DSGVO

Datenschutz-Grundverordnung

Andreas Jensch, Jastus GmbH | 13. Juni 2018

Änderung der Rechtsgrundlage

Bundesdatenschutzgesetz
(BDSG)

Seit
25.05.2018

Nach einer 2 jährigen
Übergangsfrist

DSGVO
EU-Datenschutz-Grundverordnung

+

Neue
Fassung

Rechtsgrundlage

Verbot mit Erlaubnisvorbehalt (Art. 6 Abs. 1)

=

Rechtsprinzip, nach dem ein bestimmtes Verhalten grundsätzlich verboten ist, sofern nicht ausdrücklich eine Erlaubnis erteilt wird

Jede Verarbeitung von personenbezogenen Daten ohne Rechtsgrund ist rechtswidrig!

Verarbeitung personenbezogener Daten

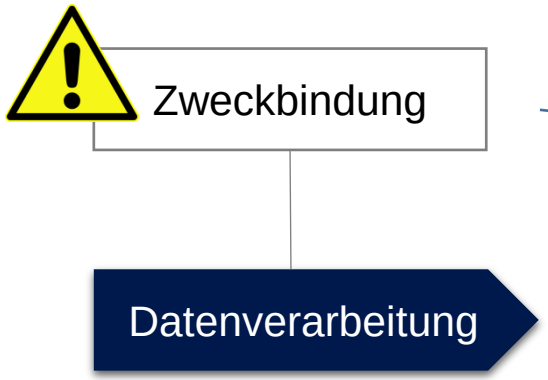
Verantwortlicher muss Einhaltung nachweisen („**Rechenschaftspflicht**“)
Art. 5 Abs. 2

Nachweis erbringen

Verarbeitung personenbezogener Daten

Rechtmäßigkeit Art. 6	**Transparenz** Art. 12	**Verant. des Verantwortl.** Art. 24	**Sicherheit der Verarb.** Art. 32	**Auftragsverarbeiter** Art. 28	**Verzeichnis** Art. 30	+	**Übermittlung Drittland** Art. 44
Spezifischer Zweck	Geeignete [illegible]ahmen zur [illegible]a-tion u[illegible] Kommunikation	Geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Einhaltung			Verzeichnis aller Verarbeitungen führen		Bestimmungen zur Sicherstellung des Schutzniveaus
Rechtsgrundlage	**Information & Kommunikation**	**Nachweis erbringen**			**Dokumentation**		**Bestimmungen anwenden**

Prüfen der Rechtmäßigkeit, Art. 6



Rechtsgrundlage

- **Einwilligung**
- Vertragserfüllung
- Berechtigtes Interesse
- Schutz lebenswichtiger Interessen
- Wahrung öffentlicher Interessen
- Zur Erfüllung einer gesetzlichen Verpflichtung

Rechtsgrundlage der Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses (Beschäftigtendaten) ergibt sich aus § 26 BDSG neu. Bewerber für ein Beschäftigungsverhältnis gelten als Beschäftigte (§ 26 Abs. 8 BDSG-neu)!

Prüfen der Rechtmäßigkeit, Art. 6

Regelmäßige Prüfung, ob valide Rechtsgrundlage für Verarbeitung vorliegt und Zweckbindung gewahrt ist

Wenn die betriebliche Notwendigkeit zur Speicherung der Daten wegfällt, muss gelöscht werden.
Hier sollte ein wirksames Vorgehen zur regelmäßigen Kontrolle festgelegt werden (sog. Löschkonzept)
Aber: Gesetzliche Aufbewahrungsfristen beachten!

Grundsätzlich nur die pb Daten erheben und speichern, die für den Zweck wirklich benötigt werden (Daten-sparsamkeit), keine „Sammelwut“

Vorsicht bei „gekauften“ Kontaktdaten

Verarbeitung personenbezogener Daten

Verantwortlicher muss Einhaltung nachweisen („**Rechenschaftspflicht**“)
Art. 5 Abs. 2

Nachweis erbringen

Verarbeitung personenbezogener Daten

Rechtmäßigkeit Art. 6	**Transparenz** Art. 12	**Verant. des Verantwortl.** Art. 24	**Sicherheit der Verarb.** Art. 32	**Auftrags-verarbeiter** Art. 28	**Verzeichnis** Art. 30	+	**Übermittlung Drittland** Art. 44
Spezifischer Zweck	Geeignete Maßnahmen zur Informa-tion und Kommunikation	Geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Einhaltung			Verzeichnis aller Verarbeitungen führen		Bestimmungen zur Sicher-stellung des Schutzniveaus
Rechtsgrund-lage	**Information & Kommunikation**	**Nachweis erbringen**			**Dokumentation**		**Bestimmungen anwenden**

Transparenz, Art. 12

Transparente Information, Kommunikation und Modalitäten

„Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen, die sich auf die Verarbeitung beziehen, in **präziser, transparenter, verständlicher** und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln“

Zweck der Datenerhebung und Rechtsgrundlage
Art. 6

Widerspruchsrecht
Art. 21

Recht auf Berichtigung, Löschung, Einschränkung
Art. 16 - 19

Einsatz von automatisierten Entscheidungen
Art. 22

Recht auf Datenübertragbarkeit
Art. 20

Recht auf Widerruf der Einwilligung
Art. 7 Abs. 3

Auskunftsrecht
Art. 15

Löschung von Daten, wenn Zweck entfällt
Art. 5 Abs. 1

Transparenz, Art. 12

Datenschutzerklärung auf Homepage anpassen

Vor dem Versand von Newslettern, Kunden (auch Bestandskunden) gem. Art. 12 ff. informieren und Einwilligung einholen (Opt-in)

Aktualisierung von AGB und Vertragsmustern zum Thema personenbezogene Daten

Informationspflicht und Betroffenenrechte gelten auch bei der Veröffentlichung von Fotos z.B. auf der Homepage

Verarbeitung personenbezogener Daten

Verantwortlicher muss Einhaltung nachweisen („**Rechenschaftspflicht**“)
Art. 5 Abs. 2

