35. Netzpolitischer Abend am 4. April 2019

im Wiener Metalab, Rathausstrasse 6, 1010 Wien

„E-Evidence – grenzüberschreitender Polizeizugriff auf Providerdaten in der EU“

eine Kritik aus Sicht der Grundrechte

Ing. Dr. iur. Christof Tschohl

www.epicenter.works

www.researchinstitute.at

research institute

EPICENTER .WORKS for digital rights

RESEARCH INSTITUTE

DIGITAL HUMAN RIGHTS CENTER
&
SMART RIGHTS CONSULTING

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, Universität Hannover, Donau Uni Krems ua)
- Mitgliedschaften:
  - epicenter.works – Plattform für digitale Grundrechte (ehem AKVorrat), Obmann
  - noyb – Vorstandsmitglied gemeinsam mit Max Schrems und Petra Loipold
  - 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

Wesentliche grundrechtliche Aspekte des Vorschlags zur e-Evidence Verordnung

- Direkter Zugriff von LEA in MS A auf Daten bei ISP in MS B
- Behördliches Rechtshilfe-Verfahren nur eingeschränkt aktiviert
- Ausdehnung des EU rechtlichen „Anerkennungsprinzips“
  - Rechtsgrundlage für Grundrechtseingriff in MS B basiert in der Rechtsordnung (Strafprozessrecht, materielles Strafrecht) von MS A
  - Extrateritoriale Jurisdiktion (Art 89 AEUV erfüllt)
- Gegenseitigkeitsprinzip und Wahrung des „ordre public“ reduziert (Art 82 AEUV als Kompetenzgrundlage – Frage der Notwendigen Involvierung von Behörden auf beiden Seiten?)
- Begriffsdefinitionen in Art 2 Verordnungsentwurf insbesondere zu Datenkategorien (zB Inhaltsdaten/Metadaten) und Provider-Begriff
- Information, Notifizierung und Rechtsschutz – Rolle der ISP und der Behörden

Betroffene Grundrechte

Aus den Erwägungsgründen zum Verordnungs-Vorschlag:

Ergebnisse der ex-post Bewertung, der Konsultation der Interessenträger und der Folgenabschätzung (Punkt 3.)

- Der Vorschlag könnte potenziell Auswirkungen auf eine Reihe von Grundrechten haben:
  - Rechte des Individuums, auf dessen Daten zugegriffen wird:
    - das Recht auf den Schutz personenbezogener Daten
    - das Recht auf Achtung des Privat-und Familienlebens
    - das Recht auf freie Meinungsäußerung; Verteidigungsrechte
    - das Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren
  - Rechte des Diensteanbieters:
    - das Recht auf unternehmerische Freiheit
    - das Recht auf einen wirksamen Rechtsbehelf
- Rechte aller Bürger: das Recht auf Freiheit und Sicherheit
  - Anmerkung: Recht auf Sicherheit und staatliche Schutzpflichten unterscheiden

GRUNDRECHTLICHER SCHUTZ

- **Datenschutz ist ein Grundrecht**:
  - Art 7 + 8 Charta der Grundrechte der EU (GRC)
  - Art 8 Europäische Menschenrechtskonvention (EMRK)
  - § 1 Datenschutzgesetz (DSG) im Verfassungsrang
- **Grundsatz: Verarbeitung personenbezogener Daten verboten, wenn nicht ausdrücklich erlaubt**
- **Staatliche Schutzpflichten-Dimension**
  - Nicht nur Eingriffs-Abwehr
  - Schutzpflichten als „Verkehrssicherungspflichten“ zur Datenübertragung
  - Datenschutz-Folgenabschätzung und „Datenschutz durch Technik“ als Konkretisierung der grundrechtlichen Schutzpflichten des Staates

Kritik am Verordnungsentwurf e-Evidence aus Grundrechtsperspektive

- Mangelnde Begriffsbestimmungen – Determinierung der Grundrechtseingriffe (Rechtsstaatsprinzip)
- Mangelnde Vorkehrungen zur Absicherung der Zweckbindung (zB Definition, ab wann ein Verdacht vorliegt)
- Mangelnde Vorkehrungen zur Absicherung des Rechtsschutzes (im Regelfall keine Absicherung durch unabhängige staatliche Aufsicht, „kommisarischer Rechtsschutz“ ausschließlich durch ISP ?)
- Keine wirksamen Vorgaben zur Wahrung der Verhältnismäßigkeit im Einzelfall (zB Kostentragungsregeln als Motivation zur Zurückhaltung)
- Mangelnde Vorkehrungen zur Identifikation und Authentifizierung der Teilnehmer beim elektronischen Datenaustausch
- Mangelnde Vorgaben zur Datensicherheit und zur revisionssicheren Protokollierung von Auskunftsvorgängen.

