COMPETENCE
YOU CAN COUNT ON.

DSGVO
Datenschutz - Grundverordnung

Dr. Ivo Rungg
TMC Seminar
Wattens, 13.April 2018

BINDER GRÖSSWANG

RECHTLICHE GRUNDLAGEN

- Inkrafttreten: **25. Mai 2016 /** Anwendbarkeit: **25. Mai 2018**
- Mit diesem Tag wird die derzeitige Datenschutz-RL aufgehoben
- DSG 2000 wird von der **unmittelbar anwendbaren DSGVO** abgelöst („one continent, one law“) – aber 69 Öffnungsklauseln
- Zur Durchführung der Öffnungsklauseln und Spielräume wurde das „Datenschutz-Anpassungsgesetz 2018“, eine Novelle des DSG 2000 (künftig: DSG) beschlossen
- Erklärtes Ziel: Datenschutz in der behördlichen und betrieblichen Praxis mehr Geltung zu verschaffen → kein Kavaliersdelikt mehr; **hohe Strafen** bis zu EUR 20 Mio oder bis 4% des weltweiten Gesamtjahresumsatzes eines Unternehmens (Art 83 DSGVO)

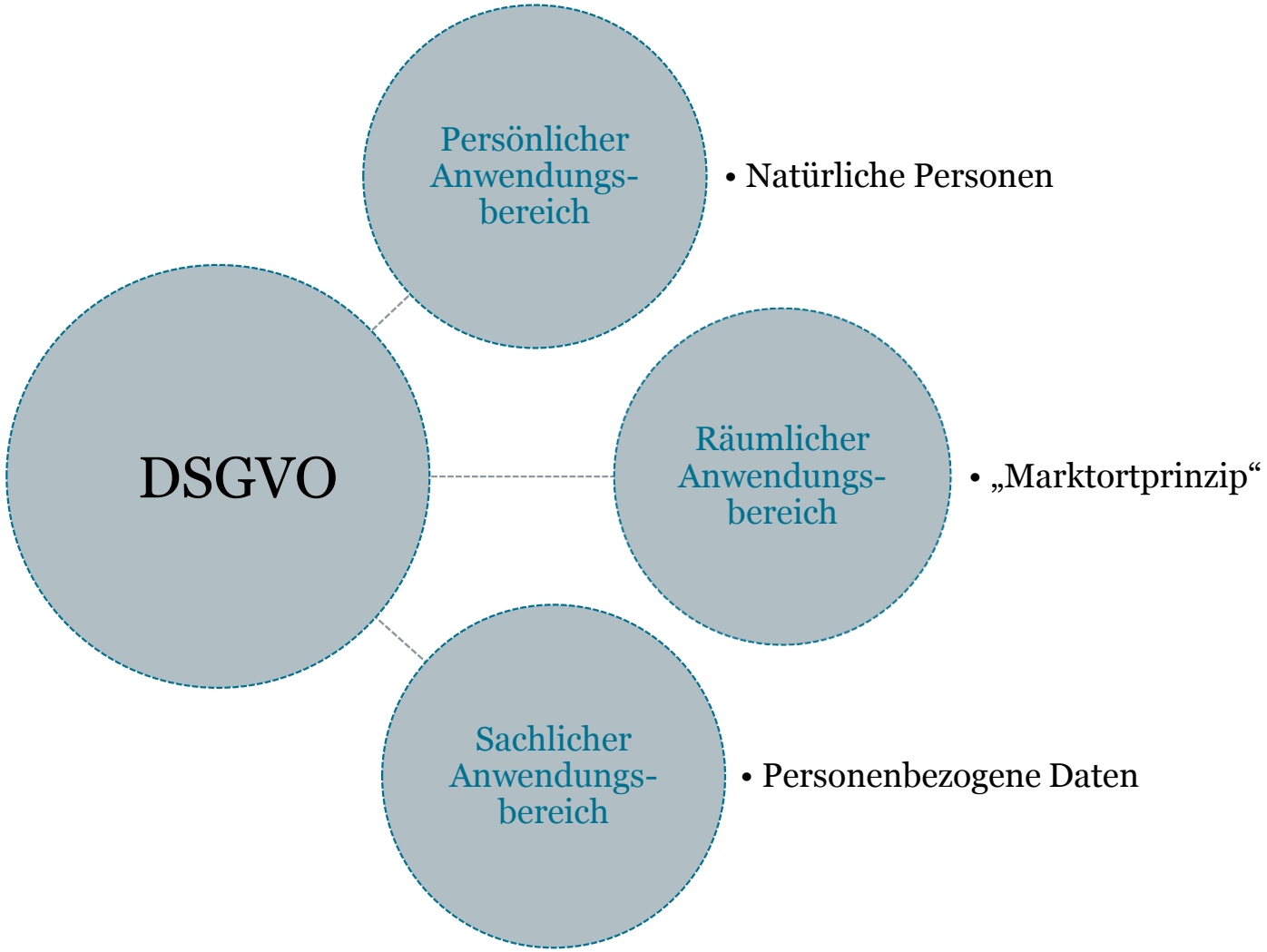
RECHTSGRUNDLAGEN

- Datenschutzgesetz (DSG)
  - Nationale Umsetzung der Öffnungsklauseln der DSGVO
  - Umsetzung der Richtlinie (EU) 2016/680

- E-Privacy Verordnung (Entwurf)
  - Überarbeitung der Datenschutz-Richtlinie für elektronische Kommunikation

- NIS-Richtlinie (Richtlinie EU 2016/1148)
  - Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (Cybersicherheit)

