Datenschutzgrundverordnung

Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Quellen: Fotos Bildquelle: 123RF.com/BvD Freie Fotos, Fachliteratur BDSG, Logo: Genehmigung GDD e. V. und BvD e. V.

ZIELSETZUNG

Erwägungsgrund 11 der Datenschutz-Grundverordnung (DS-GVO)

„Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert eine ...

Stärkung und Präzisierung der Rechte der betroffenen Personen

sowie eine

Verschärfung der Auflagen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden,

aber ebenso gleiche Befugnisse der Mitgliedstaaten bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten

sowie gleiche Sanktionen im Falle ihrer Verletzung.“

GRUNDSÄTZE

Art. 5 Grundsätze der Datenverarbeitung nach GS-DVO

Rechtmäßigkeit der Verarbeitung auf Basis von Treu und Glauben (Transparenz)	**Die Verarbeitung hat auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für den Betroffenen nachvollziehbarer Weise zu erfolgen.**
Zweckbindung	**Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten darf nur für eindeutig festgelegte und rechtmäßige Zwecke erfolgen. Eine Weitere Nutzung die mit den ursprünglichen Zwecken nicht zu vereinbaren ist, ist nicht zulässig.**
Datenminimierung	**Die Nutzung personenbezogener Daten ist auf das für den ursprünglichen Zweck der Erhebung, Verarbeitung angemessene und sachlich relevante Maß zu beschränken.**
Richtigkeit	**Nur die Verarbeitung sachlich richtiger Daten ist zulässig. Es sind Maßnahmen vorzusehen, die eine unverzügliche Löschung oder Berichtigung von unzutreffenden Daten ermöglichen.**
Speicherbegrenzung	**Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke der Verarbeitung erforderlich ist.**
Integrität und **Vertraulichkeit**	**Es sind geeignete Maßnahmen zu treffen, die einen angemessenen Schutz der Daten, insbesondere vor unbefugter oder unrechtmäßiger Verarbeitung, vor zufälligem Verlust, zufälliger Zerstörung oder Schädigung gewährleisten.**

Rechenschaftspflicht (Accountability):

- ⇨ **Verantwortlichkeiten**
- ⇨ **Rechenschaftspflicht (Nachweispflicht)**

Daraus leiten sich z. B. ab:

- ⇨ **Sicherheits-/Schutzkonzept**
- ⇨ **Datenschutzkonzept**
- ⇨ **Verarbeitungsübersicht**
- ⇨ **Systemdokumentation**
- ⇨ **Dienstleistervereinbarungen**
- ⇨ **…**

EINORDNUNG INS RECHTESYSTEM

Vorrang einer EU-Verordnung vor nationalem Recht

„Auch was klingt wie bisher, muss nicht dasselbe sein.“

Roland Mons

BISHER

- DATENSCHUTZ-RICHTLINIEN
- Richtlinie = Umsetzung durch Mitgliedsstaaten mittels nationalem Gesetz
- bspw. RL 95/46 EG => Umsetzung im BDSG

NEU

- VERORDNUNG = UNMITTELBARE GELTUNG IN JEDEM EU-MITGLIEDSSTAAT
- EU-Verordnung = Anwendungsvorrang vor jedem nationalen Gesetz
- → kein Umsetzungsgesetz im nationalen Recht erforderlich
- sofern in VO vorgesehen, dann nationale Regelungen möglich
  - bspw. generelle Öffnungsklausel für öffentlichen Bereich
- - bspw. spezielle Öffnungsklauseln wie für Beschäftigten-
- datenschutz
- - bspw. sog. ePrivacy-RL (RL 2002/58/EG)
- Ausgestaltungspflicht durch nationalen Gesetzgeber, sofern durch VO angeordnet

→ NEUER RECHTSRAHMEN MIT ANWENDUNGSVORRANG VOR NATIONALEN GESETZEN
→ KEINE DEUTSCHE AUSLEGUNG, SONDERN EU-AUSLEGUNG

DS-GRUNDVERORDNUNG

Ab wann und mit welcher Auswirkung

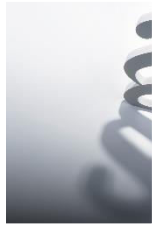
… nichts bleibt vollkommen unverändert

… und zwei Jahre sind kurz! ???

