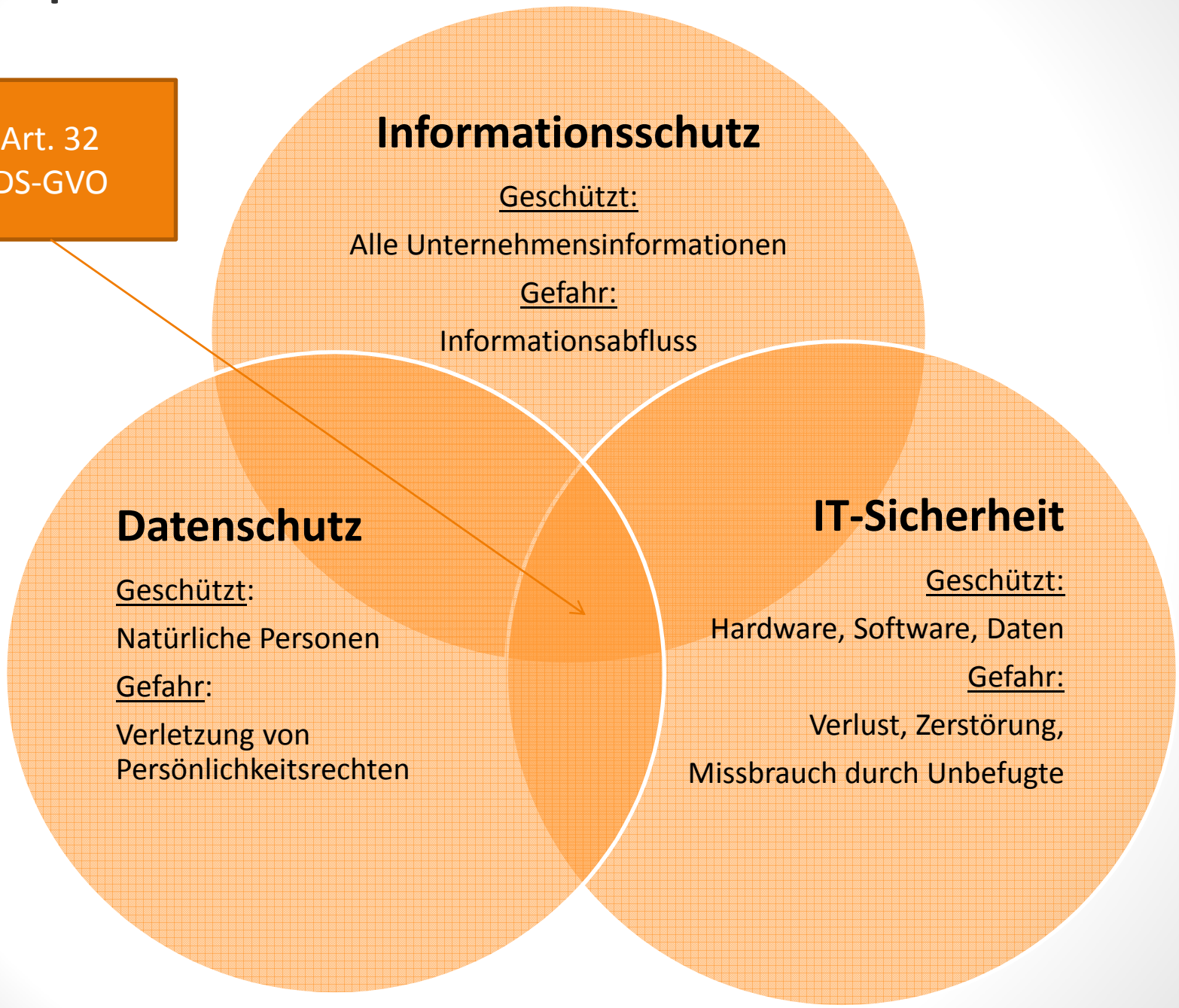
Agenda 31.05.2018

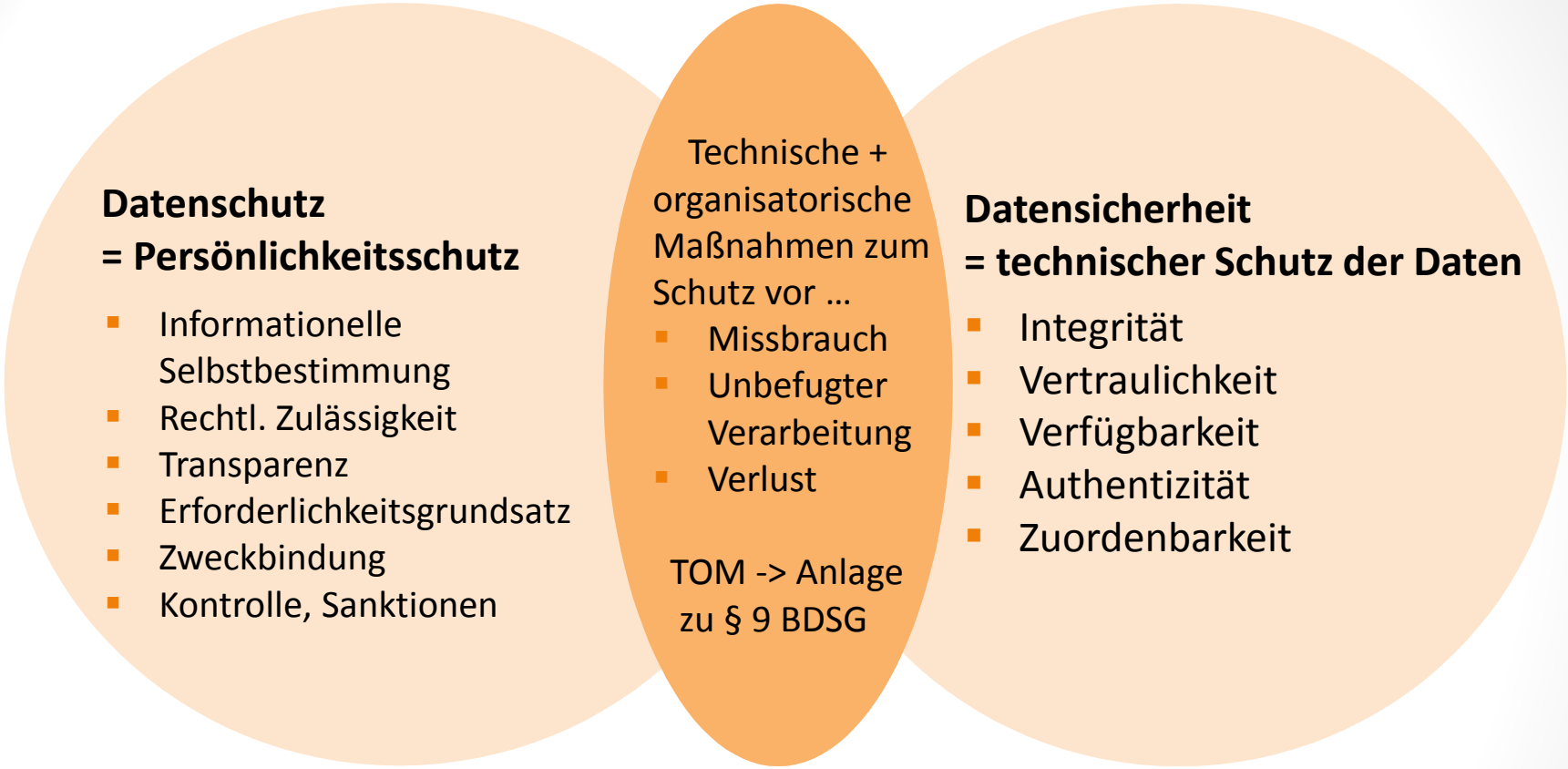
IV. Der technisch-organisatorische Datenschutz
   1. Aspekte der Datensicherheit
   2. Schutzziele nach der DS-GVO
   3. Risikobasierter Ansatz der DS-GVO
   4. Das Verzeichnis der Verarbeitungstätigkeiten (VVT)
   5. Die Datenschutz-Folgenabschätzung (DSFA)