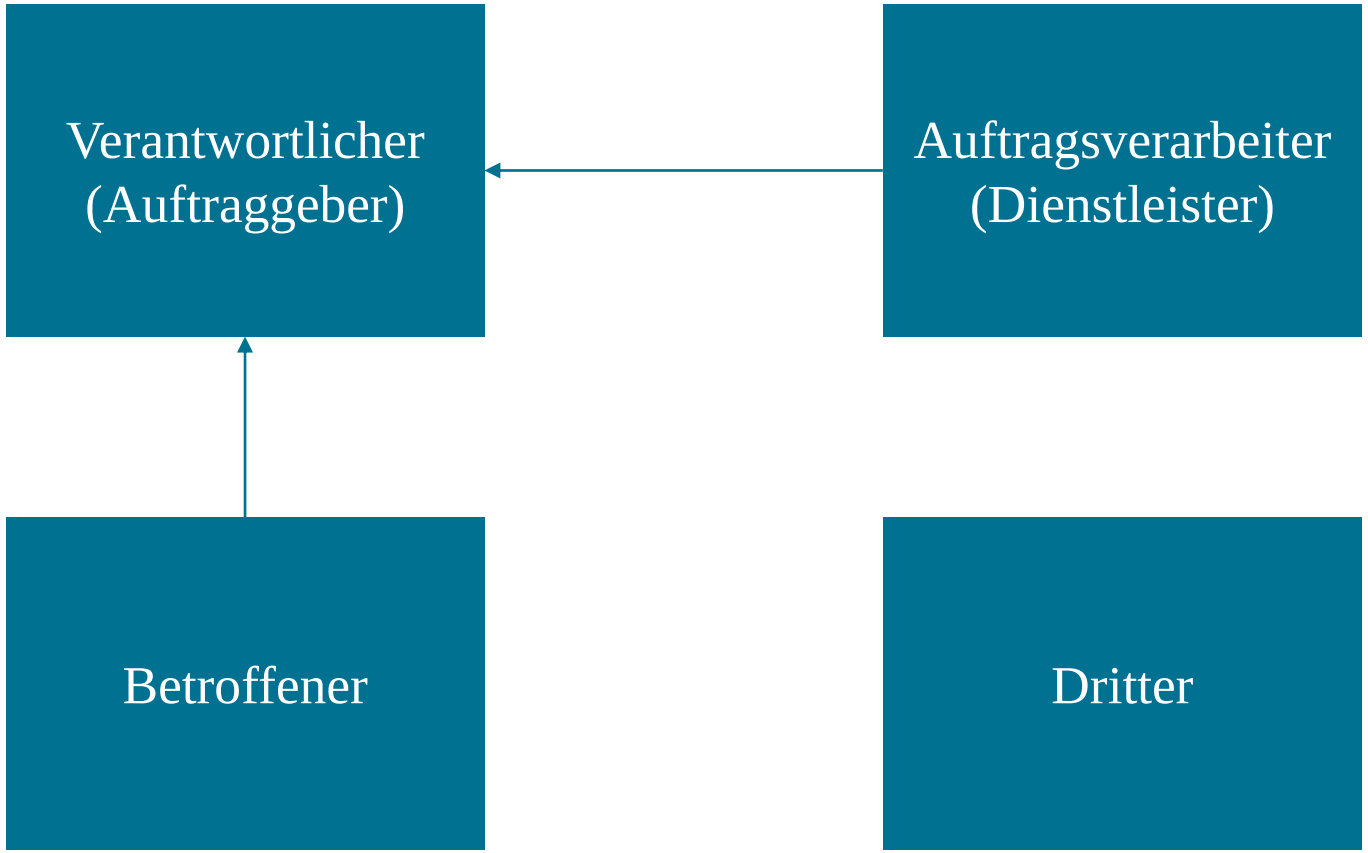
ANWENDUNGSBEREICHE DER DSGVO



DEFINITIONEN

- **Personenbezogene Daten** (Art 4 Z1 DSGVO) sind alle Informationen, die mit einer identifizierbaren natürlichen Person in Verbindung stehen z.B. Name, Geschlecht, Geburtsdatum, Adresse, Einkommen, Vermögen, E-Mailadressen, Logfiles, Lebensläufe; meist auch Kennungen wie IP-Adressen, Autokennzeichen, Steuernummer
- **Pseudonymisierung** (Art 4 Z5 DSGVO) bedeutet, dass personenbezogene Daten ohne Hinzuziehung zusätzlicher - gesondert aufbewahrter - Informationen nicht mehr zugeordnet werden können; anerkanntes Mittel zum Personenschutz/Risikominimierung – DSGVO bleibt anwendbar
- **Verarbeitung von Daten** (Art 4 Z3 DSGVO): v.a. Erhebung, Erfassung, Organisation, Ordnen, Speicherung, Veränderung, Abfragen, Offenlegung durch Übermittlung, Verbreitung, Abgleich oder Verknüpfung, Löschung, Vernichtung von Daten
- **Besondere Kategorien personenbezogener Daten** (Art 9 DSGVO): rassische Herkunft, politische Meinungen, Religion/Weltanschauung, genetische Daten, biometrische Daten zur Personenidentifizierung, Gesundheitsdaten, Sexualleben, sexuelle Orientierung; Straftaten und strafrechtliche Verurteilungen (Art 10 DSGVO)

AKTEURE IM DATENSCHUTZRECHT



AUFTRAGSVERARBEITER
ART 4 Z 8, ART 28 DSGVO

> Auftragsverarbeiter ist der Erfüllungsgehilfe des Verantwortlichen bei der Datenverarbeitung
  - Datensicherheitsmaßnahmen implementieren
  - Verzeichnis zu allen im Auftrag durchgeführten Tätigkeiten der Verarbeitung zu führen
  - verpflichtet mit der Aufsichtsbehörde auf Anfrage zusammen zu arbeiten
  - Unterstützung des Verantwortlichen bei Erfüllung seiner Pflichten nach der DSGVO (Betroffenenrechte)
> Auftragsverarbeiter darf Daten nur im Rahmen des konkreten Auftrags und nur für den vom Verantwortlichen vorgegebenen Zweck verarbeiten