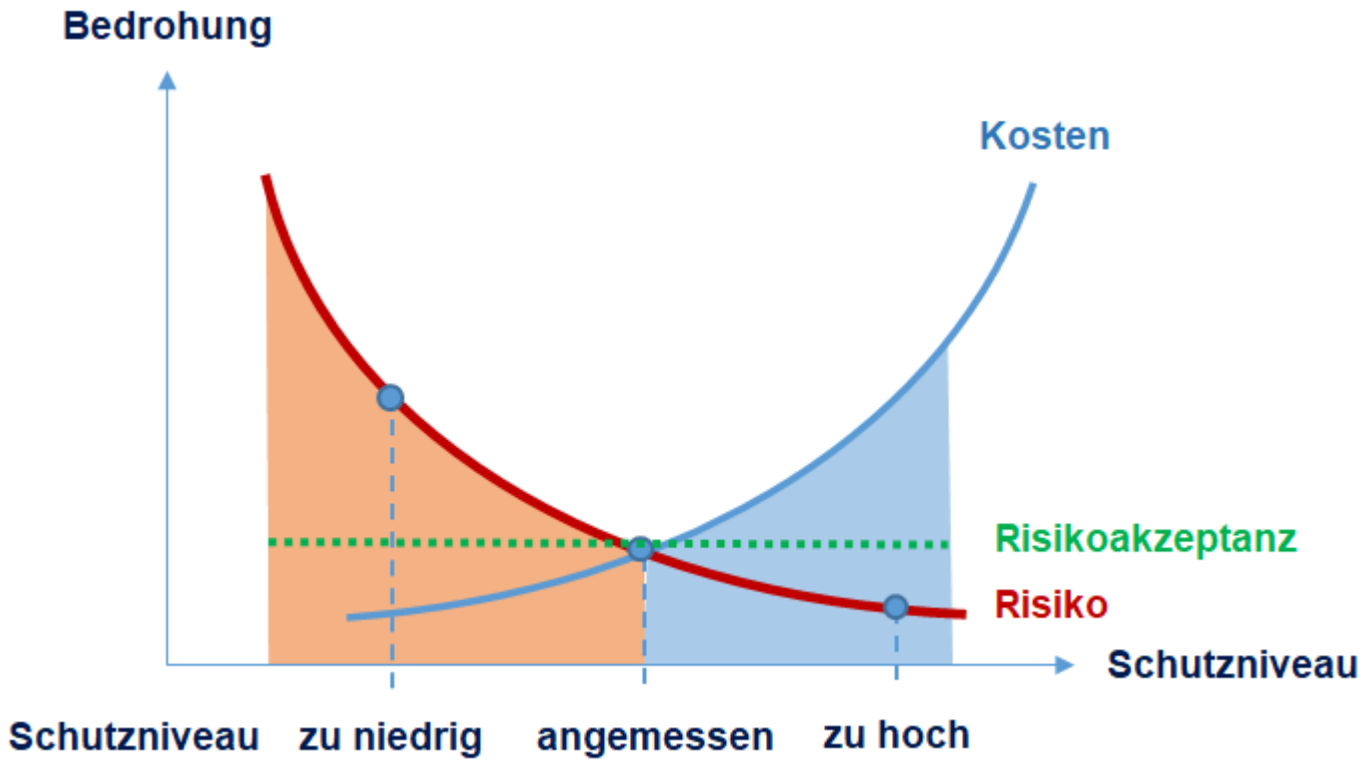
Nachweis erbringen

Verarbeitung personenbezogener Daten

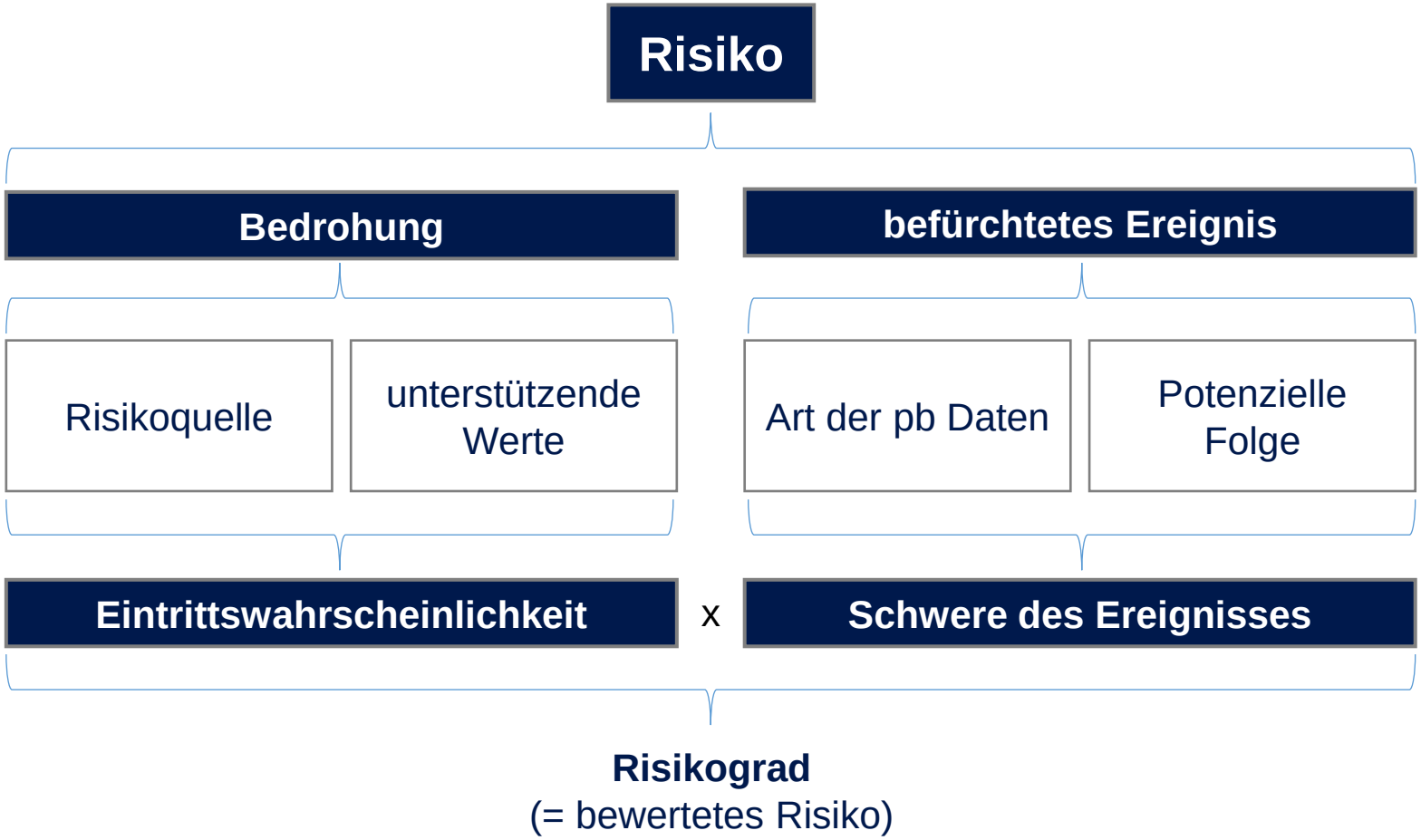
Rechtmäßigkeit Art. 6	**Transparenz** Art. 12	**Verant. des Verantwortl.** Art. 24	**Sicherheit der Verarb.** Art. 32	**Auftragsverarbeiter** Art. 28	**Verzeichnis** Art. 30	+	**Übermittlung Drittland** Art. 44
Spezifischer Zweck	Geeignete Maßnahmen zur Information und Kommunikation	Geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Einhaltung			Verzeichnis aller Verarbeitungen führen		Bestimmungen zur Sicherstellung des Schutzniveaus
Rechtsgrundlage	**Information & Kommunikation**	**Nachweis erbringen**			**Dokumentation**		**Bestimmungen anwenden**

Verantwortung des für die Verarbeitung Verantwortlichen, Art. 24

Die DSGVO verlangt einen **risikobasierten** Schutz der Daten: Je höher das Risiko der Datenverarbeitung, desto höher ist das notwendige Schutzniveau!



Verantwortung des für die Verarbeitung Verantwortlichen, Art. 24



Verantwortung des für die Verarbeitung Verantwortlichen, Art. 24

Risikoquelle	Bedrohung	unterstützende Werte
Menschliche Quelle - Intern - Unbeabsichtigtes Handeln - Vorsätzliches Handeln **Menschliche Quelle - Extern** - Vorsätzliches Handeln **Nichtmenschliche Quelle** - Intern - Extern	- Fehlverhalten / -funktion - Beschädigung - Spionage - Verlust - Veränderung - Überlastung	**Informationssysteme** - Hardware - Software - Netzwerke **Organisation** - Personen - Dokumente

Verantwortung des für die Verarbeitung Verantwortlichen, Art. 24

Die Eintrittswahrscheinlichkeit

Bereich	Realisierbarkeit der Bedrohung durch die Risikoquelle in Bezug auf einen Vermögenswert	Beispiele
1. Vernachlässigbar	Scheinbar unmöglich	z.B. Diebstahl von Papierdokumenten, die in einem von einem Ausweisleser und einem Zugangscode geschützten Raum gelagert sind
2. Begrenzt	Schwierig (machbar mit gewissem Aufwand)	z.B. Diebstahl von Papierdokumenten, die in einem durch ein Ausweislesegerät geschützten Raum aufbewahrt werden
3. Wesentlich	Möglich (machbar auch mit geringem Aufwand)	z.B. Diebstahl von Papierdokumenten, die in Büros gelagert sind, die durch Personenkontrollen geschützt sind
4. Maximal	Einfach	z.B. Diebstahl von Papierdokumenten, die in einer Lobby lagen

