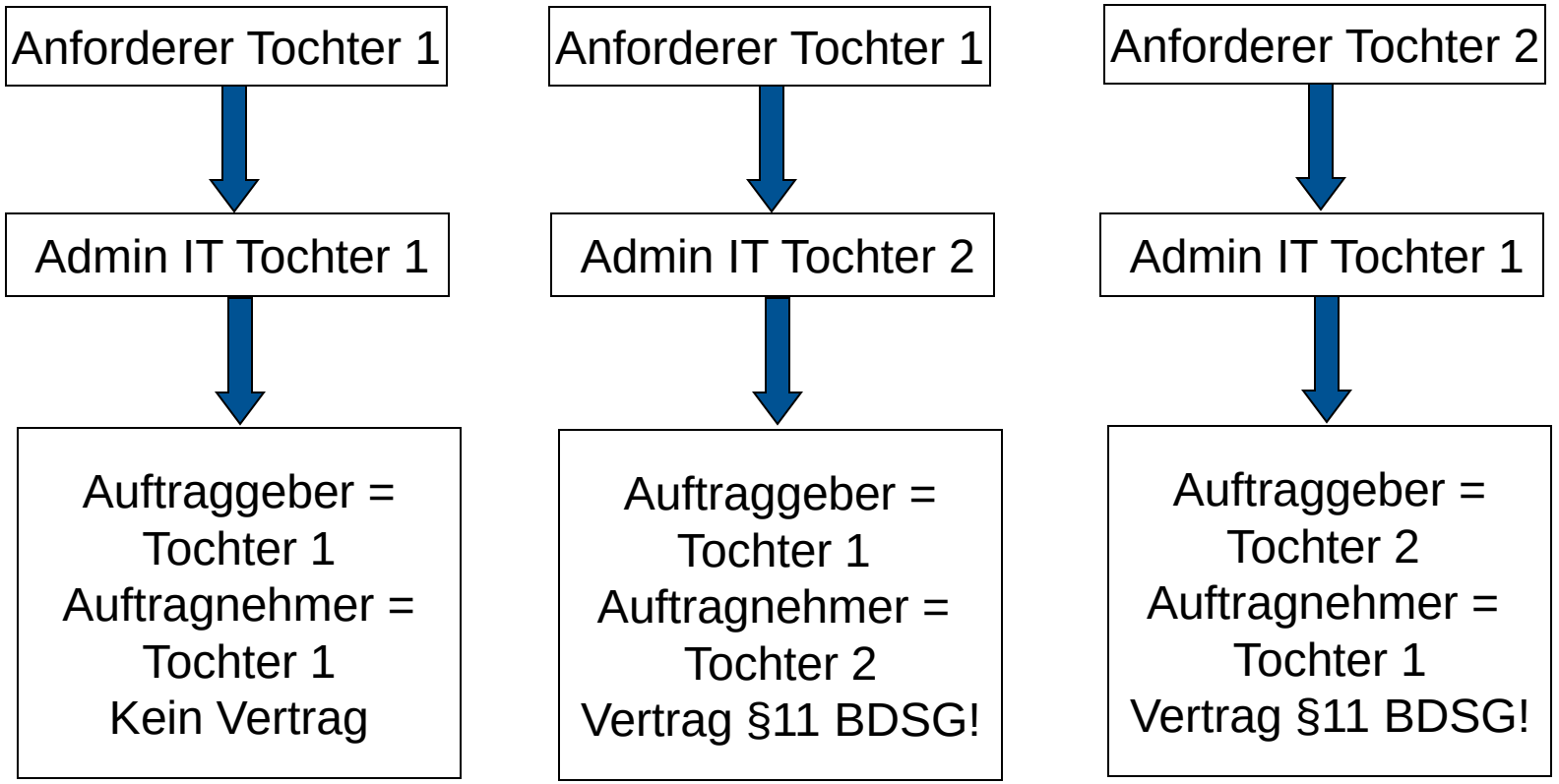
Zuständigkeiten

- Der Datenexporteur ist gegenüber den Betroffenen für die Datenübertragung verantwortlich.
- Der Datenimporteur ist einziger Vertragspartner für die Anwendung.
- Er ist verantwortlich für die Anwendung der Auftragsdatenverarbeitung (ADV).
- Hinweise an den Datenimporteur zur ADV und Benachrichtigung der Betroffenen.

→ Klare, überschaubare Zuständigkeiten.

