

## **NEXT GENERATION INTERNET (NGI)**

NGI TALKS #1: DATA PRIVACY AM 27. NOVEMBER 2018

Die Bedeutung der Datenschutz-Grundverordnung (DSGVO) und ein Ausblick in die künftige Technologie-Entwicklung:

Datenschutz durch Technikgestaltung und Voreinstellungen Artikel 25 DSGVO ("privacy by design & by default")

Ing. Dr. iur Christof Tschohl

Research Institute AG & Co KG Zentrum für digitale Menschenrechte

Web: <a href="https://www.researchinstitute.at">https://www.researchinstitute.at</a>



## 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)
- o 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



# **GRUNDRECHTLICHER SCHUTZ**

- Datenschutz ist ein Grundrecht:
  - Art 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



# **EU-DATENSCHUTZREFORM: ERGEBNIS UND STATUS QUO**

#### O 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; gilt seit 25. Mai 2018
- Ziele und Grundsätze der DSRL gelten in der DSGVO fort

#### Nationales Datenschutzrecht

 Umfassende Änderung des Datenschutzgesetzes (DSG), BGBI I 2017/120, BGBI I 23/2018, BGBI I 24/2018



Schutzgut sind nicht die Daten selbst, sondern verschiedene grundrechtlich geschützte Sphären der Menschen, über die Informationen verarbeitet werden Z.B. Privatsphäre, Opferschutz, Antidiskriminierung, faires Verfahren, ...

Datenschutz ist eine Art

Katalysator für alle Menschenrechte

und die Würde des Menschen

"Human Dignity by Design"



# Datenschutz ist nicht Selbstzweck sondern Voraussetzung für

das Funktionieren einer freien demokratischen Gesellschaft und die Ausübung zahlreicher anderer Grundrechte

Datenschutz ist einer **Abwägung**zugänglich – das Grundrecht gilt nicht
vorbehaltslos, aber unter **Gesetzesvorbehalt**:

"Rule of Law by Design"



# "Wer nichts zu verbergen hat, hat auch nichts zu befürchten"?

Umkehrung der Rechtfertigungslast:
Verletzt liberales Prinzip der
Europäischen
Menschenrechtskonvention (EMRK)

Risiko der Fehlinterpretation mit nachteiligen Folgen für die Person



# **W**AS WIRD GESCHÜTZT?

- "Personenbezogene Daten": alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ("betroffene Person") beziehen, z.B.: Alter, Beruf, Anschrift, IP-Adressen (EuGH C-582/14)
- Besonders geschützt sind dabei "sensible Daten" (besondere Kategorien personenbezogener Daten): Daten über rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit; Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung
- Wichtig: die Begriffsdefinition ist weit → der Informationszusammenhang ist beachtlich: zB Mitgliedschaft in Gruppen oder Nutzer bestimmter Apps geben schon dadurch allenfalls sensible Informationen preis



# GRUNDLAGEN ZUR RECHTFERTIGUNG DER VERARBEITUNG

- Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage
- Die Verarbeitung personenbezogener Daten ist zulässig wenn
  - eine klare gesetzliche Grundlage zur Verarbeitung besteht
  - die Verarbeitung zur Erfüllung oder zur Vorbereitung eines Vertrags erforderlich ist
  - der Betroffene seine Einwilligung gegeben hat,
  - überwiegende berechtigte Interessen eines anderen an der Verarbeitung vorliegen.
- Oft besteht eine "hybride" Rechtfertigung: zB gibt es einen Vertrag (zB Arbeitsvertrag), dessen Abschluss bestimmte gesetzliche Verpflichtungen zur Datenübermittlung vorsehen
- Am wichtigsten ist die ZWECKBINDUNG: nur eine Verarbeitung für legitime, eindeutige bestimmte Zwecke kann gerechtfertigt sein
  - Die Zweckbindung bestimmt letztlich auch das Löschkonzept
  - Wie lange Daten verarbeitet werden dürfen, hängt vom Zweck ab
- Datenverwendung durch staatliche Behörden nur aufgrund von Gesetzen, die notwendig iSd Art 8 Abs. 2 EMRK sind (öffentliches Interesse)



