# Die EU Datenschutz-Grundverordnung als Herausforderung und Chance für die Verarbeitung personenbezogener Daten im Gesundheitsbereich

Vortrag beim **eHealth Summit Austria** am 23.5.2017 in Wien


**Ing. Dr. iur. Christof Tschohl**
Wissenschaftlicher Leiter | Gesellschafter | Prokurist

Research Institute AG & Co KG
Zentrum für digitale Menschenrechte
Smart.Rights.Consulting

Annagasse 8/1/8
1010 Wien

E-Mail: christof.tschohl@researchinstitute.at
Web: http://www.researchinstitute.at

# Research Institute AG & Co KG

## Zentrum für digitale Menschenrechte

Das **Research Institute (RI)** ist ein junges 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 in datenschutzrechtlichen Fragen
- **Schulungen** für Privatpersonen und Mitarbeiter von Unternehmen/Organisationen
- **Maßgeschneiderte technische Lösungen** zur praktischen Umsetzung der Compliance-Prozesse (in Zusammenarbeit mit Software-Entwicklern)
- **Konzeption und Durchführung individueller und multidisziplinärer Projekte** mit den besten Partnern auf nationaler und internationaler Ebene.

# Zur Person

*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 – *Zentrum für digitale Menschenrechte* und *Smart.Rights.Consulting*
- 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), Arbeitskreisleiter „Forum Privacy“
  - Österreichische RichterInnenvereinigung, Fachgruppe Grundrechte, a.o. Mitglied, regelmäßig Vortragender in Aus- und Fortbildung seit 2008
  - Mitglied des CERT Beirats im österreichischen Bundeskanzleramt

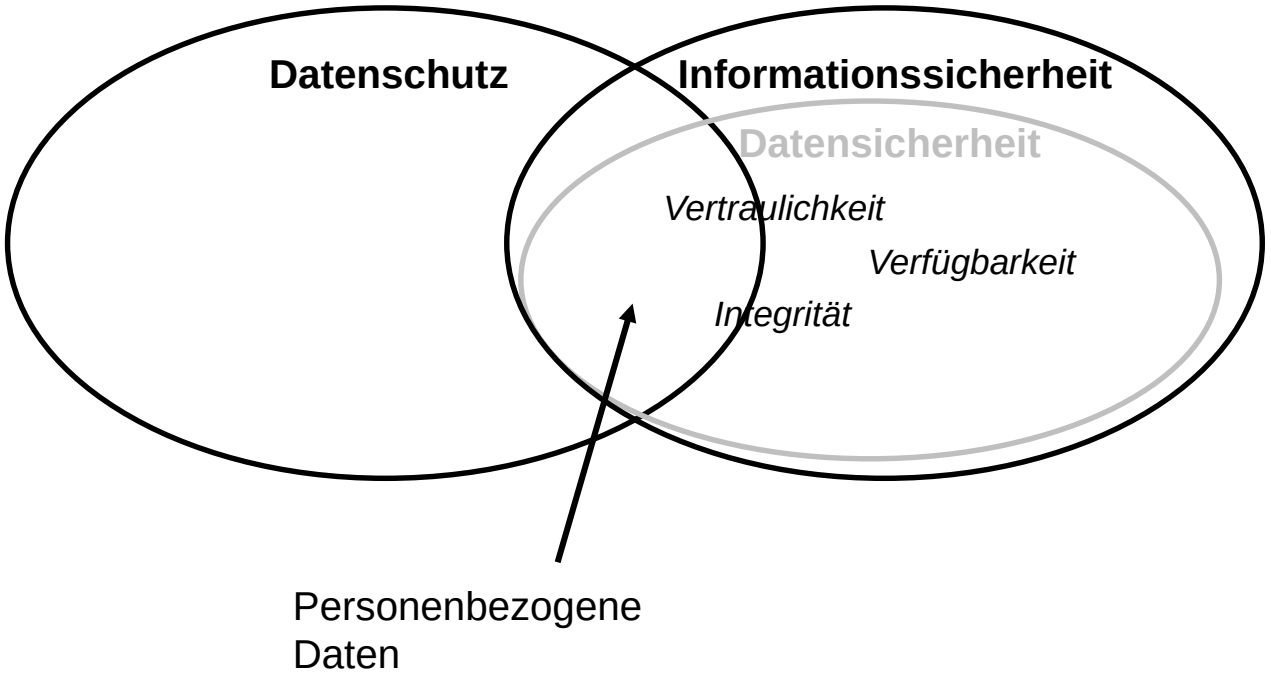
# EU-Datenschutzreform: Ergebnis und Status Quo

