

# SYSTEMATISCHES DATENSCHUTZMANAGEMENT

**Ing. Dr. iur. Christof Tschohl**

Wissenschaftlicher Leiter | Gesellschafter | Prokurist

[christof.tschohl@researchinstitute.at](mailto:christof.tschohl@researchinstitute.at)

**Dipl.-Ing. Dr. iur. Walter Hötendorfer**

Senior Researcher | Senior Consultant

[walter.hoetendorfer@researchinstitute.at](mailto:walter.hoetendorfer@researchinstitute.at)

**Mag. Markus Kastelitz, LL.M. (IT-Recht), CIPP/E**

Senior Researcher | Senior Consultant

[markus.kastelitz@researchinstitute.at](mailto: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](http://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

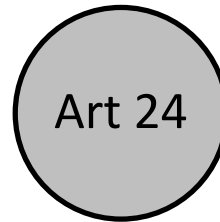
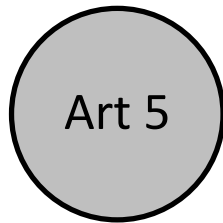
**Datenschutzgrundsätze**  
Eigenverantwortung des  
Verantwortlichen  
Rechenschaftspflicht



Art 5

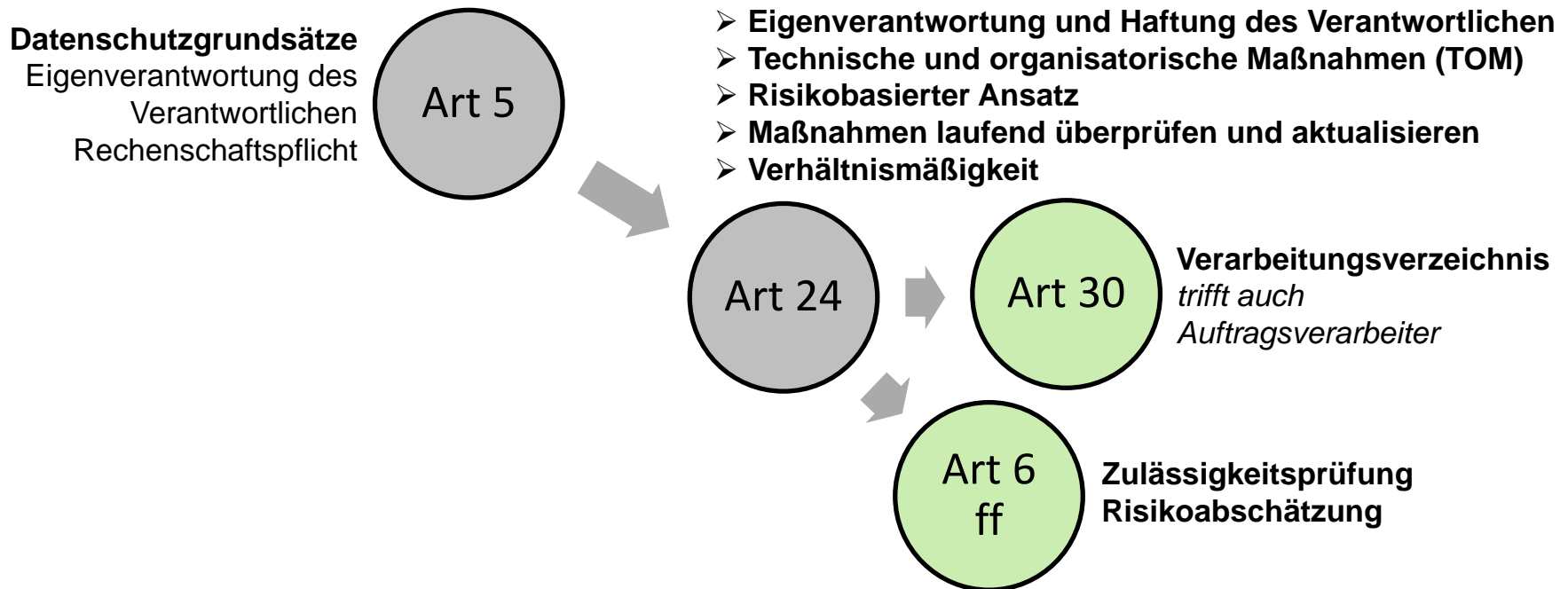
# PFLICHTEN DES VERANTWORTLICHEN: ÜBERBLICK UND ZUSAMMENHÄNGE

**Datenschutzgrundsätze**  
Eigenverantwortung des  
Verantwortlichen  
Rechenschaftspflicht

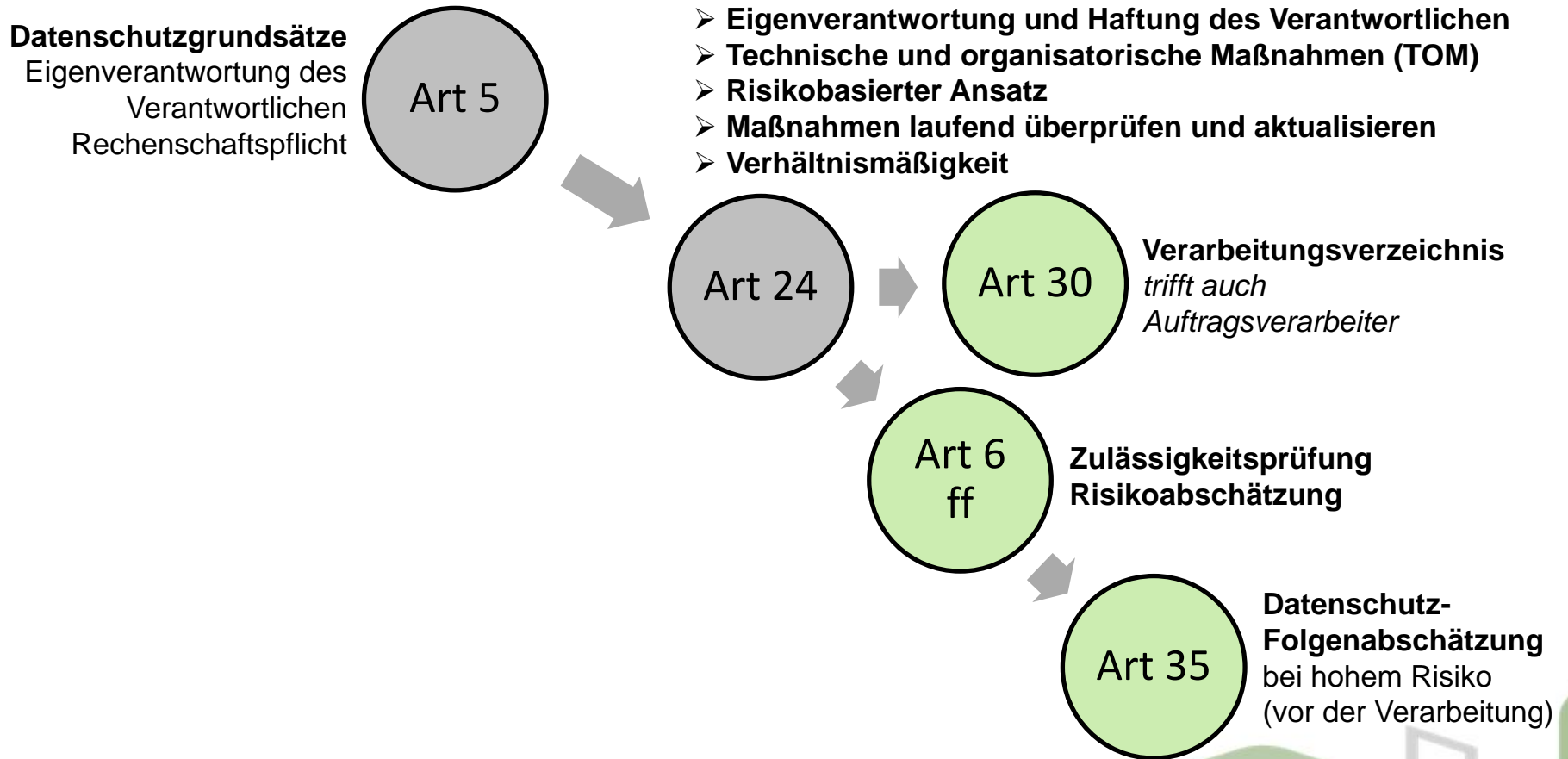


- **Eigenverantwortung und Haftung des Verantwortlichen**
- **Technische und organisatorische Maßnahmen (TOM)**
- **Risikobasierter Ansatz**
- **Maßnahmen laufend überprüfen und aktualisieren**
- **Verhältnismäßigkeit**