## **DATENSCHUTZ - EINWILLIGUNG**

### Einwilligung

- Artikel 4 Ziffer 11 DSGVO: "Einwilligung" der betroffenen Person: "jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist"
- Die Verwendung personenbezogener Daten verletzt keine schutzwürdigen Interessen des Betroffenen, wenn dieser seine Zustimmung erteilt hat
- = höchstpersönliches Recht, d.h. Zustimmungserklärungen können nicht im Wege der Stellvertretung, z.B. durch die Eltern, rechtswirksam abgegeben werden (vgl. Dako 2016/13).
- Die Einwilligung ist auch konkludent möglich! Ausnahme: Bei besonderen Datenkategorien
- Voraussetzung:
  - Kenntnis der Sachlage
  - Einsichts- und Urteilsfähigkeit (wird bei mündigen Minderjährigen vermutet, analoge Anwendung des § 173 ABGB)



# BEDINGUNGEN DER EINWILLIGUNG (ART 7 DSGVO)

#### Informierte Einwilligung

- Anforderungen an das Ersuchen um Einwilligung
  - o in verständlicher und leicht zugänglicher Form
  - o in einer klaren und einfachen Sprache
  - o von den anderen Sachverhalten klar zu unterscheiden
  - Zweck der Datenanwendung und Datenarten
  - o Übermittlungsempfänger und Übermittlungszwecke
- Beweislast des Verantwortlichen, die Einwilligung nachzuweisen
- Getrennte Einwilligung für verschiedene Zwecke (vgl. Art 7 Abs. 2 DSGVO und ausdrücklich Erwägungsgrund 32)
- Keine Junktimierung: wenn die Datenverarbeitung zur Vertragserfüllung nicht erforderlich ist ("Koppelungsverbot", Art 7 Abs. 4 DSGVO)
- Hinweis auf jederzeitigen Widerruf



## ALLE WOLLEN BIG DATA...

### "Big data is like teenage sex:

- o everyone talks about it,
- o nobody really knows how to do it,
- o everyone thinks everyone else is doing it,
- so everyone claims they are doing it..."

(Dan Ariely, Duke University)

...and if you don't be careful, it can go terribly wrong!



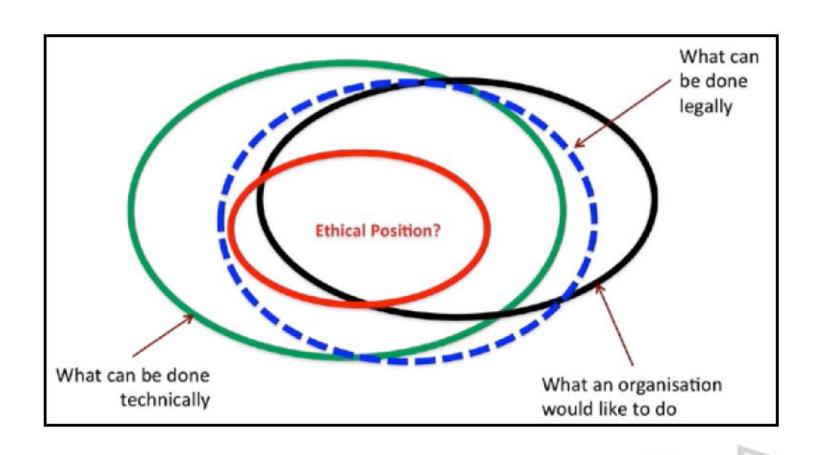
# BIG DATA: DATENSCHUTZRECHTLICHE HERAUSFORDERUNG

Im Zusammenhang mit Big Data stellen sich vielschichtige datenschutzrechtliche Fragen:

- Grundfrage: Datenschutzrecht nur anwendbar, sofern personenbezogene Daten vorliegen → Personenbezug?
- → Bestimmbarkeit d. Personenbezugs (Zusatzwissen: absolute/objektive vs. relative/subjektive Theorie; zuletzt EuGH Rs C-582/14 Breyer; s.a. BGH VI ZR 135/13)
- Kollidiert prima vista mit den Grundprinzipien des Datenschutzrechts: - Zweckbindung, - Datenminimierung, - Speicher(dauer)begrenzung, - Richtigkeit, - Rechtmäßigkeit, - Transparenz
- Rechtsgrundlage für die Datenverarbeitung erforderlich: Zustimmung möglich? Oft nicht praktikabel, da retrospektiv und Einholung "unmöglich"; wissenschaftliche Forschung?; Art 6 Abs 1 lit f DSGVO
- datenschutzrechtliche Zulässigkeitsprüfung: konkretes Big Data-Projekt in den zeitlichen Ablaufphasen zu beurteilen: Datenermittlung, -verarbeitung und -nutzung



# BIG DATA: DATENSCHUTZRECHTLICHE HERAUSFORDERUNG







# DATA PROTECTION BY DESIGN PRAKTISCHE UMSETZUNG

- 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



## RECHTSDURCHSETZUNG

## **UND DURCHSETZUNGSWEGE**

DAMIT ES NICHT NUR DIE KLEINEN TRIFFT...

# DPC / 1. VERFAHREN Max Schrems vs Facebook

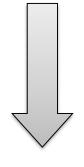


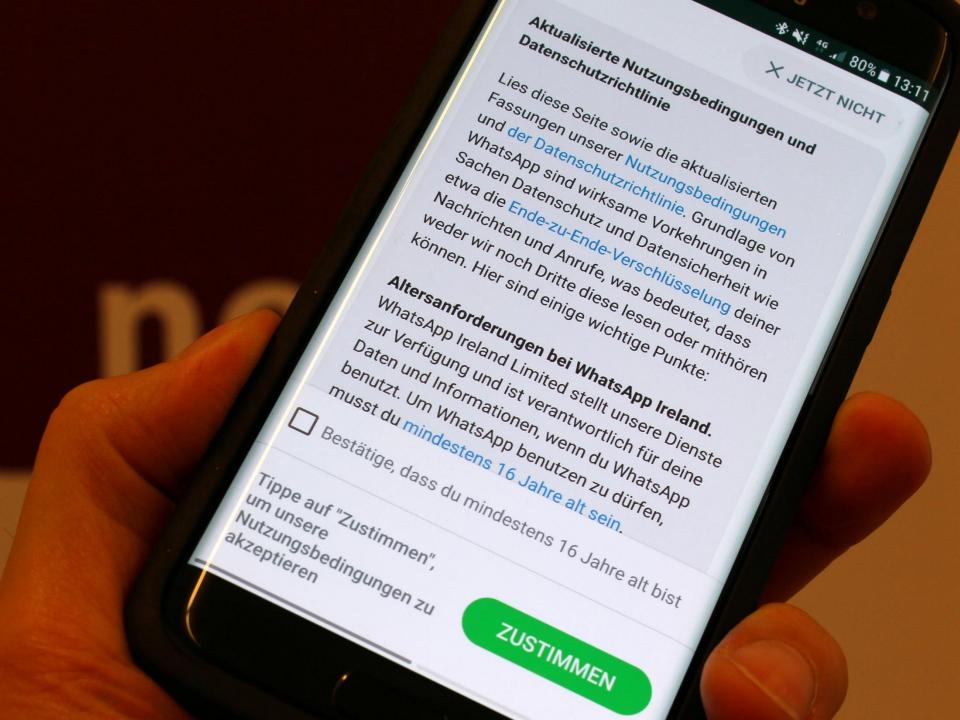
- Beschwerde (2013)
- Zurückweisung (2013)
- Klage High Court (2013)
- Vorlage (2013)
- EuGH Entscheidung (Oktober 2015)
- Neue Beschwerde (Dezember 2015)
- Zwischenentscheidungs-Entwurf (2016)
- Verhandlung (5 Wochen) (2017)
- Zweite EuGH-Vorlage (2018)