- **Bisher:**
  - EU: Datenschutzrichtlinie, RL 95/46/EG
  - Österreichisches Datenschutzgesetz 2000 (DSG 2000)
- **Datenschutz-Grundverordnung (DSGVO), VO 2016/679**
  - Seit 24. Mai 2016 im Rechtsbestand der EU; wirksam ab 25. Mai 2018
  - Datenschutzrichtlinie tritt mit 25. Mai 2018 außer Kraft
  - Ziele und Grundsätze der DSRL gelten in der DSGVO fort
- **Entwurf der EU-Kommission für eine E-Privacy-Verordnung (17.1.2017)**
  - Soll ebenfalls mit 25. Mai 2018 wirksam werden
  - Spezialregelung für den Datenschutz im Bereich der elektronischen Kommunikation
  - bildet gemeinsam mit der DSGVO den datenschutzrechtlichen Rahmen der EU
- **Datenschutzrichtlinie für Polizei und Strafjustiz (DSRL-PJ), RL 2016/680**
  - Erstmals einheitlicher Datenschutzrahmen für Strafverfolgung und Gefahrenabwehr (auch rein innerstaatliche Datenverarbeitung)
  - Seit 5. Mai 2016 in Kraft; von den Mitgliedstaaten bis 6. Mai 2018 umzusetzen
- **Zukunft:**
  - Nationales Begleitgesetz (derzeit in Ausarbeitung)
  - EU-Datenschutzausschuss (Leitlinien und Empfehlungen etc.)

# DATENSCHUTZ-GRUNDLAGEN

- **Datenschutz ist ein Grundrecht**:
  - Art 8 Charta der Grundrechte der EU (GRC)
  - Art 8 Europäische Menschenrechtskonvention (EMRK)
  - § 1 DSG 2000 im Verfassungsrang
- **Datenschutz ist nicht Selbstzweck**, sondern Voraussetzung für
  - das Funktionieren einer freien demokratischen Gesellschaft und
  - die Ausübung zahlreicher anderer Grundrechte
- **Personenbezogene Daten:** Daten, die sich auf eine bestimmte oder bestimmbare natürliche Personen beziehen
- **Anwendungsbereich DSGVO**:
  - Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung in der EU
  - Wenn keine Niederlassung in der EU: Anbieten von Waren oder Dienstleistungen in der EU
  - Beobachten des Verhaltens von Betroffenen in der EU

# Verhältnis von Datenschutz und Informationssicherheit



# Wesentl. Neuerungen der DSGVO

## Verschärfung der Sanktionsmechanismen

- Öffentlich-rechtliche Haftung: Strafzahlungen bis 20 Millionen EUR oder 4 Prozent des weltweiten Jahresumsatzes des betroffenen Unternehmens
- Auch für Verletzung von Handlungspflichten, nicht nur bei Data Breach
- Verbandsklagen zulässig

## Eigenverantwortung der „Verantwortlichen“ („Auftraggeber“)

- Dokumentationspflichten
- Rechenschaftspflicht
- Risikobasierter Ansatz
- Verpflichtende Risikoanalysen und Folgenabschätzung
- Datenschutzbeauftragter (in bestimmen Fällen)