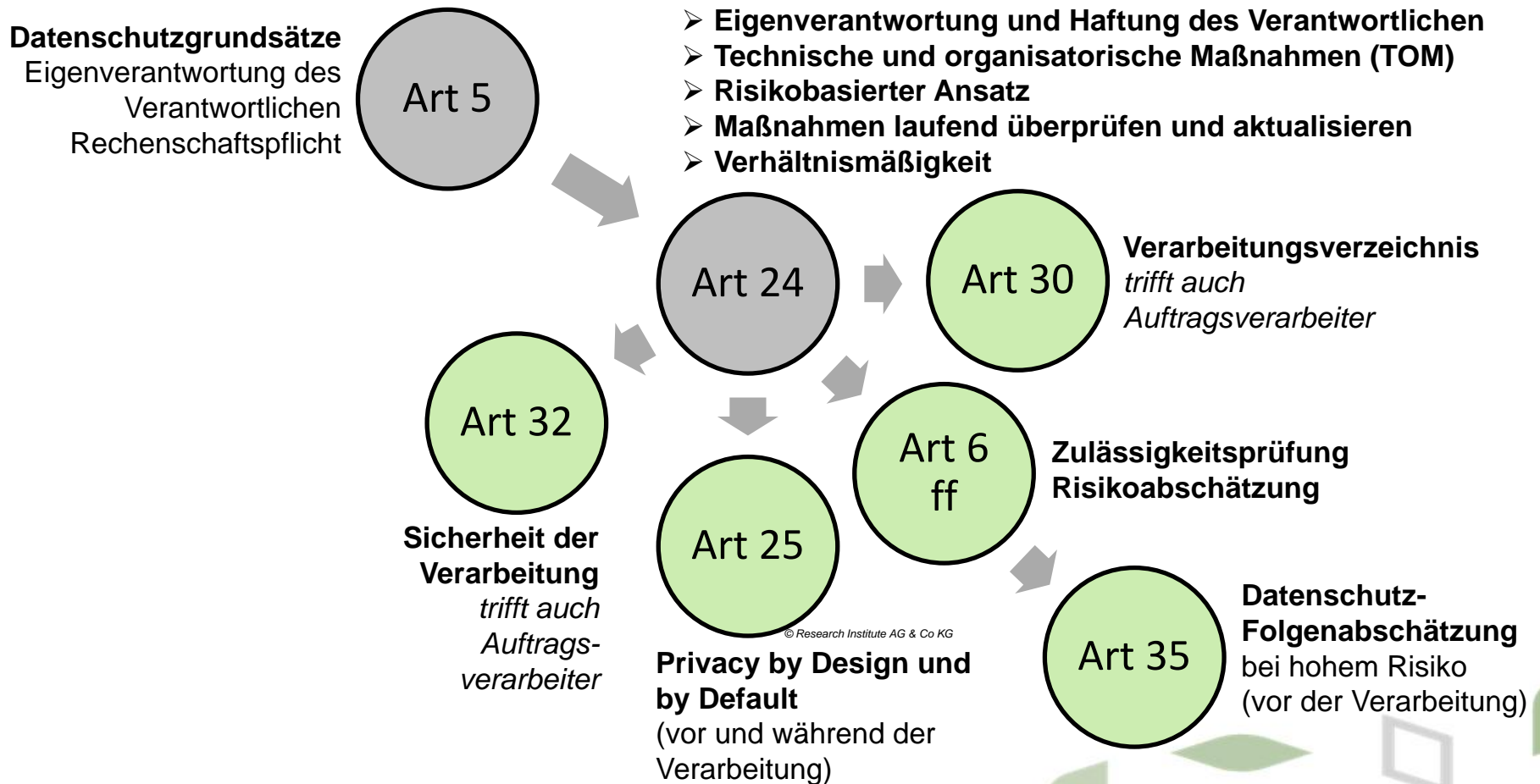
# PFLICHTEN DES VERANTWORTLICHEN: ÜBERBLICK UND ZUSAMMENHÄNGE



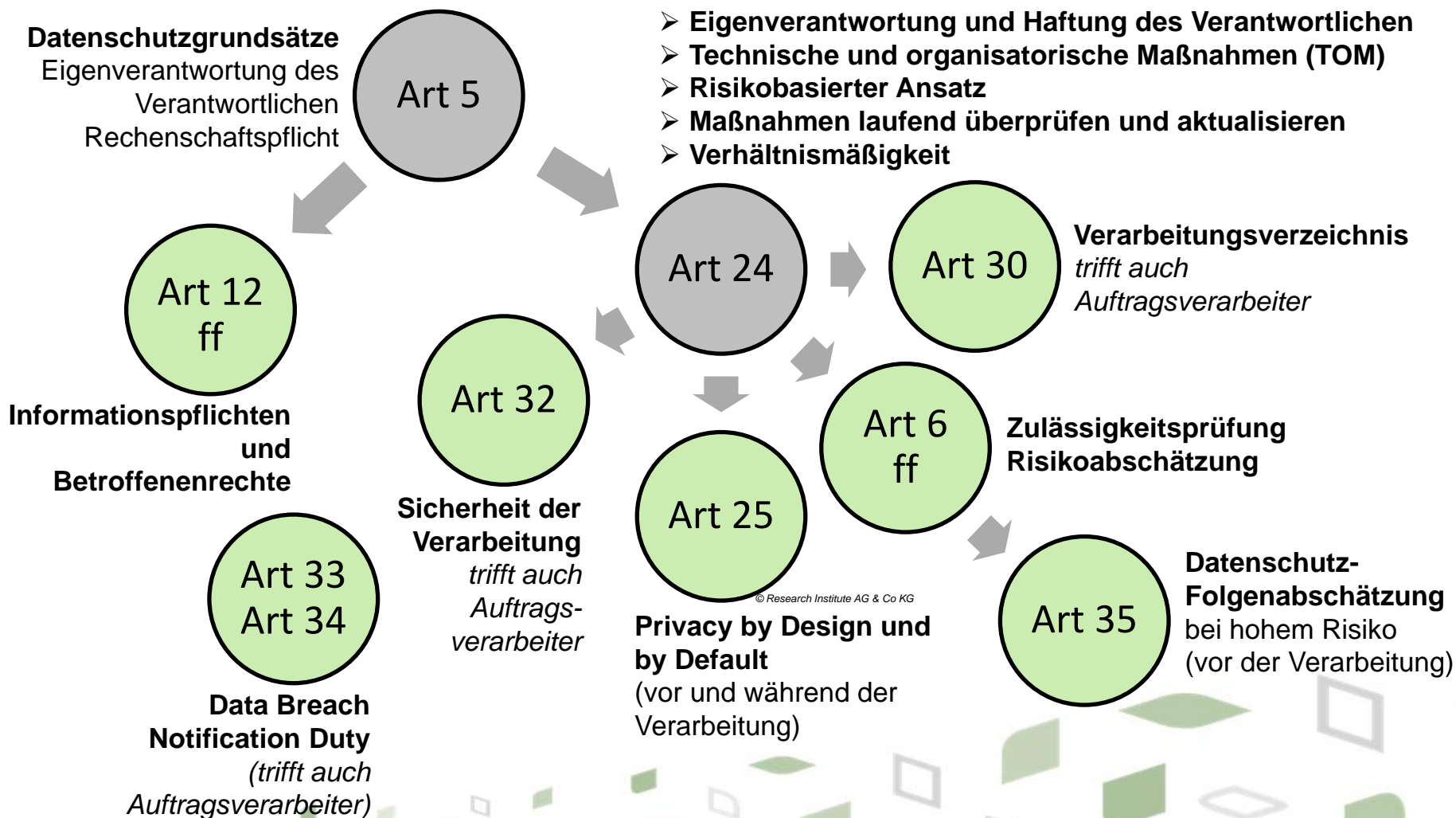
# PFLICHTEN DES VERANTWORTLICHEN: ÜBERBLICK UND ZUSAMMENHÄNGE



# PFLICHTEN DES VERANTWORTLICHEN: ÜBERBLICK UND ZUSAMMENHÄNGE



# 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-Managementsystems 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 durchzuführen: 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)