- District Court (Irland)
- High Court (Irland)
- Supemre Court







# **OPTION:** DATENSCHUTZ-NGOS VERTRETEN NACH ART 80



# **ARTIKEL 80 - NGOs**

- Absatz 1: Mandatierte NGOs
- Absatz 2: Abstrakte Klagen

- "Massenmandatierung" nach Abs 1:
  - Keine Zession nötig
  - Konzentration auf eine NGO ohne eingriff in die Rechtsbeziehung
  - Prozesskosten (in Österreich) erhöht



#### FRANCAIS:

#### PLAINTE AU TITRE DE L'ARTICLE 77(1)

#### 1. FAITS

#### 1.1. Responsable du Traitement / Défendeur

Cette plainte est dirigée contre Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irlanderesponsable de l'application "Instagram" et du site internet instagram.com.

#### 1.2. Personne concernée / Demandeur

La personne concernée nous a mandatés (l'association noyb – Centre Européen pour les Droits Numériques) afin de la représenter conformément à l'article 80, paragraphe 1 du RGPD (Pièce 1).

### 1.3. Objet du consentement allégué (À quoi la personne concernée a-t-elle prétendument consenti?)

Le Responsable du Traitement utilise une politique d'utilisation des données (Pièce 2) ainsi que des conditions générales d'utilisation (Pièce 3) qui sont applicables à compter du 25 mai 2018 et auxquelles la personne concernée a dû consentir.

Les politiques de confidentialité incluent entre autres des catégories spéciales de données au titre de l'article 9(1) du RGPD. En effet, les données des smartphones comprennent inévitablement des informations sur les croyances politiques.

#### DEUTSCH:

#### BESCHWERDE NACH ARTIKEL 77(1) DSGVO

#### 1. SACHVERHALT

#### 1.1. Verantwortlicher / Beschwerdegegenerin

Diese Beschwerde richtet sich gegen Facebook Ireland Ltd, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland – Verantwortlicher für das Soziale Netzwerk "Instagram", instagram.com.

#### 1.2. Betroffene Person / Beschwerdeführender

Der Betroffene hat uns (den gemeinnützigen Verein noyb – Europäisches Zentrum für digitale Rechte)beauftragt, ihn nach Artikel 80 Abs 1 DSGVO zu vertreten ("Beauftragung" als Anlage 1).

# 1.3. Gegenstand der vermeintlichen Einwilligung (Wozu gab der Betroffene vermeintlich seine Einwilligung?)

Der Verantwortliche nutzt eine Datenschutzrichtlinie (Anlage 2) und Nutzungsbedingungen (Anlage 3), die ab dem 25. Mai 2018 gültig sind und denen die betroffene Person zustimmen musste.

Die Datenschutzrichtlinien umfassen auch spezielle Datenkategorien gemäß Artikel 9 Abs 1 DSGVO, da die betroffene Person als Nutzer von Instagram mit vielerlei Gruppen und Einzelpersonen interagiert hat, die bei einer Informal English Translation:

#### COMPLAINT UNDER ARTICLE 77(1) GDPR

#### 1. FACTUAL BACKGROUND

#### 1.1. Controller / Respondent

This complaint is filed against Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland-the operator of the application "Instagram" and instagram.com.