**Datenschutz-Grundverordnung (DSGVO)**

## Materiell-rechtliche Änderungen, zB

- Allgemeine “Data Breach Notification”
- Privacy by Design und by Default
- Entfall der Melde- und Genehmigungspflicht (DVR)
- Kein Schutz juristischer Personen mehr
- Recht auf Datenportabilität

## Verstärkte Kooperation der nationalen Datenschutzbehörden

- „One-Stop-Shop“-Prinzip für Betroffene
- neues Gremium "European Data Protection Board“ (bisher: Art.-29-Gruppe)
- Konsultationsverfahren bei komplexen Risiken
- Mehr Koordination und Kohärenz

# Besonders schutzwürdige Daten nach der DSGVO

- ✓ Art 9 DSGVO „Verarbeitung besonderer Kategorien personenbezogener Daten“ (bisher nach DSG „sensible Daten“)
  - rassische/ethnische Herkunft, politische Meinung, religiöse/weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, genetischen/biometrischen Daten, Gesundheitsdaten, Daten zum Sexualleben/sexuelle Orientierung
  - **Nur nach strengen Voraussetzungen zulässig:**
  - Ausnahmen in Abs 2, zB Einwilligung (grundsätzlich strenger als DSG)
  - Abs 4 gibt den Mitgliedstaaten das Recht, weitere Bedingungen/Beschränkungen einzuführen/aufrechtzuerhalten

# Besonders schutzwürdige Daten nach der DSGVO

- ✓ Art 9 DSGVO „Verarbeitung besonderer Kategorien personenbezogener Daten“ (bisher nach DSG „sensible Daten“)
  - **Nur nach strengen Voraussetzungen zulässig:**
  - Grundsätzlich verboten, Ausnahmen in Abs 2, zB Einwilligung
  - nur ausdrückliche Zustimmung zulässig
  - Abwägung nur mit lebenswichtigen Interessen Dritter
- ✓ Wenn die **„Verarbeitung besonderer Kategorien personenbezogener Daten“ eine Kerntätigkeit des Verantwortlichen** darstellt:
  - Datenschutzbeauftragter verpflichtend zu bestellen
  - Verzeichnis der Verarbeitungstätigkeiten verpflichtend
  - Datenschutz-Folgenabschätzung verpflichtend

# Die DSGVO in der Praxis

- **Vorbereitung auf die DSGVO als Organisationsprojekt**
  - Professioneller Umgang mit den Daten im Unternehmen
  - Überblick über die IT-Landschaft
  - Daten als „Asset“ des Unternehmens werden systematisch gemanagt, professionell geschützt und strategisch genutzt
- Datenschutz-Folgenabschätzung
- Zertifizierung
- Datenschutz-Management-Software

# DATENSCHUTZGRUNDSÄTZE

- **Verhältnismäßigkeitsgrundsatz:** Kommt aus dem Datenschutz-Grundrecht (Art 8 Grundrechte-Charta bzw. Art 8 EMRK) und bezeichnet ein übergeordnetes Prinzip. Unter der „Verhältnismäßigkeit im engeren Sinn“ versteht man die Abwägung der Interessen bzw. Güter
- **Verbotsprinzip:** Die Verwendung personenbezogener Daten ist verboten, sofern sie nicht ausdrücklich erlaubt ist.
- **Zweckbindungsgrundsatz:** Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden.
- **Wesentlichkeitsgrundsatz:** Daten dürfe nur verwendet werden, soweit sie den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen.
- **Grundsatz der Datenlöschung:** Daten dürfen nur so lange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist.