> Hierzu wird zwingend eine Vereinbarung zwischen Verantwortlichen und Auftragsverarbeiter vorgeschrieben (Art 28 DSGVO)

GRUNDSÄTZE FÜR DIE DATENVERARBEITUNG

- **Verbotsprinzip**: jede Verarbeitung von personenbezogenen Daten bedarf einer Rechtfertigung (Art 6 DSGVO – Rechtmäßigkeit der Verarbeitung)
- **Transparenz**: Informationspflichten
- **Zweckbindung**: Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht vereinbarenden Weise weiterverarbeitet werden
- **Datenminimierung**: es dürfen nur solche Daten erhoben werden, die für den konkreten Erhebungszweck von direkter Relevanz und für dessen Erfüllung erforderlich sind
- **Richtigkeit und Speicherbegrenzung**: Ferner müssen Daten sachlich richtig sein und dürfen nicht länger, als für den Zweck erforderlich, gespeichert werden
- **Integrität und Vertraulichkeit**: Gewährleistung der Datensicherheit
- **Rechenschaftspflicht**: Verantwortliche ist für die Einhaltung der genannten Grundsätze verantwortlich und muss deren Einhaltung nachweisen können

ERLAUBNISTATBESTÄNDE - PRÜFSCHEMA

Personenbezogene Daten?

Verbot der Datenverarbeitung

Sensible Daten	Strafrechtliche Daten	Nicht-sensible Daten
> Ausdrückliche Einwilligung > Ausübung/Erfüllung arbeits- und sozialrechtlicher Rechte/Pflichten > Betroffener selbst öffentlich gemacht > Verteidigung von Rechtsansprüchen	> ausdrückliche gesetzliche Ermächtigung oder Verpflichtung > gesetzlichen Sorgfaltspflichten > Wahrung der berechtigten Interessen	> Einwilligung > Vertragserfüllung > Rechtliche Verpflichtung > berechtigtes Interesse > Vernünftige Erwartung > Opt-Out

AUTOMATISIERTE ENTSCHEIDUNGEN – PROFILING
ART 4 Z 4, 22 DS-GVO

- *„jede Art der automatisierten Verarbeitung personenbezogener Daten, …, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten…zu analysieren oder vorherzusagen“*

- **Einschränkung:**
  - Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung basierten Entscheidung unterworfen zu werden.

