

Datenschutzrecht

– Datenschutzorganisation & Risikomanagement durch die Datenverarbeiter

Prof. Dr. iur. Uwe K. Schneider, Rechtsanwalt

12.02.2026

Wintersemester 2025/26 (ILIAS-Kurs Nr. 24018)

Management von Datenschutz & Datensicherheit

Die DSGVO als Prozess- und Dokumentationsthema



Art. 5 Abs. 2: Rechenschaftspflicht („Accountability“):

„Der Verantwortliche ist für die Einhaltung des Abs. 1 [Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten] verantwortlich und muss dessen Einhaltung nachweisen können.“

Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DSGVO

- **Verzeichnis aller Verarbeitungstätigkeiten des Verantwortlichen (VVT)**
 - Name/Kontaktdaten d. Verantwortlichen u. ggf. Datenschutzbeauftragten
 - Zwecke der Verarbeitung
 - Kategorien betroffener Personen und personenbezogener Daten
 - Kategorien von Empfängern
 - ggf. Übermittlung in Drittstaaten, Dokumentation geeigneter Garantien
 - Fristen für die Löschung („wenn möglich“)
 - allgemeine Beschreibung der TOM (Technische & Organisatorische Maßnahmen der Datensicherheit, „wenn möglich“ = ist die Regel)
- **Nicht öffentlich, aber Einsicht für Aufsichtsbehörden auf Anfrage**
- **Praktisch keine Ausnahmen** (nur für Unternehmen unter 250 Mitarbeiter, wenn DV nur gelegentlich)
- **Sinnvolle Ergänzungen (wg. allgemeiner Nachweispflicht):**
 - Rechtsgrundlage (darüber ist zu informieren) und Schwellwertanalyse (oder zumin. deren Ergebnis)
- **Form:** nicht vorgegeben, also Papier oder elektronisch (z.B. .docx, .xlsx oder Datenbank)

VVT-Vorlage des Deutschen Anwaltsvereins

Microsoft Excel - dav_muster-verzeichnis-der-verarbeitungstaetigkeiten-nach-art-30-dsgvo-1 [Schreibgeschützt]

Beispiel Kanzlei Mustermann und Partner
Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO

Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters: Kanzlei Mustermann und Partner, Maa-Mustermann-Straße 123, 12345 Berlin, Deutschland

Name und Kontaktdaten des betrieblichen Datenschutzbeauftragten: Mai Mustermann, datenschutz@xyz.de

Zwecke der Verarbeitung: Tätigkeitsgegenstand der Kanzlei ist die Beratung von Mandanten sowie deren gerichtliche und außergerichtliche Vertretung.

Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten: Mandanten-, Mitarbeiterdaten sowie Daten von Lieferanten sowie anderer Geschäftspartner, sofern die Verarbeitung zur Erfüllung der unter b. genannten Zwecke erforderlich ist. Details sind in der Anlage beschrieben.

Kategorien von Empfängern, denen die Daten offengelegt worden sind bzw. werden (intern/extern) sowie Empfänger in Drittstaaten: Hierzu zählen: Verantwortliche des öffentlichen Rechts bei Vorliegen vorrangiger Rechtsvorschriften, externe Auftragnehmer gemäß Art. 28 DSGVO sowie Dritte, soweit dies zur Erfüllung der in Spalte 2 genannten Zwecke erforderlich ist. Hierzu zählen Zahlungsdienstleister, Behörden, Gerichte, sonstige öffentliche Stellen. Interne Empfänger können z.B. sein: Buchhaltung, ...

Übermittlung in Drittstaaten: Eine Übermittlung an andere Unternehmen mit Sitz außerhalb der EU finden nur in Ausnahmefällen und bei bestimmten Datenverarbeitungen statt. Siehe Spalte 1.

Regel Fristen für die Löschung der Datenkategorien: Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und -fristen erlassen. Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht. Sofern Daten hiervon nicht befreit sind, werden sie gelöscht, wenn ihre spezifischen Verarbeitungszwecke wegfallen. Die konkreten Löschfristen werden bei den jeweiligen Verfahren in der Anlage beschrieben.

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen: Die Systeme der Kanzlei Mustermann und Partner werden durch eine Vielzahl von Maßnahmen gegen unbefugten Zugriff, Verlust oder Zerstörung und unzulässige Veränderung geschützt. Details zu dem Verfahren werden in der Anlage erläutert.

