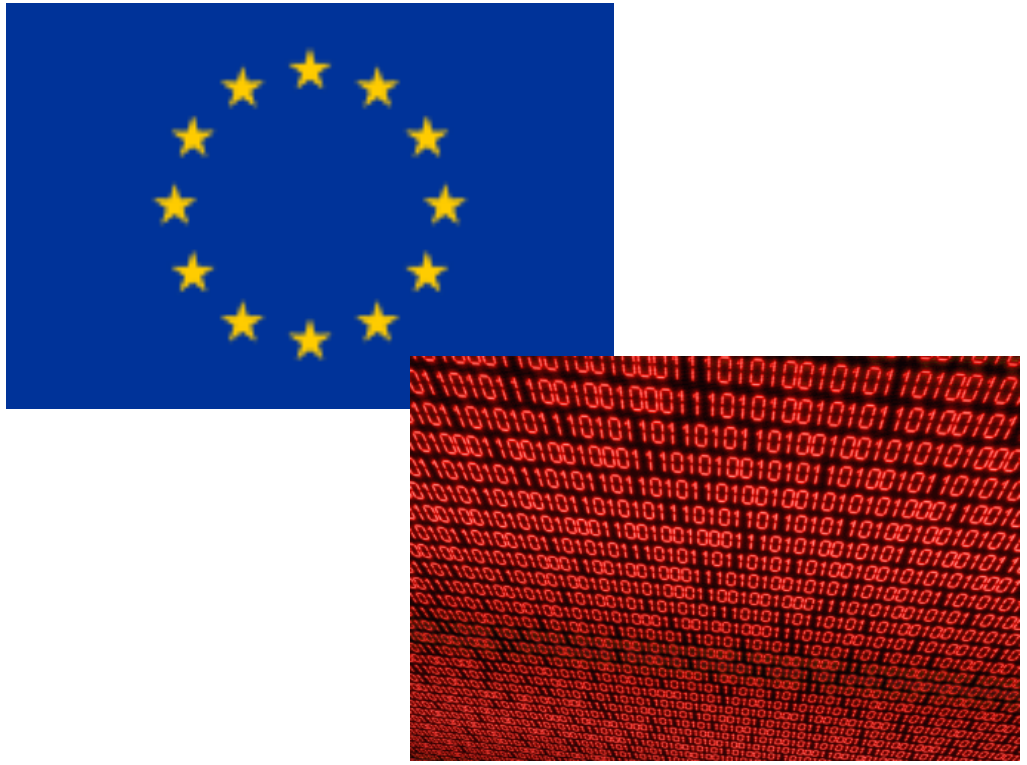
EU-Datenschutzgrundverordnung DS-GVO

Verzeichnis der
Verarbeitungstätigkeiten

Umsetzungsmaßnahmen



1.- Datenschutzleitlinie / -Managementsystem

Art. 5 DS-GVO

Grundsätze für die Verarbeitung personenbezogener Daten sind

Transparenz, Zweckbindung, Richtigkeit,

Speicherbegrenzung, Integrität und Vertraulichkeit

Personenbezogene Daten müssen

- auf rechtmäßige Art, auf Treu und Glauben, transparent verarbeitet werden,
- nur für eindeutige legitime Zwecke erhoben und verarbeitet werden
- nur dem Zweck entsprechend im notwendigen Maße erhoben werden
- sachlich richtig sein und dem neuesten Stand entsprechen
- bei Zweckentfall oder wenn die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind unverzüglich berichtigt oder gelöscht werden
- mit einer angemessenen Sicherheit einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Verlust , Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen geschützt werden.

!!! Die Rechenschaftspflicht (Accountability)
zur Einhaltung obliegt dem Verantwortlichen !!!!

2.- Verzeichnis von Verarbeitungstätigkeiten

Wir erinnern uns:

§ 3 Abs. 3 - 5 BDSG - Erheben, Verarbeiten und Nutzen
dazu gehört das: Speichern, Verändern, Übermitteln, Sperren, Löschen

und ab dem 25.05.2018 gilt:

Art. 4 DS-GVO definiert im Zusammenhang mit personenbezogenen Daten die Verarbeitung als „Vorgang oder Vorgangsreihe“

- das Erheben,
- das Erfassen,
- die Organisation,
- das Ordnen,
- die Speicherung,
- die Anpassung oder Veränderung,
- das Auslesen,
- das Abfragen,
- die Verwendung,
- die Offenlegung durch Übermittlung,
- die Verbreitung
- oder eine andere Form der Bereitstellung,
- der Abgleich
- oder die Verknüpfung. die Einschränkung,
- die Löschung
- oder die Vernichtung.

