# SYSTEMATISCHES DATENSCHUTZMANAGEMENT


Ing. Dr. iur. Christof Tschohl
Wissenschaftlicher Leiter | Gesellschafter | Prokurist
christof.tschohl@researchinstitute.at

Dipl.-Ing. Dr. iur. Walter Hötzendorfer
Senior Researcher | Senior Consultant
walter.hoetzendorfer@researchinstitute.at

Mag. Markus Kastelitz, LL.M. (IT-Recht), CIPP/E
Senior Researcher | Senior Consultant
markus.kastelitz@researchinstitute.at

Research Institute AG & Co KG
Digital Human Rights Center
Smart.Rights.Consulting

Annagasse 8/1/8
1010 Wien
www.researchinstitute.at

# Research Institute AG & Co KG
# Digital Human Rights Center

Das **Research Institute (RI)** ist ein Forschungszentrum an der Schnittstelle von **Technik, Recht** und **Gesellschaft**, das sich aus multi- und interdisziplinärer Perspektive mit der Bedeutung der Menschenrechte im digitalen Zeitalter beschäftigt.

**Portfolio:**

- **Forschung zu technischen** und **rechtlichen** Aspekten von **Datenschutz** und **Datensicherheit, Cybercrime, Technikfolgenabschätzung** und **Netzpolitik**
- **Smart.Rights.Consulting:** Beratung zu rechtlichen, technischen und organisatorischen Fragen des Datenschutzes
- **Schulungen**, auf Wunsch zugeschnitten auf Ihre Organisationen
- **Maßgeschneiderte technische Lösungen** zur praktischen Umsetzung der Compliance-Prozesse (in Zusammenarbeit mit Software-Entwicklern)
- **Konzeption und Durchführung individueller und multidisziplinärer Projekte** mit renommierten Partnern auf nationaler und internationaler Ebene.

# Pflichten des Verantwortlichen: Überblick und Zusammenhänge

**Datenschutzgrundsätze**
Eigenverantwortung des Verantwortlichen
Rechenschaftspflicht

Art 5

# Pflichten des Verantwortlichen: Überblick und Zusammenhänge

**Datenschutzgrundsätze**
Eigenverantwortung des Verantwortlichen
Rechenschaftspflicht

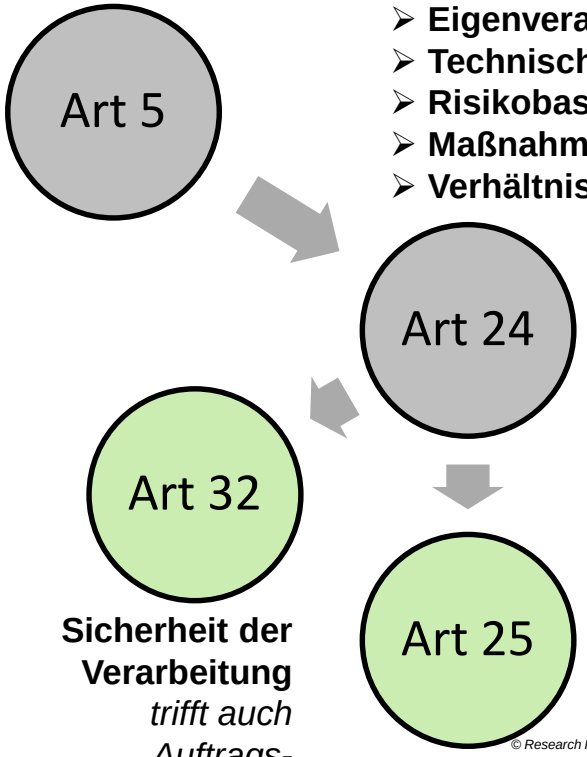
Art 5

Art 24

- **Eigenverantwortung und Haftung des Verantwortlichen**
- **Technische und organisatorische Maßnahmen (TOM)**
- **Risikobasierter Ansatz**
- **Maßnahmen laufend überprüfen und aktualisieren**
- **Verhältnismäßigkeit**

# Pflichten des Verantwortlichen: Überblick und Zusammenhänge

**Datenschutzgrundsätze**
Eigenverantwortung des Verantwortlichen
Rechenschaftspflicht




- **Eigenverantwortung und Haftung des Verantwortlichen**
- **Technische und organisatorische Maßnahmen (TOM)**
- **Risikobasierter Ansatz**
- **Maßnahmen laufend überprüfen und aktualisieren**
- **Verhältnismäßigkeit**

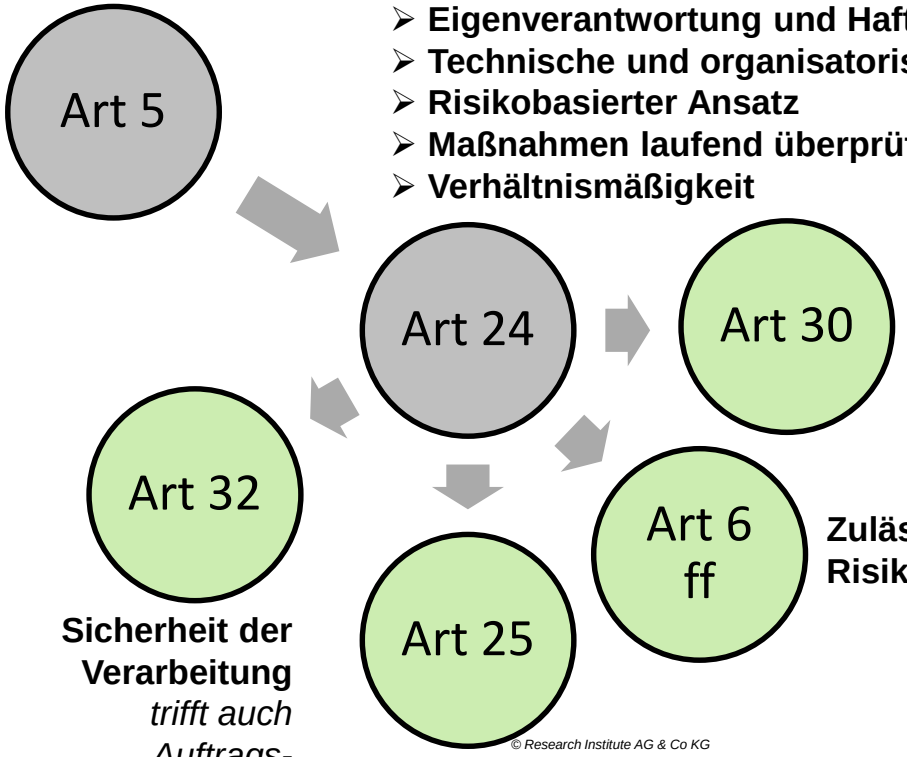
**Sicherheit der Verarbeitung**
*trifft auch Auftrags-verarbeiter*