1. Aspekte der Datensicherheit

Art. 32
DS-GVO



Aspekte der Datensicherheit



personenbezogene Daten

alle schützenswerten Daten

Aspekte der Datensicherheit

Stand der Technik

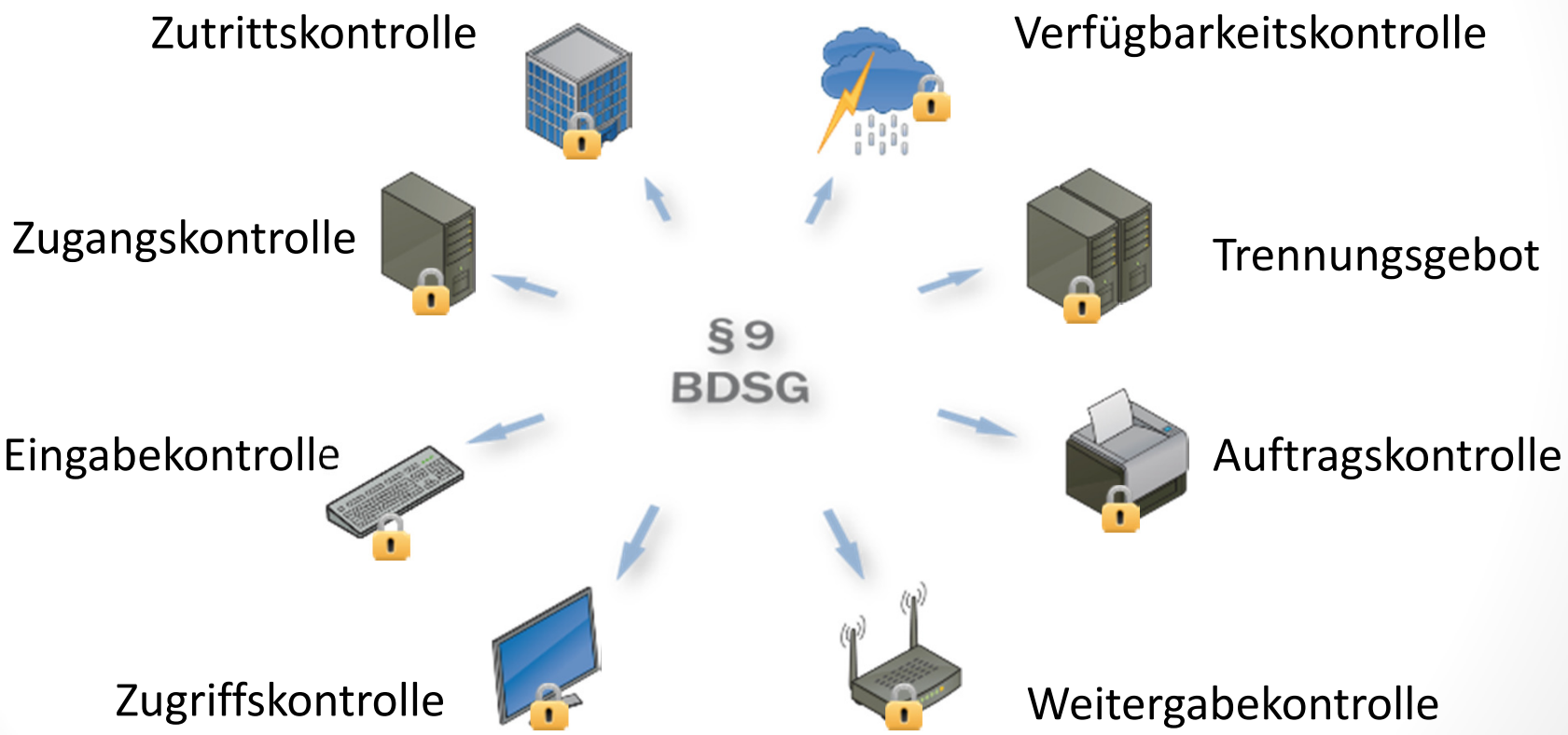
Implementierungskosten

Unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos

Art, Umfang, Umstände und Zweck der Verarbeitung

2. Schutzziele nach der DS-GVO

Bisher: Kontrollmaßnahmen der Anlage zu § 9 BDSG: „Die 8 Gebote des Datenschutzes“



Neu: Schutzziele (vgl. Art. 32 Abs. 1 lit. b DS-GVO, Erwägungsgrund 78)

1) Vertraulichkeit

Daten dürfen nur befugten Personen zugänglich sein

Maßnahmen z.B.: Passwortschutz, Alarmanlage/Videoüberwachung/ Pförtner, Zutrittsschutz, VPN, Virenschutz/ Firewall, Sperrung von Schnittstellen (z.B. USB) Pseudo-nymisierung, Verschlüsselung, Vertraulichkeitsregelungen

2) Integrität

Daten/Systeme müssen korrekt, unverändert bzw. verlässlich sein

Maßnahmen z.B.: Rollen-/ Rechte-konzept, Protokollierungen

3) Verfügbarkeit

Daten dürfen nicht unabsichtlich/ unbefugt vernichtet werden und müssen ggf. „rasch“ wiederherstellbar sein

Maßnahmen z.B.: Auslagerung von Sicherungskopien, Notstromaggregate, unterbrechungsfreie Stromversorgung, Sicherungen gegen Elementarschäden etc., regelmäßige Prüfung der Datensicherungen

4) Belastbarkeit

Begriff nicht definiert

Maßnahmen z.B.: vss. Notfallplan, Penetrationstests, Anpassungsfähigkeit

Kontrollmaßnahmen der Anlage zu § 9 BDSG:

Zutrittskontrolle

Unbefugten ist der "körperliche" Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