PROFILING
ART 4 Z 4, 22 DS-GVO

- Direktwerbung um Customer Targeting zu betreiben
  - Berechtigtes Interesse des Verantwortlichen

- Bonitätsprüfungen bei Kreditinstituten
  - Berechtigtes Interesse und gesetzliche Pflicht zur Bonitätsprüfung

- Sicherheitsvorkehrungen:
  - Geeignete mathematische oder statistische Verfahren für das Profiling verwenden
  - Technische und organisatorische Maßnahmen treffen, mit denen sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird.
  - Absolutes Widerspruchsrecht gegen Profiling, wenn es mit Direktwerbung in Verbindung steht

BILDVERARBEITUNG
§§ 12, 13 DSG

- Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu privaten Zwecken (Foto und Video)
- Allgemeine Rechtsgrundlagen für Datenverarbeitung sind gültig

- Zulässig insbesondere wenn:
  - Vorbeugendem Schutz von Personen / Sachen auf Liegenschaften des Verantwortlichen oder öffentlichen Orten, die dem Hausrecht des Verantwortlichen unterliegen und bei denen ein besonderes Gefährdungspotenzial vorliegt und kein geringeres Mittel zur Verfügung steht
  - Privates Dokumentationsinteresse

- Besondere Datensicherheitsmaßnahmen und Kennzeichnungspflicht
  - Protokollierungspflicht
  - Aufbewahrung länger als 72 Stunden muss verhältnismäßig und begründet sein
  - Bildaufnahme muss geeignet gekennzeichnet sein

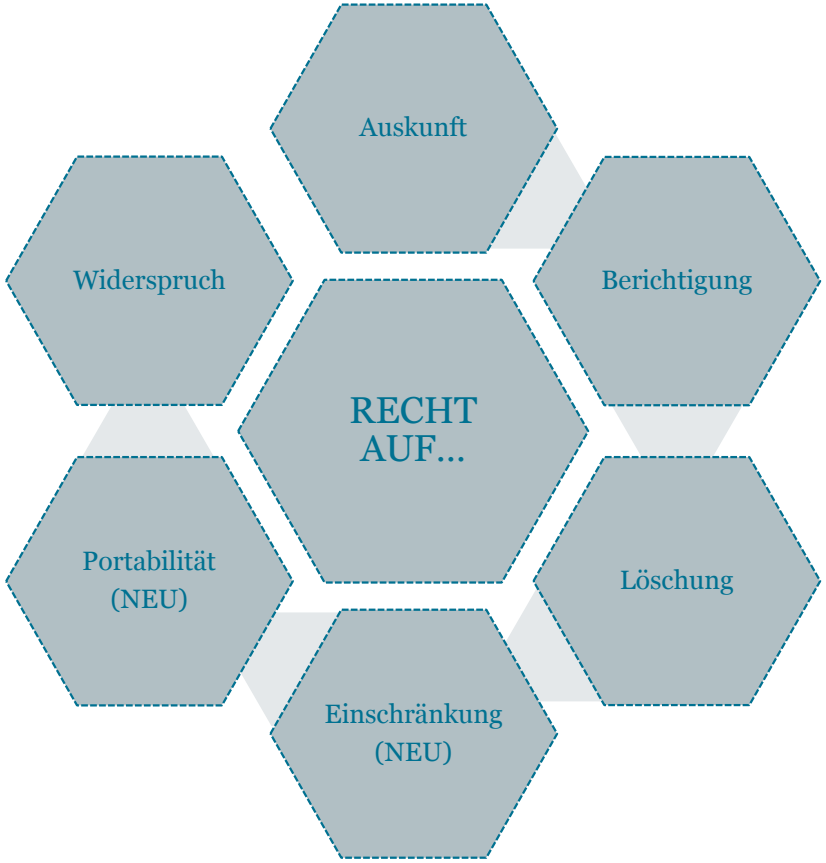
ZUSTIMMUNG ZUM ERHALT VON WERBEMAILS
§ 107 TKG 2003

- Generelles Verbot von „Cold Calling“ und von unerbetenen elektronischen Werbenachrichten
  - Vorherige Zustimmung erforderlich