**Privacy by Design und by Default**
(vor und während der Verarbeitung)

# Pflichten des Verantwortlichen: Überblick und Zusammenhänge

**Datenschutzgrundsätze**
Eigenverantwortung des Verantwortlichen
Rechenschaftspflicht




- **Eigenverantwortung und Haftung des Verantwortlichen**
- **Technische und organisatorische Maßnahmen (TOM)**
- **Risikobasierter Ansatz**
- **Maßnahmen laufend überprüfen und aktualisieren**
- **Verhältnismäßigkeit**

**Verarbeitungsverzeichnis**
*trifft auch Auftragsverarbeiter*

**Zulässigkeitsprüfung Risikoabschätzung**

**Sicherheit der Verarbeitung**
*trifft auch Auftrags-verarbeiter*

**Privacy by Design und by Default**
(vor und während der Verarbeitung)

# Pflichten des Verantwortlichen: Überblick und Zusammenhänge

**Datenschutzgrundsätze**
Eigenverantwortung des Verantwortlichen
Rechenschaftspflicht

Art 5

- **Eigenverantwortung und Haftung des Verantwortlichen**
- **Technische und organisatorische Maßnahmen (TOM)**
- **Risikobasierter Ansatz**
- **Maßnahmen laufend überprüfen und aktualisieren**
- **Verhältnismäßigkeit**

Art 24

Art 30

**Verarbeitungsverzeichnis**
*trifft auch Auftragsverarbeiter*

Art 32

**Sicherheit der Verarbeitung**
*trifft auch Auftrags-verarbeiter*

Art 6 ff

**Zulässigkeitsprüfung Risikoabschätzung**

Art 25

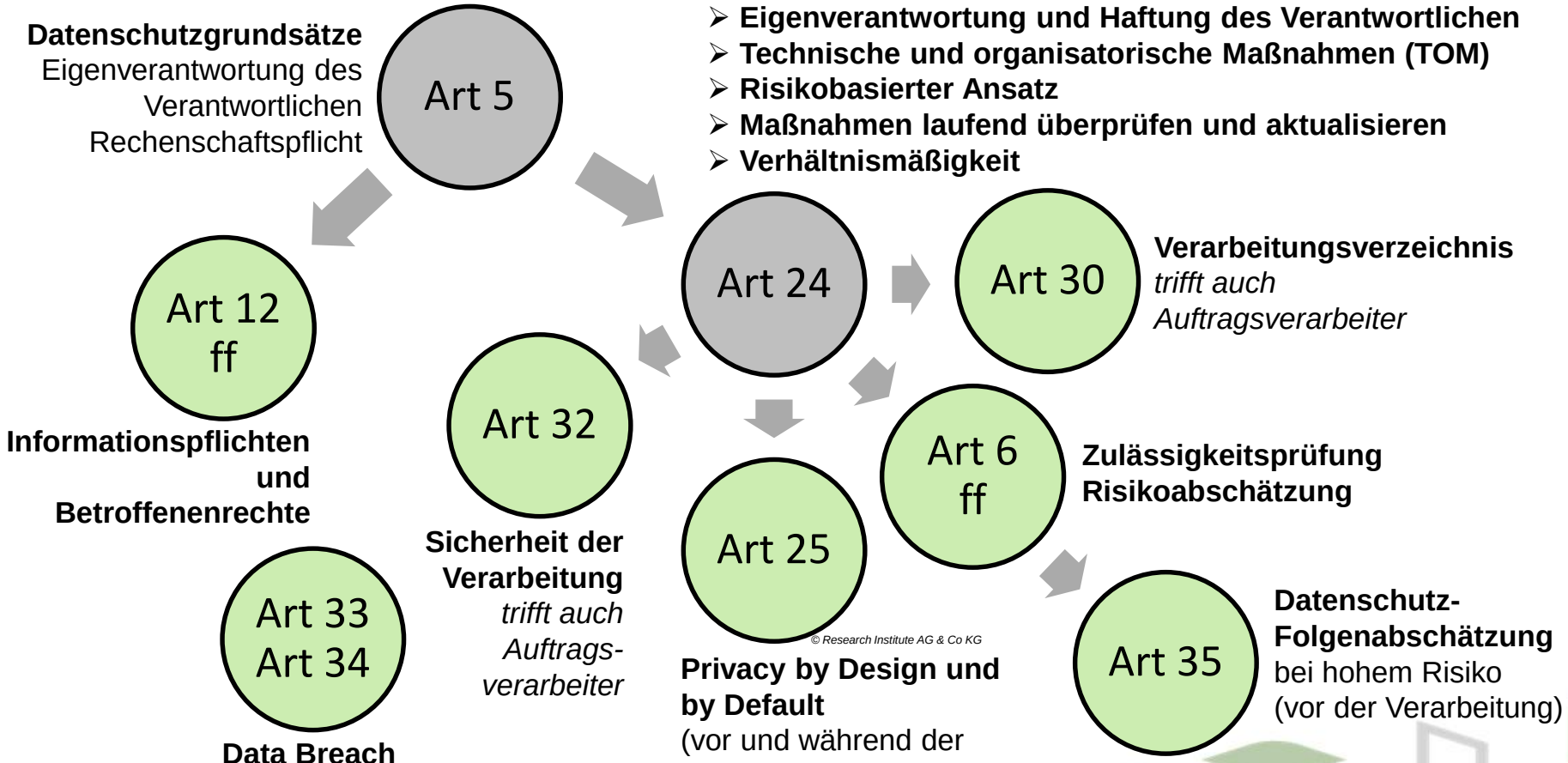


**Privacy by Design und by Default**
(vor und während der Verarbeitung)

Art 35

**Datenschutz-Folgenabschätzung**
bei hohem Risiko
(vor der Verarbeitung)

# Pflichten des Verantwortlichen: Überblick und Zusammenhänge



Die Einhaltung dieser umfangreichen Anforderungen der DSGVO erfordert ein **systematisches, risikobasiertes Datenschutzmanagement**

Das **Datenschutzmanagement** sollte in ähnlicher Weise umgesetzt werden, wie **andere Managementprozesse** in der jeweiligen Organisation gestaltet sind, und es sollte an diese möglichst eng anknüpfen

# AUFBAUORGANISATION: PERSONEN

- **Awareness und Commitment**
  - auf der **Führungsebene**
  - bei allen MitarbeiterInnen: Ein Gefühl für Datenschutz vermitteln; Datenschutz als Unternehmensmentalität und Qualitätsmerkmal
- Ressourcen
  - Jede(r) Mitarbeiter(in) muss Datenschutz im Alltag umsetzen
  - Das **Management** ist dafür **verantwortlich**, ein **System** zu schaffen, dass die **Compliance nicht vom Zufall abhängt**
- Zur Gestaltung des Datenschutz-Management Systems sollten Personen aus den folgenden Bereichen eingebunden werden:
  - Geschäftsleitung, Administration, Recht, Compliance, Controlling
  - Qualitäts- und Prozessmanagement, Organisationsentwicklung
  - IT / Informationssicherheit
  - Marketing / PR