Zugang

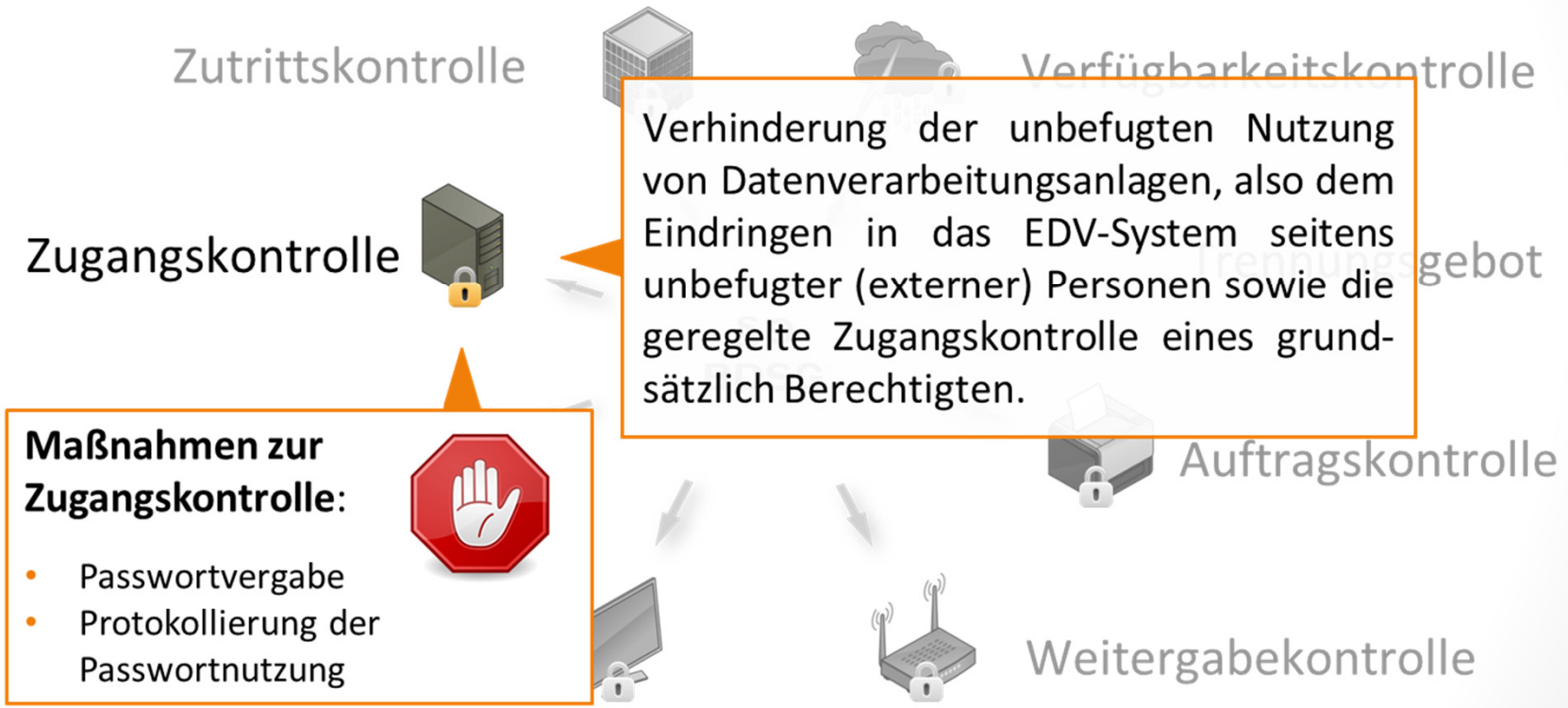
Eingab

le

Maßnahmen zur Zutrittskontrolle:

- Einteilung in Sicherheitszonen/Sperrbereiche
- Closed-Shop-Betrieb
- automatische Zutrittskontrolle
- Chipkarten/Transponderkarten
- Berechtigungsausweis
- Schlüsselregelung
- Personenkontrolle durch Pförtner
- Alarmanlage
- Gebäudeüberwachung
- Videotechnik
- Vereinzelungsanlage

Kontrollmaßnahmen der Anlage zu § 9 BDSG:



EXKURS: Passwortsicherheit

Sichere Passwörter bilden

- Mindestlänge (mindestens 10 Stellen), kryptischer Aufbau
- Bei der Anmeldung Daten des letzten Login zur Kontrolle evtl. unbefugter Zugangsversuche anzeigen lassen

Passwörter vertraulich behandeln

- Auf vertrauliche Eingabe achten
- Regelmäßiger Passwortwechsel
- Passwörter nicht notieren und nicht im PC speichern, nicht an Kolleginnen und Kollegen weitergeben

Berechtigungen einhalten

- Keine unbefugten Zugriffsversuche unternehmen (soweit dies im Einzelfall möglich sein kann). Ein Zugriff auf nicht erforderliche Dateien ist ein unbefugter Zugriff.

Kontrollmaßnahmen der Anlage zu § 9 BDSG:

Zutrittskontrolle

Verfügbarkeitskontrolle

Zugangskontrolle

Trennungsgebot

Eingabekontrolle

Gewährleistung der nachträglichen Überprüfbarkeit, welche personenbezogenen Daten durch wen zu welcher Zeit in Datenverarbeitungssysteme eingegeben bzw. dort verändert, gelöscht oder entfernt worden sind.

