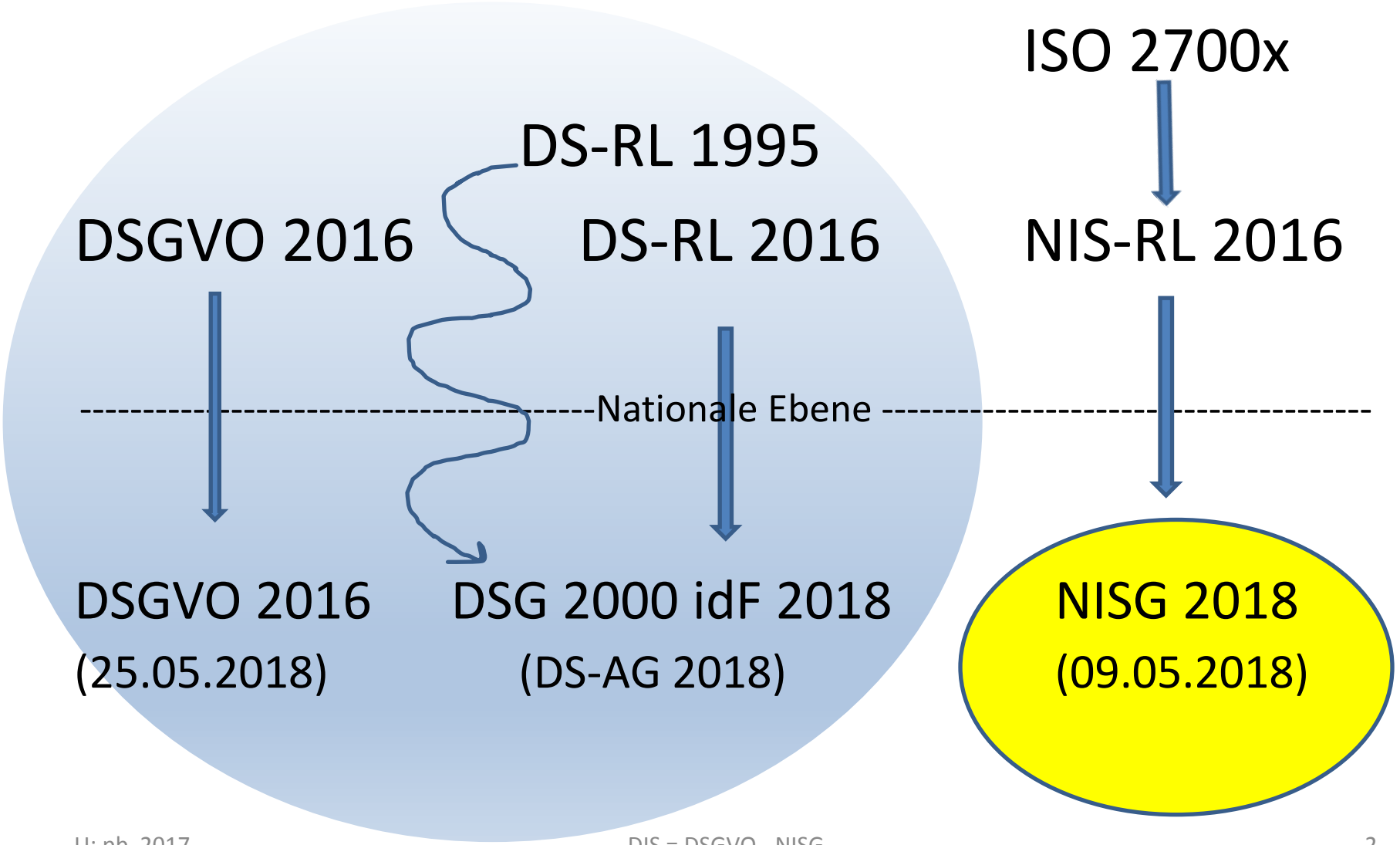
DATEN- UND INFORMATIONSSICHERHEITSRECHT (DIS) nach der