Name der Datenverarbeitung	Zwecke der Datenverarbeitung	Rechtsgrundlage	Beschreibung der Verarbeitung	Verarbeitung besonderer Arten personenbezogener Daten i.S.d. Art. 9 Abs. 1 DSGVO	Betroffene / betroffene Personengruppen	Personenbezogene Daten / Datenkategorien	Empfänger / Empfängerkategorien	Drittstaatenansatz	Zugriffsberechtigte	Regel Fristen für die Löschung	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen	Datenschutzfolgenabschätzung	Anmerkung
BUCHHALTUNG													
Finanzbuchhaltung	Durchführung der Finanzbuchhaltung	Art. 6 Abs. 1 lit. c DSGVO, § 271 HGB, § 147 AO	Nein	Nein	Mandanten, Partner und Lieferanten	Rechnungskonten von Geschäftlichen, Mandantenbezogene, Daten von Partnern und Lieferanten sowie alle dazugehörigen Abrechnungsunterlagen	Mitarbeiter der Finanzbuchhaltung	Nein	Mitarbeiter der Finanzbuchhaltung	Art. 11 Abs. 3 lit. b) DSGVO, § 147 Abs. 3 AO, zehn Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist. Achtung: Bei diesen Daten besteht eine Aufbewahrungspflicht. Eine Löschung vor Ablauf dieser Frist können nicht in Betracht.	Entzug erfolgt, sobald die TOM/DSGVOkonform sind		
Rolleplanung	Planung von Dienstreisen	Art. 6 Abs. 1 lit. f) DSGVO	Nein	Nein	Mitarbeiter	Stammdaten, dienstliche Kreditkarten, Reisekosten, Anwesenheits-/Reiseprotokolle	Fluglinien, Eisenbahnen, Autovermietungen, Hotels, Reiseveranstalter, Reisebüros, Botschaften, Messungsdienstleistungen	Bei Reisen in Drittstaaten ggf. zur Buchung und zur Beantragung von Visa etc.		Sowohl Daten gespeichert werden. Art. 11 Abs. 3 lit. c) DSGVO, § 147 Abs. 3 AO, zehn Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist. Achtung: Bei diesen Daten besteht eine Aufbewahrungspflicht. Eine Löschung vor Ablauf dieser Frist können nicht in Betracht.	Entzug erfolgt, sobald die TOM/DSGVOkonform sind		
Archivierung der Daten	Optisches Archiv zur vollständigen Archivierung von Aufträgen und Finanzbuchhaltungsdaten. Geschäftswertiges wie Finanzdokumente oder Dokumenten werden hier manuell gesammelt und archiviert.	Art. 6 Abs. 1 lit. c) DSGVO, § 271 HGB, § 147 AO, § 4 Abs. 2b DSGVO	Nein	Nein	Mandanten, Lieferanten	Eingangs-, Ausgangs-, Belegkopien, Unterlagen von Mandanten	Zugriffsberechtigt: Mitarbeiter Mandanten	Nein		Art. 11 Abs. 3 lit. b) DSGVO, § 147 Abs. 3 AO, zehn Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist. Achtung: Bei diesen Daten besteht eine Aufbewahrungspflicht. Eine Löschung vor Ablauf dieser Frist können nicht in Betracht.	Entzug erfolgt, sobald die TOM/DSGVOkonform sind		
Empfängerbeziehung und Lokalisierung	Bereitstellung der Mautgebühr in der Preistrabebuchung, Dokumentations der Erstfortung	Art. 6 Abs. 1 lit. c) DSGVO, § 147 AO, § 197 HGB, § 4 Abs. 2	Ja	Nein	Mitarbeiter	Stammdaten, Urlaubstage, Krankheitslagen (ohne Behörde), Mitarbeiterdaten	Mitarbeiter der Lohnbuchhaltung Steuerkategorien	Nein		§ 11 Abs. 3 lit. b) DSGVO, § 147 Abs. 3 AO, zehn Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist. Achtung: Bei diesen Daten besteht eine Aufbewahrungspflicht. Eine Löschung vor Ablauf dieser Frist können nicht in Betracht.	Entzug erfolgt, sobald die TOM/DSGVOkonform sind		

(eine Verarbeitungstätigkeit pro Zeile; m.E. gute erste Hilfe, längerfristig und v.a. für größere Unternehmen aber kaum handlich)

https://anwaltsblatt.anwaltverein.de/files/anwaltsblatt.de/Dokumente/2018/dav_muster-verzeichnis-der-verarbeitungstaetigkeiten-nach-art-%2030%20dsgvo.xlsx

VVT-Vorlage Vogel & Partner

20180427_Verzeichnis der Verarbeitungstätigkeiten_DSGVO - Microsoft Excel

Datei Start Einfügen Seitenlayout Formeln Daten Überprüfen Ansicht

C4

VVT nach DSGVO Muster-Vorlage © Vogel Partner Rechtsanwälte mbB, Karlsruhe/Stuttgart