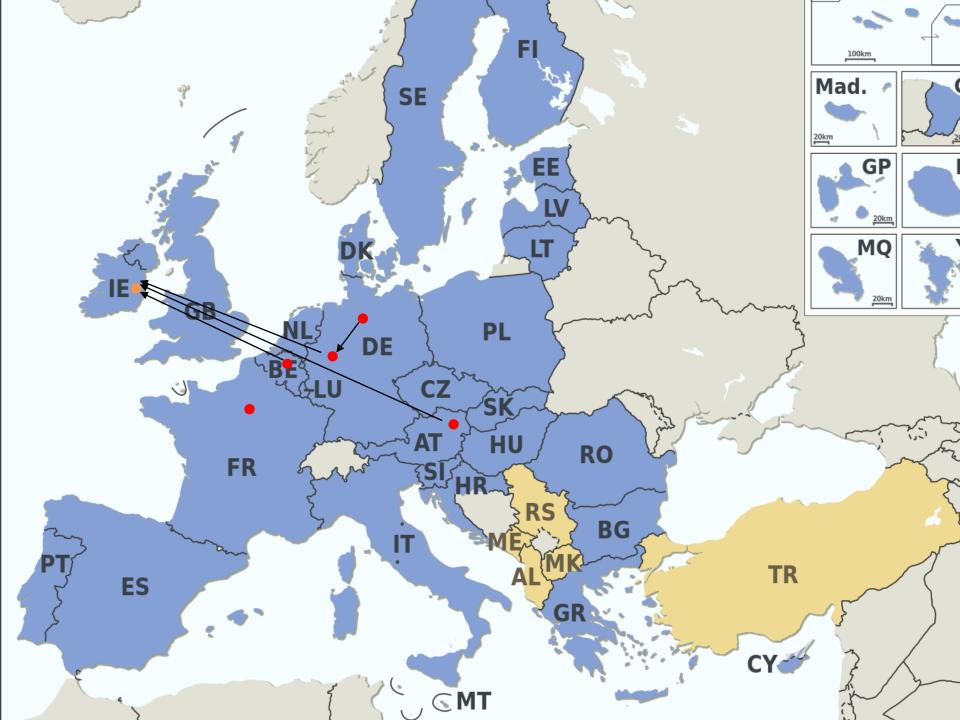
#### 1.2. Data subject / Complainant

The data subject has requested us (the non-profit noyb – European Center for Digital Rights) to represent him under Article 80(1) of the GDPR (attachment 1).

### 1.3. Subject of the alleged consent (What did the data subject allegedly consent to?)

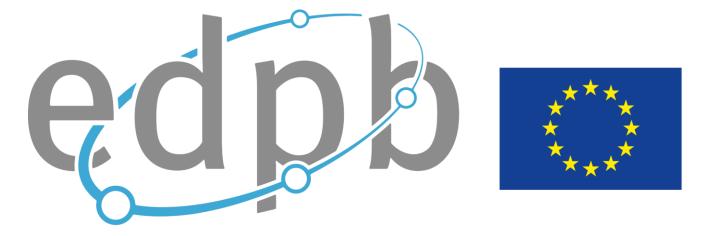
The controller uses a privacy policy (attachment 2) and terms of service (attachment 3) that are applicable from May  $25^{th}$  2018 onwards, which the data subject had to agree to.

The policies also include special categories of data under Article 9(1) of the GDPR, because the data subject, as an existing user of Instagram, has developed interactions with various groups and individuals, which could accordingly reveal the data subject's political affiliation, sexual



# **Durchsetzungswege in Europa**



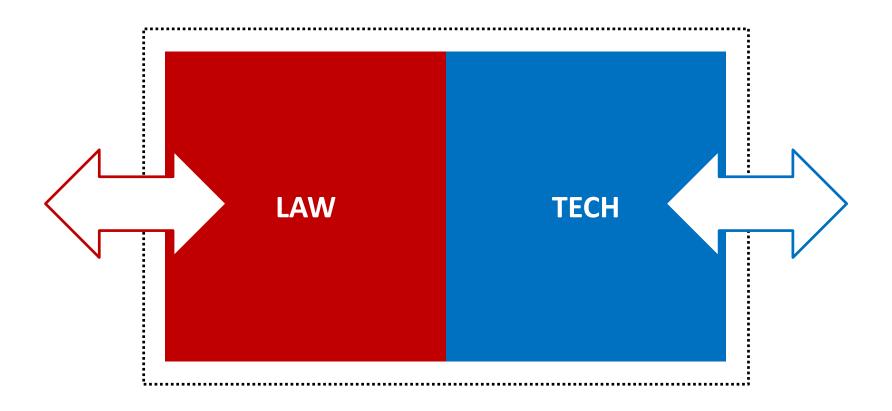


**European Data Protection Board** 



# **EDPB VERFAHREN**

- Verfahrensrechte vor Einbringungsbehörde
- Verfahrensrecht vor "Lead Authority"
- Verfahrensregeln vor EDPB
- ...?