# DATENSCHUTZKOORDINATOR/IN

- Man kann das Thema Datenschutz nicht auslagern
- Für ein effektives Datenschutzmanagement ist es entscheidend, sich Organisationsintern eine gewisse Kompetenz aufzubauen
- **Empfehlung:** Aufbau eines „**Datenschutzkoordinators**“/einer „**Datenschutzkoordinatorin**“:
  - Wenn kein Datenschutzbeauftragter bestellt werden muss, oder ggf. vor allem neben einem externen Datenschutzbeauftragten
  - Datenschutzrechtliche Grundkenntnisse; ansonsten vor allem **Kenntnisse der Betriebsorganisation und der betr. Prozesse**
  - Evtl. Koordination des Projekts zur Vorbereitung auf die DSGVO
  - Ansprechpartner für Datenschutzfragen, Schlüsselrolle in kritischen Prozessen (zB Auskunft nach Art 15 DSGVO)

# Ablauforganisation: Prozesse im Überblick

- Drei Arten von Prozessen (nach „Auslöser“):
  1. **Laufend** durchzuführen
  2. **Auf Verlangen** des Betroffenen durchzuführe: Betroffenenrechte
  3. **Anlassfallbezogen** durchzuführen: Informationspflicht, Data Breach Notification Duty (Voraussetzung: wiederum laufende Prozesse zur Erkennung solcher Anlassfälle)

- **Möglichst große Synergien mit bestehenden Prozessen**
  - Identifikation bestehender Prozessen zu verwandten Themen
  - **Möglichst** keinen neuen Prozesse schaffen sondern **bestehende ergänzen** (zB „Privacy by Design“ in Formulare für den Einkauf)
  - **Bestehende Abläufe als Vorlagen** für neue Prozesse mit ähnlichen Anforderungen

# Ablauforganisation: Prozesse Betroffenenrechte

- Wahrung und Durchsetzung der **Rechte der Betroffenen**
  - Auskunft, Berichtigung, Löschung („Recht auf Vergessenwerden“), Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruchsrecht und Widerruf der Einwilligung
  - **Beförderung der Rechtsdurchsetzung durch Systemdesign** („Privacy by Design & Default“ Art 25 DSGVO)
  - **Verzeichnis der Verarbeitungstätigkeiten** so gestalten, dass es bei der Wahrung der **Betroffenenrechte nützlich** ist
    - zB Zweckbindung und Löschkonzepte so definieren, dass daraus eine ggf. abschlägige Antwort auf ein Löschbegehren rasch ableitbar ist

# Ablauforganisation: Prozesse Recht auf Auskunft

- Kritisch bei den Betroffenenrechten: Auskunftsprozess
  - **Authentifizierung der Person des Anfragenden als Betroffener** – im selben Maß, in dem der Betroffene im Rahmen der Datenanwendung identifiziert ist
    - zB nur online-Kennung oder E-Mail Adresse → dann ist dies auch für den Auskunftsprozess genügend
  - **Zuständigkeiten, Ablauf und Textvorlagen** für Antworten definieren → Zeitkritisch (grundsätzlich 1 Monat Zeit für die Beantwortung)
  - Vorbereitung für allfällige **Mitwirkungspflicht des Betroffenen**
    - Fachbereiche einbeziehen, insbesondere wenn die Gefährdung der Rechte Dritter zu möglichen Einschränkungen der Auskunft führt

# Ablauforganisation: Prozesse
# Laufende Prozesse zur Compliance

- Prozesse zum laufenden (dynamischen) Datenschutz
  - **Neue Verarbeitungstätigkeiten, Änderungen und Erweiterungen des Umfangs oder der Zwecke**:
    - Ergänzung der Verzeichnisse, Risiko- und Schwellwertanalyse zur Einschätzung der Notwendigkeit einer Datenschutz-Folgenabschätzung
    - Data Protection (Privacy) by Design und by Default (Art 25 DSGVO)
    - Auftragsverarbeitung und Vereinbarung gem. Art 28 (3) DSGVO prüfen

- **Prozesse zu technischen und organisatorischen Maßnahmen**
  - Abläufe effektiv gestalten, damit sie auch gelebt werden
  - Kontrollsystem und Prozesse zur Umsetzung definieren
  - Ordentliche Dokumentation → nicht nur der Prozesse sondern insbesondere der konkret durchgeführten Kontrollen dokumentieren

# RECHENSCHAFTSPFLICHT

- **Gegenüber der Datenschutzbehörde**
  - Der Verantwortliche ist gegenüber der Behörde in vollem Umfang und teilweise detailliert Rechenschaftspflichtig
  - **Dokumentationen** zu Rechtfertigungen, Sicherheitsmaßnahmen und wesentlichen Prozessen – nicht erst im Kontrollfall schreiben
  - **Verzeichnis nach Art 30 DSGVO ist der Kern und Ausgangspunkt**, aber erschöpft nicht die Rechenschaftspflicht

- **Vorsicht bei ArbeitnehmerInnen:**
  - Erweiterung durch Pflichten nach dem Arbeitsverfassungsgesetz
  - zB § 91 ArbVG (2) Satz 2: „Dem Betriebsrat ist auf Verlangen die Überprüfung der Grundlagen für die Verarbeitung und Übermittlung zu ermöglichen.“

# Verzeichnis von Verarbeitungstätigkeiten (Art 30)

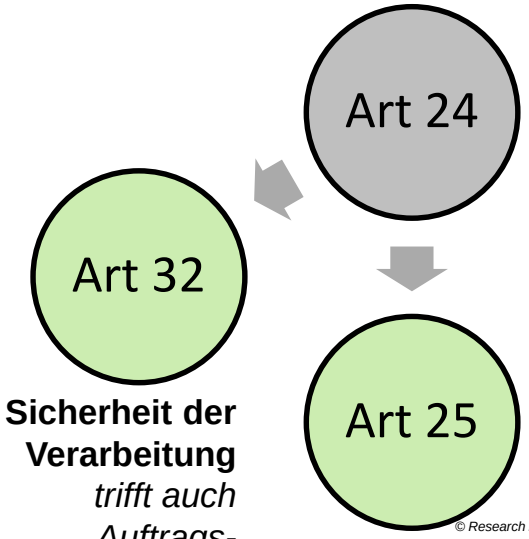
- **Bis 24.5.2018: Datenverarbeitungsregister (DVR) bei der DSB**
  - Pflicht zur Meldung von Datenanwendungen im öffentl. zugängl. DVR gemäß §§ 17 ff DSG 2000 → Exportfunktion aus DVR-Online bis 31.12.2019
- **Ab 25.5.2018: internes Verarbeitungsverzeichnis („VVZ“):**
  - Zu führen vom **Verantwortlichen** und **Auftragsverarbeiter,** aber mit unterschiedlichem Dokumentationsumfang (Art 30 Abs 1 vs. Abs 2)
  - **Ausnahme** (wenig relevant): VVZ ist von Unternehmen, die weniger als **250 Mitarbeiter** beschäftigen, nur dann zu führen, wenn
    - die von ihnen vorgenommene Verarbeitung ein (gemeint ist wohl: besonderes) **Risiko für die Rechte und Freiheiten** der betroffenen Personen birgt,
    - die Verarbeitung **nicht nur gelegentlich** erfolgt oder
    - eine Verarbeitung **besonderer Datenkategorien** gemäß Art 9 Abs 1 bzw. von **Daten über strafrechtliche Verurteilungen und Straftaten** iSd Art 10 erfolgt

# VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN (ART 30)

- **Bis 24.5.2018: Datenverarbeitungsregister (DVR) bei der DSB**
  - Pflicht zur Meldung von Datenanwendungen im öffentl. zugängl. DVR gemäß §§ 17 ff DSG 2000 → Exportfunktion aus DVR-Online bis 31.12.2019
- **Ab 25.5.2018: internes Verarbeitungsverzeichnis („VVZ“):**
  - Zu führen vom **Verantwortlichen** und **Auftragsverarbeiter,** aber mit unterschiedlichem Dokumentationsumfang (Art 30 Abs 1 vs. Abs 2)
  - **Ausnahme** (wenig relevant): VVZ ist von Unternehmen, die weniger als **250 Mitarbeiter** beschäftigen, nur dann zu führen, wenn
    - die von ihnen vorgenommene Verarbeitung ein (gemeint ist wohl: besonderes) **Risiko für die Rechte und Freiheiten** der betroffenen Personen birgt,
    - die Verarbeitung **nicht nur gelegentlich** erfolgt oder
    - eine Verarbeitung **besonderer Datenkategorien** gemäß Art 9 Abs 1 bzw. von **Daten über strafrechtliche Verurteilungen und Straftaten** iSd Art 10 erfolgt
  - **Empfehlung: VVZ jedenfalls führen**, auch weil ohne Überblick über die Verarbeitungstätigkeiten und entsprechende Dokumentation die Erfüllung der Anforderungen der DSGVO nahezu unmöglich ist (Rechenschaftspflicht, Betroffenenrechte etc.)
  - **=> Verarbeitungsverzeichnis als Management-Tool**
  - **Empfehlung:** Erweiterung um zusätzliche Angaben der (siehe insb. Art 13 ff DSGVO), wie z.B. Rechtsgrundlage, Herkunft der Daten, verwendete Software

# ART 42 DSGVO: ZERTIFIZIERUNG

- **Eigenverantwortung und Haftung des Verantwortlichen**
- **Technische und organisatorische Maßnahmen (TOM)**
- **Risikobasierter Ansatz**
- **Maßnahmen laufend überprüfen und aktualisieren**
- **Verhältnismäßigkeit**




**Sicherheit der Verarbeitung**
*trifft auch Auftrags-verarbeiter*



**Privacy by Design und by Default**
(vor und während der Verarbeitung)

# ART 42 DSGVO: ZERTIFIZIERUNG

- **Eigenverantwortung und Haftung des Verantwortlichen**
- **Technische und organisatorische Maßnahmen (TOM)**
- **Risikobasierter Ansatz**
- **Maßnahmen laufend überprüfen und aktualisieren**
- **Verhältnismäßigkeit**

**ART 32 ABS 3 DSGVO:** *Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.*

Art 24

Art 32

Art 25

**Sicherheit der Verarbeitung** *trifft auch Auftrags-verarbeiter*



**Privacy by Design und by Default**
(vor und während der Verarbeitung)

**ART 24 ABS 3 DSGVO:** *Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.*

**ART 25 ABS 3 DSGVO:** *Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.*

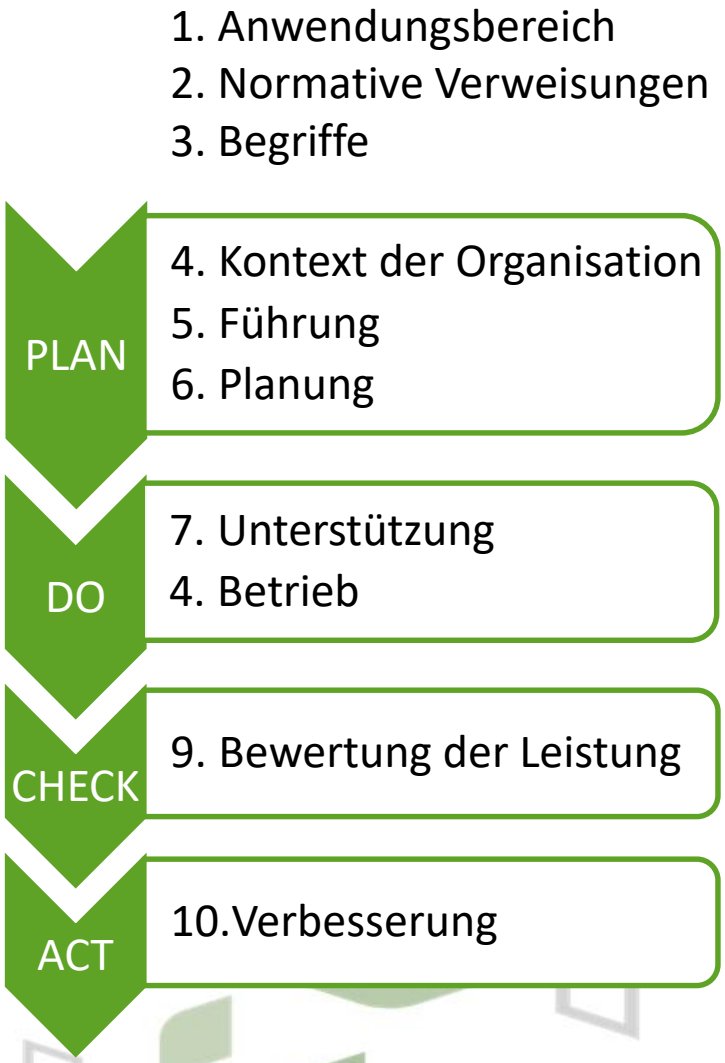
# A.S.I. AG 001 18:

# DATENSCHUTZ-MANAGEMENTSYSTEME

- Ausarbeitung einer **ÖNORM zum Datenschutzmanagement**
- Arbeitsgruppe 001 18 bei Austrian Standards International (vormals „Austrian Standards Institute“)
- **Ziel:** Genehmigung als Kriterien für die Zertifizierung nach Art 42 Abs 5 iVm Art 58 Abs 3 lit f
- Zweck:
  - Keine Anleitung für die Einrichtung eines Datenschutz-Managementsystems, sondern
  - **Norm zur Zertifizierung der Erfüllung der Anforderungen der DSGVO im Hinblick auf das Datenschutzmanagement**
- Eigenständigkeit der Norm: Zertifizierung muss auch ohne vorliegende ISO-27001-Zeritifizierung möglich sein
- Status:
  - 1. Sitzung: 30. Juni 2017
  - Derzeit Arbeit am Grundtext durch eine Kerngruppe
  - Sitzungen der Arbeitsgruppe zur Diskussion des Fortschritts ca. alle 6 Wochen