# DATENSCHUTZGRUNDSÄTZE

- **Grundsatz der Datenminimierung:** Reduktion der Verarbeitung personenbezogener Daten auf das Unvermeidbare
- **Privacy by Design und Privacy by Default**
- **Grundsatz von Treu und Glauben und Rechtmäßigkeit**
- **Grundsatz der Transparenz:** Information des Betroffenen über Vorhandensein einer Verarbeitung und deren Umstände
- **Grundsatz des Mitspracherechts:** Rechte auf Auskunft, Richtigstellung und Löschung sowie Widerspruch
- **Grundsatz der sachlichen Richtigkeit und Aktualität:** Daten dürfen nur so verwendet werden, dass sie im Hinblick auf den Verwendungszweck sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind.
- **Grundsatz der Datensicherheit**
- **Grundsatz der Rechenschaftspflicht**

# BETROFFENENRECHTE

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung („Recht auf Vergessenwerden“)
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht

# Art 24: „Verantwortung des für die Verarbeitung Verantwortlichen“

- **Eigenverantwortung** und Haftung des Verantwortlichen
- Risikobasierter Ansatz
- Rechenschafts- und Nachweispflicht
- Pflicht zu technischen und organisatorischen Maßnahmen, um sicherzustellen und den Nachweis zu erbringen, dass die Verarbeitung DSGVO-Konform erfolgt
- Pflicht, diese Maßnahmen zu überprüfen und zu aktualisieren
- Nähere Ausgestaltung dieser Pflichten durch
  - Art 25: *Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen*
  - Art 32: *Sicherheit der Verarbeitung*
  - Art 35: *Datenschutz-Folgenabschätzung*
- Abs 2: Konkretisierung des Verhältnismäßigkeitsgrundsatzes

# Ausgewählte Neuerungen der DSGVO im Detail

- Dokumentationspflichten:
  - Führen eines Verzeichnisses der Verarbeitungstätigkeiten (trifft nicht jedes Unternehmen, ist aber generell ratsam)
  - Dokumentation der getroffenen Maßnahmen (Datensicherheit, Privacy by Design etc.)
- Rechenschaftspflicht:
  - DSGVO-konformer Zustand muss jederzeit belegbar sein
  - Nicht nur „Data Breach“ führt zu Sanktionen
- Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten:
  - Meldung an die Aufsichtsbehörde unverzüglich, möglichst binnen 72 Stunden nachdem die Verletzung bekannt wurde
  - Benachrichtigung der Betroffenen, wenn voraussichtlich ein hohes Risiko für diese besteht
  - Impliziert auch Maßnahmen um Data Breaches überhaupt festzustellen

# Ausgewählte Neuerungen der DSGVO im Detail

- Privacy by Design, d.h.:
  1. Datenschutz bei der Gestaltung von Systemen von Beginn an berücksichtigen
  2. Verhindern der nicht zweckkonformen Verwendung des Systems durch technische und organisatorische Maßnahmen
- Datenschutz-Folgenabschätzung wenn voraussichtlich ein hohes Risiko für die Betroffenen besteht:
  - Systematische Beschreibung der Verarbeitungsvorgänge
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit
  - Bewertung der Risiken für die Betroffenen
  - Abhilfemaßnahmen
- Konsultation der Datenschutzbehörde -> schriftliche Empfehlungen

# DATENSICHERHEIT IN DER DSGVO

- Sicherheit neu unter den Datenschutzgrundsätzen in Art 5 Abs 1 lit f: „Sicherheit der personenbezogenen Daten“, „Integrität und Vertraulichkeit“
- Wie bisher (§ 14 DSG): Angemessene technische und organisatorische Maßnahmen
- Art 32 nennt ausdrücklich folgende Schutzmaßnahmen:
  - Pseudonymisierung und Verschlüsselung personenbezogener Daten
    - Verpflichtung zur Pseudonymisierung, wenn der konkrete Verarbeitungszweck auch mit pseudonymisierten Daten zu erreichen ist (sofern kein unverhältnismäßig hoher Aufwand)
    - Verpflichtung zur Verschlüsselung der Daten bei Speicherung und Übertragung, außer in begründeten Ausnahmefällen
  - Fähigkeit, folgende Schutzziele auf Dauer sicherzustellen:
    - Vertraulichkeit
    - Integrität
    - Verfügbarkeit
    - Belastbarkeit
  - Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Recovery)
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