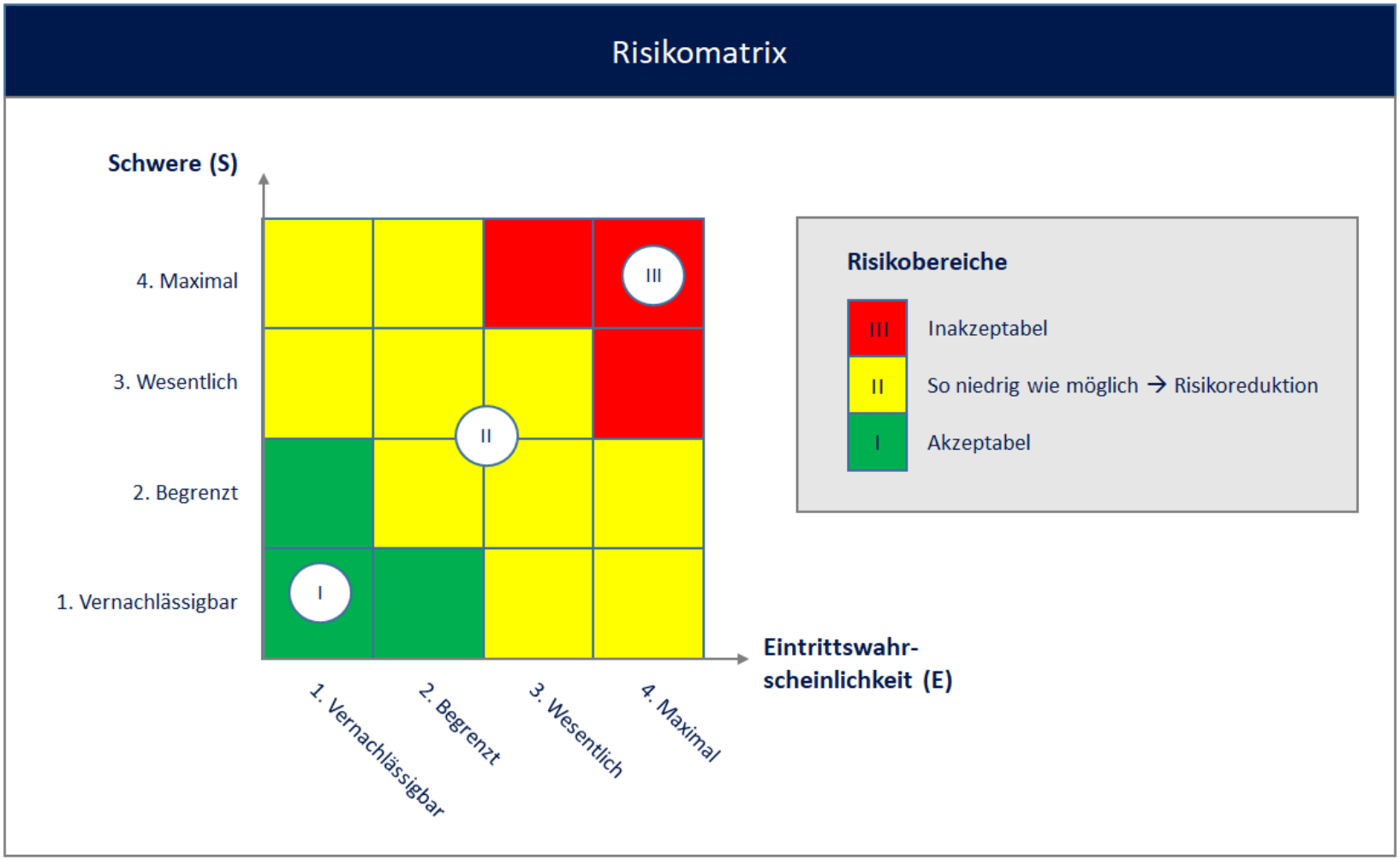
Verantwortung des für die Verarbeitung Verantwortlichen, Art. 24

Jastus GmbH
Fachberatung für Informationssicherheit und Datenschutz

Die Schwere des Ereignisses

Bereich	Auswirkung auf Betroffenen	Folgen überwinden können	Beispiele
1. Vernachlässigbar	Nicht betroffen oder nur kleine Unannehmlich-keiten	Unannehmlichkeiten sollten sich problemlos beheben lassen	Zeitverlust durch erneute Eingabe von Informationen, Ärgernisse, Irritationen, etc.
2. Begrenzt	Wesentliche Unannehmlich-keiten	Wesentliche Unannehmlichkeiten sollten sich – trotz gewisser Schwierigkeiten – überwinden lassen	Zusätzliche Kosten, Verweigerung des Zugangs zu Geschäftsdiensten, Angst, Mangel an Verständnis, Stress, leichte körperliche Beschwerden, etc.
3. Wesentlich	Wesentliche Folgen	Wesentliche Folgen sollten sich – trotz gewisser Schwierigkeiten – überwinden lassen	Missbrauch von Geldern, Blacklisting von Banken, Sachschäden, Arbeitslosigkeit, Vorladung, Verschlechterung des Gesundheitszustands usw.
4. Maximal	Wesentliche und/oder irreversible Folgen	Irreversible Folgen kaum bzw. nicht überwindbar	Finanzielle Not wie hohe Schulden oder Arbeitsunfähigkeit, langfristige psychische oder körperliche Beschwerden, Tod usw.

Verantwortung des für die Verarbeitung Verantwortlichen, Art. 24



Verantwortung des für die Verarbeitung Verantwortlichen, Art. 24

Risikobereiche

III	Inakzeptabel
II	So niedrig wie möglich → Risikoreduktion
I	Akzeptabel

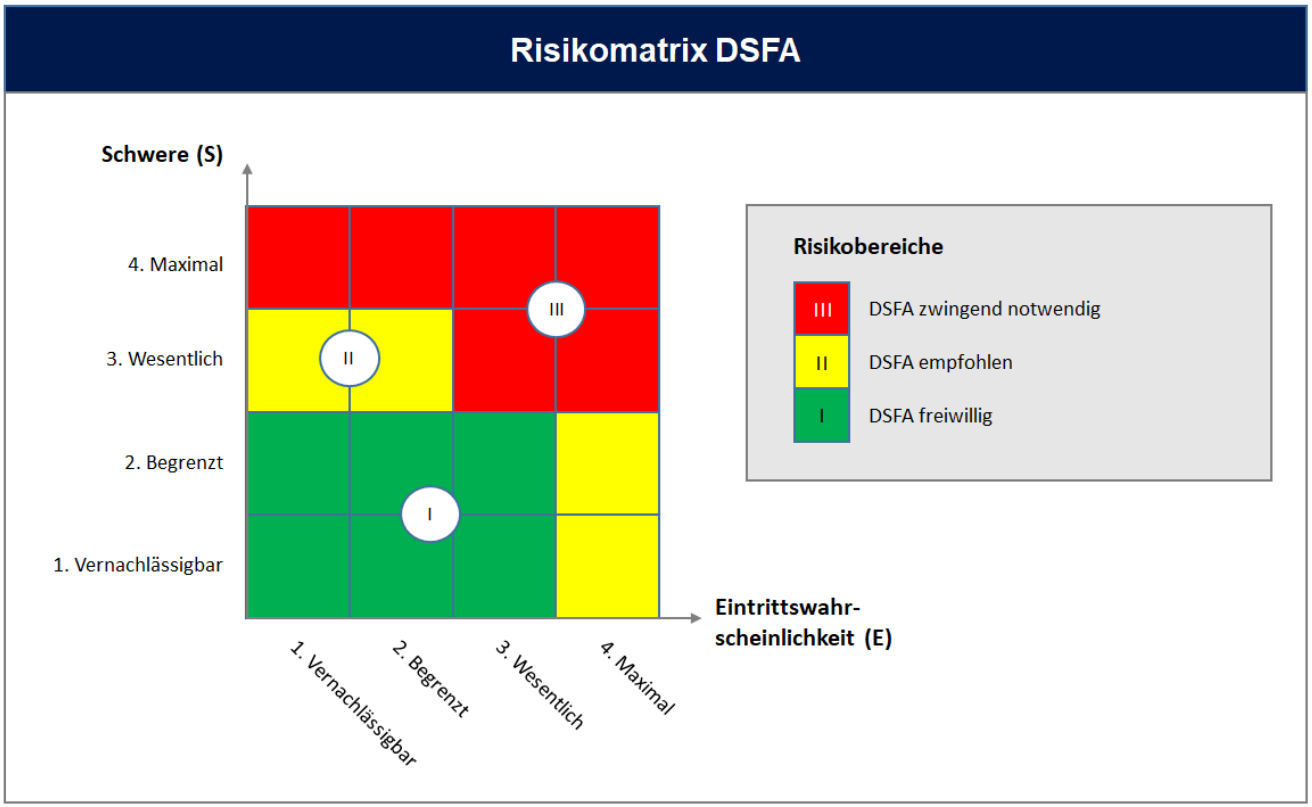
III — Risikograd zu hoch. Zwingend weitere Schutzmaßnahmen einführen oder von der Verarbeitung der Daten absehen!