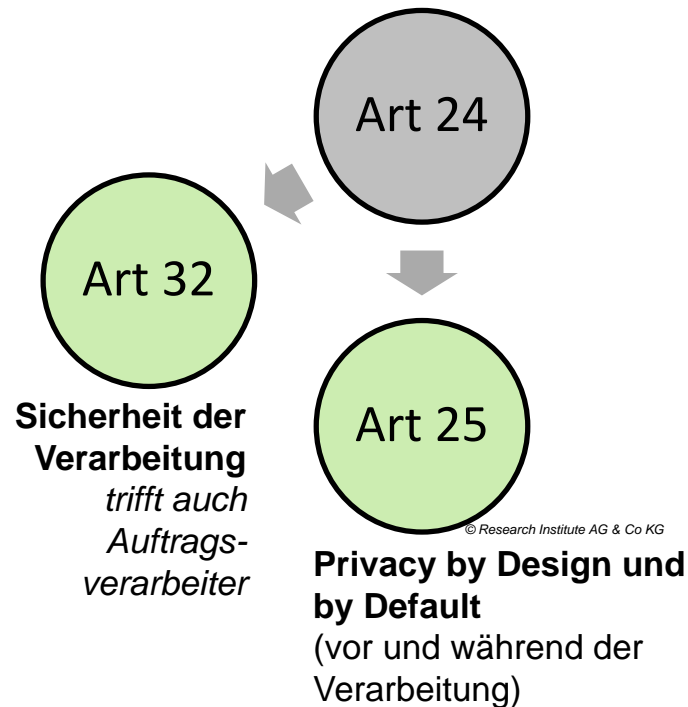
- **Bis 24.5.2018: Datenverarbeitungsregister (DVR) bei der DSB**
  - Pflicht zur Meldung von Datenanwendungen im öffentl. zugängl. DVR gemäß §§ 17 ff DSGVO 2000 → Exportfunktion aus DVR-Online bis 31.12.2019
- **Ab 25.5.2018: internes Verarbeitungsverzeichnis („VVZ“):**
  - Zu führen vom **Verantwortlichen** 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 DSGVO 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

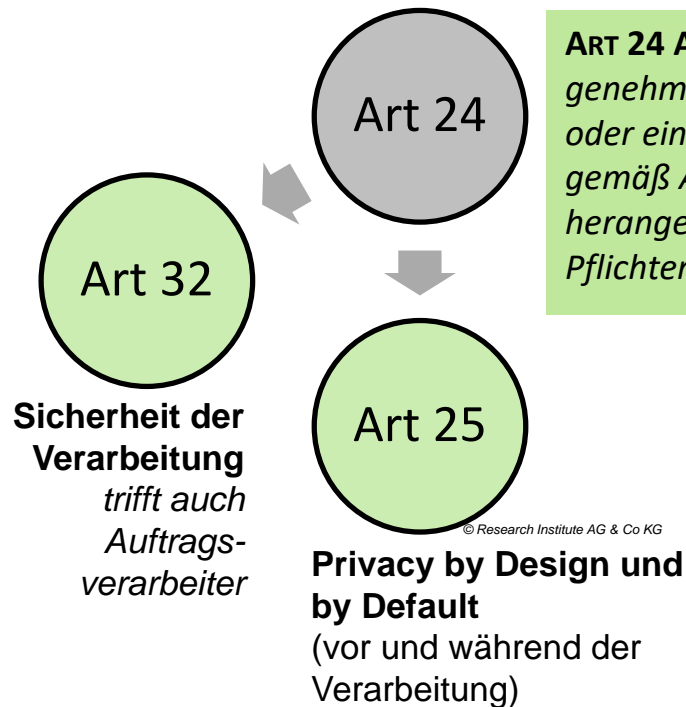
- **Eigenverantwortung und Haftung des Verantwortlichen**
- **Technische und organisatorische Maßnahmen (TOM)**
- **Risikobasierter Ansatz**
- **Maßnahmen laufend überprüfen und aktualisieren**
- **Verhältnismäßigkeit**



