Karlsruher Institut für Technologie

vogel—partner RECHTSANWÄLTE

ZAR Zentrum für Angewandte Rechtswissenschaft

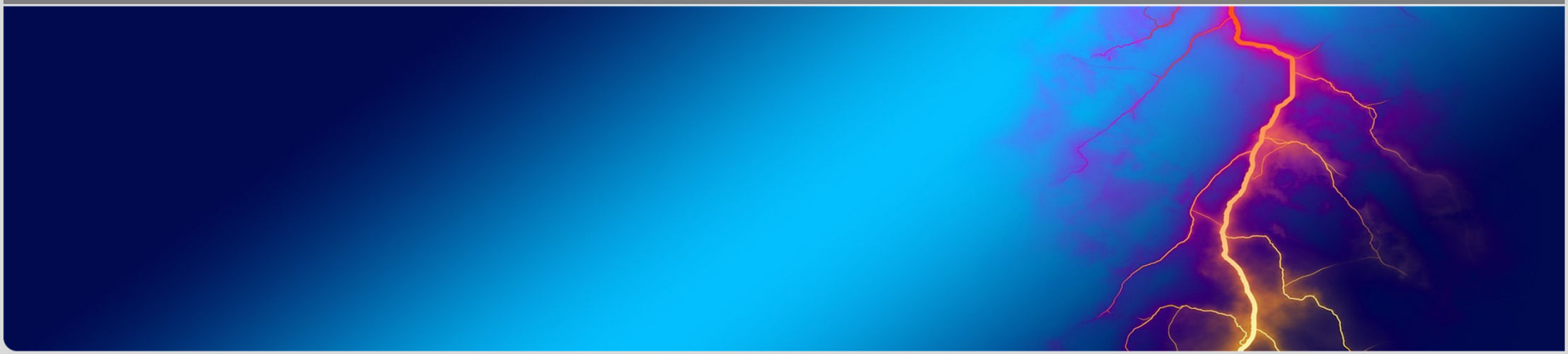
Datenschutzrecht