II — Weitere Schutzmaßnahmen in Betracht ziehen, bis Risikoakzeptanz-schwelle erreicht ist (Risikoreduktion). Alternativ, Übertragung des Risikos (Versicherung, Outsourcing). Aber: Keine Übertragung der Haftung möglich!

I — Restrisiko wird von Geschäftsleitung akzeptiert und dokumentiert

Datenschutz-Folgeabschätzung, Art. 35

Ergibt eine Abschätzung der Risiken der Verarbeitungsvorgänge für den Betroffenen ein **hohes Risiko** (sog. Schwellwertanalyse), ist eine **Datenschutz-Folgeabschätzung (DSFA)** durchzuführen!



Datenschutz-Folgeabschätzung, Art. 35

Prozess Datenschutz-Folgenabschätzung

Schwellwert-analyse

- Feststellung der Erforderlichkeit einer DSFA (voraussichtlich hohes Risiko)

Vorbereitung

- Zusammenstellung des DSFA-Teams
- DSFA-Plan erstellen und erforderliche Ressourcen ermitteln
- Beschreibung des Beurteilungsumfangs (Geschäftsprozesse, Informations-systeme)
- Stakeholder einbinden

Durchführung

- Analyse der Datenflüsse
- Ermittlung der zu berücksichtigenden Anforderungen / Faktoren
- Risikobeurteilung
- Vorbereitung der Risikobehandlung

Nachverfolgung

- DSFA-Bericht erstellen
- Umsetzung des Riskobehandlungs-plans
- Berücksichtigung von Änderungen
- Ggfs. Überprüfung und Audit der DSFA
- **Bei hohem Restrisiko: Meldung an die Aufsichtsbehörde (Art. 36 DSGVO)**

Datenschutz-Folgeabschätzung, Art. 35

Jastus GmbH
Fachberatung für Informationssicherheit und Datenschutz

Bericht DSFA

- Umfang der DSFA
  - Beschreibung Verarbeitungsprozess
    - Übersicht
    - Systemarchitektur
    - Wartung und Betrieb
  - Beteiligte Personen
  - Datenschutzanforderungen (Rechtsgrundlage)
- Risikobeurteilung
  - Risikoquellen
  - Bedrohungen / Eintrittswahrscheinlichkeiten
  - Folgen / Schwere
  - Risikobewertung (Risikomatrix)
  - Compliance-Analyse
- Maßnahmenplan zur Risikobehandlung (Auswahl geeigneter Abhilfemaßnahmen)
- Fazit und Entscheidungen

Verarbeitung personenbezogener Daten

Verantwortlicher muss Einhaltung nachweisen („**Rechenschaftspflicht**“)
Art. 5 Abs. 2

Nachweis erbringen

Verarbeitung personenbezogener Daten

Rechtmäßigkeit Art. 6	**Transparenz** Art. 12	**Verant. des Verantwortl** Art. 24	**Sicherheit der Verarb.** Art. 32	**Auftrags-verarbeiter** Art. 28	**Verzeichnis** Art. 30	+	**Übermittlung Drittland** Art. 44
Spezifischer Zweck	Geeignete Maßnahmen zur Informa-tion und Kommunikation	Geeignete technische und organi[illegible]sche Maßnahmen zur Sicherstellung der Einh[illegible]			Verzeichnis aller Verarbeitungen führen		Bestimmungen zur Sicher-stellung des Schutzniveaus
Rechtsgrund-lage	**Information & Kommunikation**	**Nachweis erbringen**			**Dokumentation**		**Bestimmungen anwenden**

Sicherheit der Verarbeitung, Art. 32-34

Art. 32 bedeutet einen gesetzlich vorgeschriebenen Mindest-standard an IT-Sicherheit, sog. **technische und organisatorische Maßnahmen (TOMs)**

Für kleine Betriebe und Vereine sind im Allgemeinen Standard-maßnahmen ausreichend:

- Alle Computer, Tablets und Handys sind mit Passwörtern oder PIN gegen fremden Zugriff geschützt
- Der Zugriff auf personenbezogene Daten ist auf bestimmte Personen beschränkt (Need-to-Know Prinzip)
- Sicherheits-Updates des Betriebssystems werden automatisch eingespielt
- Ein Virenschutzprogramm ist auf allen Computern installiert und wird regelmäßig aktualisiert
- Daten werden regelmäßig und fachgerecht gesichert (Backup)

Verarbeitung personenbezogener Daten

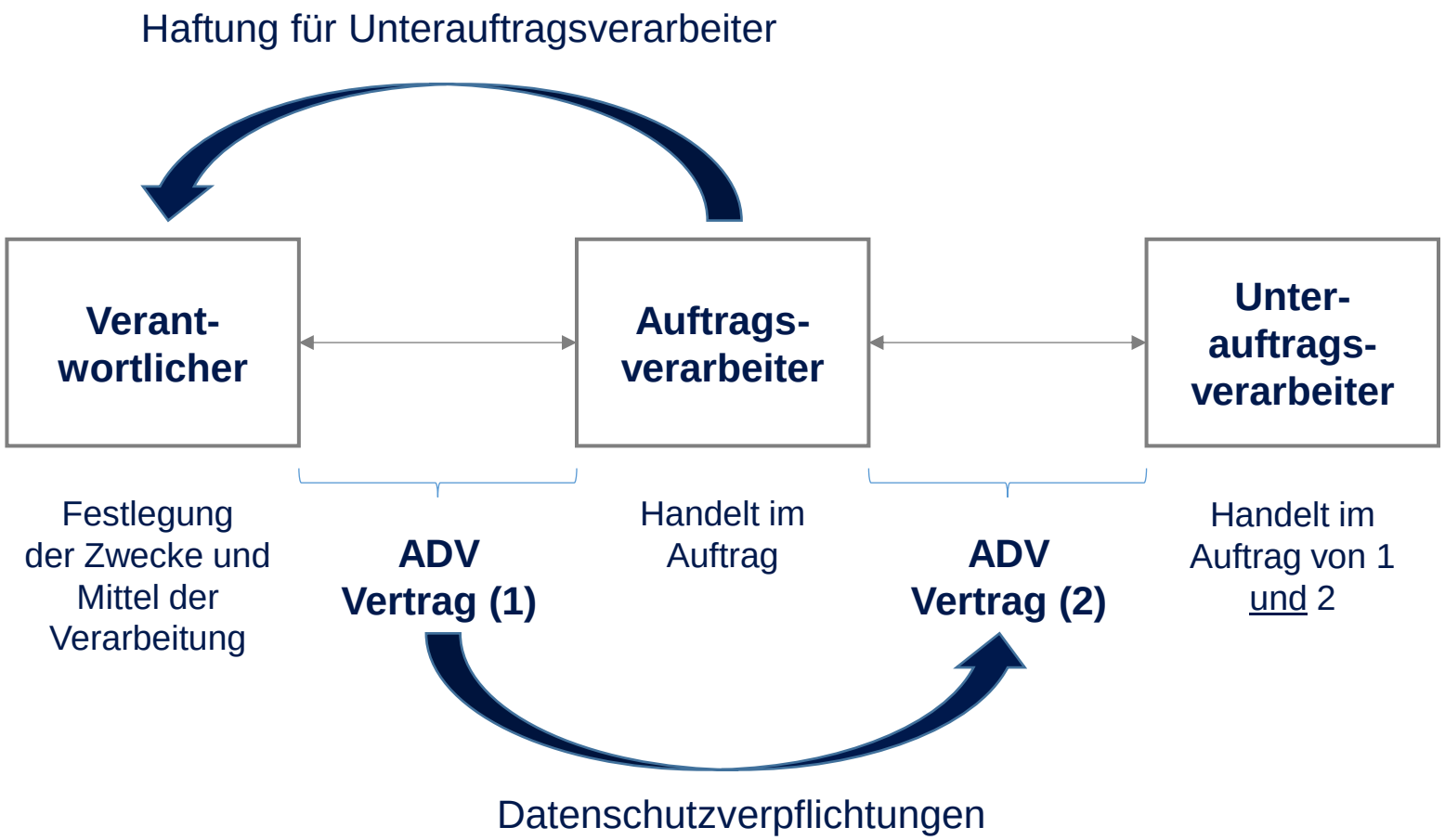
Verantwortlicher muss Einhaltung nachweisen („**Rechenschaftspflicht**“)
Art. 5 Abs. 2