# High Level Structure

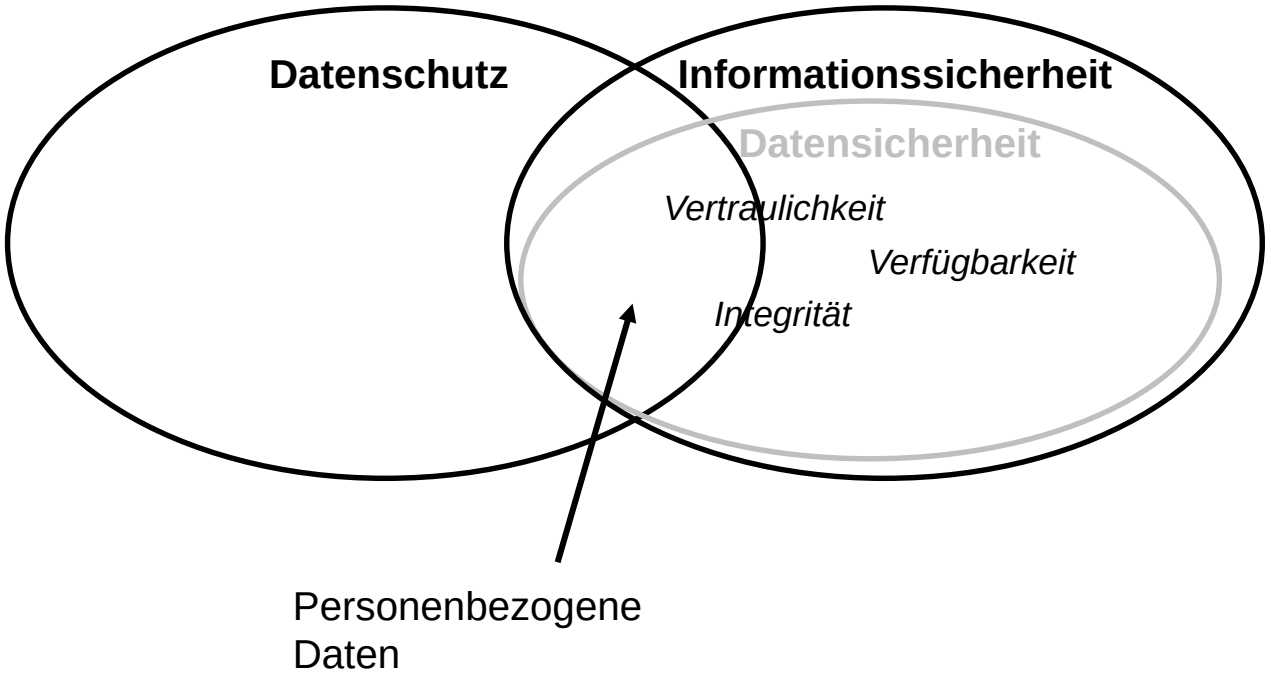
- ISO-Normen für verschiedene Managementsysteme sind nach derselben Struktur aufgebaut:
  - ISO 9001 (2015): Qualitätsmanagement
  - ISO 27001 (2013): Informationssicherheits-Management
  - etc.
- Parallele und Verschränkte Anwendungen dieser Normen
- Ein Managementsystem für die Erfüllung verschiedener Normen



# Braucht man eine eigene Norm oder genügt ISO 27001?

- HLS sieht vor: **4.1 Verstehen der Organisation und ihres Kontextes**
- Dies umfasst auch die anwendbaren gesetzlichen Rahmenbedingungen
- Es wird argumentiert, damit seien auch alle Anforderungen des Datenschutzrechts abgedeckt
- Gegenargumente:
  - Zertifizierbarkeit schwierig, wenn Anforderungen so vage sind
  - Norm will vorgeben, was ein DSMS enthalten muss
  - Man kann diskutieren, ob unter 4.1 auch Datenschutzanforderungen zu berücksichtigen sind, die über Informationssicherheit hinausgehen

# DATENSCHUTZ UND INFORMATIONSSICHERHEIT



# ISO/IEC JTC 1/SC 27/WG 5: ISO 27552

- Titel: Information technology -- Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management — Requirements and guidelines
- Nicht eigenständig, sondern ergänzend zu einer bestehenden ISO-27001-Zertifizierung
- Status: 1st Committee Draft (CD) vom 08.12.2017, 57 Seiten, Rückmeldungen bis 02.03.2017
- Umfangreich und teilweise sehr detailliert
- Internationale Perspektive – Nutzen im Hinblick auf die DSGVO muss sich daher in der Praxis erst weisen

# Sonstige Normungsaktivitäten

- In der A.S.I. AG 001 18 wurde auch die Ausarbeitung einer ÖNORM mit dem Titel „Anforderungen an die Ausbildung von Datenschutzbeauftragten“ beschlossen
  - Derzeit keine Aktivitäten dazu
  - Antragsteller derzeit nicht in der AG aktiv
- Es gibt auch noch einen British Standard BS 10012:2017 vom 31. März 2017
  - Berücksichtigt auch bereits die DSGVO
  - Anforderungen an ein Personal Information Management System (PIMS)
  - vergleichsweise umfangreich
  - Nicht ausschließlich an DSGVO orientiert (schleppt Erbe mit)

# SYSTEMATISCHES DATENSCHUTZMANAGEMENT

**Ing. Dr. iur. Christof Tschohl**
Wissenschaftlicher Leiter | Gesellschafter | Prokurist
christof.tschohl@researchinstitute.at

**Dipl.-Ing. Dr. iur. Walter Hötzendorfer**
Senior Researcher | Senior Consultant
walter.hoetzendorfer@researchinstitute.at

**Mag. Markus Kastelitz, LL.M. (IT-Recht), CIPP/E**
Senior Researcher | Senior Consultant
markus.kastelitz@researchinstitute.at

Research Institute AG & Co KG
Digital Human Rights Center
Smart.Rights.Consulting

Annagasse 8/1/8
1010 Wien
www.researchinstitute.at

# Ing. Mag. Dr. iur. Christof Tschohl

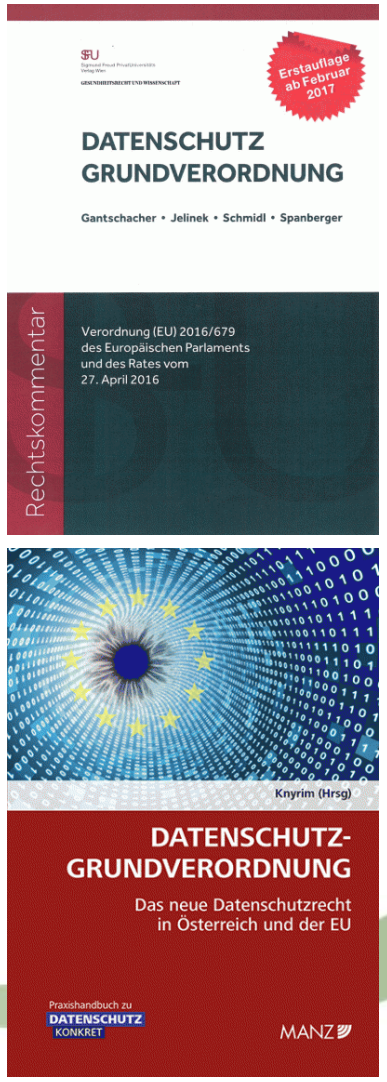
- Nachrichtentechniker (HTL Rankweil, Ericsson, Kapsch) und Jurist
- Bis 2012 Ludwig Boltzmann Institut für Menschenrechte und Uni Wien
- Seit Ende 2012: Wissenschaftlicher Leiter und Gesellschafter der Research Institute AG & Co KG
- Forschung und Beratung – Schnittstelle von Technik und Recht
- Lehre (aktuell: Uni Wien, Lehrgang für Informations- und Medienrecht; Vienna Human Rights Master; Universität Hannover, Masterprogramme IT Law; Donau Uni Krems, Big Data und Datenschutz; FH St. Pölten: Ethik in der Technologieentwicklung; Anwaltsakademie Österreich)
- Mitgliedschaften:
  - epicenter.works – Plattform für digitale Grundrechte (vormals AKVorrat), Obmann
  - Österreichische Computer Gesellschaft (OCG), Co-Leiter „OCG Forum Privacy“
  - Österreichische RichterInnenvereinigung, Fachgruppe Grundrechte, a.o. Mitglied, regelmäßig Vortragender in Aus- und Fortbildung seit 2008
  - Mitglied des CERT-Beirats im österreichischen Bundeskanzleramt
  - Akkreditiert bei ASI zur Datenschutz und ISO27000 Normung (CEN+ISO)