2.- Verzeichnis von Verarbeitungstätigkeiten

Art. 30 DS-GVO

Gesetzliche Verpflichtung:

- jeder Verantwortliche oder der Vertreter (Unternehmen, Freiberufler, Vereinsvorstand....)
- und -neu- auch jeder Auftragsverarbeiter ist zur Führung eines schriftlichen oder elektronischen Verzeichnis aller automatisierten und nicht automatisierten Verarbeitungen mit personenbezogenen Daten zu führen, die einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Ausnahme besteht:

- bei einer Mitarbeiterzahl von weniger als 250 Mitarbeiter und wenn die Verarbeitung nur gelegentlich erfolgt

eine Verpflichtung besteht aber auch dann,

- wenn die Verarbeitung ein Risiko für Rechte und Freiheiten Betroffener birgt
- bei der Verarbeitung besonderer Datenkategorien gem. Art. 9 Abs. 1 DS-GVO
- wenn personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten im Sinne Art. 10 DS-GVO betroffen sind

2.- Verzeichnis von Verarbeitungstätigkeiten

Art. 30 DS-GVO

Weitere Änderungen:

- Bekanntmachung der Daten wie im § 4g Abs.2 und Abs. 2a BDSG gefordert (im Sprachgebrauch als „Jedermann Verzeichnis“ bekannt) ist nicht mehr erforderlich.

- Meldungen wie in den $$ 4d und 4e BSDSG geregelt, sind nicht vorgesehen und entfallen.

2.- Verzeichnis von Verarbeitungstätigkeiten

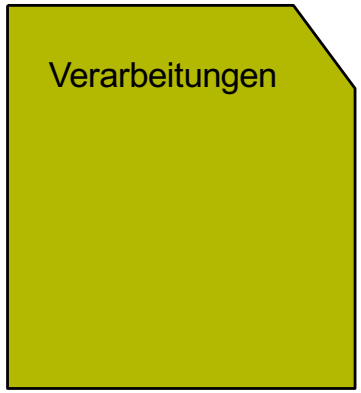
Art. 30 DS-GVO

Kontaktdaten:

- Verantwortlicher oder Auftragsverarbeiter
- Stellvertreter
- Datenschutzbeauftragter

Verarbeitungstätigkeiten als Verantwortlicher:

- Zweck der Verarbeitung
- Beschreibung der betroffenen Personen oder
- oder der Kategorien personenbezogener Daten
- Kategorien der Empfänger
- und der Empfänger in Drittländern oder internationaler Organisationen
- Angaben über Gründe der Übermittlung mit Dokumentierung
- die vorgesehen Fristen für die Löschungen der verschiedenen Datenkategorien
- eine Beschreibung technischer und organisatorischer Maßnahmen



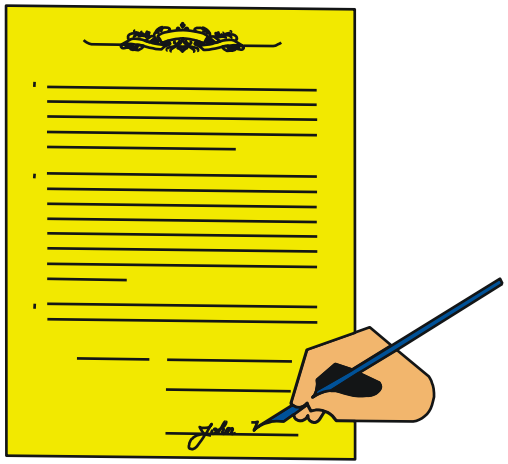
- Ergänzende Angaben zur Risikobewertung (niedrig, mittel, hoch)

2.- Verzeichnis von Verarbeitungstätigkeiten

Art. 30 DS-GVO

Verarbeitungstätigkeit als Auftragsverarbeiter:

- Kategorien der Verarbeitung die im Auftrag durchgeführt werden
- Beschreibung der betroffenen Personen oder
- Empfänger in Drittländern oder internationaler Organisationen
- Angaben über Gründe der Übermittlung mit Dokumentierung
- eine Beschreibung technischer und organisatorischer Maßnahmen



Ergänzende Angaben:

- Weitere Subunternehmer
- Angaben zur Auftragsdatenverarbeitung

Maßnahmen:

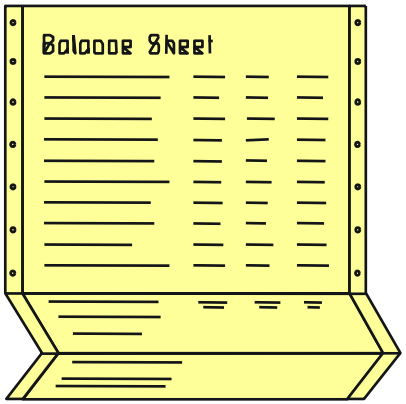
- Bisherige Verfahrensverzeichnisse des BDSG erweitern; intern /extern zusammenfassen
- Systeme und Datenflüsse verifizieren
- Template Verfahrensverzeichnis zu Template Verarbeitungstätigkeiten aktualisieren

2.- Verzeichnis von Verarbeitungstätigkeiten

Art. 30 DS-GVO

Beteiligung der Fachabteilungen

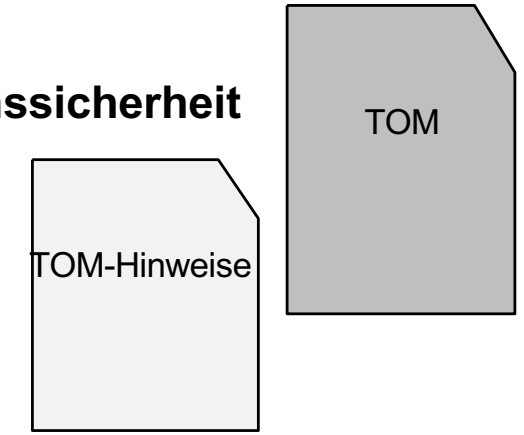
- Informationsveranstaltung für Führungskräfte
  - zur DS-GVO
  - zu Tätigkeitsbeschreibungen
  - Erstellen einer Liste mit Verarbeitungsmöglichkeiten



3.- Technische und organisatorische Maßnahmen

Artikel 32 DS-GVO

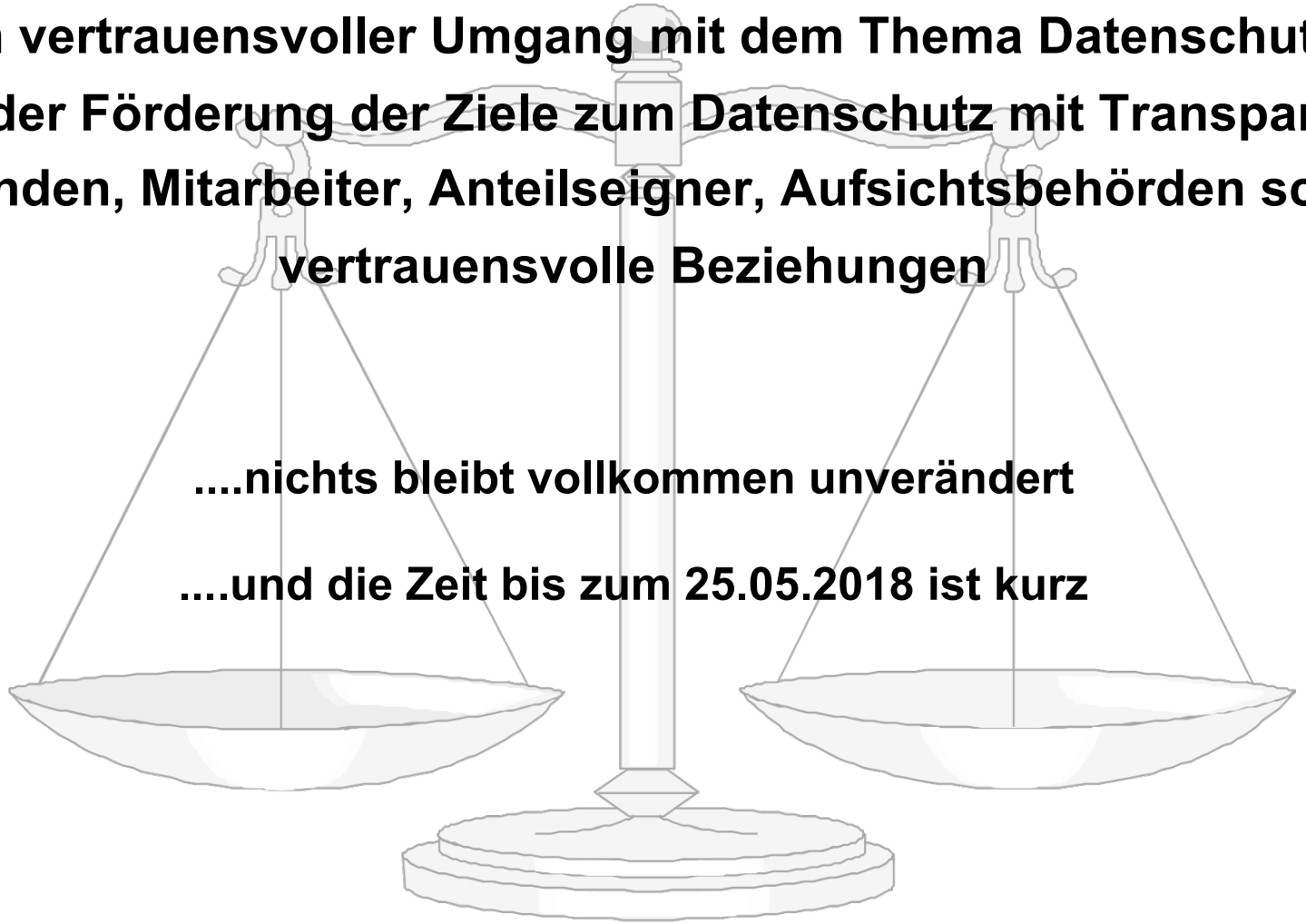
1. **Gewährleistung der Vertraulichkeit**
2. **Gewährleistung der Integrität**
3. **Gewährleistung der Verfügbarkeit als Teil der Informationssicherheit**
4. **Gewährleistung der Belastbarkeit der Systeme**
5. **Wiederherstellung (Sicherstellung) der Verfügbarkeit**
6. **Gewährleistung der Belastung der Systeme**