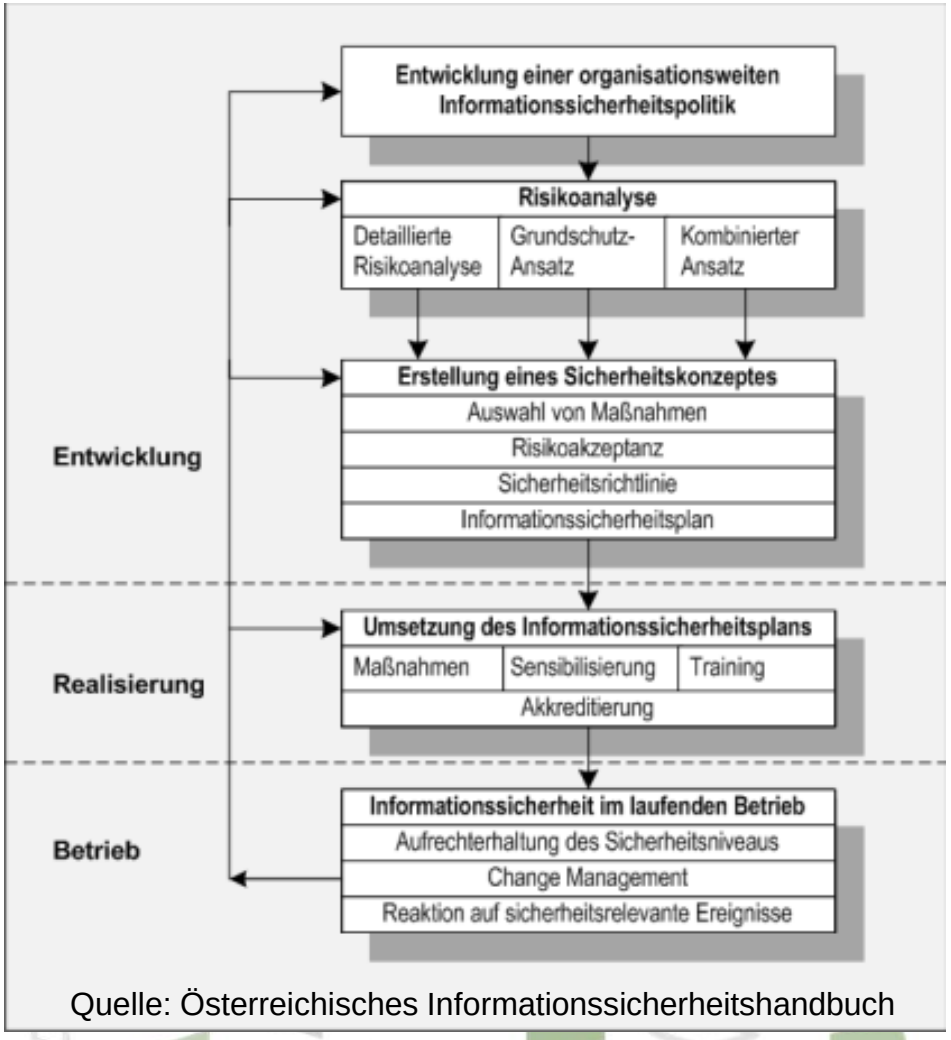
# Zum Begriff „Stand der Technik“

- Maßnahmen, die
  - aktuell technisch realisierbar sind
  - auf gesicherten Erkenntnissen der Wissenschaft und Technik beruhen
  - und in ausreichendem Maße zur Verfügung stehen

  (vgl Martini in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung, Beck [2017] Art. 25 Rz 39 mwN).
- Es kommt somit auf die praktische Umsetzbarkeit an, nicht aber auf einen bereits weit verbreiteten Einsatz in der Praxis
- Betrifft nicht nur Ausgestaltung einzelner Maßnahmen (zB Auswahl von Verschlüsselungsalgorithmen), sondern auch vorgelagerte Auswahl der Arten von Maßnahmen