# DIPL.-ING. DR. IUR. WALTER HÖTZENDORFER

- Wirtschaftsinformatiker und Jurist
- **Senior Researcher** und **Senior Consultant**, Research Institute – Zentrum für digitale Menschenrechte
- Autor des Buches „**Datenschutz und Privacy by Design im Identitätsmanagement**“ und Mitautor zweier aktueller Bücher zur Datenschutz-Grundverordnung
- Vorstandsmitglied der Österreichischen Computer Gesellschaft (**OCG**) und Co-Leiter **OCG Forum Privacy**
- Mitglied in der ASI-AG 001 18, die derzeit einen Datenschutz-Management-Standard ausarbeitet
- Vortragender im In- und Ausland
- **Erfahrungen** in:
  - Wissenschaft (RI, Uni Wien, Arbeitsgruppe Rechtsinformatik)
  - Rechtsberatung
  - Software Engineering
  - Prozessmanagement
- **Forschungsschwerpunkte**:
  - Technische und organisatorische Aspekte des Datenschutzrechts
  - Privacy Engineering, Privacy by Design
  - Datensicherheit/Netzwerk- und Informationssicherheit (NIS)
  - Identity Management
  - Telekommunikationsrecht
  - Öffentliche Sicherheit

# Mag. Markus Kastelitz, LL.M., CIPP/E

- Jurist mit IT-Rechts-Ausbildung
- Zertifizierter Information Privacy Professional (IAPP)
- **Senior Researcher** und **Senior Consultant**, Research Institute – Zentrum für digitale Menschenrechte
- Mitautor von Büchern zur Datenschutz-Grundverordnung
- Co-Gründer und Vorstandsmitglied **Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacyofficers.at**
- Lehrgangsbeiratsmitglied und Vortragender am Lehrgang **Datenschutz und Privacy** (Donau-Universität Krems)
- **Erfahrungen** in:
  - Wissenschaft (Uni Hannover, Lehrstuhl Prof. Dr. Forgó)
  - Rechtsberatung (u.a. MedUni Wien, Industriekonzern, Parlamentsdirektion, RTR)
  - Datenschutzbeauftragter (MedUni Wien, Research Institute)
- **Forschungsschwerpunkte**:
  - Umsetzung der DSGVO
  - Datenschutz in der Forschung mit Schwerpunkt medizinische Forschung
  - Moderne Technologien und Datenschutz



# RECHTLICHE HINWEISE

**Zweck**: Dieses Dokument dient als Trainingsunterlage.

Erstellt von: Ing. Mag. Dr. Christof Tschohl, Dipl.-Ing. Dr. Walter Hötzendorfer und Mag. Markus Kastelitz



Kontaktdaten: walter.hoetzendorfer@researchinstitute.at

# Backup Folien

# Für vertiefende Fragen

research institute

# Es folgen die STANDARD-FOLIEN als Ressource für die Folienerstellung

# Verzeichnis von Verarbeitungstätigkeiten (Art 30)

- **Bis 24.5.2018: Datenverarbeitungsregister (DVR) bei der DSB**
  - Pflicht zur Meldung von Datenanwendungen im öffentl. zugängl. DVR gemäß §§ 17 ff DSG 2000 → Exportfunktion aus DVR-Online bis 31.12.2019
- **Ab 25.5.2018: internes Verarbeitungsverzeichnis („VVZ“):**
  - Zu führen vom **Verantwortlichen** und **Auftragsverarbeiter,** aber mit unterschiedlichem Dokumentationsumfang (Art 30 Abs 1 vs. Abs 2)
  - **Schriftlich** zu führen, auch elektronische Führung zulässig; nicht-öffentlich
  - Ist Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen (Art 30 Abs 4)
  - **Ausnahme** (wenig relevant): VVZ ist von Unternehmen, die weniger als **250 Mitarbeiter** beschäftigen, nur dann zu führen, wenn
    - die von ihnen vorgenommene Verarbeitung ein (gemeint ist wohl: besonderes) **Risiko für die Rechte und Freiheiten** der betroffenen Personen birgt,
    - die Verarbeitung **nicht nur gelegentlich** erfolgt oder
    - eine Verarbeitung **besonderer Datenkategorien** gemäß Art 9 Abs 1 bzw. von **Daten über strafrechtliche Verurteilungen und Straftaten** iSd Art 10 erfolgt
  - **Empfehlung: VVZ jedenfalls führen**, auch weil ohne Überblick über die Verarbeitungstätigkeiten und entsprechende Dokumentation die Erfüllung der Anforderungen der DSGVO nahezu unmöglich ist (Rechenschaftspflicht, Betroffenenrechte etc.)

# Verzeichnis von Verarbeitungstätigkeiten (Art 30)

- **Mindestinhalt des VVZ des Verantwortlichen (Art 30 Abs 2):**
  - den **Namen u. die Kontaktdaten des Verantwortlichen** u. ggf. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen **Datenschutz- beauftragten**;
  - die **Zwecke** der Verarbeitung;
  - eine **Beschreibung der Kategorien betroffener Personen** u. der **Kategorien pers.bez. Daten**;
  - die **Kategorien von Empfängern**, gegenüber denen die pers.bez. Daten offengelegt worden sind oder noch offengelegt werden, einschließlich **Empfänger in Drittländern/internat. Organis.**
  - ggf. **Übermittlungen von personenbezogenen Daten an ein Drittland** oder an eine internat. Organis., einschließlich der Angabe des Drittlands oder der internat. Organis. (+ Dokumentierung geeigneter Garantien bei Übermittlungen gem Art 49 Abs 1 UAbs 2);
  - wenn möglich, die vorgesehenen **Fristen für die Löschung** der verschiedenen Datenkategorien;
  - wenn möglich, eine **allgemeine Beschreibung der technischen und organisatorischen Maßnahmen** gemäß Art 32 Abs 1
- **Empfehlenswert** ist Erweiterung um zusätzliche Angaben der Art 13 ff DSGVO, wie z.B. Rechtsgrundlage der Verarbeitung, Herkunft der Daten