Nachweis erbringen

Verarbeitung personenbezogener Daten

Rechtmäßigkeit Art. 6	**Transparenz** Art. 12	**Verant. des Verantwortl.** Art. 24	**Sicherheit der Verarb** Art. 32	**Auftrags-verarbeiter** Art. 28	**Verzeichnis** Art. 30	+	**Übermittlung Drittland** Art. 44
Spezifischer Zweck	Geeignete Maßnahmen zur Informa-tion und Kommunikation	Geeignete technische und organ[illegible]atorische Maßnahmen zur Sicherstellung der Einh[illegible]			[illegible]erzeichnis [illegible] Verarbe[illegible]n führen		Bestimmungen zur Sicher-stellung des Schutzniveaus
Rechtsgrund-lage	**Information & Kommunikation**	**Nachweis erbringen**			**Dokumentation**		**Bestimmungen anwenden**

Auftragsverarbeiter, Art. 28



Der Verantwortliche haftet immer für den Gesamtprozess!

Auftragsverarbeiter, Art. 28

Auftragsverarbeitung können regelmäßig z. B. folgende Dienstleistungen sein:

- Auslagerung der Lohn- und Gehaltsabrechnung oder der Finanzbuchhaltung (gilt nicht für Steuerberater)
- Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud-Computing (z.B. CRM-Systeme, Finanzsoftware, E-Mail Provider)
- Wartung (z. B. Fernwartung, externer Support) von Computern oder Servern, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann
- Auslagerung der Webseitenbetreuung (z. B. bei Betreuung von Kontaktformularen und Nutzerauswertungen und Statistiken über Cookies)
- Werbeadressenverarbeitung in einem Lettershop
- Personaldienstleistungen, z.B. bei Arbeitnehmerüberlassung
- Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten
- Outsourcing von Archivierungsvorgängen
- Datenträger- oder Dokumentenentsorgung durch externen Dienstleister

Verarbeitung personenbezogener Daten

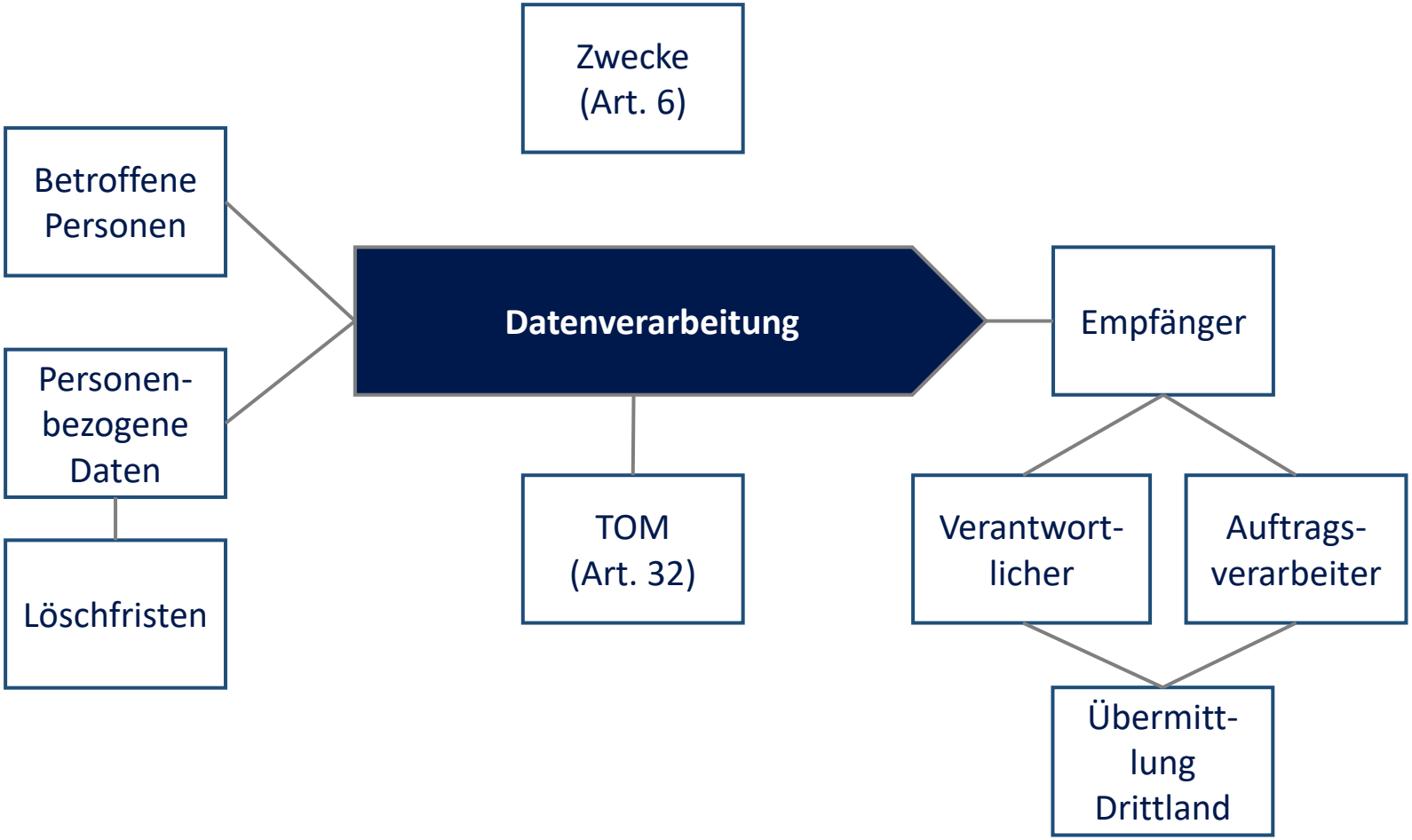
Verantwortlicher muss Einhaltung nachweisen („**Rechenschaftspflicht**“)
Art. 5 Abs. 2

Nachweis erbringen

Verarbeitung personenbezogener Daten

Rechtmäßigkeit Art. 6	**Transparenz** Art. 12	**Verant. des Verantwortl.** Art. 24	**Sicherheit der Verarb.** Art. 32	**Auftrags-verarbeiter** Art. 28	**Verzeichnis** Art. 30	+	**Übermittlung Drittland** Art. 44
Spezifischer Zweck	Geeignete Maßnahmen zur Informa-tion und Kommunikation	Geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Einhaltung			Verzeichnis aller Verarbeitungen führen		Bestimmungen zur Sicher-stellung des Schutzniveaus
Rechtsgrund-lage	**Information & Kommunikation**	**Nachweis erbringen**			**Dokumentation**		**Bestimmungen anwenden**

Verzeichnis von Verarbeitungstätigkeiten, Art. 30



Verzeichnis von Verarbeitungstätigkeiten, Art. 30

Muster 12: Einzelhändler – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
Bekleidungshaus Huber
Hinterer Weg 15
91522 Fallstadt

Tel. 0981/123456-0
E-Mail: info@modehuber-fallstadt.de
Web: www.modehuber-fallstadt.de

Inhaber: Gerhard Huber, geb. 21.02.1986

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über Buchhaltungsbüro)	Hans Klausen 0981/123456-1 hans@ modehuber- fallstadt.de	01.01.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name und Adressen der Beschäftigten • ggf. Religions-zugehörigkeit • Eindeutige Kennzahlen zur Steuer...	Buchhaltungs-büro	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Betrieb der Webseite (über Hosting-Dienstleister)	Peter Diercksen 0981/123456-2 peter@ modehuber- fallstadt.de	19.03.2018	Unternehmens-darstellung	• Kunden • Webseitenbesucher	• IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept
Kundenkarten-verwaltung	Marie Greiner 0981/123456-3 marie@ modehuber- fallstadt.de	19.03.2018	Verwaltung der Kundendaten	Kunden	• Stammdaten der Kunden • Kaufhistorien	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Zahlungsabwicklung bei Kunden (über externen Dienstleister)	Peter Diercksen 0981/123456-2 peter@ modehuber- fallstadt.de	19.03.2018	Durchführung der Zahlungsverarbeitung	Kunden	• Stammdaten der Kunden • Zahlungsdaten (Bank-verbindung)	Zahlungsdienst-leister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Werbemaßnahmen zur Kundengewinnung und -bindung	Marie Greiner 0981/123456-3 marie@ modehuber- fallstadt.de	20.03.2018	Marketing zur Kundenakquirierung	• Bestandskunden • potenzielle Neukunden	• Postadressen der Kunden	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...	...	...	...	...	...	...	...	...	...