- **Ausnahme:**
  - Kontaktinformationen im Zusammenhang mit Verkauf / Dienstleistung
  - Direktwerbung für eigene ähnliche Produkte / Dienstleistungen
  - Möglichkeit die Verwendung der Kontaktinformation problem- und kostenlos abzulehnen
    - Bei der Erhebung und bei jeder Übertragung
  - Keine Eintragung in „Robinson-Liste“

- Klassische Newsletter E-Mails nach Vertragsabschlüssen

BETROFFENENRECHTE



RECHT AUF AUSKUNFT
ART 15 DSGVO

- beim Unternehmen, auch mündlich oder elektronisch
- Zuständiger muss erkennbar sein
- Beantwortung binnen 1 Monat nach Einlangen (komplexere Fragen 2 Monate)
- klare, leicht verständliche Antwort
- kostenfrei
- Ua: Kopien der Daten (**NEU**), konkret verarbeitete Daten, Zwecke, Empfänger, Speicherfrist, Herkunft der Daten, Garantien bei Transfers in Drittländer

RECHT AUF BERICHTIGUNG
ART 16 DSGVO

- Unzutreffende Daten sind zu berichtigen
- ebenfalls 1 Monat Frist
- Information über die Berichtigung
- DSG sieht Einschränkung der Löschungspflicht vor (§ 4 Abs 2 DSG)

RECHT AUF LÖSCHUNG
ART 17 DSGVO

> Recht auf „Vergessenwerden“

> unverzügliche Löschung

> zB wenn Daten nicht mehr notwendig zur Zweckerreichung, Widerruf der Zustimmung, Widerspruch gem Art 21 DSGVO

> DSG sieht Einschränkung der Löschungspflicht vor (§ 4 Abs 2 DSG)

RECHT AUF EINSCHRÄNKUNG
ART 18 DSGVO

> Begleitrecht

> z.B. während Prüfung, ob gelöscht werden muss

> Grundsätzlich Löschung

> wenn aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten möglich → Einschränkung

RECHT AUF DATENÜBERTRAGBARKEIT
ART 20 DSGVO

- Sofern Verarbeitung auf Einwilligung oder einem Vertrag beruht
- Portabilität
- Strukturiertes, gängiges und maschinenlesbares Format
- Übertragung aller Daten an ein anderes Unternehmen
- Z.B. Wechsel von Sozialen Medien

RECHT AUF WIDERSPRUCH
ART 21 DSGVO

- nur, wenn die Daten auf Grundlage von berechtigten Interessen verarbeitet werden
- jederzeit ausübbar
- erfolgreicher Widerspruch führt zu Löschung
- Ausdrückliches Widerspruchsrecht bei Profiling und Direktwerbung

DATENÜBERMITTLUNG INS AUSLAND

- Datenübermittlung innerhalb der EU unproblematisch
- Datenübermittlung in Drittstaaten:
  - Bedingungen über den internationalen Datenverkehr müssen eingehalten werden
    - Angemessenheitsbeschluss der Kommission
    - Vorliegen geeigneter Garantien (z.B. Binding Corporate Rules, Standarddatenschutzklauseln)
    - ausdrückliche Einwilligung, Erfüllung eines Vertrages, Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
  - Regelungen gelten auch für Auftragsverarbeiter
  - Geltung auch bei Weiterleitungsketten

VORKEHRUNGEN UND MAßNAHMEN IM UNTERNEHMEN

- **Dokumentation:** Erfassen aller Datenanwendungen, Führung eines Verzeichnisses
    - Verzeichnis von Verarbeitungstätigkeiten
- **Folgenabschätzung**: Analyse und Risikoeinschätzung, Nachweis richtlinienkonformer Abläufe, Kontakt mit Behörde herstellen
- **Datenschutzerklärungen** an neue Informationspflichten anpassen – Homepage/Intranet
- **Unternehmensinterne Datenschutzrichtlinie:** Leitlinien für Arbeitnehmer, regelmäßige Überprüfungen
- **Verantwortung/Datenschutzbeauftragter**: Klare Zuständigkeiten, Kompetenzen für Zuständige
- **Data Breach Notification Duty**
- **Technik und Organisation**: Privacy by Design/Default, Datensicherheitsmaßnahmen
- Einbindung des Betriebsrats