# 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 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:

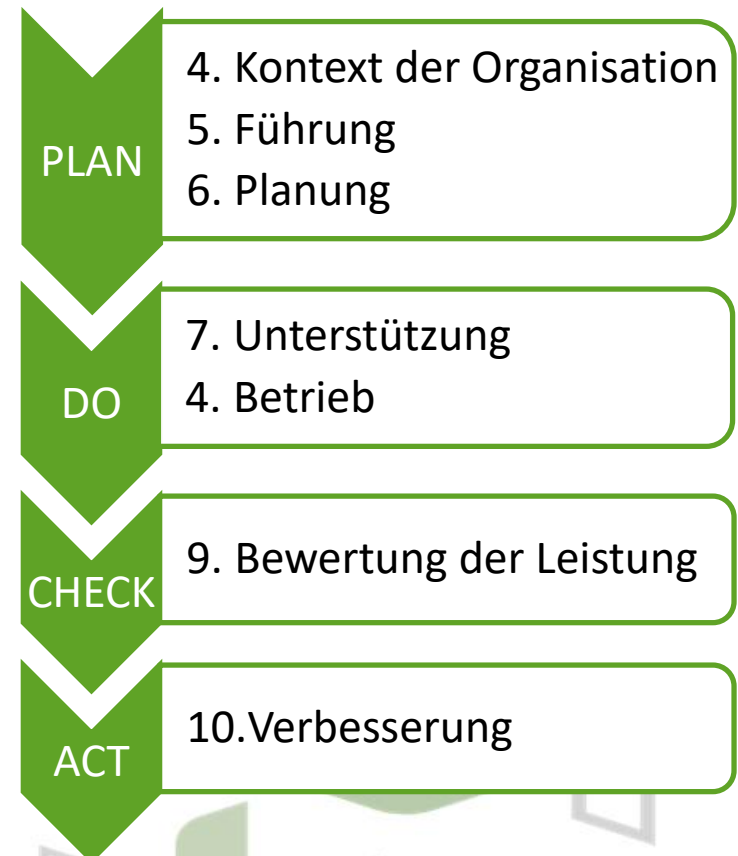
## DATENSCHUTZ-MANAGEMENTSYSTEME

- 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-Zertifizierung 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

1. Anwendungsbereich
2. Normative Verweisungen
3. Begriffe

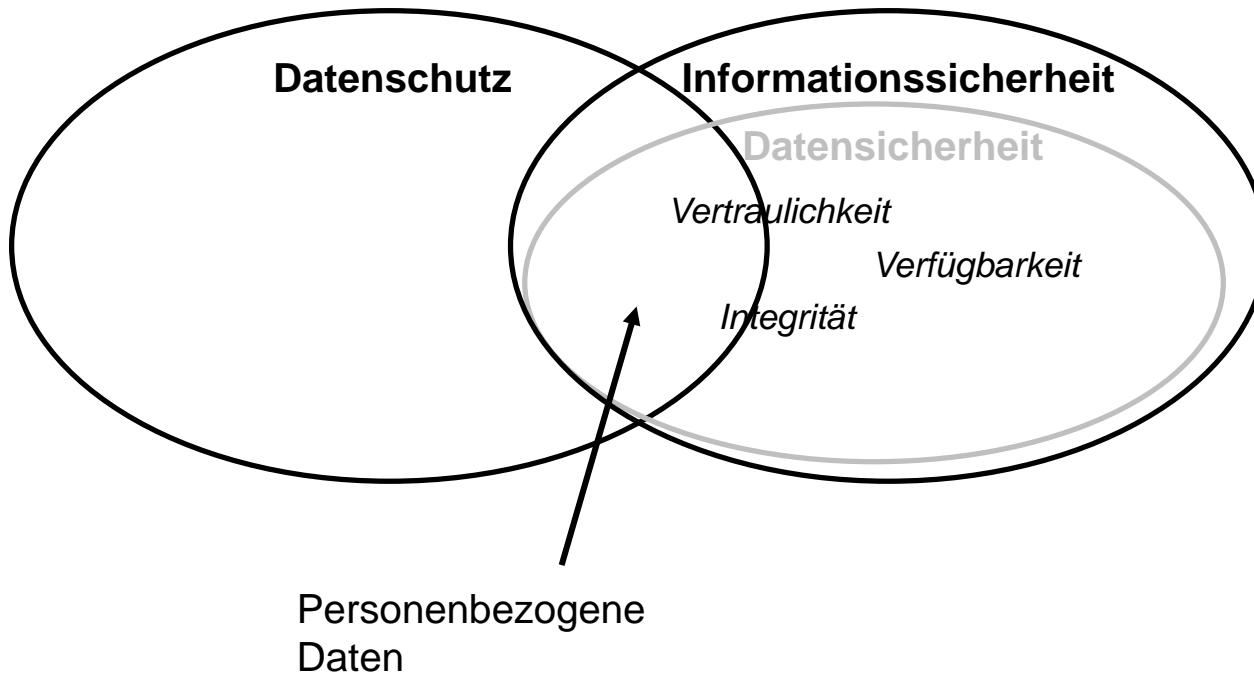


# BRAUCHT MAN EINE EIGENE NORM ODER GENÜGT ISO 27001?

- 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 Datenschutzerfordernungen 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 2017 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](mailto:christof.tschohl@researchinstitute.at)