Maßnahmen:

- Gaps identifizieren und schließen
- Risikoanalyse durchführen und dokumentieren
- Maßnamenkatalog erstellen
- Prozess einrichten

Fazit



Ein vertrauensvoller Umgang mit dem Thema Datenschutz und der Förderung der Ziele zum Datenschutz mit Transparenz für Kunden, Mitarbeiter, Anteilseigner, Aufsichtsbehörden schafft vertrauensvolle Beziehungen

....nichts bleibt vollkommen unverändert

....und die Zeit bis zum 25.05.2018 ist kurz

Fragen?

Vielen Dank für die Aufmerksamkeit

Halt, stopp, noch eine kleine Ergänzung gefällig?

Verträge - Auftragsverarbeitung / Vertragsmanagement

Art. 28 DS-GVO

Stellung des Auftragsverarbeiters

- kein Dritter im Sinne Art. 4 Abs.10 DS-GVO
- Wirkung wie ein „Innenverhältnis“ ohne Prüfschranken für eine Datenübermittlung
- keine Beschränkungen der Privilegierung der Auftragsverarbeitung im EU-/EWR-Raum
- Mehr Verantwortung und Pflichten
- Einsatz nur mit hinreichenden Garantien für einen ausreichenden Datenschutz
- Garantien können genehmigte Verhaltensregeln nach Art. 40 DS-GVO oder Zertifizierungen nach Art. 42 DS-GVO sein.
- Auftragsgegenstand ohne Umgang mit personenbezogenen Daten führt unter Umständen nicht zu einer Qualifikation als Auftragsverarbeiter ohne Anwendung des Art. 28 GS-DVO

Verträge - Auftragsverarbeitung / Vertragsmanagement

Art. 28 DS-GVO

Verträge

- weisungsgebundene Tätigkeit (wie bisher)
- können in schriftlicher oder elektronischer Form geschlossen werden
- detaillierte Darstellung der erforderlichen Maßnahmen zur Sicherheit der Verarbeitung
  - Vertraulichkeit, Integrität, Verfügbarkeit,
  - Sicherstellung der Belastbarkeit der Systeme und Dienste
- Sub-Unternehmer-Einsatz nur mit Genehmigung durch den Auftraggeber
- Führung des Verzeichnisses von Verarbeitungstätigkeiten
- bei Datenschutzverletzungen Haftung wie der Auftraggeber

Maßnahmen:

- Auftragsverhältnis identifizieren (Rolle AG und AN), gilt auch im Innenverhältnis
- Mustervertrag anpassen
- Verträge aktualisieren und ggf. neu abschließen
- Prozess definieren und Abläufe festlegen

Fragen?

Das war es. Vielen Dank.
Ihr wart eine tolle Zuhörerschaft
und habt hoffentlich genug Stoff zur Diskussion

Jörg Frahm, jfdatenschutz@hotmail.de