– 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

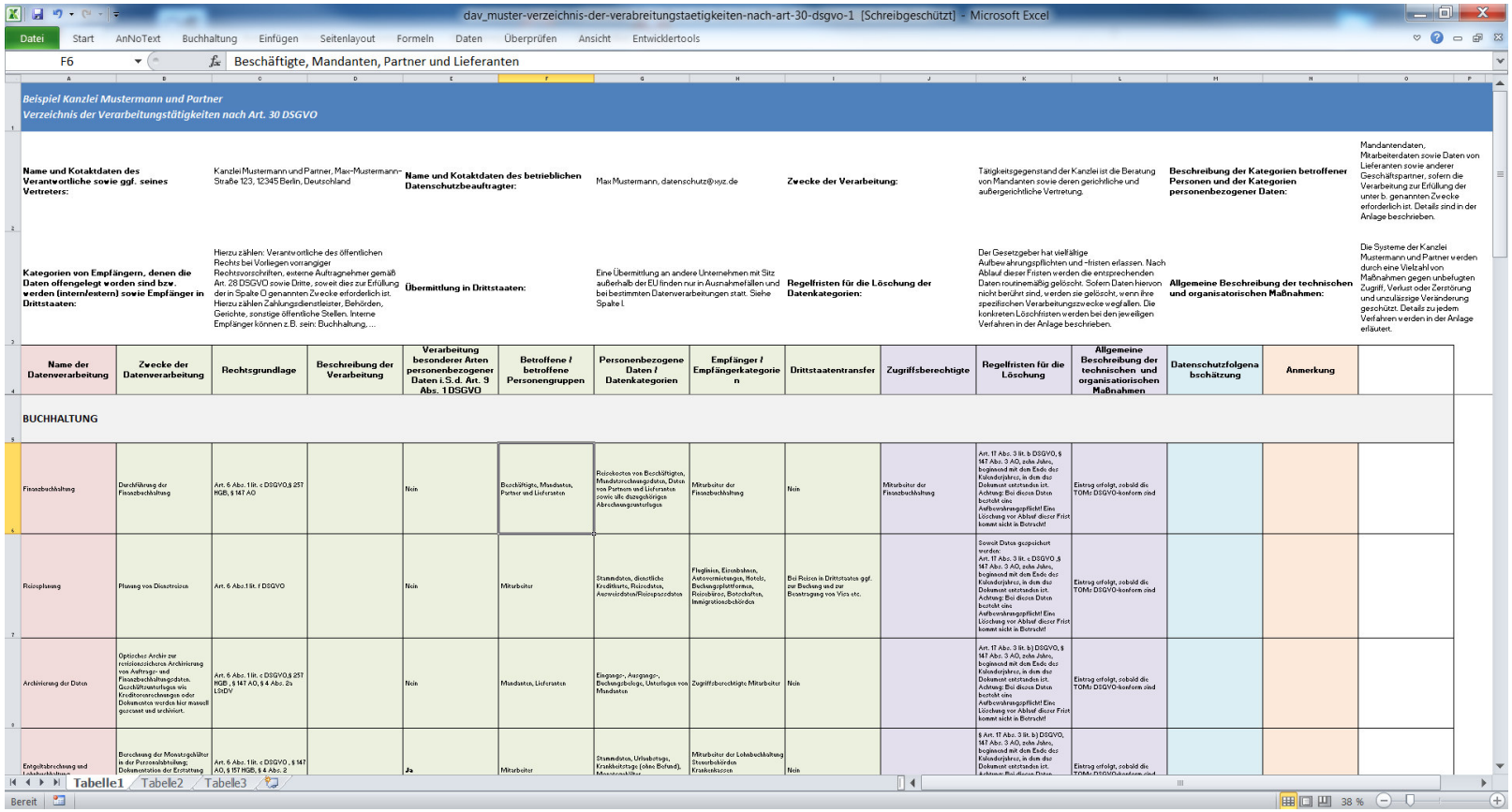
Art. 5 Abs. 2: Rechenschaftspflicht („Accountability“):

„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)

