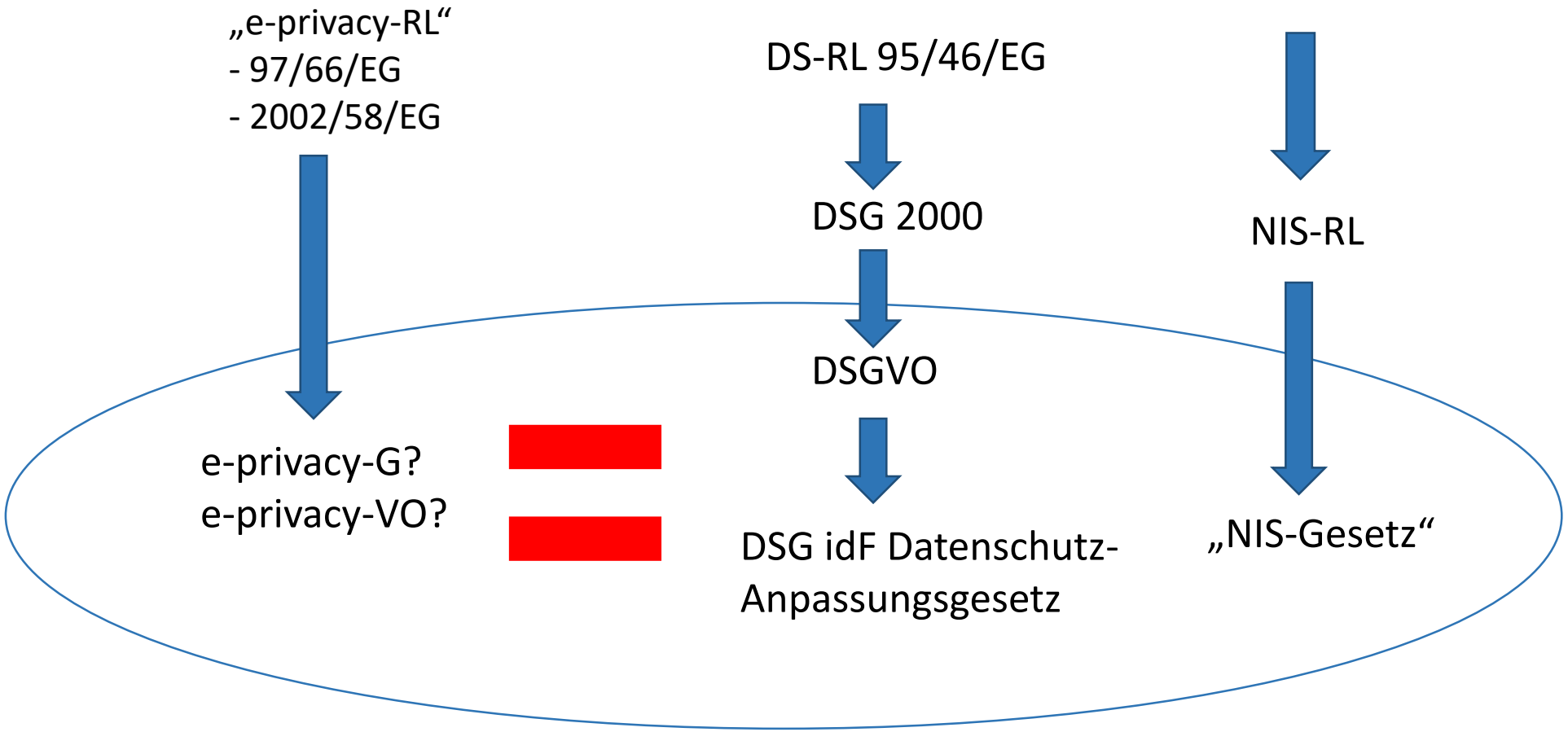
Datenschutz-Grundverordnung (EU 2016/679)

Änderungen und Neuerungen im Überblick

RAA Mag. Karin Neußl

Neues Daten- und Informationssicherheitsrecht ab 05/2018



DSGVO

Per 25.05.2018 gilt mit der DSGVO in der gesamten EU ein (fast) **einheitliches Datenschutzrecht**