DSGVO

Peter Burgstaller
Rechtsanwalt in Linz
FH-Professor für IT-/IP-Recht/Hagenberg
Gerichtssachverständiger für Urheberfragen und Medienwesen
www.lawfirm.eu

Nichts wirklich neues im Datenschutz…in der Informationssicherheit schon…



Neu ist: Verschränkung von Daten- und Informationssicherheit (DIS)

- Datenschutz – personenbezogene Daten natürlicher Personen
- Informationsschutz umfasst alle Daten, insb auch Betriebs-/Geschäftsgeheimnisse

Datenschutz ist eine Teilmenge des Informationsschutzes

- DIS sehen insb die Sicherung der Vertraulichkeit, Integrität, Verfügbarkeit vor

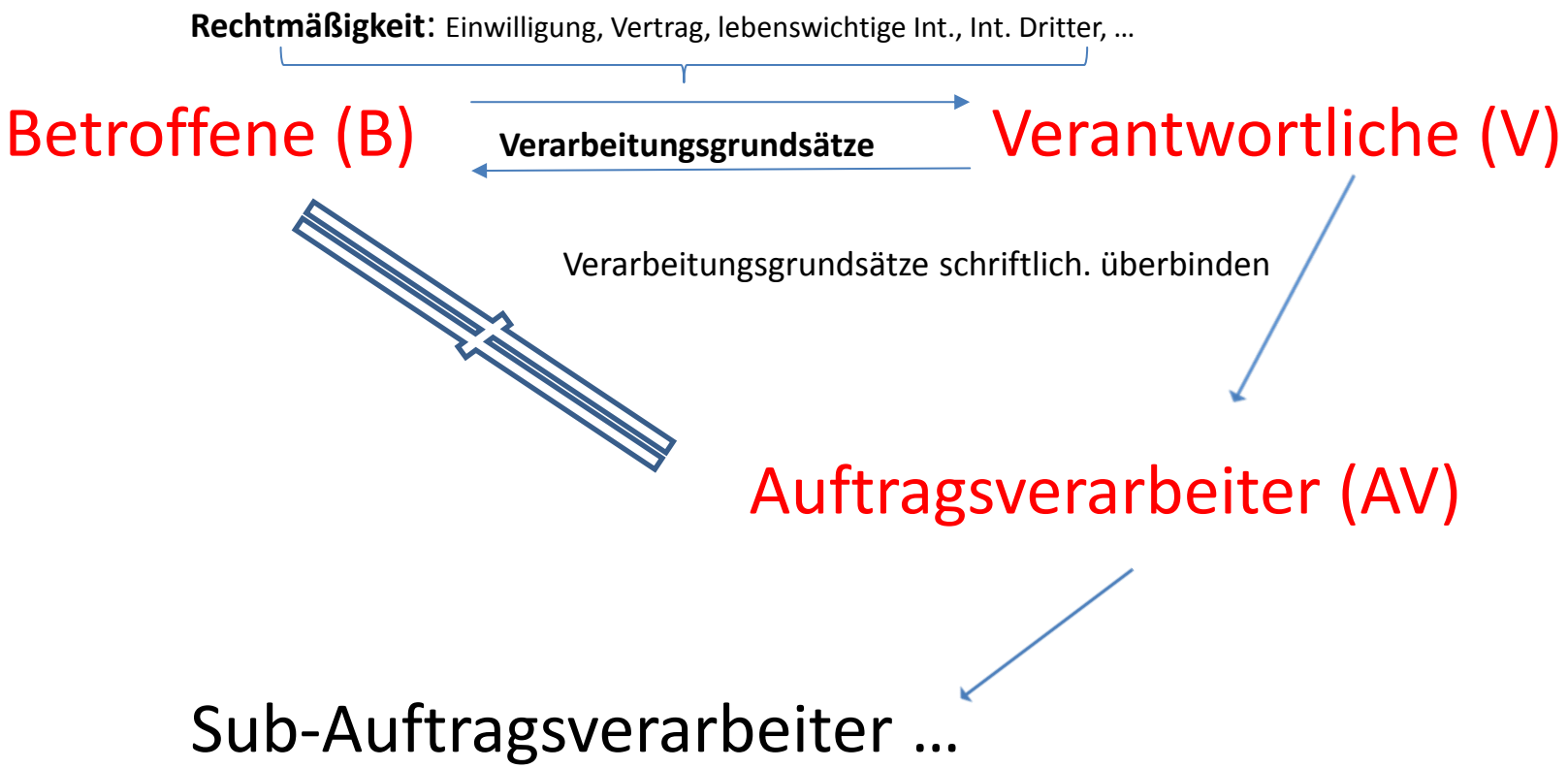
Confidentiality **I**ntegrity **A**vailability