Inkrafttreten Mai 2016

Geltung ab 25.05.2018

Übergangszeit: Anpassung an neues Datenschutzrecht



Anpassungsbedarf
- → **Auftragsdatenverarbeitung**
- → **Einwilligungen**
- → **Informationen an Betroffene**
- → **interne Dokumentation**
- → **neue Begriffe, neue Definitionen, neue Auslegung – selbst bereits im BDSG verwendeter Begriffe**

Grundlage: Erwägungsgrund (ErwGr.) 171
„innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht“
Einwilligung – Fortgeltung, sofern entsprechend der DS-GVO erteilt
Sonderreglung für Entscheidungen/Beschlüsse der EU-Kommission

SANKTIONSRAHMEN

Massive Verschärfung des Sanktionsrahmens

Art. 83 Abs. 4	Art. 83 Abs. 5	Art. 83 Abs. 6
bis 10 Mio. € oder bis 2% des weltweiten Vorjahresumsatzes	**bis 20 Mio. € oder bis 4% des weltweiten Vorjahresumsatzes**	**bis 20 Mio. € oder bis 4% des weltweiten Vorjahresumsatzes**
	je nachdem, was höher ist (!)	
• Verstöße gegen Regelungen zu z.B. • Schutzmaßnahmen • (technisch-organisatorische Maßnahmen TOM) • Auftragsverarbeitung • (NEU: auch gegen Auftragsverarbeiter) • Verzeichnis der Verarbeitungstätigkeiten • Datenschutz-Folgenabschätzung • Bestellung Datenschutzbeauftragten • …	• Verstöße gegen Regelungen z.B. • Grundsätze (Art. 5) • Rechtmäßigkeit • Einwilligung • Rechte Betroffener • Drittlandübermittlung • Zusammenarbeit mit Aufsichtsbehörde • …	• Verstöße gegen Anordnungen der Aufsichtsbehörde

AUSGANGSPUNKT:

Verbot mit Erlaubnisvorbehalt, Art. 6 Abs. 1

„Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn Art. 6 Abs. 1 beachtet ist.“

NEU: ART. 5

- Grundsätze in Bezug auf Verarbeitung personenbezogener Daten
  - Rechtmäßigkeit
  - Verarbeitung nach Treu und Glauben
  - Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Speicherbegrenzung
  - Integrität und Vertraulichkeit
  - Rechenschaftspflicht

NEU: ART. 6

- Rechtmäßigkeitsgrundlagen
- Einwilligung, Art. 6 Abs. 1 lit. a (i. V. m. Artt. 7, 8, 3 Abs. 8)
  - Art. 3 Abs. 8: Definition mit Anforderungen
  - NEU: Art. 7: Bedingungen für Einwilligung
  - NEU: Art. 8: durch Kind bei Diensten der Informationsgesellschaft
- gesetzliche Zulässigkeit, Art. 6 Abs. 1 lit. f
  - NEU: Generalklausel für Interessenabwägung (Art. 6 Abs. 1 lit. f) anstatt wie bisher differenziertere Regelungen
  - Sonderregelungen für bestimmte Daten und Verarbeitungen
- Regelungen in anderen Gesetzen

NEU: ART. 6 ABS. 4

- NEU: spezielle Maßgaben für eine Verarbeitung zu anderem Zweck, Art. 6 Abs. 4
  - *(... um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden ...)*

NEU: VERSTOß GEGEN ART. 5, 6, 7 UND 8: Bußgeld bis 20 Mio. Euro / 4 % des Vorjahresumsatzes

INFORMATIONSPFLICHTEN

UNTERSCHEIDUNG DER UNTERRICHTUNG

Art. 13: Informationspflichten zum Zeitpunkt der Erhebung (Geltung auch für Einwilligung)
Art. 14: Wenn die Daten nicht bei der betroffenen Person erhoben werden
Art. 15: Auskunftsansprüche des Betroffenen
Art. 37: Meldung des Datenschutzbeauftragten bei der Aufsichtsbehörde