# Informationssicherheits-Management

- „Technische und organisatorische Maßnahmen“: Systematische Organisation erforderlich
- Dokumentation: Teil des Verzeichnisses der Verarbeitungs-tätigkeiten (Art 30 Abs 1 lit g)
- Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27000-Normenreihe (ISO/IEC 27001 und 27002)
- ISM als kontinuierlicher Verbesserungsprozess: Plan – Do – Check – Act (Art 32 Abs 1 lit d), vor allem:
  - Veränderungen des Schutzbedarfs
    - Steigende Datenmengen
    - Neue externe Bedrohungen
  - Veränderungen des Stands der Technik
    - Neue Abwehrmaßnahmen




Quelle: Österreichisches Informationssicherheitshandbuch

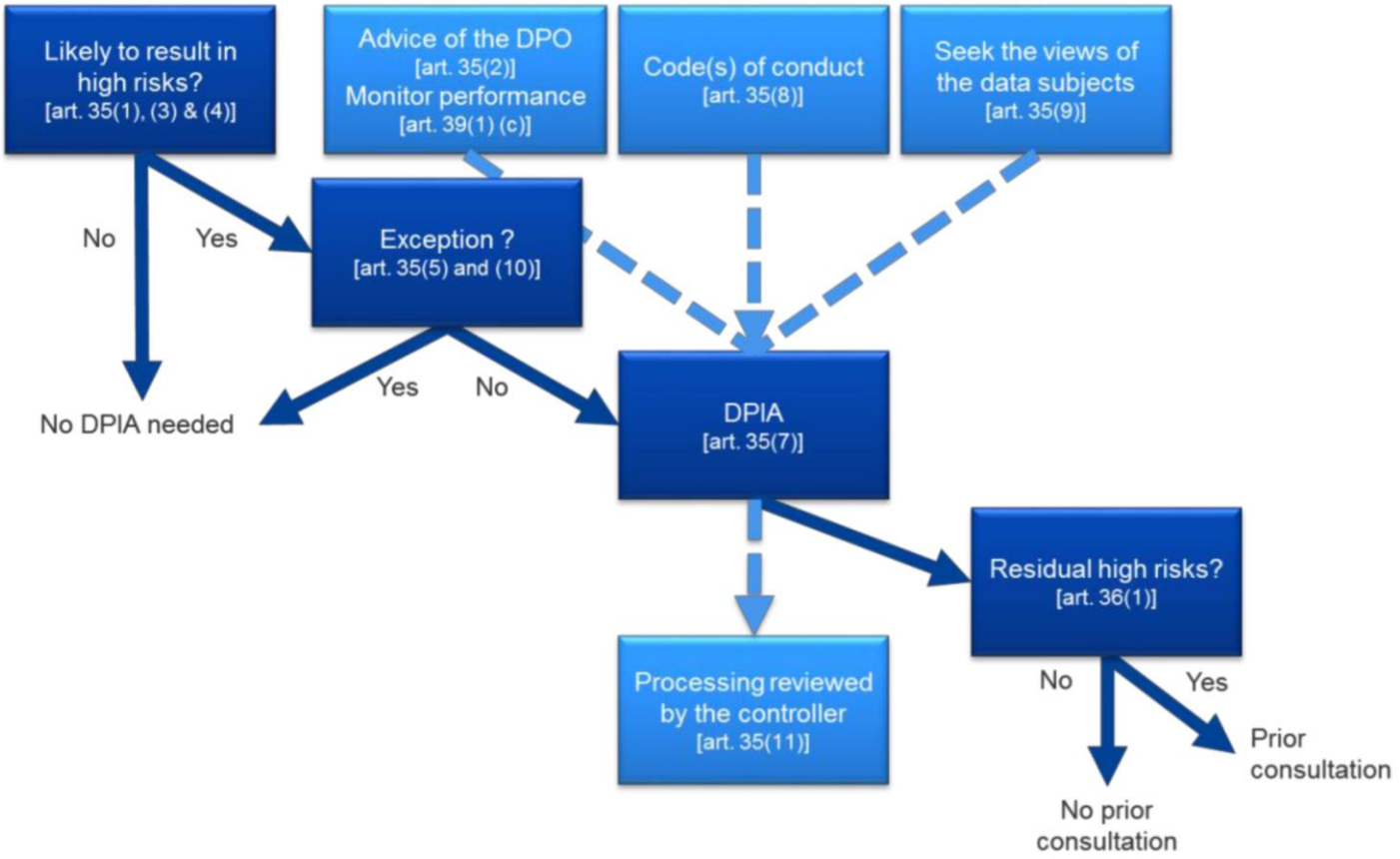
# Datenschutz-Folgenabschätzung: Intentionen des Gesetzgebers