Weitere Muster: https://www.lda.bayern.de/de/kleine-unternehmen.html

Verzeichnis von Verarbeitungstätigkeiten, Art. 30

Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
TSV Waldermühl e.V.
Steinbauerstr. 45a
98123 Sonsthausen

Tel. 0981/123456-0
E-Mail: team@waldermuehler-tsv.de
Web: www.waldermuehler-tsv.de

Vorstand: Dieter Eckbauer-Düppels, geb. 03.12.1952

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Herbert Bauer 0981/123456-1 herbert@ waldmuehler- tsv.de	02.03.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name und Adressen der Beschäftigten • ggf. Religions-zugehörigkeit • Eindeutige Kennzahlen zur Steuer/ Sozialabgaben ...	Externer Dienstleister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Mitgliederverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler- tsv.de	02.03.2018	Verwaltung der Vereinstätigkeiten	Mitglieder	• Name und Adressen • Eintrittsdatum • Sportbereiche ...	Keine	Keine	2 Jahre nach Beendigung der Vereinsmitgliedschaft	Siehe IT-Sicherheitskonzept
Betrieb der Webseite des Sportvereins (über Hosting-Dienstleister)	Max Meier 0981/123456-0 max@ waldmuehler- tsv.de	28.02.2018	Außendarstellung	• Mitglieder • Webseitenbesucher	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept + HTTPS-Verschlüsselung
Veröffentlichung von Fotos der Mitglieder auf der Webseite	Max Meier 0981/123456-0 max@ waldmuehler- tsv.de	20.02.2018	Außendarstellung	Mitglieder	Fotos von Vereinstätigkeiten	Keine	Keine	Wenn Einwilligung widerrufen - unverzüglich	Siehe IT-Sicherheitskonzept
Beitragsverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler- tsv.de	22.02.2018	Vereinsfinanzierung	Mitglieder	Bankverbindung	Steuerberater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...	...	...	...	...	...	...	...	...	...

Weitere Muster: https://www.lda.bayern.de/de/kleine-unternehmen.html

Verarbeitung personenbezogener Daten

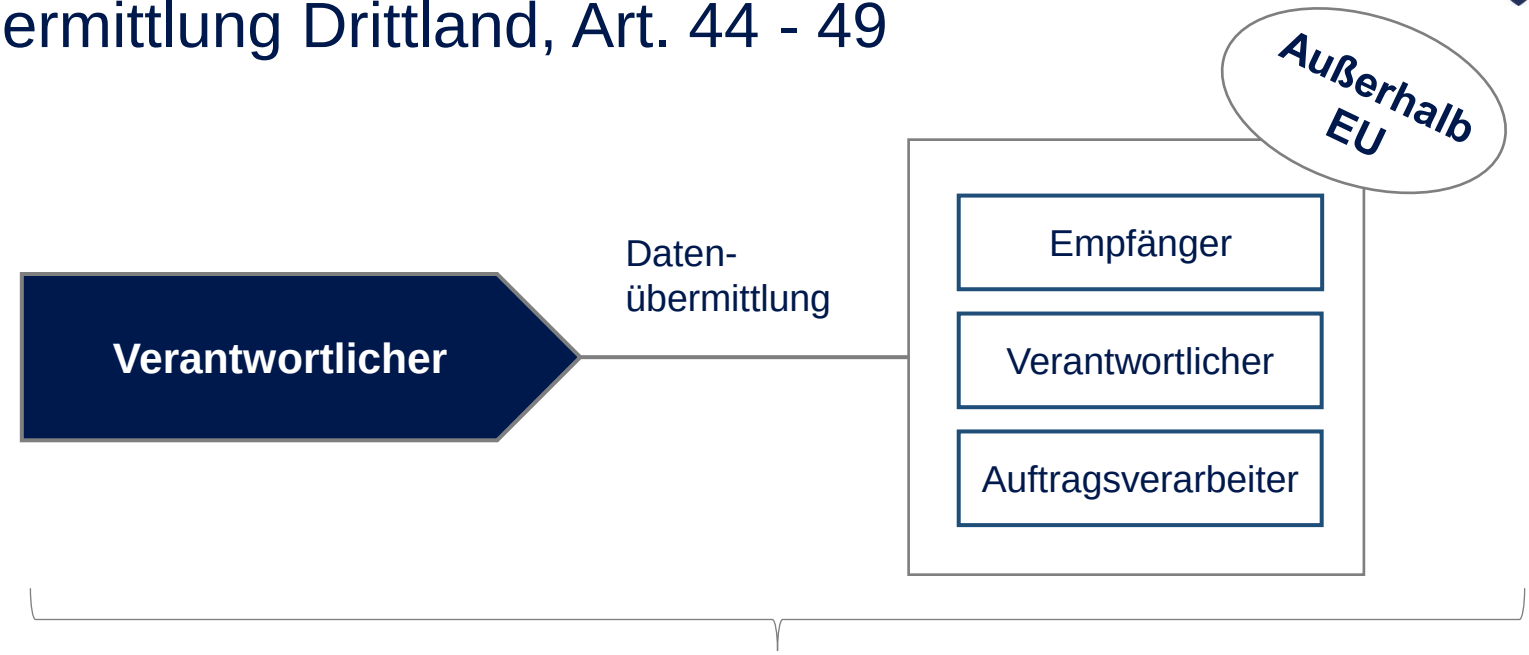
Verantwortlicher muss Einhaltung nachweisen („**Rechenschaftspflicht**“)
Art. 5 Abs. 2

Nachweis erbringen

Verarbeitung personenbezogener Daten

Rechtmäßigkeit Art. 6	**Transparenz** Art. 12	**Verant. des Verantwortl.** Art. 24	**Sicherheit der Verarb.** Art. 32	**Auftrags-verarbeiter** Art. 28	**Verzeichnis** Art. 30	+	**Übermittlung Drittland** Art. 44
Spezifischer Zweck	Geeignete Maßnahmen zur Informa-tion und Kommunikation	Geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Einhaltung			Verzeichnis all[illegible] Ve[illegible]ungen führen		Bestimmungen zur Sicher-stellung des Schutzniveaus
Rechtsgrund-lage	**Information & Kommunikation**	**Nachweis erbringen**			**Dokumentation**		**Bestimmungen anwenden**

Übermittlung Drittland, Art. 44 - 49



Angemessenheits-beschluss EU Kom.	Liste von Ländern; USA: Privacy Shield, Safe Harbour nicht mehr zulässig!	Keine weitere Maßnahme erforderlich, Aber ggf. Zertifizierung des Empfängers
Geeignete Garantien	u.a. Standardvertragsklauseln, Verbindliche interne Datenschutz-vorschriften, Binding Corporate Rules	Durchsetzbare Rechte und Rechtsbehelfe für betroffene Personen; Genehmigung Vertragsklauseln durch Aufsichtsbehörde notwendig
Ausnahmen	u.a. Ausdrückliche und freiwillige Einwilligung, Vertragserfüllung	Dokumentation der Beurteilung der Ausnahme im Verarbeitungs-verzeichnis (Art. 30), ggf. DSFA

Verarbeitung personenbezogener Daten

Verantwortlicher muss Einhaltung nachweisen („**Rechenschaftspflicht**“)
Art. 5 Abs. 2