Ziel des Datenschutzes ist

- NICHT die Verhinderung von Geschäftsabläufen/-ideen, sondern vielmehr die SICHERSTELLUNG des Grundrechts auf Geheimhaltung der personenbezogenen Daten der Betroffenen
  - Verfassungsbestimmung
  - EU-Grundrechtscharta
- Ausfluss des Menschenrechts auf Wahrung der Privatsphäre

=> In DE: **Informationelle Selbstbestimmung** = jeder soll das Recht haben, zu bestimmen, ob und was mit seinen Daten passiert (das ist nicht so bspw bei prominenten App-Anbietern!)

Wie funktioniert Datenschutz



Datenschutz-Grundverordnung (DSGVO 2016)

- Per 25.05.2018 tritt mit der DSGVO ein **einheitliches Datenschutzrecht in der EU** in Geltung, das extreme Strafdrohungen vorsieht: bis EUR 10 Mio/2 % Jahreskonzernumsatz oder bis EUR 20 Mio/4 % Jahreskonzernumsatz)
- **Anwendungsbereich:** Wenn V im EWR oder Dienste an B im EWR angeboten werden (so bspw WhatsApp)

5 Schritte zur DSGVO-Compliance

(„Grundansatz“)

(1) Sicherstellung/Einhaltung der **Verarbeitungs- und Rechtmäßigkeitsgrundsätze** (insb einwandfreie Einwilligungen für die Datenverwendung)

(2) Sicherstellung der **Betroffenenrechte**

(3) Datenverarbeitungsverzeichnis; Meldung von Datenschutzverletzungen und Sichtung von Dienstleistungsverträgen

(4) Prüfung von **datenschutz-folgenabschätzungspflichtigen** Datenanwendungen – Liste der Datenschutzbehörde

(5) Prüfen, ob **Datenschutzbeauftragter** notwendig

1. Schritt

1.1 Verarbeitungsgrundsätze, 5

Personenbezogene Daten müssen

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (**„Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“**);
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; (**„ZWECKBINDUNG“**);
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**„Datenminimierung“**);
- sachlich richtig sein (**„Richtigkeit“**);
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es erforderlich ist (**„Speicherbegrenzung“**);
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (**„Integrität und Vertraulichkeit“**).

Der Verantwortliche ist für die Einhaltung dieser Grundsätze verantwortlich und muss dessen Einhaltung nachweisen können (**„Rechenschaftspflicht“**).

1.2 Rechtmäßige Verarbeitung, 6

Die Verarbeitung ist nur rechtmäßig, wenn

- die betroffene Person ihre Einwilligung zu der Verarbeitung gegeben hat
- die Verarbeitung zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich ist,
- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt;
- die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt;
- die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Rechtmäßige Verarbeitung besonderer Kategorien (a), 9

- Die Verarbeitung von Daten aus denen die
  - **rassische und ethnische Herkunft,**
  - **politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie**
  - **die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,**
  - **Gesundheitsdaten oder**
  - **Daten zum Sexualleben oder der sexuellen Orientierung** einer natürlichen Person

  ist untersagt.
- Ausnahmen:
  - Die betroffene Person hat **ausdrücklich** für einen oder mehrere festgelegte Zwecke eingewilligt
  - Die Verarbeitung ist **im Bereich des Arbeitsrechts** und dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich
  - Verarbeitung liegt im öffentl. Interesse, lebenswichtige Interessen des Betroffenen, Katastrophenfälle, ...