VERARBEITUNGSVERZEICHNIS
ART 30 DSGVO

- Überblick über die Datenverarbeitungsprozesse: Führung von Verfahrensverzeichnissen (Verantwortung: Unternehmensleitung)
- Zentrales DVR entfällt – bestehende Meldungen können exportiert werden
- Jeder Verantwortliche und ggf. sein Vertreter (**NEU**: auch der Auftragsverarbeiter - über alle im Auftrag eines Verantwortlichen durchgeführten Verarbeitungstätigkeiten) führen ein Verzeichnis aller Verarbeitungstätigkeiten: Aufzählung der Mindestangaben
- Teilweise Befreiung von dieser Pflicht bei Unternehmen mit weniger als 250 Beschäftigte, sofern (Auslegungsfrage: Ausnahme pro Unternehmen/Verarbeitung)
  - kein erhebliches Risiko für Betroffene vorhanden (z.B. Videoaufzeichnungen wären ein derartiges Risiko) oder
  - Verarbeitung nur gelegentlich angewendet wird (d.h. alle regelmäßigen Grundfunktionen sind zu verzeichnen) oder
  - keine sensitiven Daten (Gesundheitsdaten oder Strafregisterdaten) umfasst

VERARBEITUNGSVERZEICHNIS
ART 30 DSGVO

> Prüfung pro Verarbeitung, ob Ausnahme greift → im Zweifel ins Verzeichnis aufnehmen

> Tipp: historische Komponente, Aufsichtsbehörden sollen auch für die Vergangenheit Untersuchungen durchführen können

> Möglichkeit der Nachverfolgung aller Änderungen und Ergänzungen (Dokumentation mit Zeitstempel)

> Verzeichnis schriftlich, auch elektronisches Format (übersendungsfähig)

> Pro Abteilung ein Verantwortlicher für Verzeichnis/Aktualisierung – Planung der Strukturierung

> BRD: hat schon derartige Verzeichnisse; Erfahrungsberichte; Softwareanbieter

DATENSCHUTZ-FOLGENABSCHÄTZUNG
ART 35, 36 DSGVO

- Vorabkontrolle (Vorab-Audit) bei bestimmten Datenverarbeitungen erforderlich
- Aufsichtsbehörde wird Negativlisten veröffentlichen („Black-List“)
- Jedenfalls erforderlich, wenn neues Verfahren eingesetzt wird, das hohes Risiko für Betroffenen befürchten lässt (z.B. Profiling, Verarbeitung sensibler Daten, Überwachungsmaßnahmen)
- Ergebnis ist positiv oder negativ. Im Zweifel ist Aufsichtsbehörde einzuschalten und deren Zustimmung einzuholen (Art 36 DSGVO)
- In der Praxis ist wegen der hohen Bußgelddrohung jedenfalls empfehlenswert, bei positiv-gelisteten Verarbeitungsvorgängen die Aufsichtsbehörde zu konsultieren (diese hat binnen 8 Wochen zu entscheiden)

INFORMATIONSPFLICHTEN
ART 12, 13, 14 DSGVO

> Unterscheidung zwischen Daten, die bei dem Betroffenen direkt erhoben werden (Art 13 DSGVO) und Daten, die anderweitig erhoben werden (Art 14 DSGVO)

> Informationen sind grds. zum Zeitpunkt der Erhebung der Daten zur Verfügung zu stellen

> Die Informationspflichten beinhalten (Auszug):

- Name und Kontaktdaten des Verantwortlichen (ggf. des Datenschutzbeauftragten)
- Zweck der Datenverarbeitung
- Empfänger und Kategorien von Empfängern
- Angabe zur Rechtsgrundlage der Datenverarbeitung (auch welche Interessen)
- Transfer in Drittstaaten
- Voraussichtliche Dauer der Datenspeicherung
- Rechtsbelehrung der Betroffenenrechte; Beschwerderecht an die Aufsichtsbehörde

DATENSICHERHEIT
ART 32 DSGVO

- Datensicherheit als eines der Primärziele der DSGVO
- Gewährleistung der Datensicherheit als Grundsatz für die Verarbeitung („Integrität und Vertraulichkeit“) = Schutz vor Zugriff, Verarbeitung durch unbefugte Personen
- Privacy by design / Privacy by default
- Auftragsverarbeiter sollen vertraglich zu technischen und organisatorischen Sicherheitsmaßnahmen verpflichtet werden
- Evaluierung der Sicherheit von Daten im Zuge der Datenschutz-Folgenabschätzung
- Zertifizierungen, Verhaltensregeln zur Gewährleistung von Datensicherheit
- Verpflichtung zu geeigneten Sicherheitsmaßnahmen bei Bildverarbeitung (§ 13 DSG)