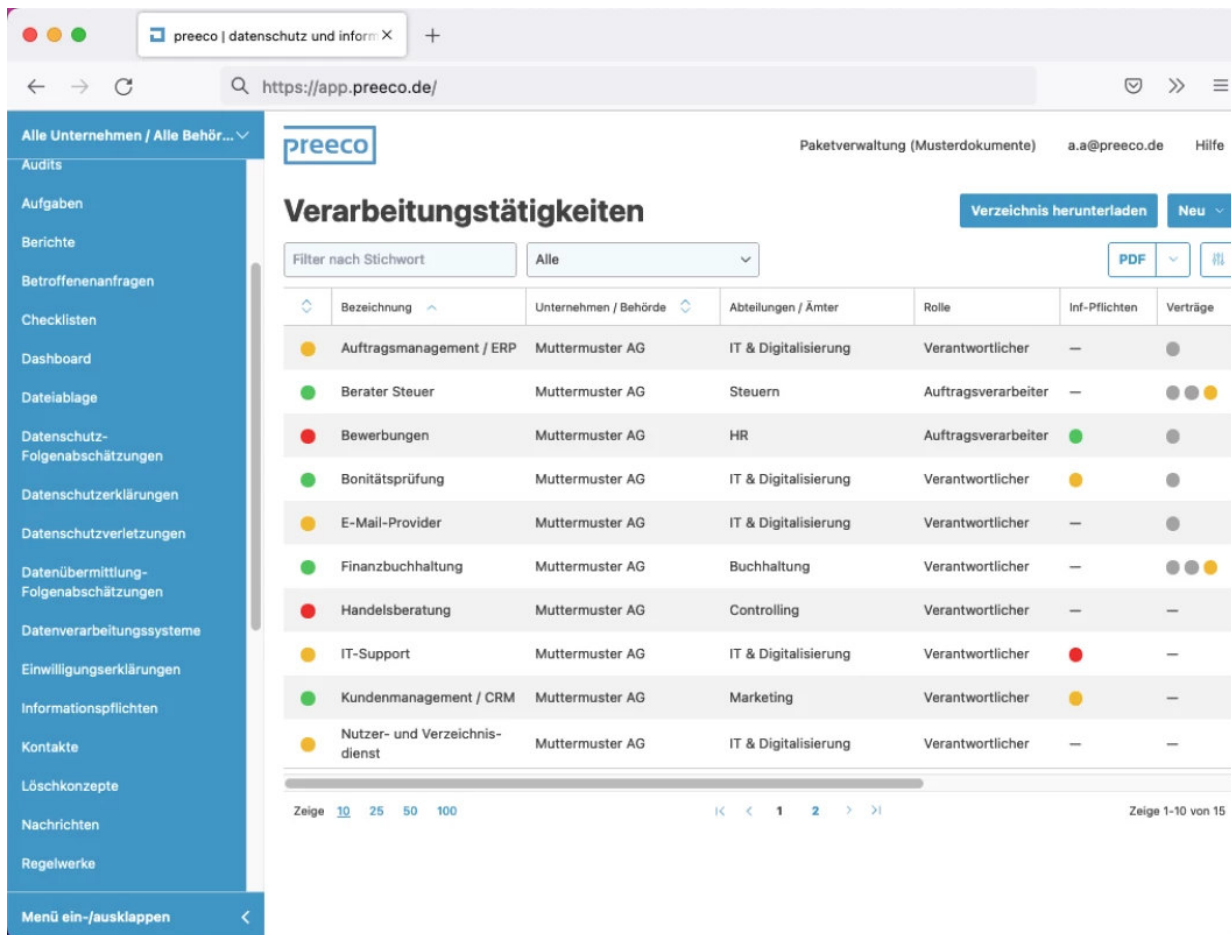
Verzeichnis für Verarbeitungstätigkeiten der X GmbH				
Hauptblatt: Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit. a DSGVO)				
Nr.	Information	Ausfüllhinweis	Erläuterung	Notizen, To Do's
1.	Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit. a DSGVO, § 70 Abs. 1 Nr. 1 BDSG-neu)	Name, Firma, Ladungsfähige Anschrift	Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DS-GVO)	
2.	Gesetzlicher Vertreter (Art. 30 Abs. 1 lit. a DSGVO)	Geschäftsführung: Name, Kontaktdaten (evtl. Link zu Web-Impressum)	Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter	
3.	Vertreter der EU (gem. Art. 27 DSGVO)	Name, Ladungsfähige Anschrift	Bei Unternehmen ohne Niederlassung in der Europäischen Union ist hier der benannte Vertreter des Verantwortlichen (Art. 4 Nr. 17 DS-GVO, Art. 27 Abs. 1 DS-GVO) anzugeben.	
4.	Datenschutzbeauftragter (Art. 30 Abs. 1 lit. a DSGVO, § 70 Abs. 1 Nr. 1 BDSG-neu)			

Hauptblatt VVT Blanko

Bereit Seite: 1 von 4

(eine Verarbeitungstätigkeit pro Reiter mit Ausfüllanleitung; hilfreicher; v.a. für größere Unternehmen aber dennoch begrenzt handlich)