Maßnahmen zur Eingabekontrolle:

- Erfassungsbelege (manuell oder automatisiert)
- Protokollierung eingegebener Daten
- Verarbeitungsprotokolle

§ 9 BDSG:

Maßnahmen zur Zugriffskontrolle:

- Benennung eines Verantwortlichen für die Datenträger
- Bestandskontrolle
- Mehraugenprinzip
- kontrollierte Vernichtung (z.B. von Fehldrucken)
- funktionelle Zuordnung einzelner Endgeräte
- automatische Prüfung der Zugriffsberechtigung
- Protokollierung der Systemnutzung und Protokollauswertung
- ausschließliche Menüsteuerung

Z… erfügbarkeitskontrolle

Trennungsgebot

Eingabekontrolle

Auftragskontrolle

Zugriffskontrolle

Gewährleistung, dass die zur Benutzung Berechtigten nur auf die für ihre jeweils rechtmäßige Aufgabenstellung benötigten Daten zugreifen können.

Kontrollmaßnahmen der Anlage zu § 9 BDSG:

Die **Verfügbarkeitskontrolle** zielt auf den Schutz vor zufälliger Zerstörung ab, wie z.B. Wasserschäden, Brand, Blitzschlag, Stromausfall.

Verfügbarkeitskontrolle

Zugangskontrolle

Eingabekontrolle

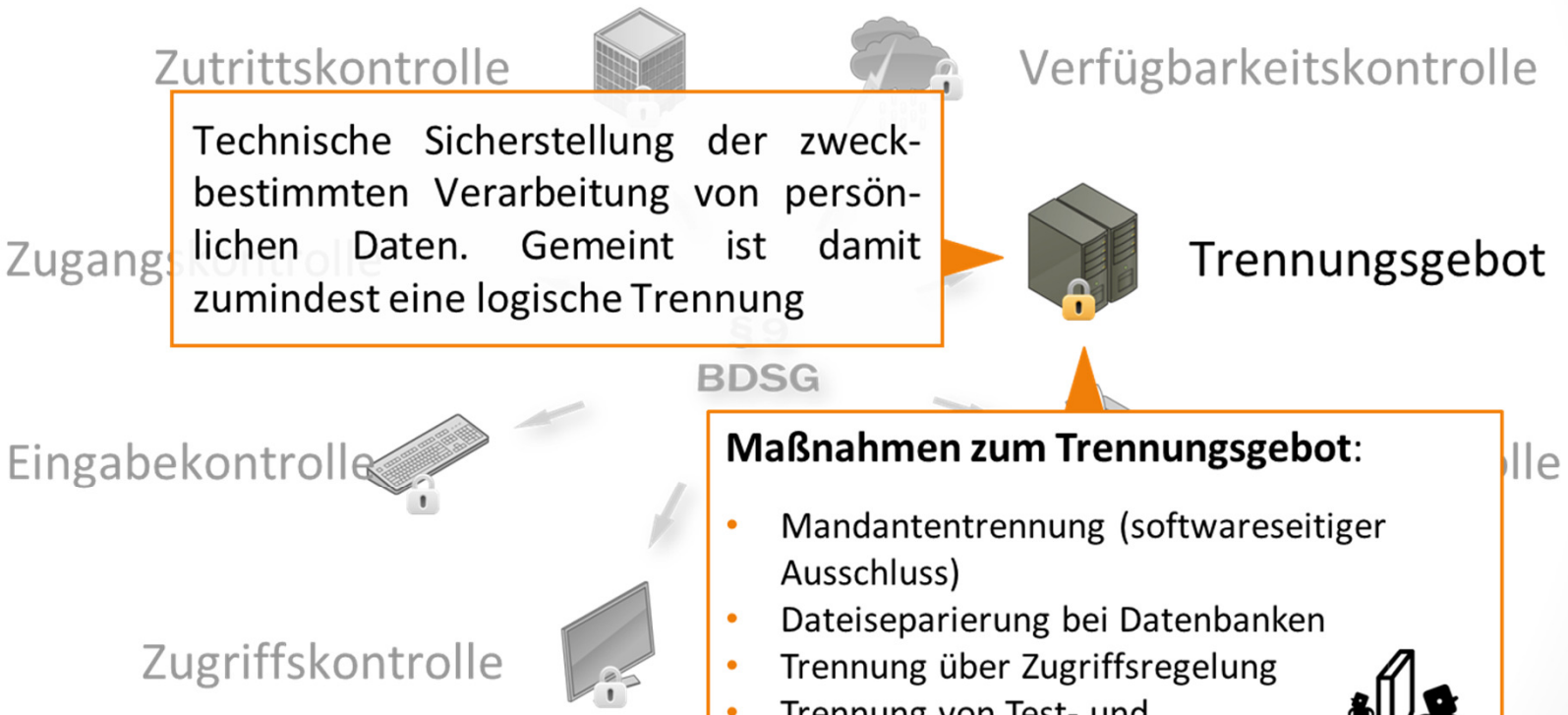
Zugriffskontrolle

Weitergabekontrolle

Maßnahmen zur Verfügbarkeitskontrolle:

- Auslagerung von Sicherungskopien
- Notstromaggregate
- unterbrechungsfreie Stromversorgung
- Katastrophenplan

Kontrollmaßnahmen der Anlage zu § 9 BDSG:



Maßnahmen zur Auftragskontrolle:

- eindeutige vertragliche Abreden nebst Kontrollabreden
- Zeitpunkt, Ort und Berechtigung/Verpflichtung zur Anlieferung bzw. Abholung der Daten
- Transport-/Versendeform
- Leistungsumfang
- Aufbewahrung von Datenträgern
- beiderseitige Verfügungsberechtigungen
- beiderseits durchzuführende Kontrollmaßnahmen
- Maßnahmen bei Verlust von Datenträgern