NEU: SIGNIFIKANTE ERWEITERUNG DES INHALTS D. UNTERRICHTUNG

insbesondere:
NEU: Name des Verantwortlichen
NEU: Kontaktdaten des/der Datenschutzbeauftragten
NEU: Zweck der Verarbeitung sowie Rechtsgrundlage
NEU: das berechtigte Interesse (Art. 6 Abs. 1 lit. f), sofern darauf beruhend
NEU: Hinweis auf Widerspruchs-recht (auch bei Einwilligung)
NEU: Absicht der Drittland-übermittlung und einen Hinweis auf die Grundlage der Zulässigkeit der Drittlandübermittlung

KONSEQUENZ:

erhebliche Umgestaltung der Informationen

HERAUSFORDERUNG:

auch für bestehende auf Basis einer Einwilligung und unter der DS-GVO fortgesetzte Verarbeitungen müssen die Anforderungen erfüllt sein (ErwGr. 171)

DOKUMENTATIONSPFLICHTEN

Verzeichnis von Verarbeitungstätigkeiten, Art. 30

- **Pflicht für den Verantwortlichen (Art. 30 Abs. 1) und Auftragsverarbeiter (Art. 30 Abs. 2)**

Ausnahmen für Unternehmen bis 250 Mitarbeitern, sofern die Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, nur gelegentlich erfolgt oder nicht besondere Datenkategorien (Art. 9) oder Straftaten (Art. 10) einschließt.

- **keine Herausgabepflicht an Jedermann (Stichwort: Jedermannsverzeichnis)**
- **Unterschiedliche Inhalte für Verantwortlichen und Auftragsverarbeiter**
- **gegenüber Aufsichtsbehörde auf Anforderung zur Verfügung stellen**
- **Aufzeichnungen sind schriftlich zu führen, elektronisches Format genügt**
- **NEU - bei Verstoß: Sanktionsrahmen bis 10 Mio. Euro / 2 % des Vorjahresumsatzes**

AUFTRAGSVERARBEITUNG

Auftragsverarbeitung, Art. 28

- **Grundsatz der Privilegierung bleibt!?**
  - **Auftragsverarbeiter ist kein Dritter, Art. 4 Abs. 10**
  - **Risiko: Unklarheiten wegen fehlender Definition von Übermittlung**

- **Verantwortlicher für Verarbeitung bleibt verantwortlich**
  - **Pflichtinhalte bei der Beauftragung**
  - **Angemessenheit der Schutzmaßnahmen**
  - **Nachweis der ausreichenden Schutzmaßnahmen, auch über Verhaltensregeln oder Zertifizierung möglich**
  - **Einbindung von Subunternehmern formalisierter geregelt**

  - **NEU: geänderte inhaltliche Anforderungen an Vereinbarung**
  - **NEU: gemeinsame Haftung (Art. 28) des Auftraggebers und des Auftragnehmers**
  - **➔ Zwingender Überprüfungsbedarf**

- **bei Verstoß: Sanktionsrahmen bis 10 Mio. Euro / 2 % des Vorjahresumsatzes**
  - **➔ auch gegen Auftragsverarbeiter möglich**
  - **NEU: Risiko für Auftragsverarbeiter: Haftung mit Auftraggeber**

TECHNISCH-ORGANISATORISCHE MAßNAHMEN

„Sicherheit der Verarbeitung“, Art. 32

- **Zielsetzung**
  - **Gewährleistung eines dem Risiko angemessenen Schutzniveaus**

- **Umsetzung durch geeignete technische und organisatorische Maßnahmen, die getroffen werden**
  - **unter Berücksichtigung des Stands der Technik,**
  - **der Implementierungskosten**
  - **der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung**
  - **sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten**

NEU: Verstoß ist bußgeldbewehrt (10 Mio. Euro / 2 % des Vorjahresumsatzes)!