NEUHEITEN:

- Akteure: Betroffener – Verantwortlicher – Auftragsverarbeiter
  statt Betroffener – Auftraggeber – Dienstleister
- Mehr Betroffenenrechte
  - Informationspflichten zusätzlich zum Auskunftsrecht
  - Recht auf Berichtigung, Einschränkung der Verarbeitung, Datenübertragbarkeit, „Recht auf Vergessenwerden“
- Erfasst sind auch Nicht-EU-Unternehmen (Benennung Vertreter)
- Verarbeitungsverzeichnis statt DVR
- Datenschutz-Folgenabschätzung statt Vorabkontrolle
- Datenschutzbeauftragter
- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- Vertraulichkeit/Integrität/Verfügbarkeit/Belastbarkeit: Verschränkung von Datenschutz und Informationssicherheit (rechtlich/technisch)
  - Stand der Technik für technische und organisatorische Maßnahmen
  - C- I- A, Data Leakage Prevention, Audits, Wirksamkeitsprüfungen
  - Risikobetrachtung steht über wirtschaftlichen Interessen
- Geldbußen (2 % weltweiter Vorjahresumsatz/10 Mio; 4 % weltweiter Vorjahresumsatz/20 Mio)

Einführung

- **Sachlicher Anwendungsbereich**
  - Automatisierte Verarbeitung
  - Nichtautomatisierte Verarbeitung in einem Dateisystem = strukturierte Sammlung nach bestimmten Kriterien
- **Räumlicher Anwendungsbereich**
  - Niederlassung in der EU
  - Keine Niederlassung in der EU
    - Anbot von Waren und Dienstleistungen an Betroffene in der EU
    - Beobachtung von Verhalten in der EU
- **Personenbezogene Daten**
  - Natürliche / juristische Personen (!)
  - Direkt od indirekt identifizierbar
- **Rollenverteilung definieren**
- **„normale“, besondere Datenkategorien**
  - Genetische Daten
  - Gesundheitsdaten
  - Biometrische Daten
  - Strafrechtliche Daten (Art 10)

Verarbeitungsgrundsätze – Art 5

- Datenverarbeitung nur, wenn
  - Rechtmäßig (Art 6, 9, 10)
  - Nach Treu und Glauben
  - Transparent (Art 12)

- Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Rechenschaftspflicht

- Integrität und Vertraulichkeit, Verfügbarkeit und Belastbarkeit durch technische und organisatorische Maßnahmen („InfoSih“)

„Erlaubnistatbestand“ – Art 6

- **Rechtmäßige Datenverarbeitung**
  - Einwilligung
    - Freiwillig, ohne Zwang, aktiv, kein Ungleichgewicht, Kopplungsverbot, jederzeitiger Widerruf, in informierter Weise und für den konkreten Fall
  - Vertrag
    - Auch vorvertragliche Maßnahmen auf Anfrage von Betroffenen
  - Rechtliche Verpflichtung
    - Gesetzliche Grundlage
  - Berechtigte Interessen des Verantwortlichen oder Dritten
    - Interessenabwägung

➡ Weiterverarbeitung zu anderen Zwecken nur wenn mit Ursprungszweck vereinbar!

„Erlaubnistatbestand“ – Art 9, 10

- Grundsatz: **Verarbeitungsverbot für besondere Datenkategorien**
  - Gilt nicht bei: ausdrücklicher Einwilligung, vom Betroffenen selbst öffentlich gemachte Daten, Geltendmachung/Ausübung/Verteidigung von Rechtsansprüchen, etc

- Datenverarbeitung über **strafrechtliche Verurteilungen und Straftaten** (gerichtlich od verwaltungsbehördlich strafbare Handlungen od Unterlassungen) nur eingeschränkt zulässig
  - Ausdrückliche gesetzliche Ermächtigung oder Verpflichtung
  - Gesetzliche Sorgfaltspflichten
  - Berechtigte Interessen des Verantwortlichen oder Dritten