VVT – spezielle Software



The screenshot shows the 'preeco' web application interface. The main content area is titled 'Verarbeitungstätigkeiten' (Processing Activities). It features a table with columns for 'Bezeichnung' (Description), 'Unternehmen / Behörde' (Company / Authority), 'Abteilungen / Ämter' (Departments / Offices), 'Rolle' (Role), 'Inf-Pflichten' (Information Obligations), and 'Verträge' (Contracts). The table lists 11 activities, all for 'Muttermuster AG'. The activities include 'Auftragsmanagement / ERP', 'Berater Steuer', 'Bewerbungen', 'Bonitätsprüfung', 'E-Mail-Provider', 'Finanzbuchhaltung', 'Handelsberatung', 'IT-Support', 'Kundenmanagement / CRM', and 'Nutzer- und Verzeichnisdienst'. Each activity has a colored status indicator in the 'Inf-Pflichten' column and a set of colored dots in the 'Verträge' column. The interface also includes a sidebar with navigation options, a search bar, and a 'Verzeichnis herunterladen' button.

Bezeichnung	Unternehmen / Behörde	Abteilungen / Ämter	Rolle	Inf-Pflichten	Verträge
Auftragsmanagement / ERP	Muttermuster AG	IT & Digitalisierung	Verantwortlicher	—	●
Berater Steuer	Muttermuster AG	Steuern	Auftragsverarbeiter	—	●●●
Bewerbungen	Muttermuster AG	HR	Auftragsverarbeiter	●	●
Bonitätsprüfung	Muttermuster AG	IT & Digitalisierung	Verantwortlicher	●	●
E-Mail-Provider	Muttermuster AG	IT & Digitalisierung	Verantwortlicher	—	●
Finanzbuchhaltung	Muttermuster AG	Buchhaltung	Verantwortlicher	—	●●●
Handelsberatung	Muttermuster AG	Controlling	Verantwortlicher	—	—
IT-Support	Muttermuster AG	IT & Digitalisierung	Verantwortlicher	●	—
Kundenmanagement / CRM	Muttermuster AG	Marketing	Verantwortlicher	●	—
Nutzer- und Verzeichnisdienst	Muttermuster AG	IT & Digitalisierung	Verantwortlicher	—	—

→ Bei mittleren und jedenfalls größeren Unternehmen zu empfehlen.

→ Leichter arbeitsteilig zu pflegen und aktuell zu halten.

→ Z.B. [preeco](https://preeco.de).

→ Es gibt aber eine Vielzahl anderer, spezialisierter Tools (auch mit Zusatzfunktionen zum VVT, z.B. Unterstützung für Schwellwertanalyse und DSFA), sei es OnPrem oder SaaS.

Risikobewertung und TOMs

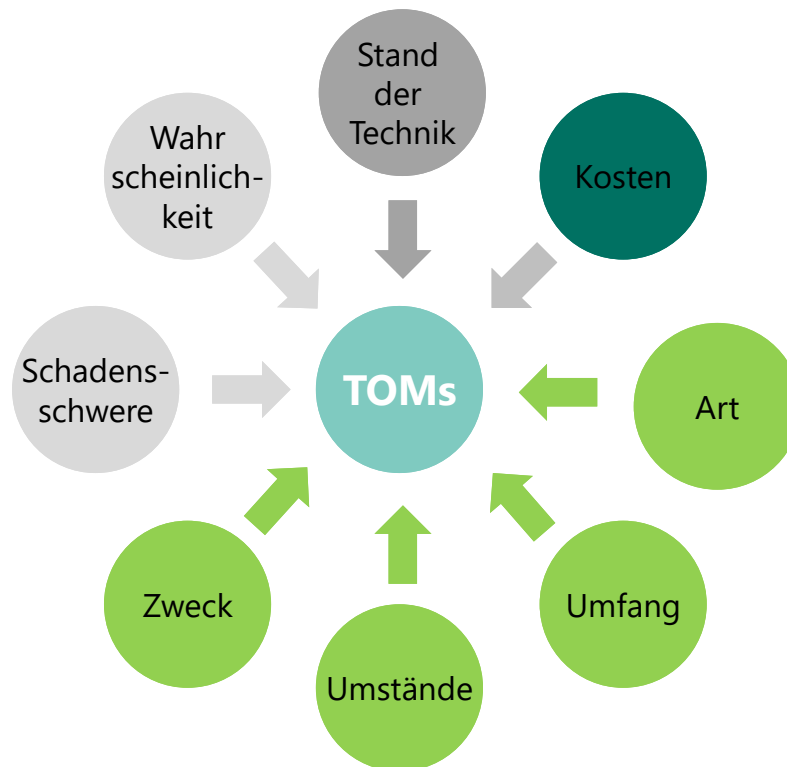
Art. 24 – Verantwortung des für die Verarbeitung Verantwortlichen