  - **Beachten: auch im Kontext der Auftragsverarbeitung**

- **Auswirkung in der Zukunft: Wird die Risikobewertung eine zentrale Aufgabe einer Datenschutzorganisation?**

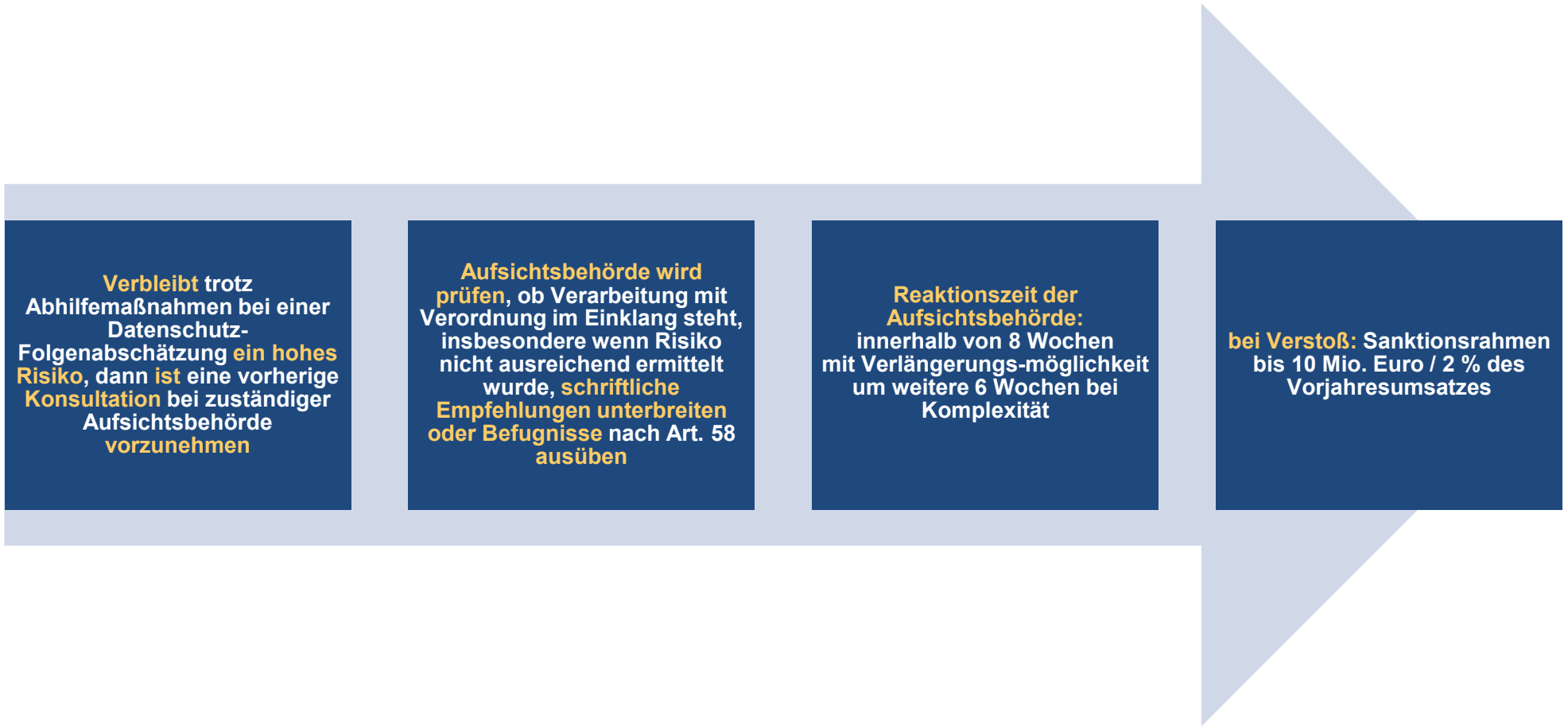
DATENSCHUTZ-FOLGENABSCHÄTZUNG

Privacy Impact Assessment, Art. 35

- **durch den für die Verarbeitung Verantwortlichen (Art. 35 Abs. 1)**
- **wenn die Form der Verarbeitung *„aufgrund der Art, des Umfangs und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge“* hat**
- **Dokumentation der eingesetzten Abhilfemaßnahmen zur Eindämmung des Risikos, einschließlich Nachweisanforderungen**
- **bei Verstoß: Sanktionsrahmen bis 10 Mio. Euro / 2 % des Vorjahresumsatzes**