Hackers
IT-Community
Privacy Bounties
Whistleblowers
Access Requests
Research & Testing

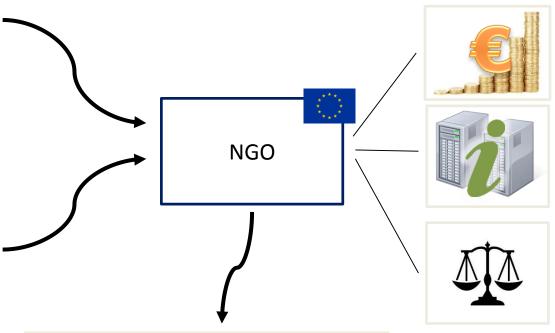
...



Foundations
Crowd Funding
Donations
Class Actions
Industry Funding

DPAs / Consumer Rights Groups Abstract Lawsuits & Complaints Class Actions / Individual Cases Campaigns / Education





#### Support Us!

We are mainly funded by supporting members. We have passed our minimal funding goal of €250.000 through a kickstarter-like campaign in January 2018, but we are still seeking to reach our funding goal of € 500.000 by the end of 2018 to pay for lawyers, staff and alike.

We raised 370.112 Euro of the 500.000 Euro goal (75%)

mini noyb 250.000 Euro full noyb 500.000 Euro

#### Join noyb as a Supporting Member!

Updates

In order to get *noyb* off the ground, we need stable, long-term funding for a core team of experts. You can play an integral part in this task by joining *noyb* as a supporting member. We are grateful for any amount you want to invest in *noyb*. Our supporting members will receive thank-you gifts, based on the amount of their contribution. Please understand that some goodies will change over time (\*).

100% Risk-Free Membership: We want you to feel absolutely comfortable in becoming a long-term supporting member of noyb:

– We offer a 14 day money back guarantee (in the unlikely event that you decide that actually privacy is not your thing).

- Finally, you can also cancel your membership at any time after these 14 days - with just one click



#### **Gold Supporting Member**

Support povb with € 100 per year or more

- · Invest in the future of your privacy
- . nout Gold member card
- . noyb Gold welcome box

#### **Silver Supporting Member**

Support noyb with € 50 per year or more

- Invest in the future of your privacy
- noyb Silver member card
- novb Silver welcome letter

#### Basic Supporting Member

Support povb with up to € 50 per year.

- Invest in the future of your privacy
- novb welcome ema



# **EUGH:** ALLE WEGEN FÜHREN NACH LUXEMBURG...





# ABSCHLUSS / AUSBLICK



- Interdisziplinärer Austausch Technologie/Gesellschaft/Recht
- V Technikfolgenabschätzung Risikoabschätzung
- V Klarer normativer Rahmen transparente Vertragsgestaltung
- Stärkere Verantwortung von Unternehmen
- Privacy & Security by Design

**Gesamtheitliche Sicht:** 

**Human Dignity by Design & Rule of Law by Design** 







# RESEARCH INSTITUTE AG & CO KG ZENTRUM FÜR DIGITALE MENSCHENRECHTE

Forschung und Beratung an der Schnittstelle von Technik, Recht und Gesellschaft

### 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

#### Dr. Heidi Scheichenbauer

Senior Researcher | Senior Consultant heidi.scheichenbauer@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 ZENTRUM FÜR DIGITALE MENSCHENRECHTE

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 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 renommierten Partnern auf nationaler und internationaler
   Ebene.



## RECHTLICHE HINWEISE

Zweck: Dieses Dokument dient als Trainingsunterlage.

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

#### 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 Urheberschutzrechtes 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 Tschohl 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.

Kontaktdaten: walter.hoetzendorfer@researchinstitute.at