(1) Der Verantwortliche setzt unter **Berücksichtigung** der Art, des Umfangs, der **Umstände** und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der **Risiken** für die **Rechte und Freiheiten natürlicher Personen** [der betroffenen Personen] geeignete **technische und organisatorische Maßnahmen** um, um **sicherzustellen** und den Nachweis dafür erbringen zu können, dass die **Verarbeitung gemäß dieser Verordnung** erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Art. 32 – Sicherheit der Verarbeitung

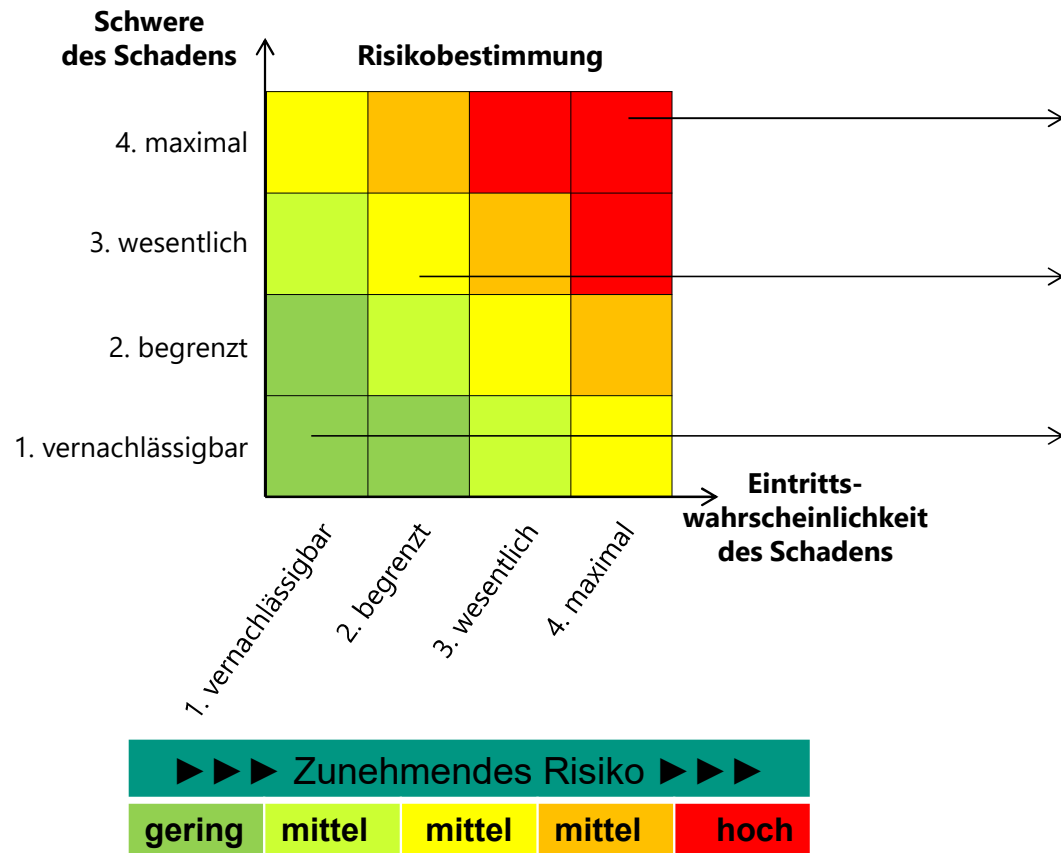
(1) Unter Berücksichtigung des **Standes der Technik**, der **Implementierungskosten** und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der **Verantwortliche** und der **Auftragsverarbeiter** geeignete technische und organisatorische Maßnahmen, um ein dem **Risiko angemessenes Schutzniveau** zu gewährleisten; [...]

Faktoren der Risikobewertung -> TOMs nach Art. 32 DSGVO



Geeignete **technische und organisatorische Maßnahmen** (TOMs) sollen Sicherheit („Security“) gewährleisten.

Matrix der Risikobewertung und Folgen



- „Umfangreiche“ TOMs bei hohem Risiko
- Datenschutzfolgenabschätzung nötig
- im Fall von Datenschutzverletzungen (Art. 33 f. DSGVO): Meldung bei Aufsichtsbehörde (72 h) & Benachrichtigung der Betroffenen
- „Normale“ TOMs bei mittlerem Risiko
- im Fall von Datenschutzverletzungen (Art. 33 DSGVO): Meldung bei Aufsichtsbehörde (binnen 72 h)
- „Kleinere“ TOMs bei geringem Risiko

Geringes und mittleres Risiko:
zumindest **summarische Bewertung**

Hohes Risiko: explizite Feststellung,
ob dieses vorliegt oder nicht &, falls ja,
detaillierte Bewertung nach Schutzzielen,
Teilsystemen, Angriffsvektoren etc.