VORHERIGE KONSULTATION

Zwingende Einbeziehung der Datenschutzaufsichtsbehörde, Art. 36



MELDEPFLICHT BEI DATENSCHUTZVERSTÖßEN

Mehrteilige Regelung, Art. 4 Abs. 9, Artt. 33, 34, ErwGr. 59, 67 ff.

AUSLÖSER DER MELDEPFLICHT

„Verletzung des Schutzes personenbezogener Daten", Art. 4 Abs. 9

NEU: keine Beschränkung auf bestimmte Daten

➔ Risiko steigt!

ZWEISTUFIGE MELDEPFLICHT

Meldung an Aufsichtsbehörde, Art. 33

- **72 Std. nachdem die Verletzung bekannt wurde**
- **Ausschluss, falls „*voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt*“**

➔ grds. Meldepflicht, aber Ausnahmen

Benachrichtigung der betroffenen Personen, Art. 34

- **Meldepflicht, falls Wahrscheinlichkeit für hohes Risiko**
- **aber dennoch: Ausnahmen möglich**

➔ nicht allein ausreichend: Verletzung des Schutzes personenbezogener Daten

- **plus: Verlangen der Unterrichtung bzw. Feststellung der Pflicht zur Unterrichtung**

BEI VERSTOß

bis 10 Mio. Euro / 2 % des Vorjahresumsatzes

ZEITPLAN UND UMSETZUNG Regelung, Art. 4

„Bis zum Inkrafttreten muss die Verarbeitung personenbezogener Daten und die Daten-schutzorgansitaion umgestellt sein. Keine (weitere) Übergangszeit!“

8.4.16
- **Abstimmung EU-Rat**

12.4.16
- **Zustimmung Ausschuss LIBE, Europäisches Parlament**

14.4.16
- **Zustimmung EU-Parlament**

24.5.16
- **Veröffentlichung im Europäischen Amtsblatt**
- **nach 20 Tagen Inkrafttreten**
- **nach 2 Jahren zur Anwendung kommen**

25.5.18
- **Inkrafttreten der Datenschutzgrundverordnung und der neuen nationalen Regelungen aus den Öffnungsklauseln**

Umsetzung
Nationaler Gesetzgeber hat „muss“ - und „kann“-Öffnungsklauseln

Gesetzgebungs-verfahren muss bis Anwendungszeitpunkt abgeschlossen sein

SICHERSTELLEN DES DATENSCHUTZNIVEAUS

Sensibilisierung Information

Information Geschäftsleitung und Mitarbeiter über die Auswirkungen der neuen Rechtsrundlage zum Datenschutz, zu den neuen Risiken und des notwendigen Handlungsbedarfs

IST-Aufnahme inkl. Beratung

Erhebung der Geschäftsprozesse und der Datenverarbeitungen in Systemen zum ersten Nachweis und zur Schwachstellenfeststellung (Risiken erkennen)

Auswertung

Bewerten der Risiken und Einordnen in den Sanktionskatalog der Datenschutzgrundverordnung und des neuen Bundesdatenschutzgesetzes (Risikobewertung) und Ableitung von Maßnahmen (Risikoreduktion)