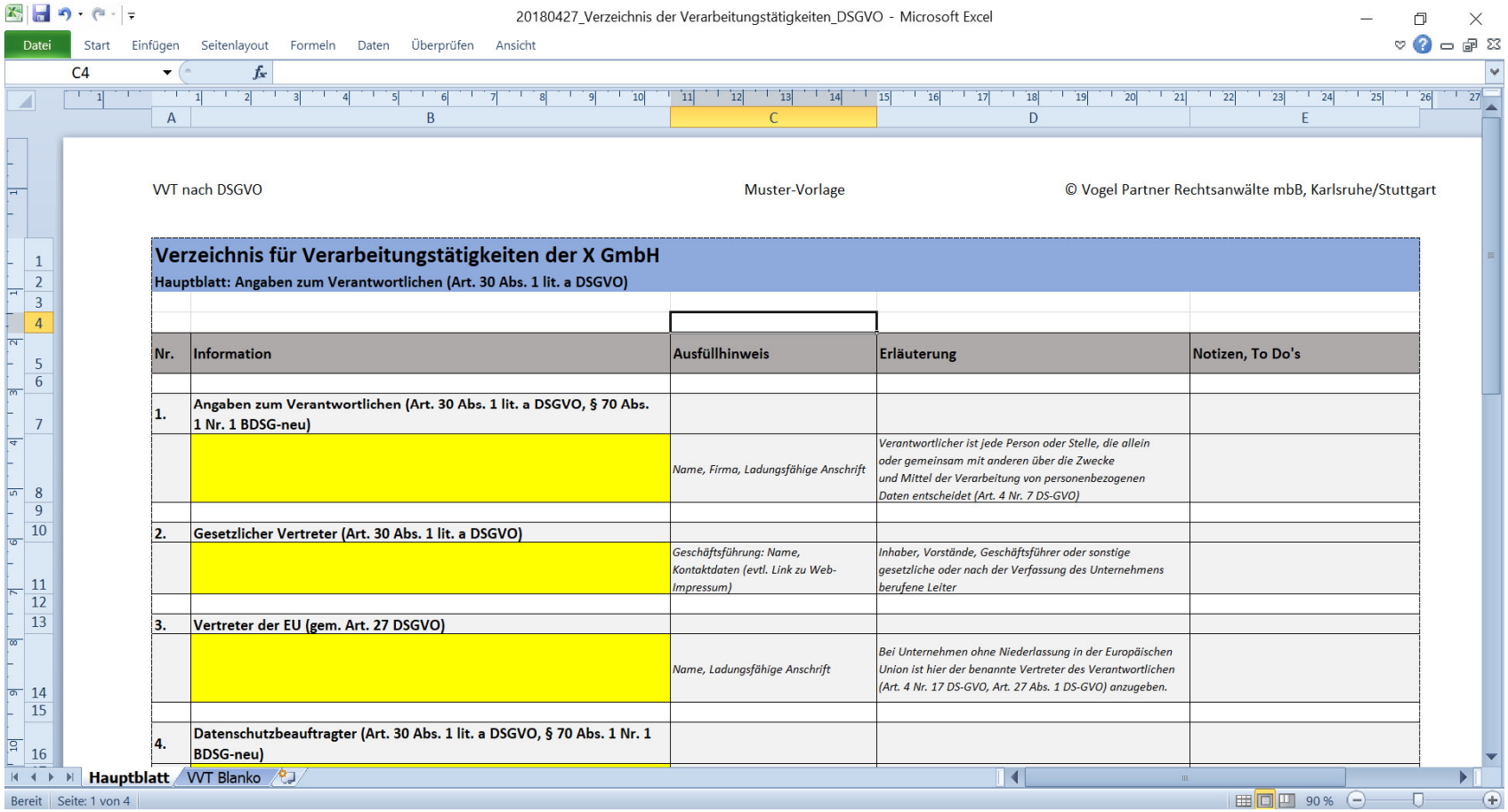
VVT-Vorlage des Deutschen Anwaltsvereins



(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-verabreitungstaetigkeiten-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)