- DSGVO ersetzt Meldepflicht und Genehmigungspflicht (ErwGr 89: „bürokratisch“) durch
  - Eigenverantwortung des Verantwortlichen und
  - risikobasierten Ansatz
- Intensive Befassung mit jenen Verarbeitungsvorgängen, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen
  => Prüfen, ob ein hohes Risiko besteht, und ggf.
  Datenschutz-Folgenabschätzung durchführen
  oder dokumentieren, warum nicht
- Die damit verbundenen Abwägungen und Einschätzungen muss der Verantwortliche treffen
- Keine Pflichtverletzung, wenn auf Basis des zum Zeitpunkt der Prognose verfügbaren Wissens deren Unrichtigkeit nicht abzusehen war

# Datenschutz-Folgenabschätzung: Motivation

- Wenn eine Datenverarbeitung (insbesondere bei Verwendung neuer Technologien) **voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen** zur Folge hat, führt man eine Datenschutz-Folgenabschätzung durch, zwecks
  - Erkennen und Analyse der Risiken für die Betroffenen aufgrund der geplanten Verarbeitung
  - Ergreifen von Gegenmaßnahmen
  - Steigerung der Rechtssicherheit
  - Verringerung des (wirtschaftlichen) Risikos nachträglicher Anpassungen

# PRÜFSCHEMA




Quelle: Artikel-29-Datenschutzgruppe, WP 248 vom 4. April 2017

# Kriterien für „hohes Risiko“ (Art-29-Datenschutzgruppe)

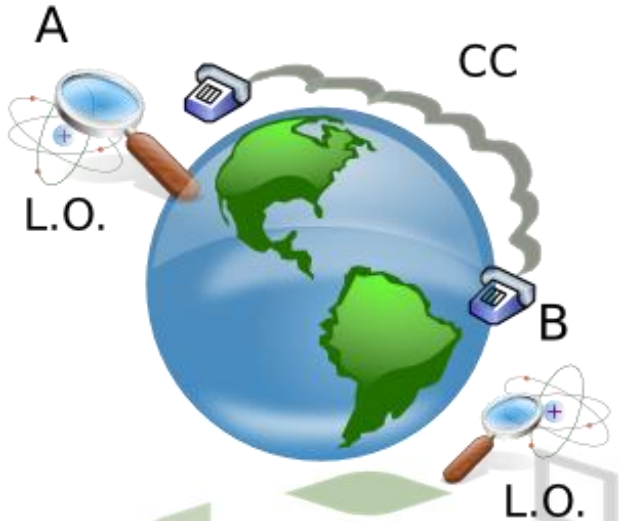
- Profiling/Scoring natürlicher Personen
- Automatisierte Entscheidungen, die rechtliche oder vergleichbare Wirkung gegenüber natürlichen Personen entfalten
- Systematische Überwachung
- Sensible Daten
- Datenverarbeitung in großem Umfang
- Verknüpfung verschiedener Datenbestände
- Daten schutzbedürftiger natürlicher Personen
- Neue Technologien oder neuartiger Einsatz von Technologien
- Datenübermittlung in Drittländer
- Datenverarbeitungen, die Betroffene an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern

# ZUSAMMENFASSUNG

- **Eigenverantwortung** und Haftung des Verantwortlichen
- Risikobasierter Ansatz
- Pflicht zu technischen und organisatorischen Maßnahmen, um sicherzustellen und den Nachweis zu erbringen, dass die Verarbeitung DSGVO-Konform erfolgt
- Nähere Ausgestaltung dieser Pflichten durch
  - Art 25: *Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen*
  - Art 32: *Sicherheit der Verarbeitung*
  - Art 35: *Datenschutz-Folgenabschätzung*
- **Datensicherheit**
  - Neu unter den Datenschutzgrundsätzen in Art 5 Abs 1
  - Art 32 neu gestaltet, aber Anforderungen ähnlich wie bisher
  - Systematische Organisation und Dokumentation erforderlich
  - Verhältnismäßigkeitsabwägung

# VIELEN DANK

# FÜR IHRE AUFMERKSAMKEIT!



# Die EU Datenschutz-Grundverordnung als Herausforderung und Chance für die Verarbeitung personenbezogener Daten im Gesundheitsbereich

Vortrag beim **eHealth Summit Austria** am 23.5.2017 in Wien


**Ing. Dr. iur. Christof Tschohl**
Wissenschaftlicher Leiter | Gesellschafter | Prokurist

Research Institute AG & Co KG
Zentrum für digitale Menschenrechte
Smart.Rights.Consulting

Annagasse 8/1/8
1010 Wien

E-Mail: christof.tschohl@researchinstitute.at
Web: http://www.researchinstitute.at

# BACKUP FOLIEN

# Weiterführende Informationen

- Artikel-29-Datenschutzgruppe, WP 248 vom 4. April 2017: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
- *De Hert, Paul/Kloza, Dariusz/Wright, David,* Recommendations for a privacy impact assessment framework for the European Union http://www.piafproject.eu/ref/PIAF_D3_final.pdf
- Brussels Laboratory for Data Protection and Privacy Impact Assessments http://www.vub.ac.be/LSTS/dpialab/
- *Wright, David/De Hert, Paul* (Hrsg.), Privacy Impact Assessment, Springer Science & Business Media, Dordrecht, Heidelberg, London, New York 2012

# Weiterführende Literatur


- Hörbe/Hötzendorfer, Privacy-by-Design-Anforderungen für das Federated Identity Management, in Jahnel (Hrsg), Jahrbuch Datenschutzrecht [2014], 305–325
- ENISA, Privacy and Data Protection by Design – from policy to engineering, 2014 https://www.enisa.europa.eu/activities/identity-and-trust/library/ deliverables/privacy-and-data-protection-by-design/at_download/full Report
- Gürses/Troncoso/Diaz, Engineering Privacy by Design, Proceedings of Computers, Privacy & Data Protection (CPDP 2011) [2011]
- Spiekermann/Cranor, Engineering Privacy, IEEE Transactions on Software Engineering 2009, 67–82
- Deng et al, A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements, Requirements Engineering 2011, 3–32
- van Rest et al, Designing Privacy-by-Design, Proceedings of the First Annual Privacy Forum, APF 2012, LNCS, vol 8319 [2014] 55–72;
- Kung, PEARs: Privacy Enhancing ARchitectures, Proceedings of the Second Annual Privacy Forum, APF 2014, LNCS, vol. 8450 [2014] 18–29
- Koops/Leenes, Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law, International Review of Law, Computers & Technology, 28:2 [2014] 159–171
- Hörbe/Hötzendorfer, Privacy by Design in Federated Identity Management, Proceedings of the 2015 IEEE Security and Privacy Workshops [2015] 167–174
- Tsormpatzoudi/Berendt/Coudert, Privacy by Design: From Research and Policy to Practice – the Challenge of Multi-disciplinarity, Proceedings of the Third Annual Privacy Forum, APF 2015, LNCS, vol. 9484 [2016] 199–212