    → § 4 Abs 3 DSG / Art 10 DSGVO

Transparenzgrundsatz – Art 12

- Art 13, 14; Art 15 – 22; Art 34
- Klare und einfache Sprache
  - Keine Fachausdrücke, knappe Sätze, Durchschnittsmensch, aufklappbare Texte, aktiv statt passiv
- Schriftliche oder elektronische „Informationen“
  - Auf Verlangen auch mündlich
- Unverzüglich, max 1 Monat ab Antragseingang
  - Verlängerung um weitere 2 Monate möglich (Komplexität, Anzahl)
    - Benachrichtigung von Fristverlängerung und über Verzögerungsgründe binnen 1 Monat
  - Kein Tätigwerden → Benachrichtigung binnen 1 Monat und Info über Gründe und Beschwerdemöglichkeit bei Aufsichtsbehörde oder gerichtlicher Rechtsbehelf
- Unentgeltlich
  - Gilt nicht bei exzessiven oder offenkundig unbegründeten Anträgen
    - Angemessenes Entgelt
    - Möglichkeit der Weigerung zum Tätigwerden, aber beweispflichtig
- Identitätsprüfung, elektronische Antragsmöglichkeit (nach Möglichkeit)

Informationspflichten – Art 13, 14

- Transparenzgedanke
- **Zeitpunkt**
  - Art 13: Zeitpunkt der Datenerhebung
  - Art 14: innerhalb angemessener Frist, max 1 Monat/Zeitpunkt der ersten Mitteilung (Kommunikationszwecke)/Zeitpunkt der ersten Offenlegung (Offenlegung an anderen Empfänger – nicht Auftragsverarbeiter)
    - **Je nachdem welcher Zeitpunkt früher ist!**
    - Daten kommen von Dritten, öffentlich verfügbaren Quellen, anderen Betroffenen
  - Vor Weiterverarbeitung zu anderem Zweck
- Keine Informationspflicht, wenn
  - Betroffener bereits über die Informationen verfügt
  - Unmöglich/unverhältnismäßiger Aufwand, insb statistische Zwecke, wissenschaftliche Forschungszwecke
  - Erhebung und Offenlegung von pb Daten gesetzlich geregelt
  - Gesetzliches Berufsgeheimnis und daher vertrauliche Behandlung von pb Daten
- Verschiedene Quellen → allgemeine Information

Informationspflichten - WIE?

- WP 29: zusätzlich zu Infos nach Art 13, 14 auch die wichtigsten Konsequenzen der Datenverarbeitung = Auswirkungen und Folgen auf Betroffene, ggf Teile der durchgeführten DSFA
- Betroffenen müssen die Informationen **aktiv** zur Verfügung gestellt werden!
  - Website: gut sichtbarer Link auf jeder Unterseite, Link auf selber Seite wo Daten abgefragt werden (Formulareingaben)
  - App: im App-Store vor dem Download und zusätzlich im Menübereich der App (< „two taps away“)
- Genaue, konkrete Zweckangabe und Angabe des Erlaubnistatbestands
  - Nicht: „to develop new services“, „for research purposes“, „to offer personalised services“
- Schriftliche Erklärungen, Informationen auf Vertragsdokumenten, mündliche Erklärungen durch reale Personen, sichtbare Schilder, Zeitungen/Medieninserate, etc

„…the very high level of internet access in the EU and the fact that data subjects can go online at any time, from multiple locations and different devices …“

Informationspflichten - WAS?

- Name, Kontaktdaten des Verantwortlichen
- Kontaktdaten DB
- Zwecke und Rechtsgrundlage
- Berechtigtes Interesse bei Art 6 Abs 1 lit f
- Empfänger oder Empfängerkategorien
- Absicht Übermittlung in Drittland oder internationale Organisation samt Drittlandangaben
- Speicherdauer oder -kriterien
- Auskunftsrecht, Berichtigungs- und Löschungsrecht, Einschränkung der Verarbeitung, Widerspruchsrecht, Recht auf Datenübertragbarkeit
- Widerrufsrecht bei Einwilligung
- Beschwerderecht bei Aufsichtsbehörde = DSB
- Ob automatisierte Entscheidungsfindung/Profiling besteht und bejahendenfalls Angaben zur involvierten Logik und Tragweite sowie Auswirkungen für die Betroffenen
- Ob pb Daten gesetzlich od vertraglich bereitgestellt werden müssen od für Vertragsabschluss erforderlich sind, ob Betroffene verpflichtet ist Daten bereitzustellen und welche möglichen Folgen eine Nichtbereitstellung hat (Art 13)
- Kategorien personenbezogener Daten (Art 14)
- Quelle und ggf ob pb Daten aus öffentlich zugänglichen Quellen stammen (Art 14)