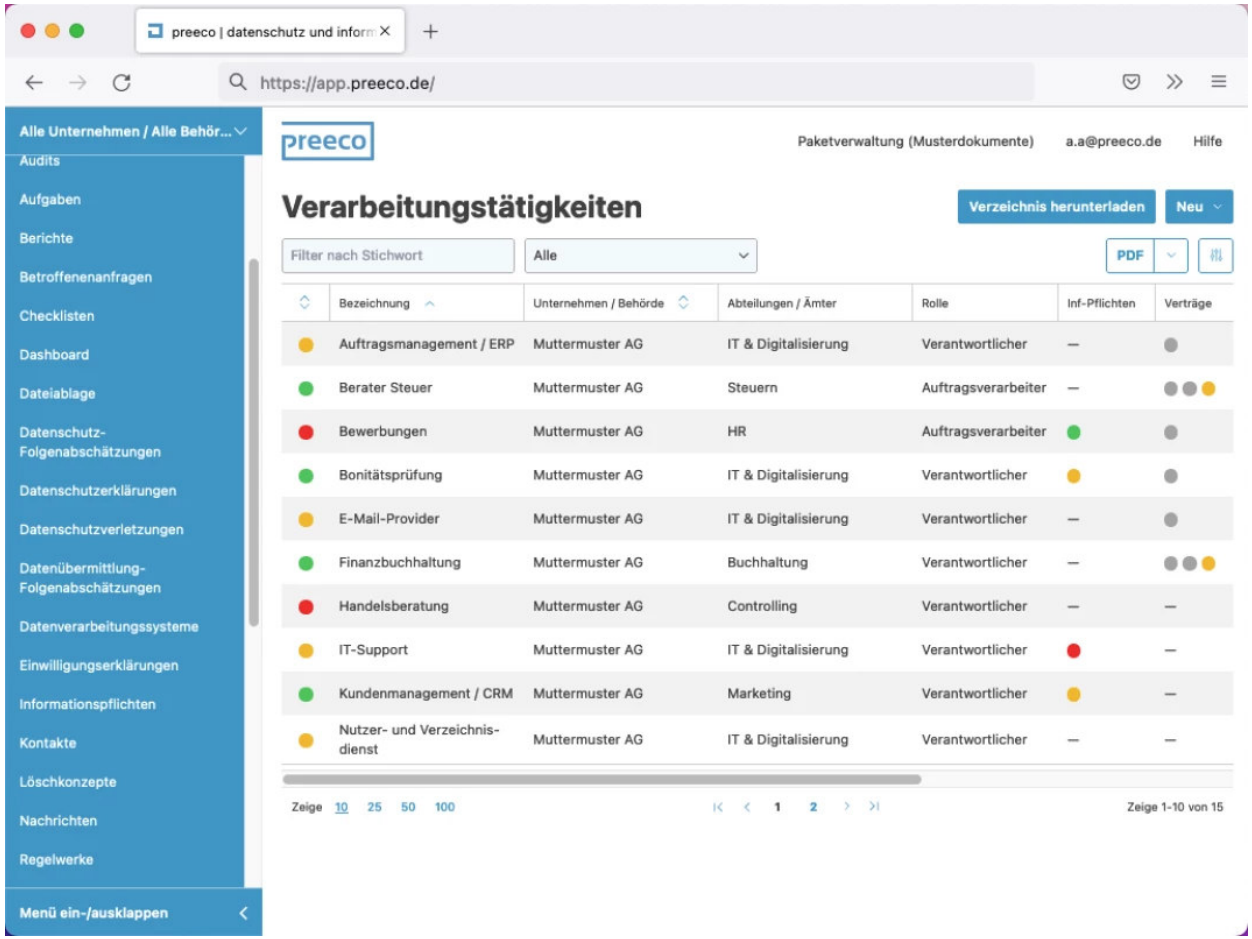
Nr.	Information	Ausfüllhinweis	Erläuterung	Notizen, To Do's
1.	**Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit. a DSGVO, § 70 Abs. 1 Nr. 1 BDSG-neu)**			
		Name, Firma, Ladungsfähige Anschrift	*Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und 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 | 90 %

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

VVT – spezielle Software



→ Bei mittleren und jedenfalls größeren Unternehmen zu empfehlen.

→ Leichter arbeitsteilig zu pflegen und aktuell zu halten.

→ Z.B. preeco.