Risiken für Rechte des Betroffenen

– ErwGr 75 (Bsp.)

Diskriminierung

Teurere Kredite für Bewohner bestimmter Stadtviertel

Identitätsdiebstahl

Hacking eines Online-Shops und Verkauf der E-Mail-Adressen im Darknet

Profilbildung von Aufenthaltsorten

Unzulässige Zweckänderung von Daten eines PayAsYouGo-Drive-Versicherers fürs Marketing

Rufschädigung

Veröffentlichung negativer Bonitätsdaten

Verlust der Vertraulichkeit

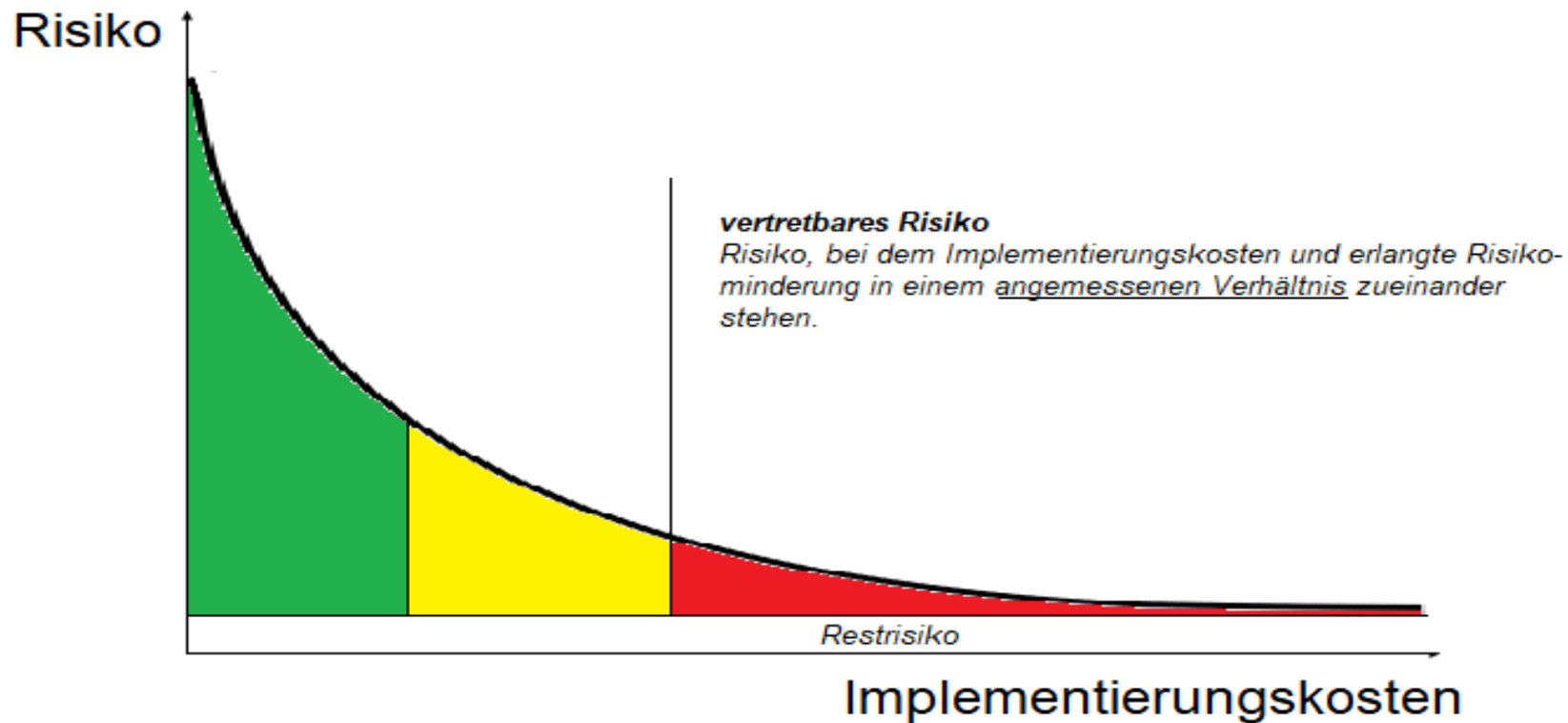
Fehlversand einer Privatrechnung durch Psychiater