EU-Datenschutzrecht mit besonderen Schutzpflichten

- **Datenschutz-Grundverordnung (DSGVO), VO 2016/679**
  - Seit 24. Mai 2016 im Rechtsbestand der EU; seit 25. Mai 2018 allgemein verbindlich
  - Ziele und Grundsätze der DSRL gelten in der DSGVO fort

- **Entwurf der EU-Kommission für eine E-Privacy-Verordnung (17.1.2017)**
  - Sollte ebenfalls mit 25. Mai 2018 wirksam werden (mittlerweile äußerst unwahrscheinlich)
  - Spezialregelung für den Datenschutz im Bereich der elektronischen Kommunikation (derzeit Richtlinie)
  - 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

- **Künftig: DSGVO-Auslegung durch EU-Datenschutzausschuss (Leitlinien, Empfehlungen etc.)**

Grundverordnung und Richtlinie als Gesamtpaket

RECHTLICHE RAHMENBEDINGUNGEN

- Kritik:
  - Datenaggregierung auf Grundlage unterschiedlicher Eingriffsermächtigungen
  - Unterschiedlicher Rechtsschutz (Einbindung der Rechtsschutzbeauftragten)
  - Auswertung kumulierter Datenbestände mithilfe eines neuartigen, teilweise automatisierten Systems
- Beachtung der jeweiligen gesetzlichen Vorgaben (Zwecke, Verwendungsbeschränkungen etc.);
- ausreichende Bestimmtheit der Eingriffsermächtigungen?

INTERNAT. DATENAUSTAUSCH (DATENÜBERMITTLUNG)

- **Polizeikooperationsgesetz** (PolKG):
  - Organisator. Rahmen für die internationale Zusammenarbeit
  - Voraussetzung für die Anwendbarkeit des PolKG ist eine materiellrechtliche Ermächtigung, als rechtliches Instrument kommen bi- oder multilaterale Polizeikooperationsabkommen in Frage, Ausnahme Amtshilfe
  - Regelungen zur Übermittlung personenbezogener Daten (§§ 8 ff)
  - im Einzelfall Amtshilfe; strenge Voraussetzungen für Teilnahme an **internationalen Informationsverbundsystemen** (§ 8a – neu, siehe BGBl I 2017/91)
- **EU-Polizeikooperationsgesetz** (EU-PolKG):
  - Polizeiliche Kooperation mit Sicherheitsbehörden der anderen der EU-Mitgliedstaaten und Europol
- **Gerichte/StA: § 76 Abs 3 und 4 StPO**

→ Generell ist ausreichende Determinierung u. ausreichender Rechtsschutz zu hinterfragen. Es bestehen demokratische und rechtsstaatliche Defizite in den europäischen Regelungen zur Polizeikooperation (*Lachmayer*, JBl 2011, 409); Kritik des österr. Datenschutzrats im Gesetzgebungsverfahren zu § 8a PolKG

DATENSCHUTZ-FOLGENABSCHÄTZUNG

Wenn eine Datenverarbeitung „aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung“ **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

- Sowohl in **DSGVO** (Art 35) als auch in **DSRL-PJ** (Art 27)

  Art 27 DSRL-PJ umgesetzt in Österreich in **§ 52 DSG**, worin wiederrum auf Art 35 Abs 1, 2, 3, 7 und 11 DSGVO verwiesen wird

  → Ausnahme von der Durchführung einer (individuellen) DSFA gem. Art 35 Abs 10 nicht vorgesehen

  → Erforderlichkeit der Durchführung einer DSFA hängt maßgeblich von der geplanten Ausgestaltung ab – immer unter der Voraussetzung, dass die Schwelle für die Durchführung einer DSFA erreicht ist (Schwellwertanalyse)