Maßnahmenplan

Priorisierung und Planung der Maßnahmen zur Risikoreduktion / -vermeidung

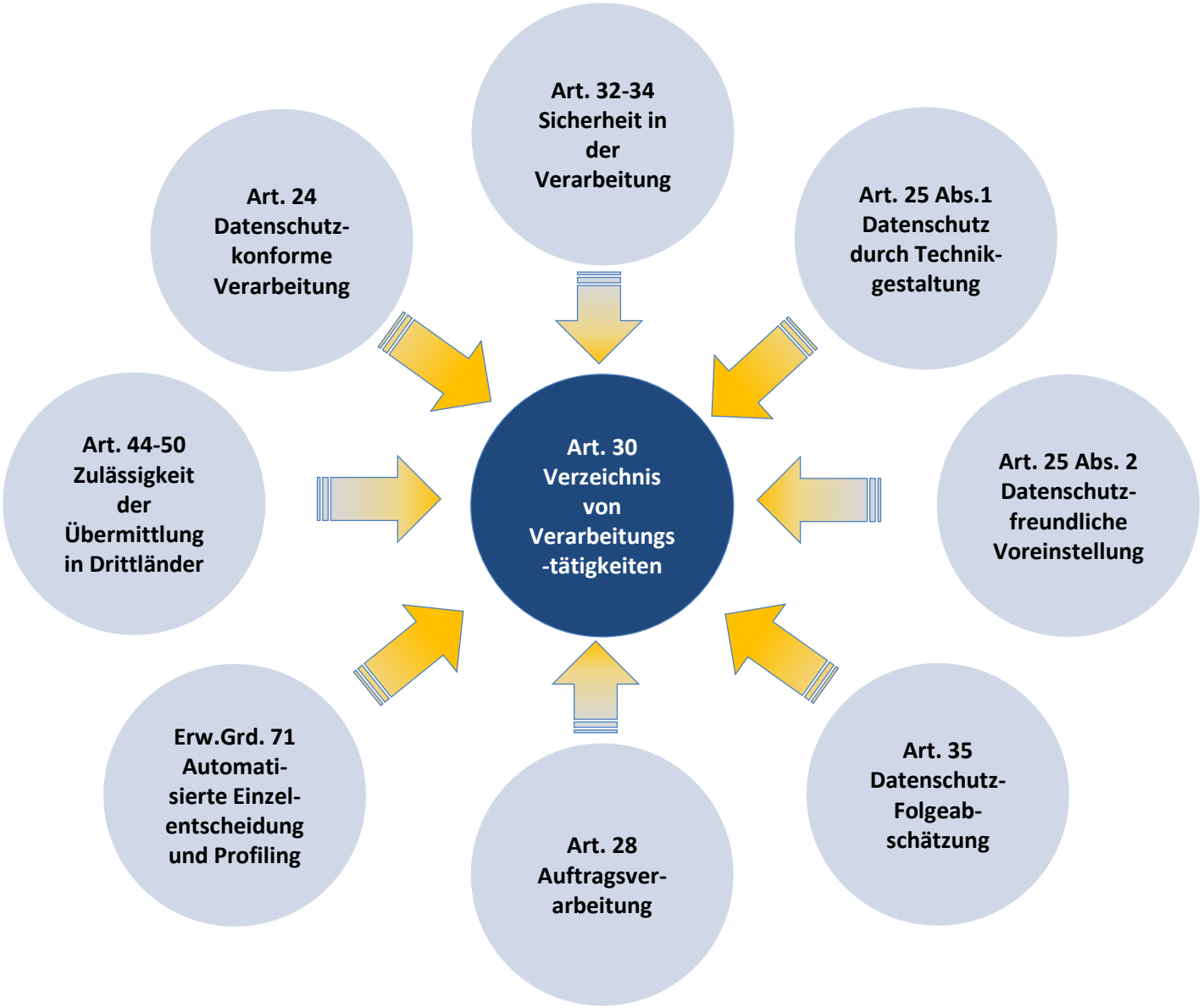
Umsetzung

Umsetzen der Maßnahmen zur Risikoreduktion / -vermeidung

Pflege

Festlegen und Einführen eines standardisierten Prozesses für neue Verarbeitungen und eines Regelprozesses Zur Sicherstellung der Datenschutzkonformität für bestehende Verarbeitungen.