# Verzeichnis von Verarbeitungstätigkeiten (Art 30)

- **Mindestinhalt des VVZ des Auftragsverarbeiters (Art 30 Abs 3):**
  - **Namen und die Kontaktdaten des Auftragsverarbeiters** oder der Auftragsverarbeiter und jedes **Verantwortlichen**, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
  - die **Kategorien von Verarbeitungen**, die im Auftrag jedes Verantwortlichen durchgeführt werden;
  - gegebenenfalls **Übermittlungen** von personenbezogenen Daten an ein **Drittland** oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation (+ Dokumentierung geeigneter Garantien bei Übermittlungen gem Art 49 Abs 1 UAbs 2);
  - wenn möglich, eine **allgemeine Beschreibung der technischen und organisatorischen Maßnahmen** gemäß Art 32 Abs 1

# DATENSCHUTZ-FOLGENABSCHÄTZUNG (DSFA)

- Besteht insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen ist eine Datenschutz-Folgenabschätzung verpflichtend, insbesondere in folgenden Fällen :
  a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen,
  b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
  c) Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche
- Vorherige Konsultation der DSB (Art 36 DSGVO) falls die DSFA ein hohes Risiko zeigt, falls der Verantwortliche keine geeigneten Maßnahmen trifft

# Art-29-Datenschutzgruppe: Kriterien für hohes Risiko

**Faustregel: Ein hohes Risiko besteht jedenfalls, wenn mindestens zwei der folgenden neun Kriterien erfüllt sind:**

1. Bewerten oder Einstufen (Profiling/Scoring natürlicher Personen)
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
3. Systematische Überwachung
4. Vertrauliche Daten oder höchst persönliche Daten (Art 9, 10)
5. Datenverarbeitung in großem Umfang (ErwGr 91)
6. Abgleichen oder Zusammenführen von Datensätzen
7. Daten zu schutzbedürftigen Betroffenen (ErwGr 75)
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
9. Datenverarbeitungen, die Betroffene an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern (Art 22, ErwGr 91)

# Datenschutz-Folgenabschätzung: Empfehlungen

- Dokumentation aller Entscheidungen, insbesondere warum ggf. keine Datenschutz-Folgenabschätzung durchgeführt wurde
- Im Zweifel Durchführung einer Datenschutz-Folgenabschätzung
- Einbeziehung der internen und externen Betroffenen
- Heranziehen von Mustern, Best Practices und ggf. ähnlichen, bereits durchgeführten Datenschutz-Folgenabschätzungen
- Veröffentlichen der Datenschutz-Folgenabschätzung
  - Insbesondere durch öffentliche Stellen
  - Zeigt Datenschutz-Bewusstsein und schafft Vertrauen

- Literatur: *Kastelitz/Hötzendorfer/Riedl*, Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, in: Jahnel (Hrsg.), Jahrbuch Datenschutzrecht 2017, *erscheint im November 2017*

# AUFTRAGSVERARBEITUNG

- Geregelt in **Art 28, 29 DSGVO** (relevante Bestimmungen finden sich z.B. auch in Art 32, 33, 37, 38, 60 Abs 10; § 6 Abs 2 DSG neu: Datengeheimnis)
- „**Verantwortlicher**“ (bisher „Auftraggeber“): „Herr der Daten“; entscheidet allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten
- „**Auftragsverarbeiter**“ (bisher „Dienstleister“): verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen
- Verarbeitung nur auf Weisung des Verantwortlichen
- **Privilegierung:** Auftragsverarbeiter ist nicht „Dritter“ iSv Art 4 Z 10; keine gesonderte Zulässigkeitsprüfung der Übermittlung an Auftragsverarbeiter

# Auftragsverarbeitung: Anforderungen der DSGVO

- **Sorgfältige Auswahl des Auftragsverarbeiters** durch Verantwortlichen (Art 28 Abs 1; vgl bereits § 10 Abs 1 DSG 2000):
  - Gestiegene Bedeutung durch DSGVO (Anforderungen an Vertrag, Sanktionsregime etc)
  - Hinreichende Garantien dafür, dass **geeignete technische und organisatorische Maßnahmen** (TOM) so durchgeführt werden, dass die Verarbeitung durch Auftragsverarbeiter im Einklang mit den Anforderungen dieser Verordnung erfolgt und **Schutz der Betroffenenrechte** gewährleistet ist (möglicher Nachweis durch: Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42)
- **Schriftlicher Vertrag** zwischen Verantwortlichem und Auftragsverarbeiter (Art 28 Abs 3 und 9) oder „ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten“
  - Auch in elektron. Format möglich (Art 28 Abs 9)
  - Zwingende Mindestinhalte (siehe nächste Folie)
  - Empfehlung: Nicht nur Mindestinhalte gem Art 28 Abs 3 zu beachten (Art 27, 32, 33, 37 etc)
- Auftragsverarbeiter im Drittland: Regelungen für grenzüberschreitenden Datenverkehr beachten (Art 44 ff)

# Mindestinhalte des Auftragsverarbeitungsvertrags (Art 28 Abs 3)

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten
- Kategorien betroffener Personen
- Pflichten und Rechte des Verantwortlichen
- Verarbeitung nur auf dokumentierte Weisung(en) des Verantwortlichen (lit a)
- Verpflichtung der Mitarbeiter des Auftragsverarbeiters zur Vertraulichkeit (lit b)
- Einhaltung erforderlicher Maßnahmen gem Art 32 (Datensicherheit; lit c)
- Einhaltung der Vorgaben gem Art 28 Abs 2 u 4 bei Sub-Auftragsverarbeitern (lit d)
- Unterstützung des Verantwortlichen bei Wahrung der Betroffenenrechte (lit e)
- Unterstützung bei Sicherheit, Data Breach, Datenschutz-Folgenabschätzung (lit f)
- Datenlöschung bzw -rückgabe nach Erbringung der Verarbeitungsleistungen (lit g)
- Zurverfügungstellung aller erforderlichen Informationen und Ermöglichung von Überprüfungen bzw Inspektionen (lit h)
- [§ 6 DSG neu: Verpflichtung der Mitarbeiter auf Datengeheimnis; Belehrung]

# AUFTRAGSVERARBEITUNG: HANDLUNGSEMPFEHLUNGEN

- **IST-Zustand erheben**: Welche Dienstleisterverträge bestehen?
- **GAP-Analyse**: Prüfung auf Konformität mit den Anforderungen der DSGVO, besteht Anpassungsbedarf? → im Regelfall zu bejahen, wenn bislang Muster der Datenschutzbehörde oä verwendet wurde
- **Weitere wichtige Schritte strategisch planen**:
  - Eigenes Vertragsmuster erstellen (bis 25.5.2018: „doppelgleisig“ DSG 2000 und DSGVO)
  - Kontakt mit Auftragsverarbeiter(n) aufnehmen; große Auftragsverarbeiter werden ihr eigenes Muster einsetzen wollen (Achtung auf Abweichungen von den Vorgaben der DSGVO bzgl Haftung etc)
  - Dokumentation insbesondere der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters
  - Laufende Kontrolle des Auftragsverarbeiters
  - Verarbeitungsverzeichnis: Auftragsverarbeiter-Tätigkeiten berücksichtigen
  - Einbindung bei Durchführung einer Datenschutz-Folgenabschätzung
- **Sanktionsmöglichkeit auch für Verletzung von Handlungspflichten, nicht nur bei Data Breach!**
- **Mustervertrag nach DSGVO der WKO:** https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag.html