Privacy by Design
Als neues Prinzip

1. **Datenschutz bei der Gestaltung von Systemen von Beginn an berücksichtigen, sodass die Verwirklichung der Datenschutzgrundsätze bereits in den Systemen angelegt ist**

2. **Verhindern der nicht intendierten/nicht zweckkonformen Verwendung des Systems durch technische und organisatorische Maßnahmen**

Privacy by Design wirkt sich sowohl auf die Architektur als auch auf viele Detailaspekte der Gestaltung von Systemen aus

Zentrale Maßnahme: **Datenminimierung**

Der Gesetzgeber ist als erstes gefordert, das Prinzip schon in der Rechtssetzung zu wahren und zu befördern!

Datenschutz durch Technik
§ 46 DSG ivm Art 25 Abs 1 DSGVO

§ 46 DSG verweist auf die in Art 25 Abs 1 und 2 DSGVO angeführten Verpflichtungen (Umsetzung Art 20 DSRL-PJ)

- Gänzlich neue Pflicht (vgl jedoch bereits die Formulierung in ErwGr 46 Datenschutzrichtlinie)
- Begriff:
  - DSGVO (EN): „Data Protection by Design“
  - DSGVO (DE): „Datenschutz durch Technikgestaltung“
  - Wissenschaft: „Privacy by Design“ (PbD)
  - eIDAS-VO (EN): „Privacy by Design“
  - eIDAS-VO (DE): „eingebauter Datenschutz“

- **Verhältnismäßigkeitsabwägung** zwischen den Risiken für die Rechte und Freiheiten natürlicher Personen und der wirtschaftlichen Belastung des Verantwortlichen durch die Maßnahmen unter Berücksichtigung
  - des Stands der Technik
  - der Implementierungskosten
  - der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung

Praktische Umsetzung von Privacy by Design & by Default

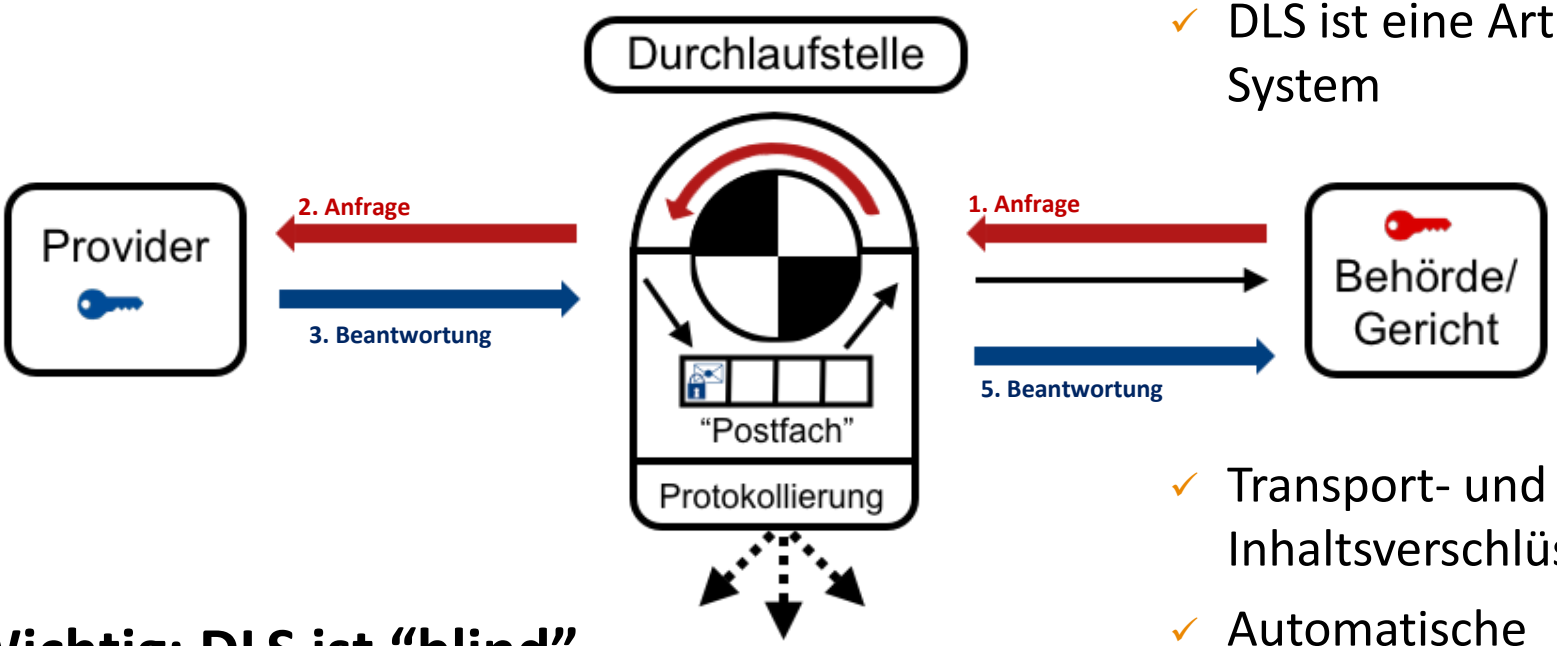
- Zentrale Maßnahme: **Datenminimierung** (auch „Datensparsamkeit“) – Reduktion der Verarbeitung personenbezogener Daten auf das Unvermeidbare; zahlreiche Dimensionen:
  - Art der Daten (zB nicht Geburtsdatum, wenn Alter oder Geburtsjahr ausreicht)
  - Umfang der Daten
  - Speicherdauer
  - Kreis der Zugriffsberechtigten