→ 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

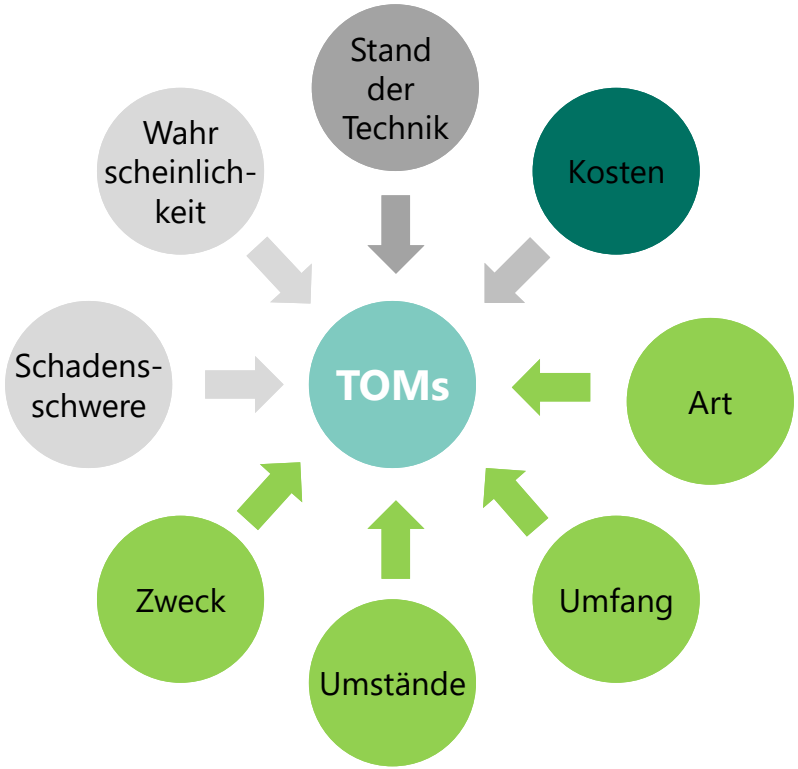
Art. 24 – Verantwortung des für die Verarbeitung Verantwortlichen

*(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

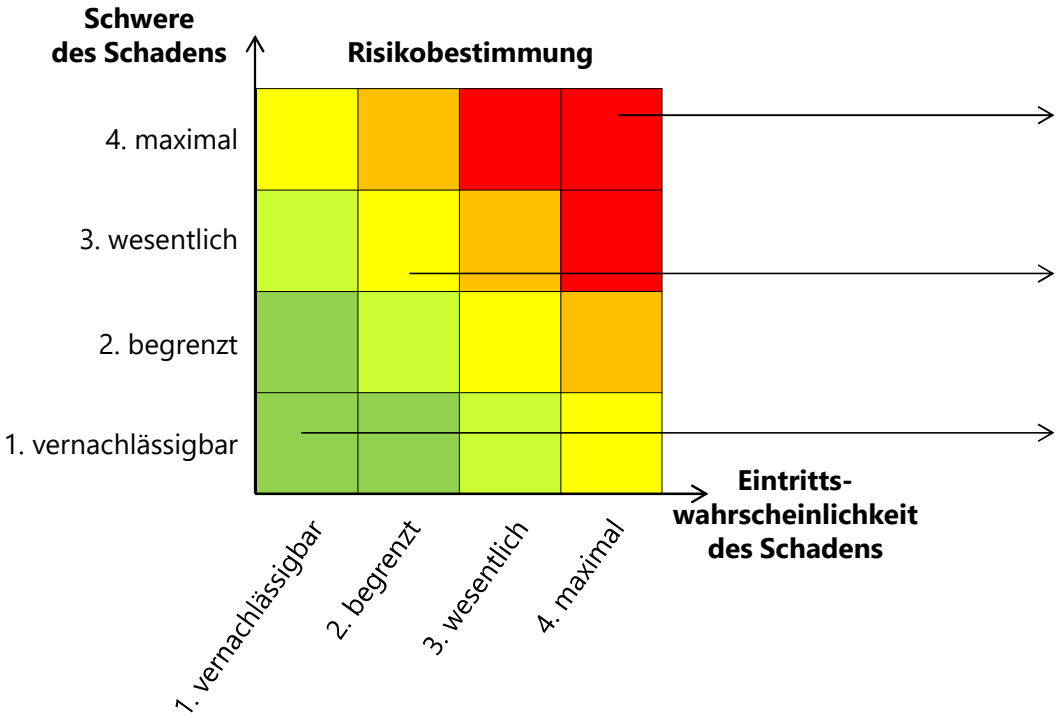
*(1) Unter Berücksichtigung des **Stands der Technik**, der **Implementierungskosten** und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der **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