DATENSICHERHEIT
ART 32 DSGVO

- Unter Berücksichtigung von Stand der Technik, Implementierungskosten, Zweck und Risiko der Verarbeitung muss der Verantwortliche und Auftragsverarbeiter dafür sorgen, dass
  - Daten weitgehend pseudonymisiert und verschlüsselt werden
  - Systemvertraulichkeit und -integrität sichergestellt werden
  - Daten bei Zwischenfällen richtig wiederhergestellt werden
  - Prozesse und Verfahren vorliegen, um eine regelmäßige Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen gewährleisten zu können.
- Maßstab ist der zum Zeitpunkt der Datenverarbeitung jeweilige Stand der Technik unter Berücksichtigung der „Sensibilität der Daten“
- Entwicklung eines Informationssicherheitsmanagement-Systems (ISMS)

DATENSICHERHEIT
MÖGLICHE MAßNAHMEN

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
  - Passwortsicherungen von Dateien
  - 2-Faktor-Authentifizierung
- Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung
  - Zutritts-/Zugangskontrollen, Zugriffsbeschränkungen
  - Aufgabenverteilung
  - Verarbeitung nur auf Anweisung des Verantwortlichen verarbeiten („Auftragsprinzip“)
- regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen
  - Selbstevaluierungsprozesse
  - Schulungen

PRIVACY BY DESIGN
ART 25 DSGVO

- Datensicherheit durch **Technikgestaltung**
- Angemessenheit beurteilt nach:
  - Stand der Technik
  - Implementierungskosten
  - Art, Umfang und Zweck der Datenverarbeitung
  - Risiken hinsichtlich Schwere und Eintrittswahrscheinlichkeit
- Beispiele:
  - Technische Mittel zur Erhöhung der Datenminimierung, -sparsamkeit und -begrenzung
  - Technische Mittel zur PseudonymisierungZugriffsschranken und -kontrollen in technischer und organisatorischer Hinsicht
  - Unternehmenspolicies