- Zulässigkeit der Heranziehung von Subunternehmern

Kontroll

Zutrittskontr

Zugangskontrolle

§ 9

Eingabekontrolle

Der Auftragnehmer hat zu gewährleisten, dass die im Auftrag zu verarbeitenden Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Auftragskontrolle

Zugriffskontrolle

Weitergabekontrolle

Kontrollmaßnahmen der Anlage zu § 9 BDSG:

Zutrittskontrolle

Zugangskontrolle

Die **Weitergabekontrolle** soll verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder gelöscht werden können und gewährleisten, dass überprüft werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

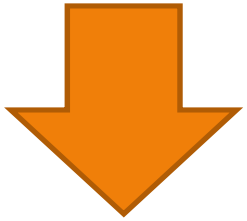
Maßnahmen zur Weitergabekontrolle:

- Standleitung oder Wählleitung mit automatischem Rückruf
- Datenverschlüsselung, Regelung zur Datenträgervernichtung
- Botentransport durch Auftragnehmer oder Auftraggeber
- Postversand verschlossen in Transportbehältern
- Transportbegleitung
- Vollständigkeits- und Richtigkeitsprüfung
- Taschenkontrollen

Weitergabekontrolle

Wichtige Maßnahmen zu IT-Sicherheit und Datenschutz

- ✓ Inventarisierung autorisierter Geräte und Software
- ✓ Sicherheitskonfiguration
  - ➢ für mobile Geräte, Workstation, Server, Netzwerke, WLAN etc.
  - ➢ für Anwendungen
- ✓ (regelmäßige, automatisierte) Schwachstellenanalyse, Penetrationstests
- ✓ Anti-Viren und Malware Software
- ✓ Backup Konzept, Schutz vor Datenverlust (Data Lost Prevention)
- ✓ Incident Response Management (Störungsmanagement)
- ✓ Sensibilisierung der Mitarbeiter und Schulung
- ✓ Aktives Management von Netzwerk Ports, Protokollen und Services
- ✓ Berechtigungsmanagement für Administratoren
- ✓ Berechtigungskonzept für Benutzer