Muster für eine Einwilligung

Ich stimme zu, dass meine persönlichen Daten, nämlich [*Datenarten aufzählen, zB „Name, Adresse, Geburtsdatum …“*] zum Zweck der [*genauen Zweck anführen, zB „zur Zusendung von Werbeprospekten über unsere XY Produkte“*] verarbeitet werden und an [*genauen Übermittlungsempfänger anführen, zB XY GmbH in…*] zum Zweck [*genauen Übermittlungszweck angeben, zB Zusendung von Informationen über XY-Produkte*] übermittelt werden.

Diese Zustimmung kann ich jederzeit [*mittels Brief an …/telefonisch an …/per E-Mail an … etc*] widerrufen.

2. Schritt

Wahrung der **Rechte der Betroffenen, 12 - 22**

- Informationsrecht
- Auskunftsrecht
- Berichtigungsrecht und Löschungsrecht (Recht auf Vergessen)
- Widerspruchsrecht
- Recht auf Datenübertragbarkeit
- Recht auf „menschliche Entscheidung“

3. Schritt

3.1 Verarbeitungsverzeichnis, 30

- das A&O zur DSGVO-Compliance -

- Verantwortlicher und Auftragsverarbeiter haben (schriftlich=elektronisch) ein Verarbeitungsverzeichnis zu führen (ersetzt DVR-Meldung)
- Für alle Verarbeitungen von pb Daten, ausg. nur vorübergehend
- Inhalt nach Art 30 DSGVO (vgl auch § 49 DS-AG):
  - Art der Daten
  - Zweck
  - Beabsichtigter Datentransfer in Drittland (zusätzliche Aspekte sind zu prüfen!)
  - Empfänger
  - Fristen zur Löschung
  - Datensicherheitsmaßnahmen

Verarbeitungsverzeichnis

- Verarbeitungsverzeichnis erfordert (datenschutzrechtliches) „Selbst-Assessment“ des eigenen Unternehmens
- Verarbeitungsverzeichnis soll Verarbeitungsprozesse mit den Vorgaben nach Art 30 DSGVO beinhalten
  - CRM
  - Personalverwaltung
  - Kunden-/Lieferantenverwaltung
  - ...
- Export-Funktion im DVR-Online – pdf-Dokumente oder XML-Dateien
- Keine formalen Vorgaben zum Führen des Verzeichnisses von der DSB – Muster eines Verzeichnisses:
  - WKÖ:
    - https://www.wko.at/.../EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-**Auftragsverarbeiter**...
    - https://www.wko.at/.../EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-**Verantwortlicher**...

3.2 Data Breach Notification, Art 33

- Meldung einer Datenschutzverletzung binnen 72 Stunden nachdem sie bekannt wurde an die **zuständige Aufsichtsbehörde**
- Unverzügliche Benachrichtigung der **betroffenen Person** von Datenschutzverletzung

=> Keine Meldung wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt – Risikoabschätzung!

3.3 Sichtung von Dienstleistungsverträgen

- Verträge mit Auftragsverarbeiter (=Dienstleister) sind **schriftlich** abzufassen
- Auftragsverarbeiter hat jene Datensicherheitsmaßnahmen zu ergreifen, die der Verantwortliche einhalten muss
- „Verlässlichkeit“ des Auftragsverarbeiters ist zentral, um nicht selber als Verantwortlicher in Haftung gezogen zu werden

Schritt 4

Datenschutz-Folgenabschätzung

- Der Verantwortliche hat **vorab** eine Abschätzung der datenschutzrechtlichen Folgen vorzunehmen, und zwar insbesondere in folgenden Fällen
  - **systematische und umfassende Bewertung persönlicher Aspekte** natürlicher Personen - Profiling;
  - **umfangreiche Verarbeitung besonderer Kategorien** von personenbezogenen Daten oder Daten über strafrechtliche Verurteilungen und Straftaten oder
  - systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.
- Der Verantwortliche holt sich den Rat des Datenschutzbeauftragten ein. Die Datenschutzbehörde hat eine Liste mit datenschutz-folgenabschätzungspflichtigen Datenanwendungen zu erstellen (Art 35 Abs 4 DSGVO)
- Meldung an DSB – binnen 8 Wochen Reaktion, sonst Genehmigung