Ein Fallbeispiel: Der Vorgang

- IT Service = Auftragsdatenverarbeitung



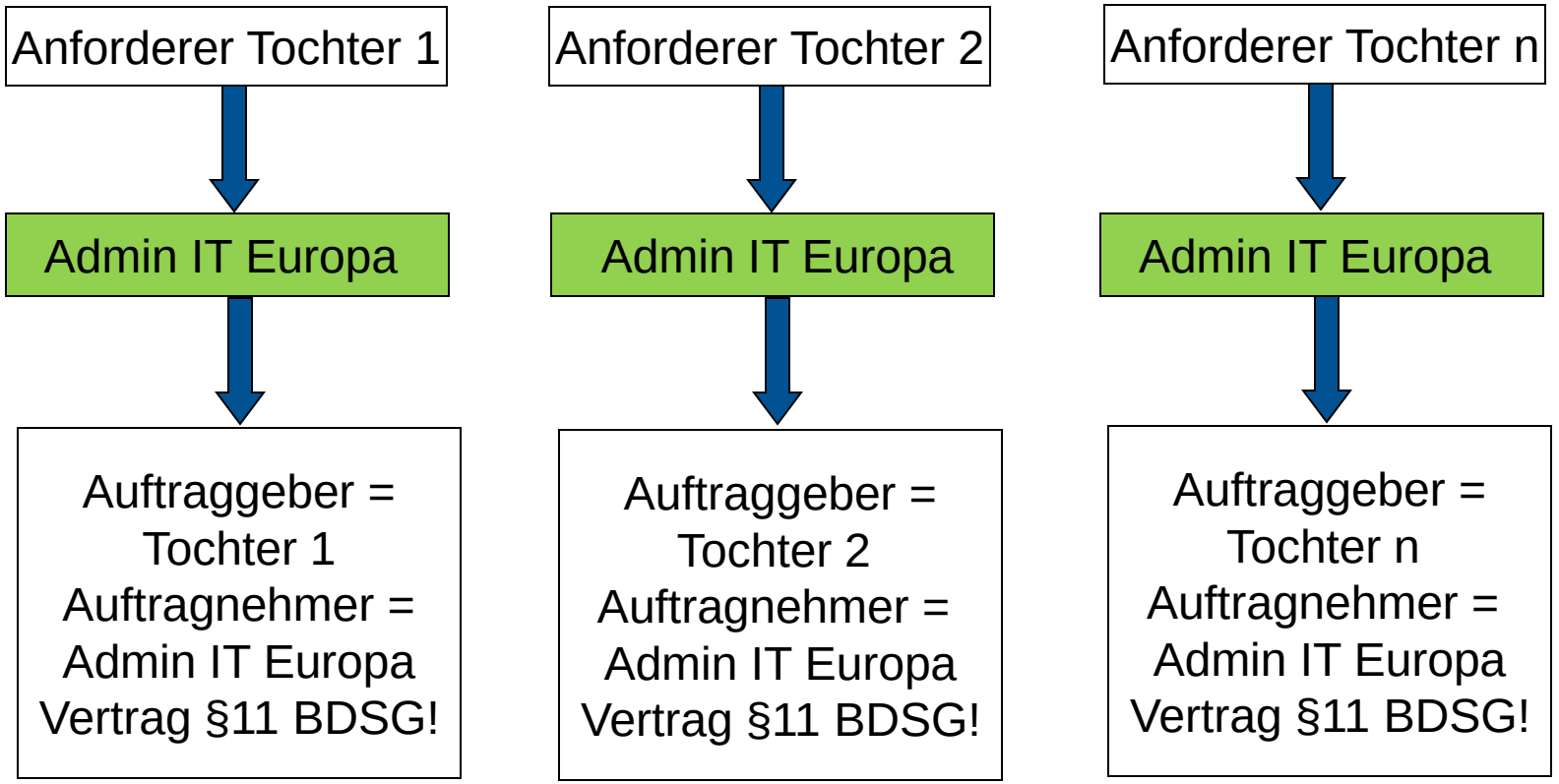
Ein Fallbeispiel: Das Problem

Dies bedeutet:

- Die Beteiligten im Beispiel Tochter 1 und Tochter 2, rechtlich eigenständige Firmen, sind mal Auftraggeber und mal Auftragnehmer.
- Fazit: in dem Vertrag gemäß § 11 BDSG müssten beide jeweils als Auftraggeber und Auftragnehmer unterschreiben.
- Dies ist absolut unübersichtlich und bei vielen Töchtern innerhalb eines Konzerns nicht praktikabel.
- Lösung? →

Ein Fallbeispiel: Die Lösung

- IT Service = Auftragsdatenverarbeitung



Ein Fallbeispiel: Das Ergebnis

Ergebnis:

- Die Beteiligten im Beispiel Tochter 1, Tochter 2 und Tochter n, rechtlich eigenständige Firmen, sind nur Auftraggeber.
- Auftragnehmer ist der Bereich IT Admin Europa, eine fachlich vorgesetzte und weisungsbefugte Stabsstelle der IT Admin in den Töchtern.
- Fazit: der Vertrag gemäß § 11 BDSG ist eindeutig und übersichtlich, da mehrere Auftraggeber und nur ein Auftragnehmer unterschreiben.

Fazit: Datenschutz international

Schlussbetrachtung:

- Datenschutz ist und bleibt spannend.
- Die meisten Anforderungen sind ganz legal umsetzbar, man muss nur die Spielregeln (Vorschriften) beachten, im Zweifelsfalle die Aufsichtsbehörde qualifiziert um Rat bitten.
- Mittels korrekter Benachrichtigungen beugen Sie unnötigen Gerüchten oder Mutmaßungen vor und gelten zudem als seriöses Unternehmen.
- Transparenz im Datenschutz schafft Vertrauen sowohl intern als auch bei Ihren Kunden.

Das war‘s von meiner Seite.

Ihre Fragen bitte !


Ingersoll Rand
Inspiring Progress™