Grundlegende Pflichten am Arbeitsplatz

- Jeder Mitarbeiter muss sicherstellen, dass keine andere Person (auch kein anderer Mitarbeiter) Unterlagen einsehen kann, ohne dazu berechtigt zu sein bzw. ohne dass hierfür eine geschäftliche Notwendigkeit besteht.
- Unterlagen oder Datenträger mit personenbezogenen Daten müssen bei Abwesenheit - auch z.B. während Pause oder Besprechung - sicher (z.B. abgeschlossener Schrank) aufbewahrt werden.
- Bildschirmsperrung bei Verlassen des Arbeitsplatzes
- Unterlagen mit personenbezogenen Daten (bereits Name etc.!) müssen, sobald sie nicht mehr benötigt werden, sicher (z.B. Schredder) entsorgt werden.

Erteilung von Auskünften

- Behörden, Gerichte, Staatsanwaltschaft
  - Rechtsgrundlage belegen lassen
  - Auskünfte grundsätzlich nur in Textform erteilen

- Nichtöffentliche Stellen
  - Berechtigtes Interesse prüfen und schutzwürdiges Interesse der Betroffenen beachten
  - Betroffene vor der Auskunftserteilung unterrichten, ggf. Einwilligung einholen

- Telefonische Auskünfte (Problem: Identität des Anrufers)
  - Auskunftsbefugnis prüfen
  - Keine Personalauskünfte (Personalabteilung einschalten)
  - Auskünfte nur im notwendigsten Umfang (nicht ausfragen lassen)
  - bei unterdrückten Rufnummern:

  → Rückruf vereinbaren und Nummer überprüfen

Sichere E-Mail- und Internet-Nutzung

- Kein ungesicherter Versand von vertraulichen Informationen, ggf. Daten verschlüsseln
- Vorsicht bei E-Mails von unbekannten Absendern
- Vorsicht bei Anhängen von E-Mails
  - ✓ insbesondere bei E-Mails von unbekannten Absendern
  - ✓ bei Anhängen mit ausführbaren Dateien, Bildern etc.
- Anzeige aller Dateitypen aktivieren
- Keine Weiterleitung von Kettenbriefen
- interne Richtlinien, insbes. zur (Un-) Zulässigkeit der Nutzung für private Zwecke (Art, Umfang, Dauer)

- Keine internen Passwörter im Internet verwenden
- Keine Angabe von persönlichen Daten im Internet (Phishing)
- Vorsicht bei Links auf unbekannten Seiten
- Keine Speicherung von Passwörtern im Browser
- Mehrfachnutzung von Passwörtern?
- Löschen von Cookies und gespeicherten Links
- Beachtung: Veränderung von bekannten Seiten, fehlerhaftes Logo, Schreibfehler, ungewöhnliche Schriftarten etc., fehlende Verschlüsselung achten
- Keine unüberlegte Veränderung von Sicherheitseinstellungen
- Gruppenrichtlinien, z.B. zum Download

Pflichten beim Arbeiten von außerhalb

- **Grds. nur dienstliche und administrierte Technik**
- **bei Bearbeitung von Mails auf privaten Geräten: Arbeit nur im zu Verfügung gestellten Mail-Zugang, kein lokaler Download**
- **keine Weiterleitung an private Mail-Adressen**
- in öffentlichen Verkehrsmitteln oder an sonstigen öffentlichen Orten sicherstellen, dass Dritte keinen Einblick in die Daten haben (z.B. Blickschutzfolien)
- bei Notebook, Tablet, Smartphone etc. Sperrfunktion und **Verschlüsselung** der Festplatte bzw. relevanter Ordner, Software zu Fernlöschung
- WLAN und Bluetooth nur bei tatsächlicher Benutzung einschalten