Schritt 5

Datenschutzbeauftragter (DSB), 37

- Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten und übermitteln der Behörde Kontaktdaten, insbesondere wenn:
  - die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen** erforderlich machen, oder
  - die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung **besonderer Kategorien von Daten** oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten besteht.
- Kerntätigkeit ist Haupttätigkeit des Verantwortlichen – wenn zur Erfüllung der Haupttätigkeit die Verarbeitung von besonderen Datenkategorien ist, ist ein DSB zu bestellen (insb Gesundheitsdiensteanbieter; denkbar wären auch Energieversorger aufgrund der Möglichkeiten von Smart-Meters)

Datenschutzbeauftragter

- DSB ist bei der Erfüllung seiner Aufgaben weisungsfrei
- DSB berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters
- DSB kann auch ein Dienstleister sein
- DSB ist der Datenschutzbehörde zu melden
- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten
- Überwachung der Einhaltung der DSGVO und anderer Datenschutzvorschriften
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung

BESONDERHEITEN DES DS-AG, DSG 2000 idF 2018

1. Bildverarbeitung (§§ 12, 13)

- Bildaufnahme samt akustischen Infos im öffentlichen und nicht-öffentlichen Raum
- **Bildaufnahme zulässig**, wenn
  - Einwilligung, lebenswichtige Int., gesetzliche Erlaubnis, überwiegende berechtigte Interessen
  - Insb. zulässig priv. Liegenschaft; priv. Doku ohne Ziel Dritte zu erfassen; öffentlich zugänglich aber vom Hausrecht umfasst
- Bildaufnahme **unzulässig im höchstpers. Bereich**, **AN-Kontrolle**, automationsunterstützter Abgleich mit anderen Daten
- Datensicherheit bei Bildaufnahme, durch
  - Protokollpflicht
  - **Max. Speicherdauer 72**, ausg. besonderes Interesse
  - Zutritts- und Zugriffskontrolle
  - Kennzeichnungspflicht (aus. Private Doku)

2. **Datensicherheit** „TOM“ (§ 54 DSG idF 2018)

An sich nur für Sicherheitsbehörden, Militär, Staatsschutz udgl anwendbar, aber durchaus interessant auch im Unternehmensumfeld als Anhaltspunkte:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (**Zugangskontrolle**);
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (**Datenträgerkontrolle**);
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (**Speicherkontrolle**);
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (**Benutzerkontrolle**);
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (**Zugriffskontrolle**);

6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (**Übertragungskontrolle**);
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (**Eingabekontrolle**);
8. Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (**Transportkontrolle**);
9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (**Wiederherstellung**);
10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (**Zuverlässigkeit**) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (**Datenintegrität**).

Wichtige Dokumente (frei verfügbar)

- **DSGVO 679/2016**: http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016R0679
- **DSG idF der Novelle 2018**: www.ris.bka.gv.at/bundesrecht
- **Leitfaden der DSB** zur DSGVO, Juli 2017: https://www.dsb.gv.at/documents/22758/116802/DSGVO-2016-Leitfaden.pdf/93d6cb80-8d8e-433d-a492-a827e3ed81a2
- **Das Standard-Datenschutzmodell** der DE-DSB, Nov. 2016: https://www.datenschutzzentrum.de/sdm/
- **Stand der Technik in der Informationstechnologie** – TeleTrusT-Handreichung 2016: https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

Herzlichen Dank für Ihre Aufmerksamkeit

Peter Burgstaller
Rechtsanwalt in Linz
FH-Professor für IT-/IP-Recht
Gerichtssachverständiger für Urheberfragen/Medienwesen
www.lawfirm.eu