- Etablieren von **Privacy by Design als Mentalität** im Unternehmen: Privacy by Design ist vor allem eine Einstellung, wie man an Dinge herangeht

- **Schaffung von Prozessen**:
  - Entwicklung oder Beschaffung neuer Systeme darf nicht genehmigt werden, wenn man sich nicht über den Datenschutz Gedanken gemacht hat
  - Dokumentation, dass man bei der Planung von Systemen („zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung“) eine Abschätzung der Datenschutzrisiken durchgeführt und entsprechende Maßnahmen getroffen hat
  - Beschaffte Software muss Privacy by Design entsprechen: Hersteller und Auftragsverarbeiter in die Pflicht nehmen

- **Dokumentation dieser Prozesse und Maßnahmen**

Durchlaufstelle (DLS) in Ö
Beispiel für „Rule of Law by Design“



- ✓ DLS ist eine Art Mailbox-System
- ✓ Transport- und Inhaltsverschlüsselung
- ✓ Automatische Protokollierung der Auskunftsvorgänge

Wichtig: DLS ist “blind” gegenüber Inhalten

CONCLUSIO

- Grundrechtsschutz ist in der derzeitige Fassung jedenfalls unzureichend
- Gegenseitigkeitsprinzip und Rechtsschutz in VO verankern
- Durchführung einer ordentlichen Datenschutz-Folgenabschätzung
- Vorgaben auf Basis der DSFA für „Datenschutz durch Technik“:
  - Grundlegende Bestimmungen in der Verordnung
  - Evtl. delegierter Rechtsakt zur näheren Bestimmungen der Sicherheitsvorgaben
  - Bestimmungen zur technischen Umsetzung und Evaluierung/Zertifizierung

Ing. Dr. iur. Christof Tschohl
Obmann

christof.tschohl@epicenter.works

Epicenter.Works – Zivilgesellschaft wirkt
Widerhofergasse 8/2/4
1090 Wien
www.epicenter.works