Hinderung der Kontrolle über die eigenen Daten

Keine Möglichkeit eigene Fotos in Portal für Mitarbeiter zu löschen

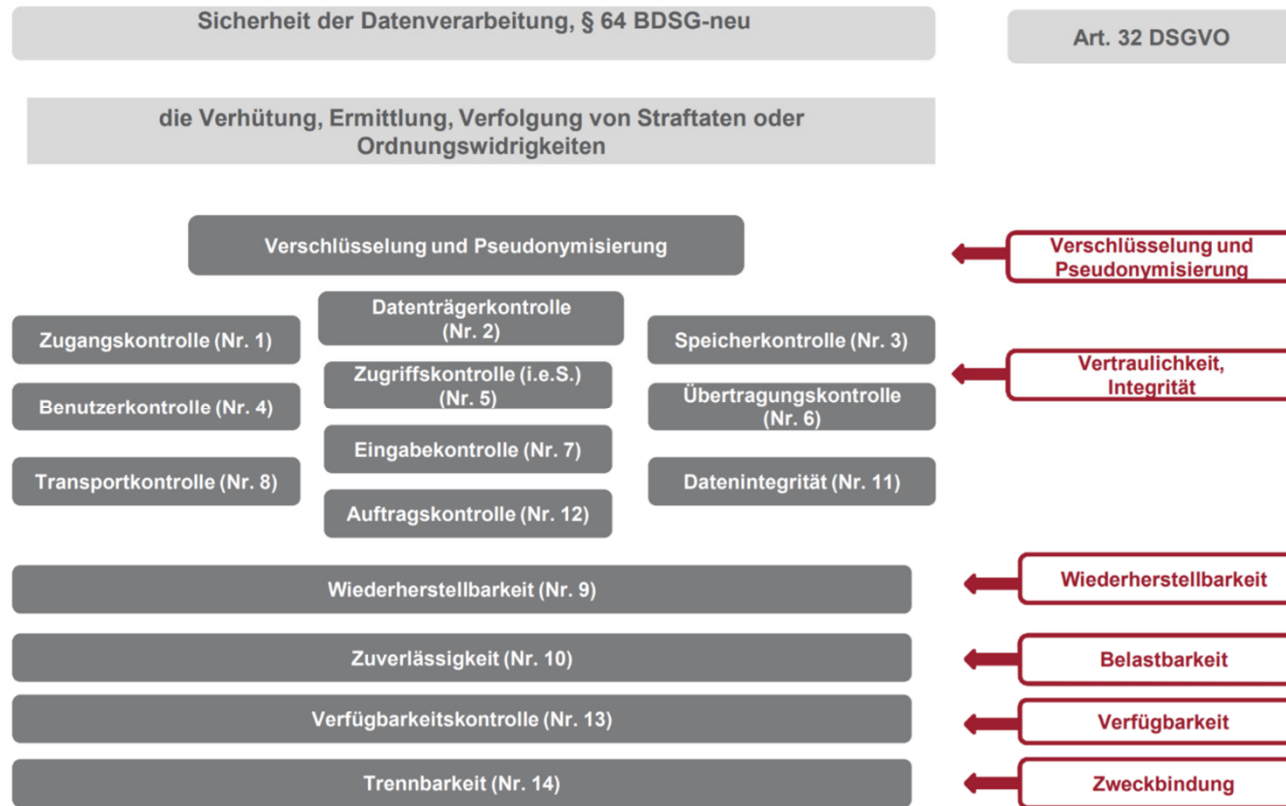
Angemessenheit von TOMs

Verhältnis von Risiko und Implementierungskosten



Achtung:
Farbwahl hier anders als in voriger Matrix, rot soll hier das akzeptable Restrisiko andeuten

Feinstruktur möglicher TOMs – Art. 32 DSGVO



Quelle: https://www.jahrestagung.governikus.de/wp-content/uploads/2017/11/GovJT17_DSGVO_Anforderungen_bei_der_Einschaltung_von_Auftragsverarbeitern_KI_oos.pdf S. 18 (Stand 27.02.2018)

Achtung:
§ 64 BDSG gilt nur für öffentliche Stellen außerhalb des Anwendungsbereichs der DSGVO (Polizei, Justiz, Geheimdienste). Auch im Übrigen kann man sich daran aber orientieren.

Datenschutz-Folgenabschätzung – Art. 35 DSGVO

Voraussetzung: Verarbeitung hat voraussichtlich ein hohes Risiko (Schwellwert)

Hierbei insbesondere zu berücksichtigende Umstände (je mehr Punkte erfüllt, desto eher)

- Verwendung neuer Technologien (z.B. Künstliche Intelligenz / machine learning)
- große Datenmengen, große Anzahl Betroffener (Big Data)
- Bildung von umfassenden Persönlichkeitsprofilen
- Sensibilität der Daten (z.B. Gesundheitsdaten)

Mindest-Inhalte der Folgenabschätzung

- systematische Beschreibung der Verarbeitungsvorgänge und Zwecke
- Bewertung der Notwendigkeit und Verhältnismäßigkeit
- Bewertung der Risiken & Beteiligung des betriebliche/behördlichen Datenschutzbeauftragten (if any)
- TOM zur Risikoverringerung und Bewertung → **Restrisiko**