**Dipl.-Ing. Dr. iur. Walter Hötendorfer**

Senior Researcher | Senior Consultant  
[walter.hoetendorfer@researchinstitute.at](mailto:walter.hoetendorfer@researchinstitute.at)

**Mag. Markus Kastelitz, LL.M. (IT-Recht), CIPP/E**

Senior Researcher | Senior Consultant  
[markus.kastelitz@researchinstitute.at](mailto: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](http://www.researchinstitute.at)

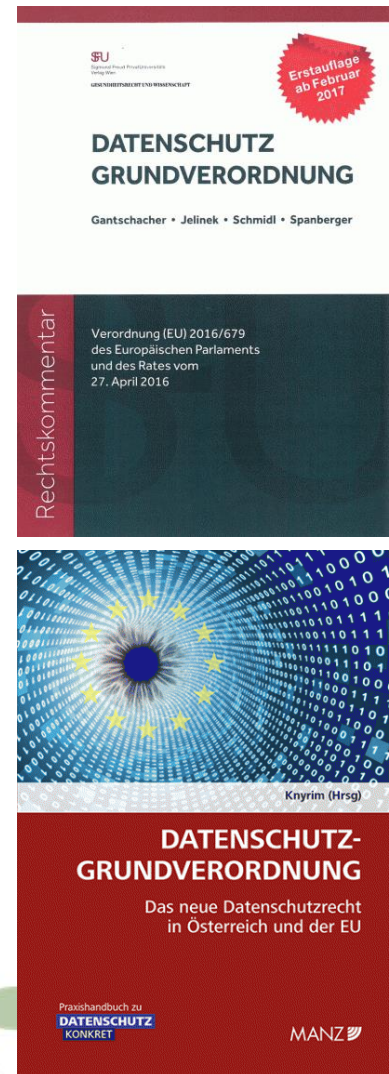
# ING. MAG. DR. IUR. CHRISTOF TSCHOHL

- 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)

- 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



- 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 Tsochl, Dipl.-Ing. Dr. Walter Hötendorfer und Mag. Markus Kastelitz

## **Copyright:**

Die vorliegenden elektronischen Unterlagen und Dateien wurden von den genannten Erstellern entwickelt und sind frei von Urheberrechten Dritter. Wir dürfen Sie daher bitten, das geistige Eigentum im Sinne des Urheberrechts zu respektieren. Als Seminarteilnehmer/in erwerben Sie selbstverständlich das Recht, alle vermittelten Methoden und Konzepte selbst anzuwenden (Nutzungsbewilligung), nicht aber das Recht, diese in organisierter Form weiterzuvermitteln. Auch die Vervielfältigung der Unterlagen und Dateien, die kein veröffentlichtes Werk darstellt, ist nicht gestattet. Ohne schriftliche Genehmigung von Christof Tsochl dürfen weder die Unterlagen selbst noch einzelne Informationen daraus reproduziert oder an Dritte weitergegeben werden.

## **Disclaimer:**

Dieses Dokument wurde auf Basis jener Informationen erstellt, die dem Autor als für den Zweck des Dokuments relevant erschien. Der Autor übernimmt jedoch keine Haftung/Gewähr für Vollständigkeit und Richtigkeit der in diesem Dokument zur Verfügung gestellten Informationen. Die Angaben in diesem Dokument können von dem Empfänger nicht als Zusicherung oder Garantie verstanden werden. Die in diesem Dokument enthaltenen Informationen können sich im Laufe der Zeit verändern oder zum Übergabezeitpunkt bereits verändert haben. Technische Änderungen vorbehalten.

Kontakt Daten: [walter.hoetendorfer@researchinstitute.at](mailto:walter.hoetendorfer@researchinstitute.at)