RESEARCH INSTITUTE
DIGITAL HUMAN RIGHTS CENTER
&
SMART RIGHTS CONSULTING

Forschungszentrum an der Schnittstelle von Recht, Technik und Gesellschaft

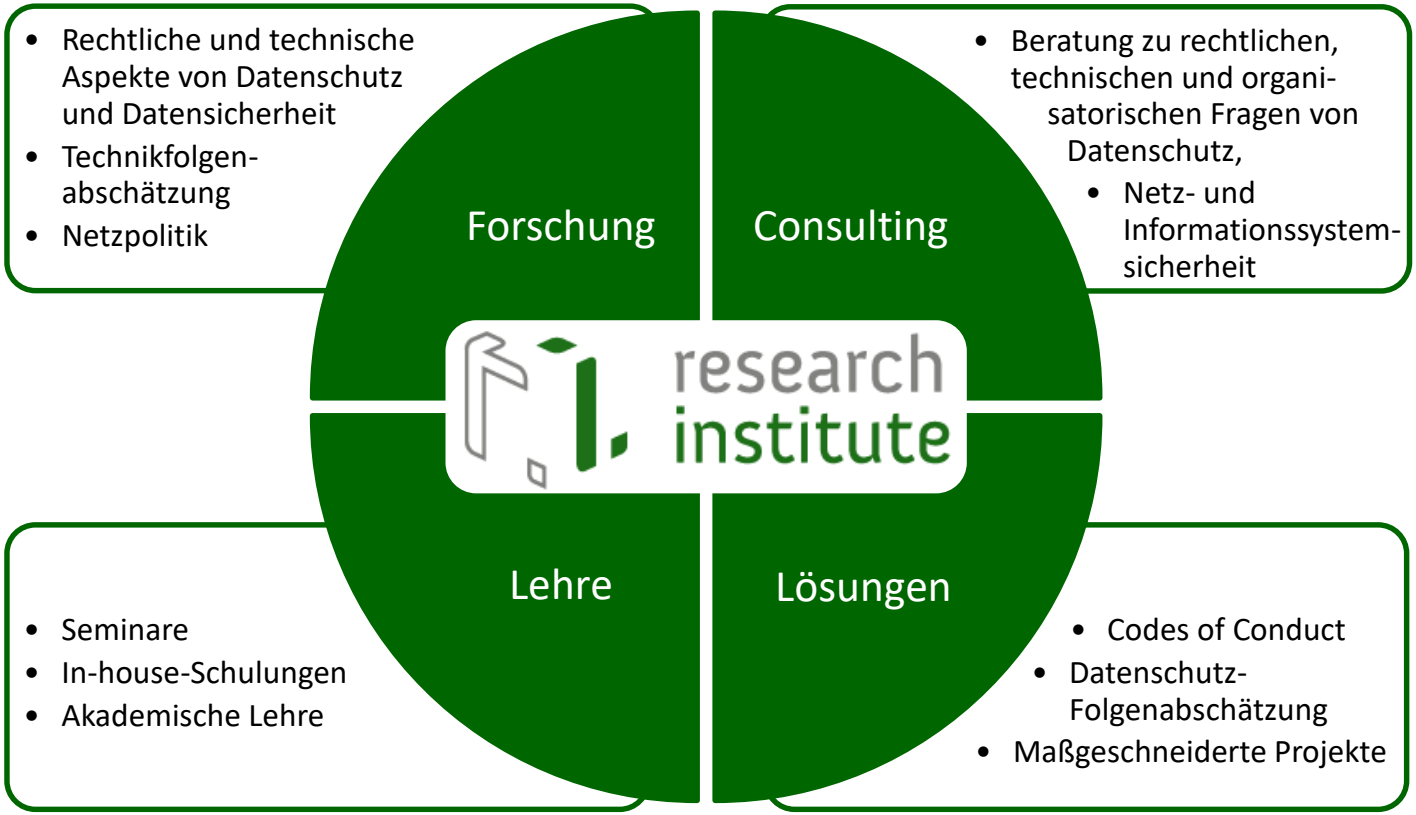
Ing. Dr. iur. Christof Tschohl
Wissenschaftlicher Leiter | Gesellschafter | Prokurist
christof.tschohl@researchinstitute.at

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

Widerhofergasse 8/2/4
1090 Wien
www.researchinstitute.at

Research Institute
Digital Human Rights Center

Forschungszentrum an der Schnittstelle von **Recht, Technik** und **Gesellschaft**



- Rechtliche und technische Aspekte von Datenschutz und Datensicherheit
- Technikfolgen-abschätzung
- Netzpolitik

- Beratung zu rechtlichen, technischen und organi-satorischen Fragen von Datenschutz,
  - Netz- und Informationssystem-sicherheit

- Seminare
- In-house-Schulungen
- Akademische Lehre

- Codes of Conduct
- Datenschutz-Folgenabschätzung
- Maßgeschneiderte Projekte

Research Institute. Menschenrechte im digitalen Zeitalter.