Betroffenenrechte – Art 15 ff

- Auskunftsrecht
- Recht auf Berichtigung
- Recht auf Löschung („Recht auf Vergessenwerden“)
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Automatisierte Entscheidungen im Einzelfall einschl Profiling

➡ **Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung**

Auskunftsrecht – Art 15

- **Bestätigung** ob pb Daten verarbeitet werden
- **Auskunft** über diese pb Daten und insb folgende Infos:
  - Verarbeitungszwecke
  - Datenkategorien
  - Empfänger oder –kategorien (inkl Drittländer)
  - Speicherdauer oder –kategorien
  - Recht auf Berichtigung od Löschung oder Einschränkung oder Widerspruch
  - Beschwerderecht bei Aufsichtsbehörde
  - Bei Art 14: alle verfügbaren Informationen über Datenherkunft
- **Bereitstellung Kopie** der pb Daten
  - Für weitere Kopien ist angemessenes Entgelt möglich
  - Bei elektronischen Anträgen → gängiges elektronisches Format
- Identitätsprüfung, sicherer Fernzugang

Recht auf Berichtigung – Art 16

- Berichtigung unrichtiger Daten

- Vervollständigung unvollständiger Daten
  - Ggf ergänzende Erklärung
  - ZB Personalakt

Recht auf Vergessenwerden – Art 17

- Löschungsrecht des Betroffenen
- Unverzügliche Löschungspflicht des Verantwortlichen insb bei:
  - Zweckerreichung
  - Widerruf Einwilligung und Fehlen anderer Rechtsgrundlage
  - Widerspruch des Betroffenen
  - Unrechtmäßige Datenverarbeitung
  - Erfüllung rechtliche Verpflichtung
- Bei öffentlich gemachten pb Daten durch den Verantwortlichen → angemessene Maßnahmen zur **Unterrichtung anderer Verantwortliche** (Löschung Links, Kopien od Replikationen der pb Daten)

Recht auf Einschränkung der Verarbeitung – Art 18

- Nur unter folgenden Voraussetzungen:
  - Richtigkeit der Daten wird bestritten
    - Dauer der Prüfung
  - Unrechtmäßige Datenverarbeitung und Betroffener lehnt Löschung ab
  - Verarbeitungszweck ist erreicht, aber Betroffener benötigt die Daten noch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
  - Betroffener hat Widerspruch eingelegt
    - Dauer der Prüfung, ob berechtigte Gründe des Verantwortlichen überwiegen
- Daten dürfen nur mit Einwilligung oder für Rechtsansprüche oder zum Schutz anderer natürlicher od juristischer Personen od wg einem wichtigen öffentlichen Interesse verarbeitet werden – ausgenommen Speicherung

Unterrichtung des Betroffenen vor Aufhebung der Einschränkung!

Mitteilungspflicht – Art 19

Wurden Daten anderen Empfängern **offengelegt**

- Mitteilung an alle Empfänger über
  - ➢ Berichtigung, Löschung, Einschränkung der Verarbeitung
  - ➢ Gilt nicht bei unverhältnismäßigem Aufwand oder Unmöglichkeit
- Auf Verlangen: Mitteilung an Betroffene über diese Empfänger

Recht auf Datenübertragbarkeit – Art 20

- **Nur wenn** die Datenverarbeitung auf einer Einwilligung oder auf einem Vertrag beruht
- Verantwortlicher muss dem Betroffenen die Daten in einem strukturierten, gängigen und maschinenlesbaren Format übermitteln
- Betroffene haben das Recht, dass ihre pb Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden
  - Entwicklung interoperabler Dateiformate
  - Keine Pflicht zur Übernahme/Beibehaltung von technisch kompatoblen Datenverarbeitungssystemen

Widerspruchsrecht – Art 21

- Recht **besteht nur**, wenn Datenverarbeitung aufgrund von Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt oder aufgrund berechtigter Interessen des Verantwortlichen oder Dritten
- Verantwortlicher muss im Streitfall nachweisen/darlegen können, dass seine zwingenden berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten des Betroffenen haben
  - Einschränkung nach Art 18 Abs 1 lit d
- Keine Datenverarbeitung mehr, sofern nicht überwiegende schutzwürdige Gründe oder zur Ausübung/Verteidigung von Rechtsansprüchen
  - Löschung nach Art 17 Abs 1 lit c
- Gilt auch für Datenverarbeitungen zur Betreibung für Direktwerbung => **jederzeitiger** Widerspruch
- Verantwortlicher muss spätestens zum Zpkt der ersten Kommunikation auf dieses Recht ausdrücklich hinweisen („Datenschutzerklärung“)
  - Art 13, 14

Automatisierte Entscheidungen im Einzelfall – Art 22

- Recht nicht einer ausschließlich auf automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die **rechtliche Wirkung** entfaltet oder **in ähnlicher Weise erheblich beeinträchtigt**
  - ➢ Online-Kreditantrag, Online-Einstellungsverfahren, etc
- **Umfasst auch „Profiling“**
  - ➢ = automatisierte Datenverarbeitung unter Bewertung der persönlichen Aspekte, insb zur Analyse od Prognose von Arbeitsleistung, Gesundheit, wirtschaftliche Lage, persönliche Vorlieben, Zuverlässigkeit, Verhalten, etc
- Wenn Datenverarbeitung für Vertragsabschluss oder –erfüllung erforderlich ist, auf Basis von Rechtsvorschriften od mit ausdrücklicher Einwilligung erfolgt, **besteht das Recht <u>nicht</u>**
  - ➢ Aber: Wahrung der Betroffenenrechte und –freiheiten und berechtigten Interessen
    - – Recht auf Erwirkung des Eingreifens einer Person, Darlegung des eigenen Standpunkts, Anfechtung der Entscheidung (Mindestmaßnahmen)

Verarbeitungsverzeichnis – Art 30

- Verantwortlicher und Auftragsverarbeiter **müssen** ein Verarbeitungsverzeichnis führen
  - Ersetzt DVR-Meldung → Kosteneinsparung
  - Jedenfalls wenn mehr als 250 Beschäftigte, für alle anderen gemäß Abs 5 nur dann nicht, wenn kein Risiko für Rechte und Freiheiten von Betroffenen, Verarbeitung nur gelegentlich oder keine Art 9- od 10-Datenarten verarbeitet werden
    - Grds sollte jeder ein VVZ führen
  - Inhalt: Kontaktdaten, Zweck, Datenkategorie, Übermittlungsempfänger, Drittländerangaben, Fristen für Löschung, Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen (Art 32)
    - Kontaktdaten Verantwortlicher und Auftragsverarbeiter, Verarbeitungskategorie, Übermittlung in Drittländer samt Angaben dazu, Sicherheitsmaßnahmen

Datenschutzbeauftragter – Art 37 ff

- Behörde oder öffentliche Stelle, ausgenommen Gerichte
- Kerntätigkeit liegt in der Durchführung von Verarbeitungsvorgängen, die aufgrund Art, Umfang und/oder Zweck eine **umfangreiche regelmäßige und systematische Überwachung** von betroffenen Personen erforderlich machen oder
- Kerntätigkeit liegt in **umfangreichen Verarbeitung** von besonderen Datenkategorien gem Art 9 und/oder Art 10 (sensible Daten, strafrechtlich relevante Daten)
- KANN auch externer Dienstleister sein (Art 37 Abs 6)
- Eventuelle Unvereinbarkeit mit anderen Funktionen (GF, CIO) beachten! (unabhängig und weisungsfrei, Abberufung nur eingeschränkt möglich)
- Liste (ähnlich Gewerberecht)??

Datenschutz-Folgenabschätzung – Art 35

- Abschätzung der Risiken der geplanten Datenanwendung ist durchzuführen (notwendig auch für Festlegung der erforderlichen Schutzmaßnahmen)
  - ➢ Bei hohem Risiko für Rechte und Freiheiten Betroffener => DSFA
- DSFA: Konsultation des DB und ggf Aufsichtsbehörde

  Insbesondere in folgenden Fällen ist eine DSFA erforderlich
  - ➢ Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschl Profiling gründet und als Entscheidungsgrundlage dient
  - ➢ Umfangreiche Verarbeitung besonderer Datenkategorien (Art 9 und/oder 10-Daten)
  - ➢ Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche
- Regelmäßige Überprüfung, jedenfalls bei Risikoänderungen

⇨ Risikoanalyseprozess implementieren

„Data Breach Notification“ – Art 33, 34

- Bisher in § 24 Abs 2a DSG 2000, nun strenger in Art 33 DSGVO
- Meldung **unverzüglich** (höchstens 72 Stunden) nachdem die Verletzung **bekannt** wurde an die zuständige Aufsichtsbehörde (Begründungspflicht bei Verzögerungen)
- Bei Verletzung des Schutzes personenbezogener Daten mit voraussichtlich hohem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zusätzlich unverzügliche Benachrichtigung der betroffenen Person od öffentliche Bekanntmachung bei unverhältnismäßigem Aufwand der Einzelbenachrichtigung

Datenschutz durch Technikgestaltung/datenschutzfreundliche Voreinstellungen – Art 25

- Abs 1: **geeignete technische und organisatorische** Maßnahmen zum Schutz der Daten unter Berücksichtigung: Stand der Technik, Implementierungskosten, Art/Umfang/Umstände/Zweck der Verarbeitung, Risiken für Betroffene (Eintrittswahrscheinlichkeit, Schwere)
  - ➢ Informationssicherheit, ISMS
- Abs 2: **Voreinstellungen** durch geeignete technische und organisatorische Maßnahmen insbesondere um Zugänglichkeit zu Daten einzuschränken (Informationssicherheit/Vertraulichkeit)
  - ➢ Datenmenge, Verarbeitungsumfang, Speicherfrist
- Abs 3: **genehmigtes Zertifizierungsverfahren** gem Art 42 kann als Faktor herangezogen werden, um Erfüllung der Datenschutzpflichten nachzuweisen

Datensicherheitsmaßnahmen – Art 32

- Abs 1: Unter Berücksichtigung Stand der Technik, Implementierungskosten und Art, Umfang, Umstände und Zwecke der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für Rechte und Freiheiten natürlicher Personen müssen Verantwortlicher und Auftragsverarbeiter geeignete **technische und organisatorische** Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten
  - Dazu gehören insb:
    - Pseudonymisierung und Verschlüsselung pb Daten
    - Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste auf Dauer
    - Rasche Wiederherstellung der Verfügbarkeit und Zugang bei Zwischenfällen
    - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung
- Abs 3: **genehmigte Verhaltensregeln gem Art 40** oder **genehmigtes Zertifizierungsverfahren gem Art 42** kann als Faktor herangezogen werden, um Anforderungen zu erfüllen
- **§ 6 DSG - Datengeheimnis**

Sanktionen

- Zivilrechtliche Ansprüche
  - Schadenersatz
  - Verantwortlicher und Auftragsverarbeiter müssen sich freibeweisen!
- Verwaltungsbehördliche Sanktionen
  - Bis zu **€ 10.000.000** od bis zu **2%** des gesamten weltweit erzielten Vorjahresumsatzes, je nachdem welcher Betrag höher ist
  - Bis zu **€ 20.000.000** od bis zu **4%** des gesamten weltweit erzielten Vorjahresumsatzes, je nachdem welcher Betrag höher ist
    - Verstöße gegen Verarbeitungsgrundsätze (Art 5, 6, 9)
    - Verstöße gegen Bedingungen für Einwilligung (Art 7)
    - Verstöße gegen Betroffenenrechte (Art 12 – 22)
    - etc

FRAGEN ???

PROF. HINTERMAYR & PARTNER
rechtsanwälte | attorneys at law
www.lawfirm.eu

Danke für die Aufmerksamkeit

RAA Mag. Karin Neußl

Prof. Hintermayr & Partner, Landstraße 12/Arkade, 4020 Linz, office@lawfirm.eu

Lektorin FH OÖ Department Sichere Informationssysteme

TÜV-zertifizierte Datenschutzbeauftragte