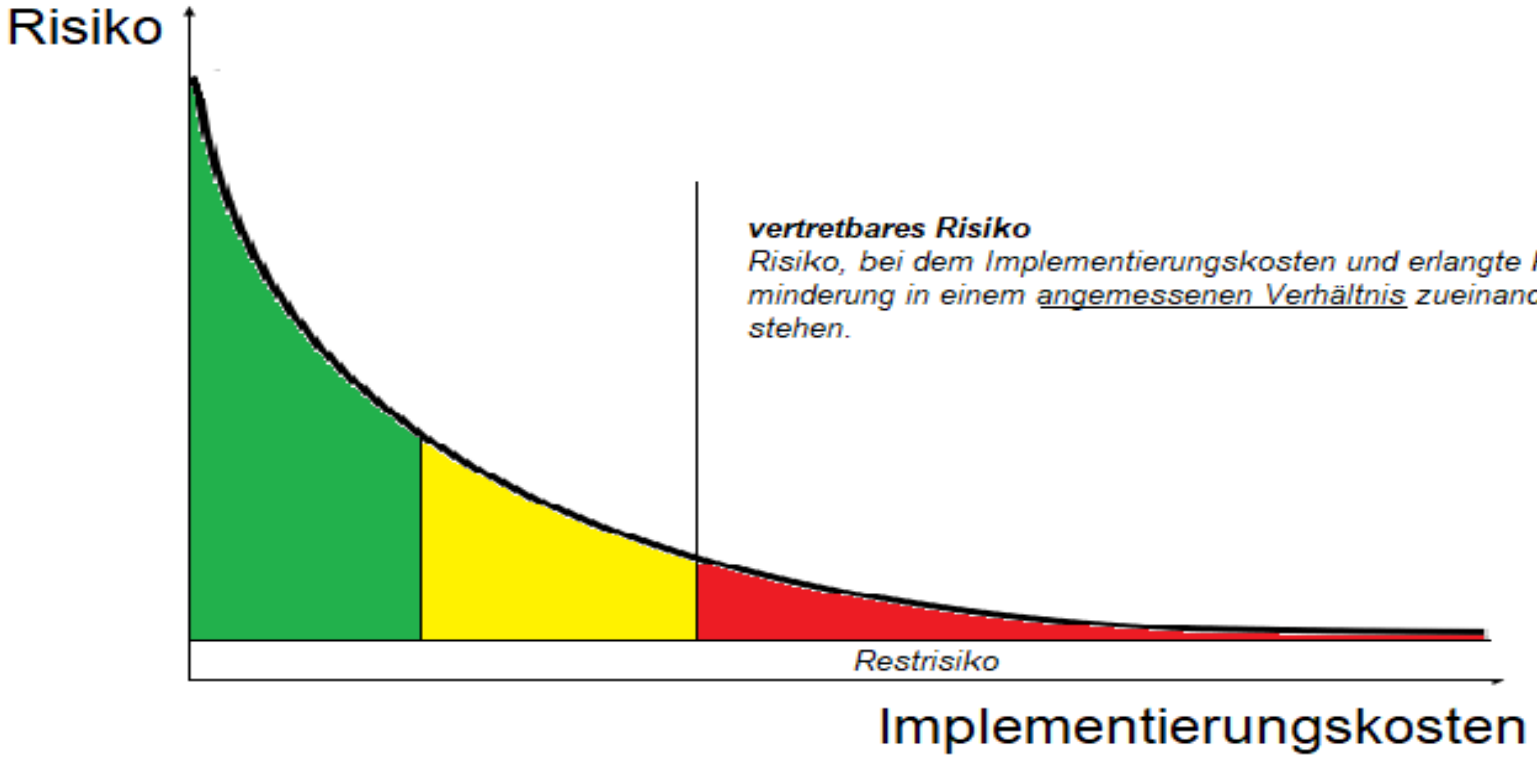
Profilbildung von Aufenthaltsorten
Unzulässige Zweckänderung von Daten eines PayAsYouGo-Drive-Versicherers fürs Marketing