VERARBEITUNGSÜBERSICHT



PROZESS-/VERARBEITUNGSAUFNAHME

Erfassung einer Verarbeitungstätigkeit

(bitte an den Datenschutzbeauftragten übersenden)
Nur auszufüllen, wenn personenbezogene Daten (Hinweis Nr. 1) verarbeitet werden!
Anmerkung: Soweit der Platz dieses Formulars nicht ausreicht fügen Sie bitte zusätzliche Anlagen bei.

Datum:	< Text >
Ausfüllende Person:	< Text >
Telefonnummer:	< Text >
E-Mail-Adresse:	< Text >

Bezeichnung der Verarbeitung (Hinweis Nr. 2):	< Text >
Übergeordneter Geschäftsprozess:	< Text >
Beginn der Verarbeitung (Hinweis Nr. 3):	< Text >

☐ **Änderung bestehende Verarbeitung**
☐ **neue Verarbeitung**
☐ **Abmeldung bestehende Verarbeitung (Hinweis Nr. 4)**

1. Grundsätzliche Angaben zur Verarbeitung und zur Verantwortlichkeit.

1.1	Bezeichnung des Verfahrens (Hinweis Nr. 5)	< Text >
1.2	Verantwortliche Stelle	< Text >
	Fachbereich	< Text >
	Verantwortliche Führungskraft:	< Text >
	Ggf. Stellenbezeichnung	< Text >

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung (Hinweis Nr. 7)

2.1	Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung (Hinweis Nr. 8):	< Text >

2.2 Rechtsgrundlage (zutreffende bitte ankreuzen und erläutern)

☐	Spezialgesetzliche Regelung außerhalb der DSG-VO (Bitte benennen: Vorschrift, Paragraph, Absatz, Satz)	< Text >
☐	Einwilligung des Betroffenen (Art. 6 Abs. 1 a) DSG-VO): Bitte fügen Sie die Einwilligungsklausel und den Einwilligungsmechanismus hier ein	< Text >
☐	Kollektivvereinbarung (z.B. Betriebsvereinbarung, Tarifvertrag): (Bitte benennen: Genaue Bezeichnung, Paragraph, ggfs. Absatz)	< Text >
☐	Begründung, Durchführung oder die Beendigung eines Beschäftigungsverhältnisses (national geregelt im BDSG)	< Text >
☐	Vertrag oder Vertragsanbahnung mit dem Betroffenen (Art. 6 Abs. 1 b) DSG-VO.)	< Text >
☐	Interessenabwägung (Art. 6 Abs. 1 f) DSG-VO): Bitte benennen Sie die vorrangigen Interessen	< Text >

3. Kreis der betroffenen Personengruppen

Kreis der betroffenen Personengruppen (Hinweis Nr. 9)	Art der Daten / Datenkategorien (Hinweis Nr. 10)	Werden besonderen Kategorien von Daten verarbeitet? (Hinweis Nr. 11)
		☐ Ja ☐ Nein Welche:
		☐ Ja ☐ Nein Welche:

EU DS-GVO 25. Mai 2018

There´s not two ways about it!

EU DATENSCHUTZ GRUNDVERORDNUNG

25. MAI 2018

Alles hat seinen Preis, besonders die Dinge, die nichts kosten.

Art van Rheyn

Vielen Dank für Ihre Aufmerksamkeit

Roland Mons & Winfried Rau
Senior Consultants, Datenschutzbeauftragte

Unternehmen:
MDS IT + Datenschutz Consulting
68307 Mannheim ▪ Obergasse 26

Kontakt:
Telefon: 0621 91109080 ▪ Mobil: 0163 694168
Email : dsb@tintus-consulting.de
Homepage: www.mds-consulting.de

Geschäftsleitung: Roland Mons

Unternehmen:
Winfried Rau Consulting & Tintus Consulting UG
67281 Bissersheim/Pfalz ▪ Hollergasse 10

Kontakt:
Telefon: 06359 8727507 ▪ Mobil: 0173 7555203
Email: dsb@tintus-consulting.de
Homepage: www.tintus-consulting.de

Geschäftsleitung: Winfried Rau