Nachweis erbringen

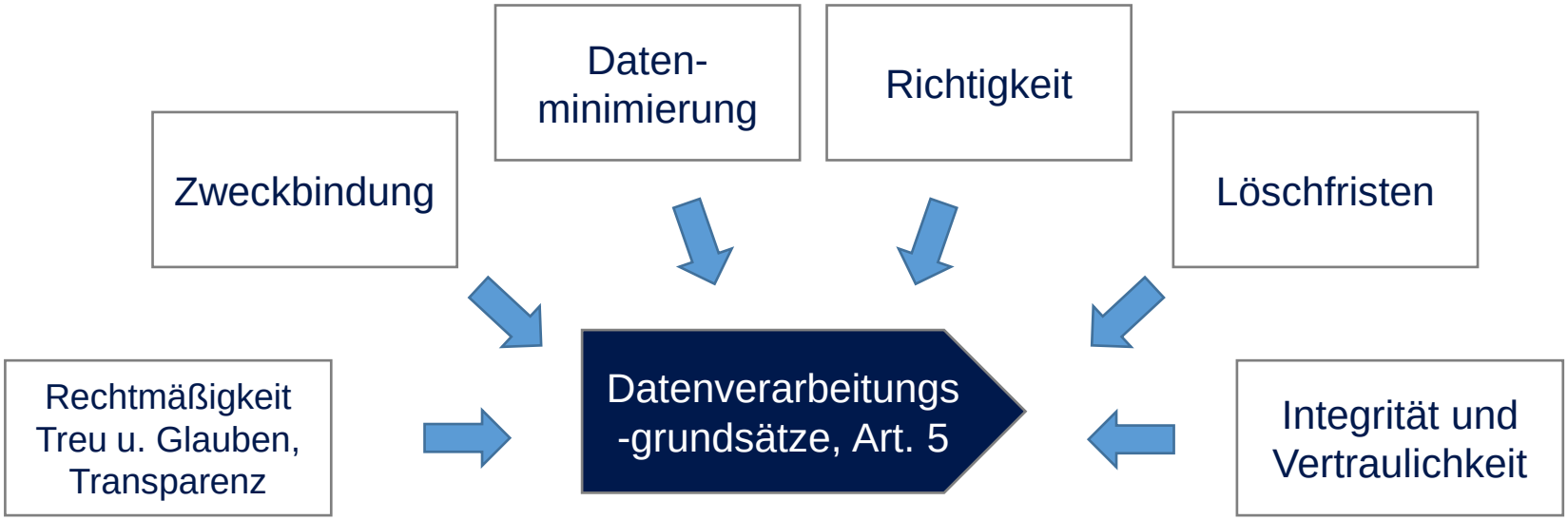
Verarbeitung personenbezogener Daten

Rechtmäßigkeit Art. 6	**Transparenz** Art. 12	**Verant. des Verantwortl.** Art. 24	**Sicherheit der Verarb.** Art. 32	**Auftragsverarbeiter** Art. 28	**Verzeichnis** Art. 30	+	**Übermittlung Drittland** Art. 44
Spezifischer Zweck	Geeignete Maßnahmen zur Information und Kommunikation	Geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Einhaltung			Verzeichnis aller Verarbeitungen führen		Bestimmungen zur Sicherstellung des Schutzniveaus
Rechtsgrundlage	**Information & Kommunikation**	**Nachweis erbringen**			**Dokumentation**		**Bestimmungen anwenden**

Grundsätze der Verarbeitung, Art. 5

Neu

Verantwortlicher muss Einhaltung nachweisen (**„Rechenschaftspflicht“**)
Art. 5 Abs. 2



Beweislastumkehr: Die Beweislast liegt beim Verantwortlichen!

Rechenschaftspflicht, Art. 5 Abs. 2

Grundsätze der Verarbeitung pbD
Art. 5 Abs. 1

1 **Verantwortlicher muss rechtmäßigen Datenumgang nachweisen (Rechenschaftspflicht, Art. 5 Abs. 2)**

2 **Verantwortung des Verantwortlic**
Art. 24

DV by design & by default
Art. 25

Auftrac verarbe.
Art. 28

Verzeichnis
Art. 30

Verletzung
Art. 33, 34

gen- ab nätzung
Art. 35, 36

Datenschutzbeauftragter
Art. 37 - 39

Nachweis der Einhaltung

Rechte der betroffenen Person
Art. 12 - 23

nsparente Information, nikation und Modalitäten
Art. 12

ung
13, 14

Auskunft
Art. 15

Widerspruch
Art. 21

Berichtigung Löschung Einschränkung
Art. 16 - 19

Automat. Entscheid.
Art. 22

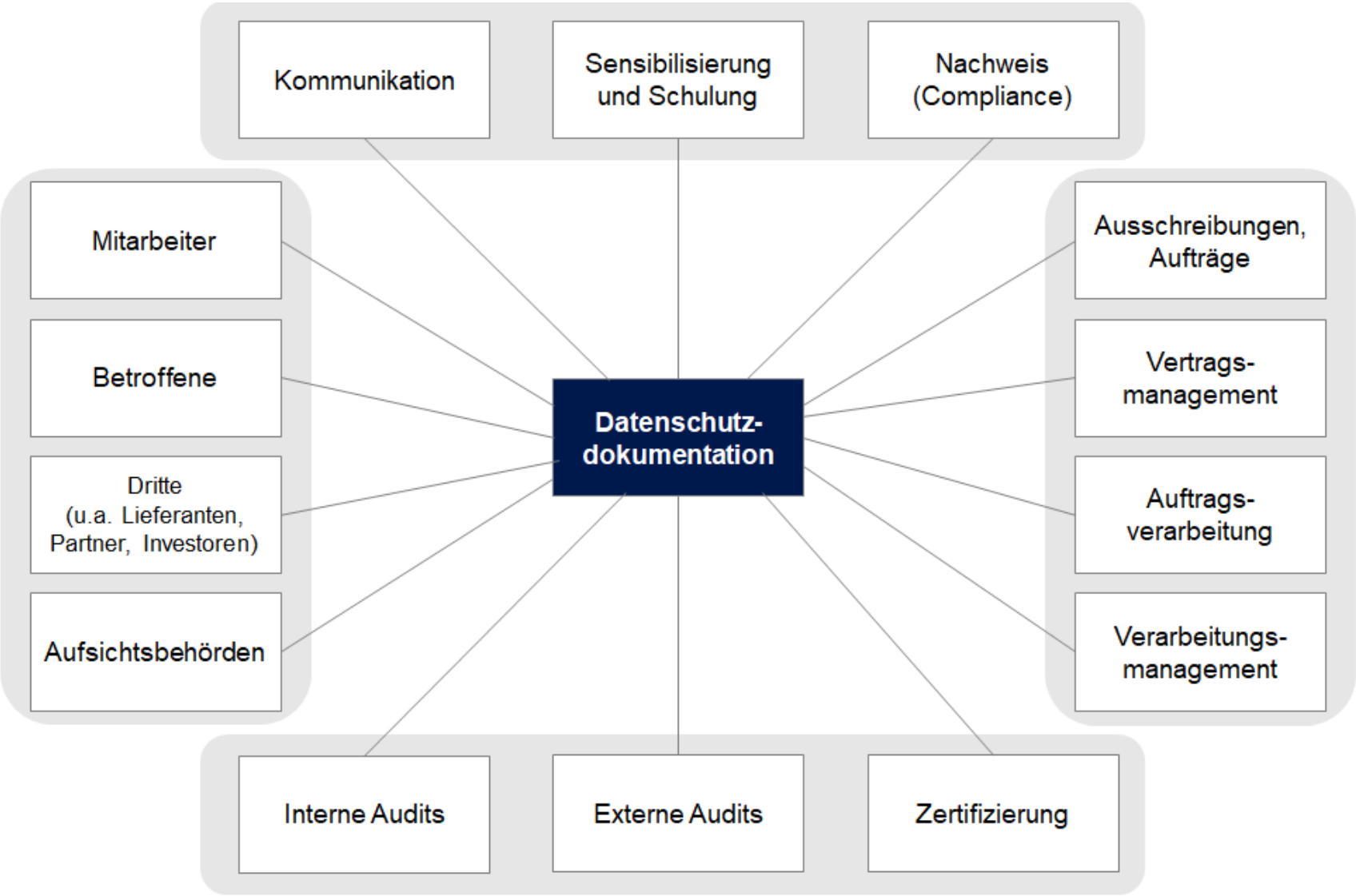
Datenüber-tragbarkeit
Art. 20

Verletzung
Art. 34

Information

Kommunikation

Rechenschaftspflicht, Art. 5 Abs. 2



Rechenschaftspflicht, Art. 5 Abs. 2

Das Datenschutzkonzept

Aktualisierung

Datenschutzkonforme Datenverarbeitung

- Rechtsgrundlage
- Zweck
- Transparenz
- Risikobewertung
- DSFA
- Löschkonzept
- TOMs
- ADVs
- (Drittland)