Rufschädigung
Veröffentlichung negativer Bonitätsdaten

Verlust der Vertraulichkeit
Fehlversand einer Privatrechnung durch Psychiater

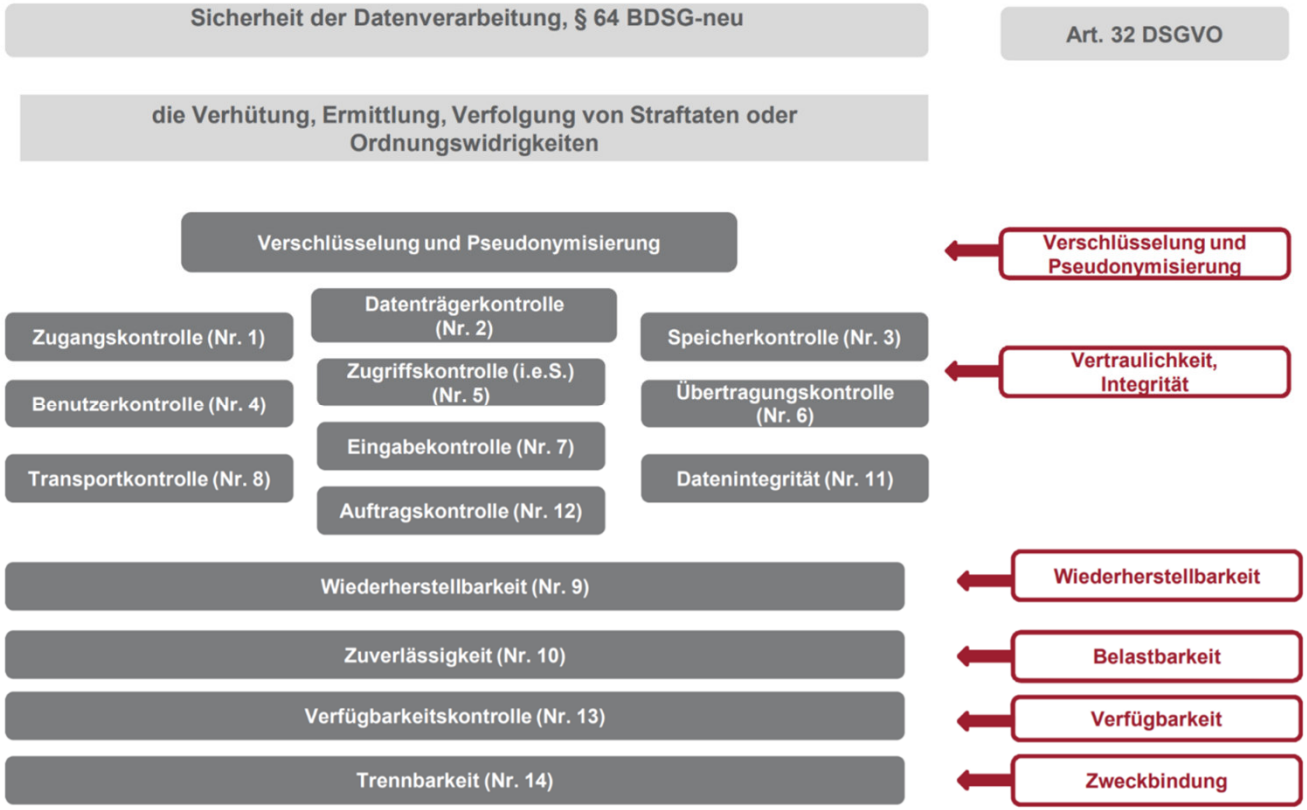
Hinderung der Kontrolle über die eigenen Daten
Keine Möglichkeit eigene Fotos in Portal für Mitarbeiter zu löschen

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_Klaos.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 Datenschutzanforderungen, 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