Konsultation der Aufsichtsbehörde (Art. 36)

- MUSS bei immer noch **hohem Restrisiko** (sonst: KANN)

Beispiel und Vorlagen für die DSFA
(ausführlich, insbes. für das Gesundheitswesen):
<https://www.gesundheitsdatenschutz.org/html/dsfa-beispiel.php>

Artikel 33 & 34 DSGVO – Datenschutzverletzungen

Art. 4 Nr. 12 DSGVO: „Verletzung des Schutzes personenbezogener Daten“
eine Verletzung der Sicherheit, die, ob **unbeabsichtigt oder unrechtmäßig**,
zur **Vernichtung**, zum **Verlust**, zur **Veränderung**, oder zur unbefugten **Offenlegung** von
beziehungsweise zum unbefugten **Zugang** zu **personenbezogenen Daten** führt,
die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

Artikel 33: Meldung an Aufsichtsbehörde

- Innerhalb von 72 Stunden
- Begründung bei Verzögerung
- Details zur Verletzung erforderlich

Artikel 34: Benachrichtigung Betroffener

- Falls hohes Risiko besteht
- Verständliche und klare Information
- Maßnahmen und Kontaktstelle angeben

Der Datenschutzbeauftragte

Pflicht zur Bestellung eines DSB – Art. 37 DSGVO

- öffentliche Stellen
- umfangreiche regelmäßige und systematische Überwachung
- umfangreiche Verarbeitung besonderer Datenkategorien
- Öffnungsklausel für MS / § 38 BDSG in DE:
 - i.d.R. mindestens 20 Personen ständig mit automatisierter DV beschäftigt, oder
 - DS-Folgenabschätzung, Auskunfteien, Markt-/Meinungsforschung
 - Aktuelle Koalition plant Aufhebung dieser zusätzlichen Bestellpflicht, steht dafür aber teils in der Kritik, Kompromisslinie evtl. Anhebung der Mitarbeiterschwelle

Aufgaben des DSB – Art. 39 DSGVO

- Unterrichtung und Beratung des Verantwortlichen oder Auftragsverarbeiters (AVer)
- Überwachung der Einhaltung der DSGVO

Stellung des DSB – Art. 38 DSGVO

- fachliche Unabhängigkeit
- Benachteiligungsverbot
- berichtet direkt an Geschäftsleitung, Verschwiegenheit über Betroffene
- kann auch eine externe Person sein (externer DSB)

Achtung: Der Verantwortliche oder AVer bleibt aber den betroffenen Personen und Aufsichtsbehörden gegenüber haftbar. Der behördliche od. betriebliche DSB hat nur, aber immerhin eine Unterstützungsfunktion.

Auswirkungen auf Organisation und Compliance-Systeme

Haupt-Aufgaben des Unternehmens



Etablierung durch TOP-Management (Geschäftsführung o.Ä.)

- Datenschutz-Management
- Letztlich für den Datenschutz verantwortlich
- Gerade auch wenn z.B. kein DSB bestellt wird (zu Recht od. nicht)

Haupt-Aufgaben der Mitarbeiter



Umsetzung:

- Dokumentation/Nachweise/Meldepflichten
- Prozesse für Rechte der Betroffenen
- Prozessgestaltung (Privacy by design/default)
- Datenschutzfolgenabschätzung/PIA

Datenschutz- beauftragter (DSB)

- Bestellpflicht nach europäischem und deutschem Recht
- jede rechtliche Einheit (kein Konzernprivileg)
- Unterstützungs- und Kontrollfunktion

Haupt-Aufgaben des DSB



Beratung:

- Abstimmung bei „Strategien“ und in gesetzl. bestimmten Fällen

Überwachung:

- der Umsetzung der Datenschutzerfordernungen, risikoorientiert

Verpflichtungserklärung auf den Datenschutz

- § 5 BDSG a.F. sah eine solche Verpflichtung verbindlich vor
- die DSGVO dagegen nicht mehr unbedingt,
außer für Mitarbeiter von Auftragsverarbeitern (Art. 28 Abs. 3 S. 2 lit. b DSGVO)
- gleichwohl **für die Sensibilisierung aller Mitarbeiter zu empfehlen**
- **Information über die Prinzipien der DSGVO & Verpflichtung hierauf**
- diese sollten durch Richtlinien/Policies ergänzt werden, in Abwesenheit konkreter Policies den Kopf aber nicht ausschalten, sondern (kurzfristig) versuchen die Prinzipien anzuwenden und (mittelfristig) die internen Datenschützer / Unternehmensleitung / DSB um konkretere Handlungsanleitung bitten

Nächstes Mal:

**Behördliche Aufsicht &
Haftung für Datenschutzverstöße**

Übungsaufgabe(n)

Vorlesungsevaluation