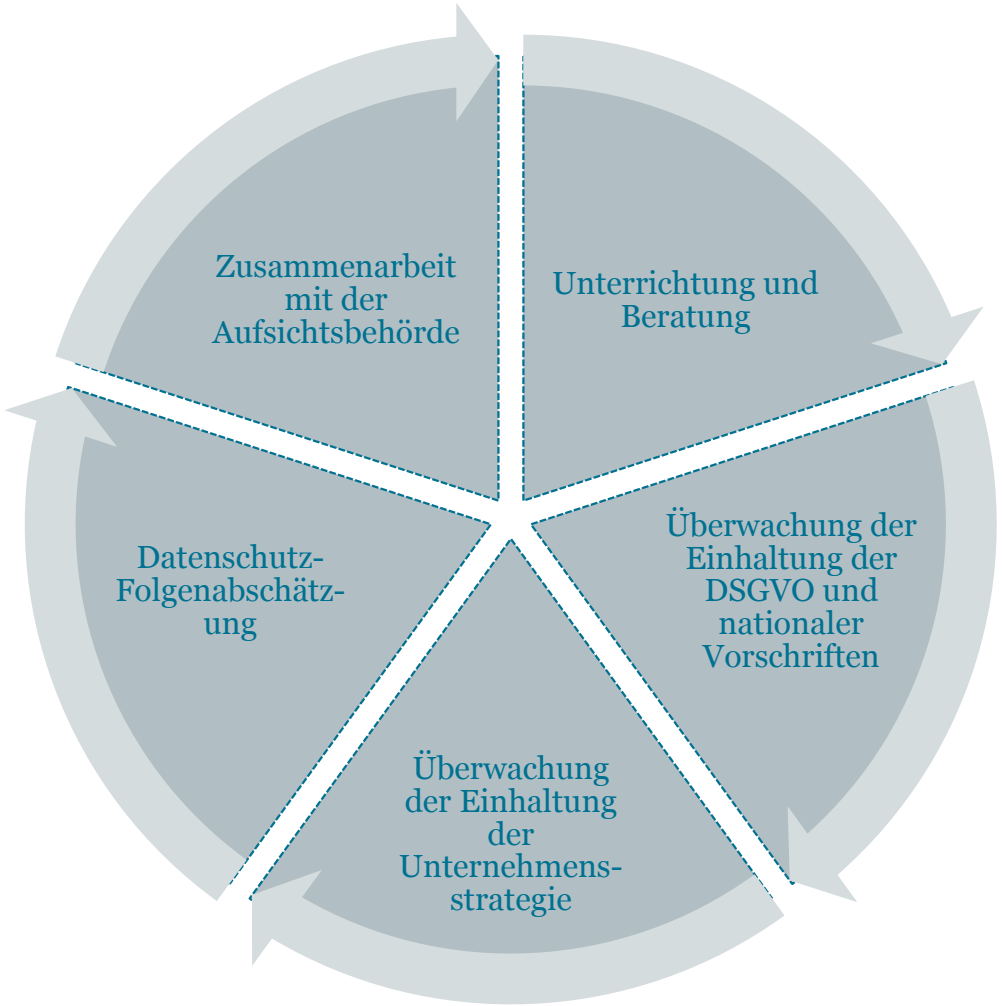
PRIVACY BY DEFAULT
ART 25 DSGVO

- Datensicherheit durch **datenschutzfreundliche Voreinstellungen**
- Soll sicherstellen, dass nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden
- Betrifft:
  - Menge der erhobenen Daten
  - Umfang der Verarbeitung
  - Speicherfrist
  - Zugänglichkeit
- Wichtigste Adressaten: „Social Media“

DATENSCHUTZBEAUFTRAGTER
ART 37 DSGVO

- Bestellung notwendig, wenn
  - die Verarbeitung von einer **Behörde oder öffentlichen Stelle** durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln
  - zu den **Kernaktivitäten des Unternehmens**
    - die umfangreiche regelmäßige und systematische Überwachung von Betroffenen oder
    - die umfangreiche Verarbeitung sensibler Daten zählt
- Im DSG keine weiteren Fälle vorgeschrieben
- Freiwillige Bestellung möglich
- Bestellung intern oder extern möglich
- Gemeinsamer Datenschutzbeauftragter für Unternehmensgruppe möglich, sofern der dieser von jeder Niederlassung aus leicht erreicht werden kann

AUFGABEN DES DATENSCHUTZBEAUFTRAGTEN
ART 39 DSGVO



MELDUNG VON DATENSCHUTZVERLETZUNGEN (DATA BREACH NOTIFICATION)
ART 33, 34 DSGVO

> „*Verletzung des Schutzes personenbezogener Daten*“ (data breach) ist eine Verletzung der Sicherheit (z.B. Verlust eines Datenträgers, Hackerangriff)

> Der betroffenen Personen kann dadurch ein physischer, materieller oder immaterieller Schaden entstehen

> **Meldung an die zuständige Aufsichtsbehörde**

- wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt
- möglichst binnen 72 Stunden nachdem dem Verantwortlichen diese Verletzung bekannt wurde

> **Benachrichtigung der betroffenen Person**

- wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein **hohes Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat

STRAFEN
ART 83 DSGVO, §§ 30, 62, 63 DSG

- Pflichten der Verantwortlichen, der Auftragsverarbeiter: **bis zu EUR 10 Mio** oder bis 2% des weltweiten Gesamtjahresumsatzes
- **Grundsätze** für die Verarbeitung; **Betroffenenrechte**; **Übermittlung in ein Drittland**; Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten; Nichtbefolgung einer Anweisung/Beschränkung/Aussetzung der Datenübermittlung durch die Aufsichtsbehörde; Nichtgewährung des Zugangs : **bis zu EUR 20 Mio** oder bis 4% des weltweiten Gesamtjahresumsatzes
- Einheitliches Strafniveau in den Mitgliedstaaten angestrebt
- DSG sieht zusätzlich Verwaltungsstrafen von bis zu **EUR 50.000** vor
- Datenverarbeitung in Gewinn- und Schädigungsabsicht; **Freiheitsstrafe** bis zu **einem Jahr** oder Geldstrafe bis zu **720 Tagessätzen**

UNTERLASSUNG UND SCHADENERSATZ
ART. 82 DSGVO

- Schadenersatz wird ausgebaut
- Ersatz von materiellen und immateriellen Schäden
- Gerichtsstand
- Klagsbefugte Vereinigungen
- Anspruchsgegner: Verantwortlicher und Auftragsverarbeiter
- Gesamtschuldnerische Haftung (Regressanspruch)

HAFTUNG
VERANTWORTUNG IN UNTERNEHMEN

- Sanktionsbestimmungen richten sich grundsätzlich gegen Unternehmen selbst (Unternehmensdefinition wie im Kartellrecht!)
- Öffnungsklausel: Mitgliedstaaten können auch weitere Sanktionen festsetzen (z.B. Einziehung rechtswidrig erzielter Gewinne, Shaming)
- Haftungserleichterungen für natürliche Personen (Möglichkeit der Verwarnung, Berücksichtigung der wirtschaftlichen Lage)

Danke für Ihre Aufmerksamkeit!

Dr. Ivo Rungg
T +43(512)579973 - 510
T +43 (1) 534 80 - 510
rungg@bindergroesswang.at

COMPETENCE
YOU CAN COUNT ON.