Handhabung von Datenschutzverletzungen

- Reaktionsplan
- Meldungen
- Kommunikation
- Schulung MA

Verarbeitungs-verzeichnis

Sicherstellung der Betroffenenrechte

- Reaktionsplan
- Schulung MA

Rechenschaftspflicht, Art. 5 Abs. 2

Reaktionsplanung für Datenschutzverletzung (= vorbereitet sein)

Wahrneh-mung von Verletzungen → Training → Aufzeichnung der Erkennt-nisse und Anpassung

Reaktions-plan für Datenschutz-verletzungen

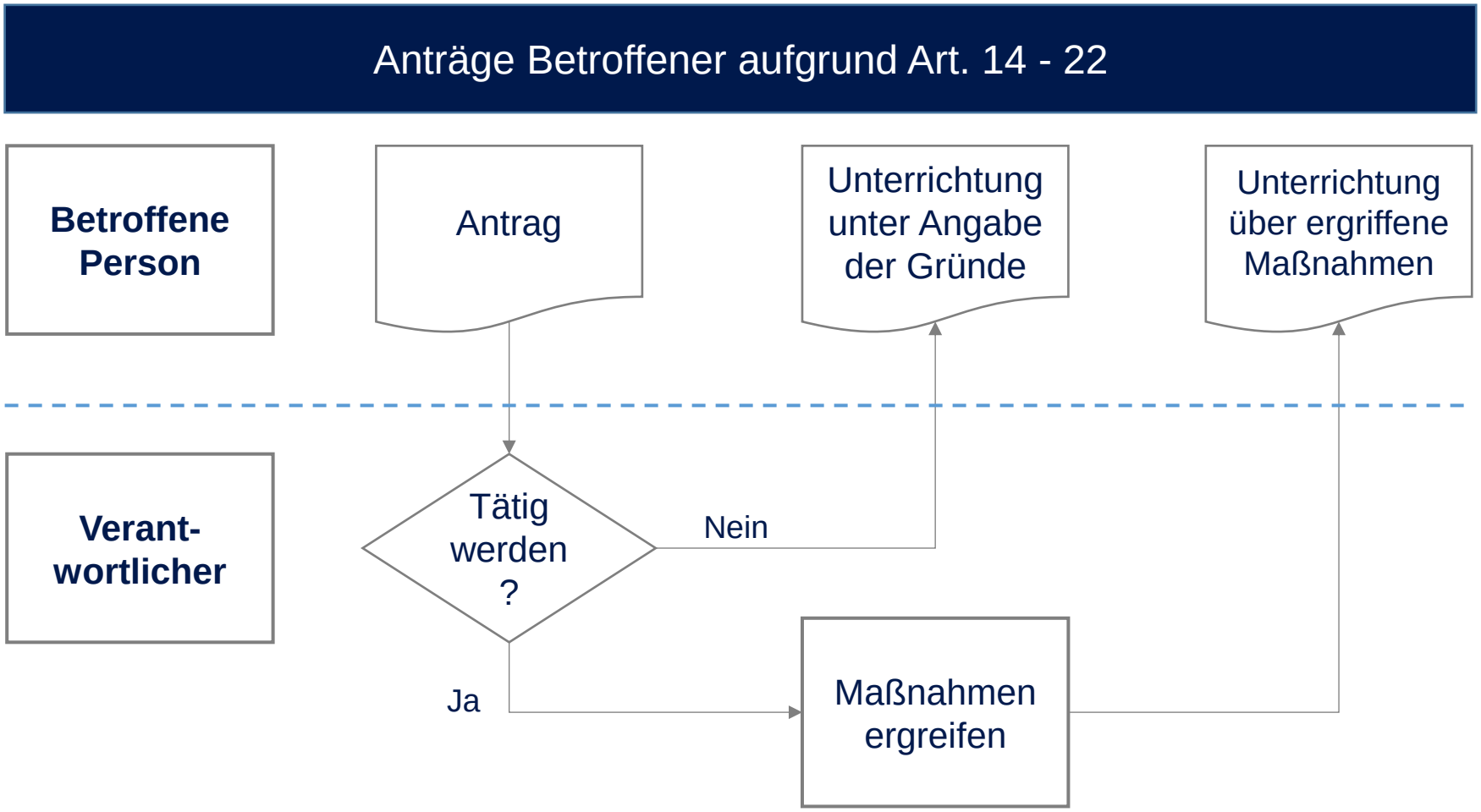
„Feuerwehr-übung"

Reaktion auf Verletzungen

- Maßnahmen (Reaktionsplan für Datenschutzverletzungen)
- Qualifizierte Information an die Betroffenen
- Prüfung, ob Meldung an Behörde notwendig (innerhalb 72 Stunden), Art. 33

Prozessablauf dokumentieren

Rechenschaftspflicht, Art. 5 Abs. 2



Prozessablauf dokumentieren

Rechenschaftspflicht, Art. 5 Abs. 2

Weitere Aufgaben zur Nachweispflicht

- Bestimmen eines Verantwortlichen für den Datenschutz, ggf. eines DSB (Art. 37 -39, § 38 BDSG-neu)
- Datenschutz-Verpflichtung von Beschäftigten (Muster unter: https://www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf
- Technische und organisatorische Maßnahmen (IT-Security) dokumentieren und Kontrollen durchführen
- Mitarbeiter im korrekten Umgang mit pb Daten, Betroffenen-rechten und Datenschutzvorfällen schulen
- Bei Einsatz einer Videoüberwachung, Vorgaben gem. § 4 BDSG-neu beachten

Sanktionen, Art. 83 und § 42 BDSG-neu

Verantwortlicher muss Einhaltung nachweisen („**Rechenschaftspflicht**“)
Art. 5 Abs. 2

Nachweis erbringen

Bis zu **20 Mio. € / 4% Jahres-umsatz**

Verarbeitung personenbezogener Daten

Rechtmäßigkeit Art. 6	Transparenz Art. 12	Verant. des Verantwortl. Art. 24	Sicherheit der Verarb. Art. 32	Auftrags-verarbeiter Art. 28	Verzeichnis Art. 30	+	Übermittlung Drittland Art. 44
Spezifischer Zweck	Geeignete Maßnahmen zur Informa-tion und Kommunikation	Geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Einhaltung			Verzeichnis aller Verarbeitungen führen		Bestimmungen zur Sicher-stellung des Schutzniveaus
Rechtsgrund-lage	Information & Kommunikation	Nachweis erbringen			Dokumentation		Bestimmungen anwenden

Bis zu **20 Mio. € / 4% Jahres-umsatz**

Bis zu 2 Jahre Freiheitsstrafe bei Gewinnerzielungs-absicht

Bis zu **10 Mio. € / 2% Jahres-umsatz**

Bis zu **20 Mio. € / 4% Jahres-umsatz**

Datenschutzmanagementsystem

Weiterentwicklung eines Datenschutz-Managementsystems auf Basis eines ISMS

Informationssicherheitsmanagementsystem (ISMS) + Datenschutzmanagementsystem (DSMS)

ISO 27001
Anford. an ein ISMS

+

2
ISO 27552
Erweiterung für ISO 27001 für das Daten-schutzmanagement

Informations-sicherheits- und Datenschutzrisiken

ISO 27002
Informations-sicherheits-Maßnahmen

+

1
ISO 29151
Leitfaden für den Schutz pbD

Vielen Dank!

Teilweise unter Verwendung von: Kranig/Sachs/Gierschmann, Datenschutz-Compliance nach der DS-GVO, Bundesanzeiger Verlag GmbH