# UMSETZUNG DSGVO-PROJEKT IM DETAIL

1. Erhebung und Dokumentation
   - 1.1 Verarbeitungstätigkeiten identifizieren
   - 1.2 Verfahrensverzeichnis erstellen
2. Rechtmäßigkeit der Datenverarbeitungen prüfen
   - 2.1 Risikoanalyse durchführen / allenfalls Datenschutz-Folgenabschätzung durchführen
   - 2.2 Identifikation notwendiger Maßnahmen zur Risikobeherrschung
   - 2.3 Nachweise der Einhaltung der Datenschutz-Grundsätze (Rechenschaftspflicht/Dokumentation)
   - 2.4 Einwilligungsprozess einführen/anpassen falls erforderlich
   - 2.5 Auftragsverarbeiter: Rahmenbedingungen sicherstellen
   - 2.6 Datenübermittlung prüfen (EWR/international)
   - 2.7 Rechtstexte mit Relevanz für den Datenschutz überarbeiten/anpassen

# Umsetzung DSGVO-Projekt im Detail

3. Technische und Organisatorische Maßnahmen (TOM) zu Datensicherheit und Datenschutz umsetzen
   - 3.1. Maßnahmen dokumentieren
   - 3.2. Unterscheidung spezifischer Maßnahmen pro Anwendung in Abgrenzung allgemeiner Maßnahmen
4. Betroffenenrechte wahren
   - 4.1. Prozesse für Auskunft, Berichtigung, Einschränkung, Löschung Datenübertragbarkeit und Widerspruch definieren
   - 4.2 Informationspflichten einführen
5. Privacy by Design / Privacy by Default sicherstellen

# UMSETZUNG DSGVO-PROJEKT IM DETAIL

6. Datenschutz-Management-System: Prozesse zur laufenden Erfüllung P1-P5 dokumentieren und prüfen

- 6.1. Aufgaben des Datenschutzbeauftragten abklären
- 6.2. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- 6.3. Datenschutz-Policy erstellen
- 6.4. Mitarbeiter schulen
- 6.5. Prozesse zu den (pro-aktiven) Informationspflichten einführen/dokumentieren
- 6.6. Data Breach Notifikation Duty - Prozess einführen
- 6.7. Prozess zur laufenden Überprüfung und Aktualisierung aller Maßnahmen und Prozesse

Siehe auch *pirvacyofficers.at*: Kompakte Checkliste zur Umsetzung der Datenschutz-Grundverordnung, Version 2.0

https://www.privacyofficers.at/Privacyofficers_Checkliste_Umsetzung_DSGVO_v2.0.pdf

# Durchführung der Datenschutz-Folgenabschätzung (Abs 7)

1. Aufsetzen des Projekts:
   - Zusammenstellung des Teams: Fachabteilung, Juristen, Techniker, ggf. Datenschutzbeauftragter, ggf. externe Berater
   - Zeit- und Ressourcenplanung
   - Commitment des Managements
2. Beschreiben der geplanten Verarbeitung inkl. ihrer Zwecke (im Kontext)
3. Einholen der Standpunkte der betroffenen Personen oder ihrer Vertreter (Abs 9)
   - Verpflichtung, wenn ein solcher Standpunkt vorliegt oder abzusehen ist
   - Impliziert auch die Information der Betroffenen
4. Zulässigkeitsprüfung inkl. Bewertung der Notwendigkeit und Verhältnismäßigkeit
5. Identifizieren, Analysieren und Bewerten der Risiken für die Betroffenen:
   - Eintrittswahrscheinlichkeit
   - Auswirkungen der Risikoverwirklichung
6. Identifizieren von Maßnahmen zum Umgang mit den nicht tragbaren Risiken
7. Dokumentation der Datenschutz-Folgenabschätzung (Bericht) mit Nachweisen, wie die Anforderungen der DSGVO eingehalten werden
8. Laufende Überprüfung, ob die bei der Datenschutz-Folgenabschätzung getroffenen Annahmen und Prognosen richtig waren und die Verarbeitung gemäß (den Vorgaben) der Datenschutz-Folgenabschätzung durchgeführt wird

# Beispiel einer Risikomatrix als Grundlage der Risikobewertung

# Datenschutz-Folgenabschätzung bei bestehenden Verarbeitungen?

Ist für Datenverarbeitungen, die bei In-Geltung-Treten der DSGVO schon in Betrieb sind, ebenfalls eine Datenschutz-Folgenabschätzung durchzuführen?

Differenzierte Meinung der *Art-29-Datenschutzgruppe* in WP248 rev.01:

- Folgenabschätzung nicht erforderlich, wenn eine bestehende Verarbeitung im Zuge der Vorabkontrolle (dh in Österreich: von der DSB) geprüft wurde und diese unverändert geblieben ist
- Folgenabschätzung jedenfalls dann erforderlich, wenn sich die Umstände der Verarbeitung geändert haben und sich ein hohes Risiko ergeben könnte
- Der große Bereich zwischen diesen beiden Fällen (unveränderte Verarbeitung ohne Vorabkontrolle) wird offen gelassen

# Datenschutz-Folgenabschätzung: Empfehlungen

- Dokumentation aller Entscheidungen, insbesondere warum ggf. keine Datenschutz-Folgenabschätzung durchgeführt wurde
- Im Zweifel Durchführung einer Datenschutz-Folgenabschätzung
- Einbeziehung der internen und externen Betroffenen
- Heranziehen von Mustern, Best Practices und ggf. ähnlichen, bereits durchgeführten Datenschutz-Folgenabschätzungen
- Veröffentlichen der Datenschutz-Folgenabschätzung
  - Insbesondere durch öffentliche Stellen
  - Zeigt Datenschutz-Bewusstsein und schafft Vertrauen

- Literatur: *Kastelitz/Hötzendorfer/Riedl*, Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, in: Jahnel (Hrsg.), Jahrbuch Datenschutzrecht 2017, *erscheint im November 2017*

# Weitere Muster/Vorlagen

- Datenschutz-Folgenabschätzung für ELGA: https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_01457/fnameorig_579068.html
- BRD: Forum Privatheit White Paper DSFA (3. Aufl. 2017), https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf
- GDD-Praxishilfe DS-GVO X - Voraussetzungen der Datenschutz-Folgenabschätzung, Version 1.0, Stand Nov. 2017, https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_10.pdf
- Planspiel DSFA des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und der Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern: https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Hilfsmittel%20zur%20Umsetzung/Planspiel_Datenschutz_Folgenabschaetzung.pdf
- CNIL, The open source PIA software, https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment