Universität Wien
Fakultät für Rechtswissenschaften

Wahlfachkorb Technologierecht
Ringvorlesung

Internet und Datenschutz

10. Oktober 2017

Ing. Mag. Dr. iur. Christof Tschohl

1

Der Referent / die Referentin

- Ing. Mag. Dr. iur. Christof Tschohl (36)
- Nachrichtentechniker (HTL, 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 Organisationsberatung – 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 (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
  - Open Government Data Austria (OGD), Mitglied des wissenschaftlichen Beirats
  - Amnesty International, Mitglied

2

Grundlagen

Struktur des Internets und jüngere technische und gesellschaftliche Entwicklungen

3

research institute

Zwecke des Datenschutzes

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, geheimes Wahlrecht,...

Die Frage der „Digitalen Menschenrechte" geht über Datenschutz hinaus:

- Online-Versammlungsfreiheit, Online-Meinungsfreiheit, Recht auf Netzzugang, Netzneutralität,...

Nur wenige Grundrechte gelten vorbehaltslos – Eingriff z.B. durch gesetzliche Auskunftspflichten von Telekomanbietern an Sicherheitsbehörden

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

- Umkehrung der Rechtfertigungslast verletzt liberales Prinzip der Verfassung
- Stärkung des Menschenrechtsbewusstseins

4

research institute

WEB 2.0 und soziale Medien

WEB 2.0	• "Mitmach-Internet" – Entwicklung seit 2003 • Inhalte im www auch von Nutzern ohne technische Spezialkenntnisse möglich
Beispiele für WEB 2.0 Anwendungen	• Youtube, Wikipedia, Flickr (Bilder), Blogs • Soziale Medien: Facebook, Twitter, Linkedin
Kommunikation statt nur Konsum	• Gemeinsames Arbeiten, Denken, Gestalten • Soziale und politische Dimension des "Web"

5

research institute

Das Internet: Architektur und Dienste

Internet:

- Infrastruktur aus Teilnetzen die über Knoten verbunden sind
- Eigenschaften: nicht hierarchisch, redundant, neutral (?)

World Wide Web (www):

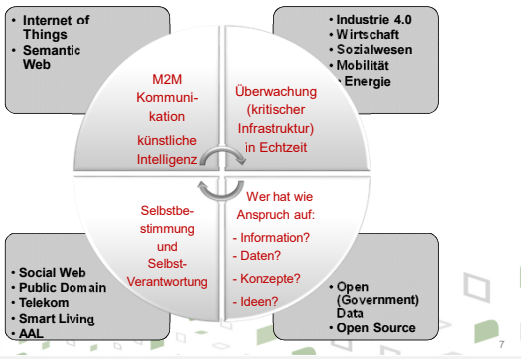
- Der verbreitetste Dienst, praktisch synonym für Internet
- Inhalte verbreiten via "hyper text transfer protocol" (http)

Andere wichtige Dienste des Internet zB:

- E-Mail ("simple mail transfer protocol", smtp)
- Datenübertragung via "file transfer protocol" (ftp)

6

Anwendungsfelder und neue Entwicklungen



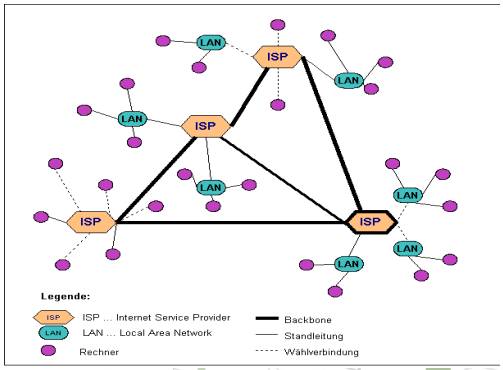
7

Das Internet der Dinge

Quelle: www.das-vernetzte-leben.de/internet-der-dinge-kritik/

8

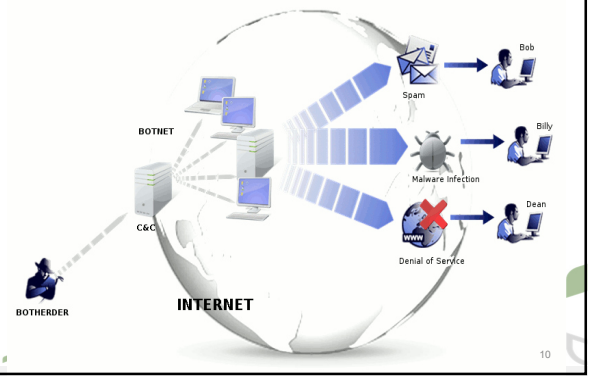
Aufbau und Struktur des Internet



9

research institute

Das Konzept „Botnet“



10

research institute

Phänomene der „Cyber-Kriminalität“

Botnet: Ferngesteuertes Netzwerk aus infizierten Rechnern (Computervirus)

Phishing: e-Mail Betrug gegen Leichtgläubige

Medienkompetenz Führerschein?

Bildungsmängel (Lesen, verstehen)

Haftung für Anschlussinhaber?

11

research institute

Verfügbare Daten und Informationen mit Relevanz für Ermittlungen

- Inhalte der Kommunikation
- Abgerufene Informationen

Inhaltsdaten

Verbindungs-daten

- Wer mit wem, Zeit+Dauer, Ort, welcher Dienst
- Metadaten

- Persönlichkeits-Profile
- Sozialprofile
- Sensible Daten

Abgeleitete Daten

Problem: Wenn ein Angriff von einem “Botnet” kommt, jagt man nach der IP-Adresse nicht den Täter sondern ein anderes Opfer !

12

research institute

Die Ermittlungsschritte rund um die IP-Adresse, oder: Inhaltsüberwachung über die Bande und um die Ecke

Woher haben Ermittler "die IP-Adresse"? Zusammenhang mit konkretem Dienst/Inhalt?

Inhalt/Zusammenhang/Dienst ist bereits bekannt – es fehlt die Verbindung zum Urheber

"Lenkererhebung" auf dem Datenhighway – IP Adresse identifiziert nur den Vertragspartner zu einem ("gekaperten"?) Internetanschluss

13

research institute

Herausforderungen in Bezug auf „neue Ermittlungsmethoden"

„Dualtät" der Methoden zur Datensicherheit	• Die selben Methoden der Datensicherheit können auch Verbrechern zur „digitalen Spurenverwischung" dienen • Bsp Verschlüsselung und „Virtual Private Network" (VPN): Standard für jede kritische Anwendung → wenn durch Kriminelle genutzt spricht man von „Darknet"
Zuverlässigkeit ist begrenzt und manipulationsanfällig	• Bsp Standortdaten von Mobiltelefonen – Kontrollfrage: können Standortdaten auch die Unschuld beweisen? • Sonderproblem „IP-Adresse": Täter oder Person mit schlechtem PC-Virenschutz? → Gefährdungshaftung für einen Internetanschluss (ähnlich EKHG)?
Tendenz zur Automatisierung (zB zur Mustererkennung, va präventiv)	• Algorithmen und Programme zur automatisierten Erkennung „verdächtiger Aktivitäten" im Internet? • Wieviel Gewicht hat die menschliche Entscheidung? Wieviel Aufwand leisten Ermittler zur Widerlegung eines automatisch generierten Verdachts?

14

research institute

Gegenstand SIND DATEN AUS DER „PUPLIC DOMAIN"

Alles was im Internet frei zugänglich ist: online Medien, social media, Profession und Academia, Geodaten, Öffentliche Daten (Umwelt)…

Zweck: Früherkennung von Sicherheitsbedrohungen (online & afk) durch Mustererkennung in den riesigen Datenbeständen

Moderne Tendenz zur Nutzung von OSINT Tools für polizeiliche Aufklärung von Straftaten – Geheimdienstmethoden in der Strafverfolgung

Probleme:

- Öffentlich verfügbar = keine schutzwürdigen Geheimhaltungsinteressen (vgl. § 1 Abs. 1 DSG 2000) – siehe aber die Judikatur in Europa: weitere Verknüpfung ist neue Anwendung
  - EGMR, Rotaru v. Romania (28341/95), 3.5.2000
  - EuGH, Google Spain (C-131/12), 13.5.2014
- OSINT-Tools geben die Ermittlungsalgorithmen vor – Anbieter sind aber zumeist private Unternehmen (demokratische Legitimation?)
- Zusammenhang mit Cybercrime und die Frage der Zuverlässigkeit der Ergebnisse – zB falsche „digitale Fährten" durch Identitätsdiebstal uä

15

Datenschutz als Grundrecht / Menschenrecht

16

Moderne Grundrechte mit ausdrücklichem Bezug zur „digitalen Welt“

- **Grundrecht auf Datenschutz**
  - Ausdrücklich in Artikel 8 Grundrechte-Charta der EU garantiert
  - Recht auf Privat- und Familienleben parallel in Artikel 7 Grundrechte-Charta
  - Artikel 1: § 1 Datenschutzgesetz 2000 im Verfassungsrang (Datenschutzgrundrecht)
  - Verfassungsgerichtshof im „Vorratsdaten“-Urteil: „Recht auf informationelle Selbstbestimmung“
- **Deutschland:**
  - **Grundrecht auf „Informationelle Selbstbestimmung“**
  - **Grundrecht auf Vertraulichkeit und Integrität von Computersystemen**
    - Bundesverfassungsgericht schafft ein neues „Grundrecht auf Vertraulichkeit und Integrität von Computersystemen„ (kurz „Computer-Grundrecht“ – Entscheidung zum „Bundestrojaner“)
      - **Datenschutz ist nicht Selbstzweck – eher ein „Katalysator“**
        - **zum Grundrechtsschutz in allen Bereichen**
- **UN Menschenrechtsrat hat per Resolution A/HRC/20/L.13 klargestellt, dass alle Menschenrechte auch Online gelten → neuer Sonderberichterstatter eingerichtet!**

17

Selbstbestimmung und Eigenverantwortung in der digitalen Welt

Deutschland: Recht auf informationelle Selbstbestimmung (Art 1+2 GG)
Österreich: Grundrecht auf Datenschutz (§ 1 DSG)

Praktische Herausforderungen

Was einmal im Netz zugänglich ist, kann theoretisch endlos dupliziert werden

Kontrolle des Individuums über Datenverwendung in sozialen Netzwerken?

Eigenverantwortliches *Management der „digitalen Identität“ (Profil)*

Informierte Zustimmung und Verletzung der Zweckbindung: Aus der Initiative „Europe vs Facebook“ von Max Schrems – vgl. „Safe Harbour“ Urteil des EuGH (Große Kammer), 6.10.2015 („Schrems vs Irish Data Protection Commissioner “) C-362/14

Vgl. auch die Diskussion um das „Recht auf Vergessenwerden“
derzeit explizit nur Recht auf Richtigstellung und Löschung im Einzelfall
Vgl aber Urteil des EuGH (Große Kammer), 13.5.2014 „Google Spain“ C-131/12

18

Recht auf Richtigstellung und Löschung
Recht auf "Vergessenwerden" II

- ✓ **„Recht auf Vergessenwerden":** Urteil des **EuGH** (Große Kammer) vom 13. Mai 2014 in der Rechtssache C-131/12, **Google Spain** SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González
  - Bemerkenswert: Google unterliegt der EU Jurisdiktion und dem Datenschutzrecht, auch wenn in der EU nur eine Vertriebsniederlassung liegt
  - Trefferliste zur Personensuche ist eine neue Informationskategorie und lässt das "Schutzwürdige Geheimhaltungsinteresse" (vgl. § 1 DSG) "wieder aufleben"
  - Bedeutung für Ausnahme "öffentlich verfügbarer Daten" aus dem Schutzbereich?

19

Vorratsdatenspeicherung, oder: das Wechselbad der Paradigmen

EU Richtlinie 2006/24/EG: Öffentliche elektronische Kommunikation

- **Verbindungsdaten: wer, mit wem, wann, wie lang, wo, welcher Dienst**
- **Internet-Zugang: IP-Adresse zu einem bestimmten Zeitpunkt**
- **Flächendeckend auf Vorrat, ohne konkreten Verdacht oder anderen Grund**

Grundrechtseingriff ist unverhältnismäßig und daher nicht gerechtfertigt

- Pauschale Speicherung ohne Anlass und ohne Ausnahme ist überschießend
- Betrifft Privatsphäre, Datenschutz und freie Meinungsäußerung
- Besonderes Problem: Berufsgeheimnisse können umgangen werden

Aufhebung durch den Gerichtshof der EU (EuGH) am 8.4.2014

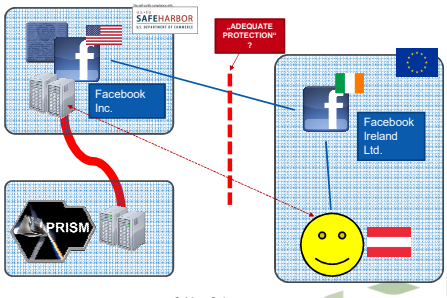
- Ua aufgrund österr. "Massenbeschwerde" an VfGH durch 11.139 Menschen
- Vorratsdatenspeicherung nach RL nicht vereinbar mit den EU Grundrechten
- Strafverfolgung zwar legitimes Ziel, Maßnahme aber überschießend
- Allfällige neue Richtlinie wird das Grundkonzept ändern müssen

20

Marktmacht und Rechtsdurchsetzung
zB Initiative „Europe vs Facebook" (Max Schrems)

21

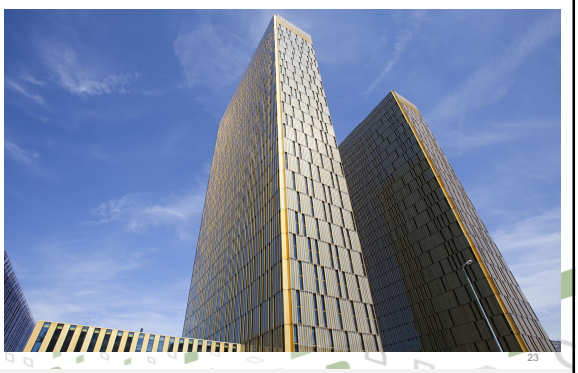
Zusammenhänge Datenschutz Beschwerdeweg EU - USA



© Max Schrems

22

Der Gerichtshof der Europäischen Union (EuGH)



23

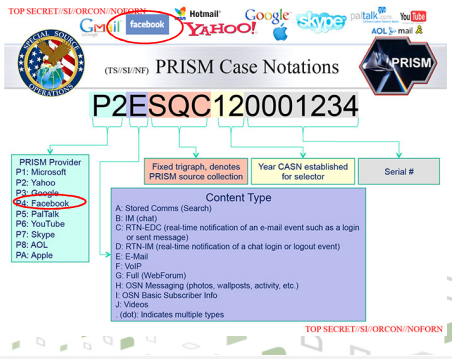
Vorabentscheidungsverfahren vor dem EuGH Gegenstand und Fragen

- **Entscheidung 2000/520 der Kommission auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46 (sog. „Safe Harbor Decision")**
  - Angemessenes Schutzniveau besteht für einen US-amerikanischen Auftraggeber oder Dienstleister, wenn der für die Verarbeitung Verantwortliche die „Grundsätze des ‚sicheren Hafens' zum Datenschutz (vorgelegt vom amerikanischen Handelsministerium am 21. Juli 2000) beachtet
  - „Selbst-Zertifizierung" mit Bestätigung durch das US Handelsministerium
  - einseitige Anerkennung durch die EU Kommission (kein „Abkommen" im rechtlichen Sinn)
- **Wesentliche Fragen:**
  - Hat die nationale Datenschutzbehörde Spielraum zur Prüfung im Einzelfall? (Rechtssicherheit?)
  - Ist die Entscheidung 2000/520 der Kommission „post-Snowden" noch als mit der EU Grundrechte-Charta vereinbar zu sehen? (inzidente Normenkontrolle des EuGH)

24

research institute

Zusammenhang mit „Snwoden-Leaks“



25

research institute

Entscheidung des EuGH „Schrems C-362/14“ oder „Safe Harbor“-Urteil

- ✓ Rz 94: Insbesondere **verletzt** eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den **Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens**
- ✓ Rz 95: Desgleichen **verletzt** eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den **Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz**.

26

research institute

Konsequenzen der Save Harbor Entscheidung des EuGH „Schrems C-362/14“

- ✓ Aufhebung der „Save Harbor“ Entscheidung 2000/520 der Kommission
- ✓ Nationale Datenschutzbehörden dürfen durch auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46/EG ergangene Entscheidungen nicht beschränkt werden (Überschreitung der Zuständigkeit durch die Kommission)
- ✓ Nachfolgeregelung: „EU US Privacy Shield“

einige Verbesserungen

Problem im Kern unveränd

27

Neue Rechtsquellen auf EU-Ebene

- ✓ Datenschutz-Grundverordnung (DSGVO), VO 2016/679
  - Seit 24. Mai 2016 in Kraft; gilt ab 25. Mai 2018
  - Datenschutzrichtlinie (DSRL) tritt mit 25. Mai 2018 außer Kraft
  - Ziele und Grundsätze der DSRL gelten in der DSGVO fort
- ✓ Datenschutzrichtlinie für Polizei und Strafjustiz (DSRL-PJ), RL 2016/680
  - Erstmals einheitlicher Datenschutzrahmen für Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, Strafvollstreckung und Schutzes vor und Abwehr von Gefahren für die öffentliche Sicherheit (auch rein innerstaatliche Datenverarbeitung)
  - Seit 5. Mai 2016 in Kraft; von den Mitgliedstaaten bis 6. Mai 2018 umzusetzen
  - Rahmenbeschluss 2008/977/JI tritt mit 6. Mai 2018 außer Kraft

28

Grundverordnung und Richtlinie als Gesamtpaket

29

Datenschutz-Grundverordnung: Überblick

Verschärfung der Sanktionsmechanismen

- Strafdrohung: Höchstbetrag auf 20 Millionen EUR oder 4 Prozent des weltweiten Jahresumsatzes des betroffenen Unternehmens (jeweils die höhere Summe)
- Auch immaterielle Schäden
- Verbandsklagen zulässig

Erhöhte Anforderungen an Datensicherheit

- Datenschutz-Policy und geeignete technische und organisatorische Maßnahmen, alle 2 Jahre zu überarbeiten.
- Verpflichtende Risikoanalysen Datenschutz-Folgenabschätzung
- kontinuierliches "Lifecycle Datenschutz-Management"

Datenschutz-Grundverordnung (DSGVO)

Materiell-rechtliche Änderungen

- zB IP-Adressen als personenbezogene Daten
- zB Allgemeine "Data Breach Notification"
- zB Recht auf „Vergessenwerden"
- zB Recht auf „Datenportabilität"

Verstärkte Kooperation der nationalen Datenschutzbehörden

- „One-Stop-Shop" Prinzip für Betroffene
- neues Gremium "European Data Protection Board" (vgl. Art. 29 Gruppe)
- Mehr Koordination und Kohärenz

30

Grundrechte als Determinanten der Technologieentwicklung

„Human Dignity by Design“

31

Rahmenbedingungen der „Smart City“
The Need of Smart Rights for Smart Citizens

1. Technologie dient den Menschen und der Gesellschaft
2. Konzept hat Auswirkungen auf das soziale Gefüge
3. Komplexität erfordert Werte und Orientierungsnormen

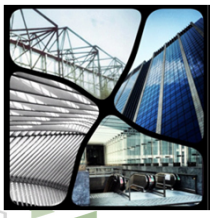
WERTE-RASTER oder die Suche nach dem kleinsten gemeinsamen Nenner in der Globalisierung

NORMATIVER RAHMEN birgt Dilemma zwischen Rechtssicherheit und notwendiger Dynamik

DATENSCHUTZ ist kein Selbstzweck → Katalysator für Grundrechte in der digital geprägten Welt

INFORMATIONSFREIHEIT UND TRANSPARENZ
Open Government Data / „wisdom of the croud“

KRITISCHE INFRASTRUKTUREN sind exponiert (IT-)Sicherheit im Spannungsverhältnis zu Freiheit



32

künstliche Intelligenz als „Entscheidungsträger“?

33

Chancen und Risiken – neue Dimensionen für Datenschutz und Datensicherheit

34

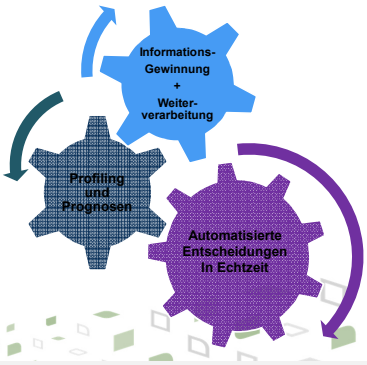
Grundsatzfragen

Gretchen trifft Big Data:
"Wie hältst du's mit der D e m o k r a t i e ?..."

Wer definiert die Standards?
ICANN, ITU, ETSI,... ?!
Who is who defines
"The Net" ?

Wer legitimiert Standars?
Oft: die normative Kraft des Faktischen

- der "freie Markt" ?!
- Die Gemeinschaft ?!
- Netzneutralität ?!
- Anonymität ?!



35

Privacy by Design und Privacy by Default

- „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen" (Art. 25 DSGVO, Art. 20 DSRL-PJ)
- Systematischer Ansatz zur Einhaltung der Datenschutzbestimmungen und um Datenschutzrisiken bereits im Vorhinein entgegenzuwirken
- Verpflichtung, „geeignete technische und organisatorische Maßnahmen zu treffen" um
  - Datenschutzgrundsätze und Datenschutzbestimmungen wirksam umzusetzen
  - Sicherzustellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden
- D.h. *bereits bei der Gestaltung der Systeme* sicherzustellen, dass
  - diese möglichst wenig in die Privatsphäre der Betroffenen eingreifen und
  - Eingriffe, die nicht dem Zweck des Systems entsprechen, *faktisch* wenn möglich gänzlich ausgeschlossen oder
  - ansonsten zumindest in den Defaulteinstellungen deaktiviert sind.
- Kernelement: Datenminimierung

36

research institute

Der „Human Rights Based Approach“ als Maxime der Technologie-Entwicklung

Menschenrechte: gemeinsame internationale Determinanten für neue Technologien – Konkretisiert durch Rechtsprechung

Menschenrechtskonvention als **„lebendiges Instrument“** (vgl. EGMR, Tyrer vs UK 1978)

UN Menschenrechtsrat: Resolution 2012 A/HRC/20/L.13 → **alle MR gelten auch „online“**

Unteilbarkeit der Menschenrechte: Immer das große Ganze sehen – **Balance und Grundsatz der Verhältnismäßigkeit**

37 37

research institute

Notwendige Schritte auf dem Weg zur menschenwürdigen „Smart City“

Entwicklung der Konzepte und des Marktes

Definition **Rechtsrahmen und ethische Grundsätze**

soziale Verantwortung (CSR) durch die gesamte Wertschöpfungskette

Staatliche **Schutz- und Gewährleisungs-pflichten**

Stärkung der **Eigenverantwortung** der Menschen durch **Bildung** und **Kompetenz im Umgang mit Technologie**

38 38

research institute

Abschluss / Ausblick

- ✓ **Interdisziplinärer Austausch Technologie/Gesellschaft/Recht**
- ✓ **Wirkungsfolgenabschätzung Risikoabschätzung**
- ✓ **Klarer normativer Rahmen transparente Vertragsgestaltung**
- ✓ **Stärkere Verantwortlichkeit von Unternehmen**
- ✓ **Thinking by Design**

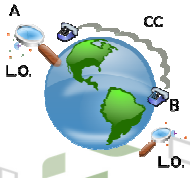
Human Dignity by Design

Zeitalter der „Aufklärung 2.0“ und der Ausweg aus der (selbstverschuldeten?) Unmündigkeit: wir sind NICHT machtlos!

39

VIELEN DANK

FÜR IHRE AUFMERKSAMKEIT!



40

Kontakt

Research Institute AG & Co KG

- **Die Gesellschafter:**
- Georg Benedikt Schmidt (Vorstand)
- georg.schmidt@researchinstitute.at
- Ing. Dr. Christof Tschohl (Wissenschaftliche Leitung, Prokurist)
- christof.tschohl@researchinstitute.at

- Annagasse 8, 1010 Wien
- Tel: +43 (650) 7503718
- Fax: +43 (1) 48 0 49 83 – 2400
- office@researchinstitute.at
- http://www.researchinstitute.at

41

Backup und Nachlese: Weitere Informationen zur EU Datenschutzreform

Mit besonderem Fokus auf die Aufgaben von Polizei und Justiz

42

Wichtige Neuerung der DSGVO im Überblick

Artikel 32 ff: Erhöhte Anforderungen an die Datensicherheit

- Schutz der Daten vor unbeabsichtigter oder widerrechtlicher Zerstörung, vor unbeabsichtigtem Verlust sowie zur Vermeidung jedweder unrechtmäßigen Verarbeitung, insbesondere jeder unbefugten Offenlegung, Verbreitung beziehungsweise Einsichtnahme oder Veränderung
- Weitere Konkretisierungen sowie Ermächtigung für „delegierte Rechtsakte" vorgesehen
- Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
- Meldepflichten an Behörden und Informationspflichten an Betroffene („Data Breach Notification")

Artikel 35: Verpflichtende Datenschutz-Folgenabschätzung

- Bei besonders risikobehafteten Datenanwendungen
- Demonstrative Aufzählung, insbesondere: **systematische und umfassende Bewertung persönlicher Aspekte** natürlicher Personen, beispielsweise zwecks **Analyse ihrer wirtschaftlichen Lage, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit** oder **ihres Verhaltens** oder zwecks diesbezüglicher Voraussagen, die sich auf eine automatisierte Verarbeitung von Daten gründet

Artikel 42: programmatische Bestimmung zu Datenschutz-Zertifizierung

- Mitgliedstaaten und Kommission fördern insbesondere auf EU Ebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln
- Ziel: Rasche und einfache Kenntnis des Datenschutzniveaus
- Zweck: ordnungsgemäßen Anwendung der Datenschutz-Grundverordnung

43

Datenschutz-Richtlinie für den Polizei- und Strafjustizsektor (RL 2016/680)

Anwendungsbereich — **Sowohl grenzüberschreitende als auch nationale Sachverhalte**

- *Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr*
- Sachlicher Anwendungsbereich: automatisierte oder manuell-strukturierte Datenverarbeitung
- Ausgenommen:
  - Wenn nicht im Anwendungsbereich des Unionsrechts, etwa im Bereich der nationalen Sicherheit
  - Datenverarbeitung durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union
    - Für diesen Bereich soll weiterhin Verordnung (EG) Nr. 45/2001 gelten (umstritten)

Regelungsdichte — **Kohärenz - weniger Umsetzungsspielraum als Rahmenbeschluss**

- Erwägungsgründe zum Harmonisierungsbedarf und zur Subsidiarität:
- reibungsloser Transfer personenbezogener Daten innerhalb der EU
- EU weit wirksamer und Datenschutz Betroffener erfordert mehr Kohärenz

- **Ergänzung Parlament zu Art. 1: Strengere Vorschriften auf nationaler Ebene sollen zulässig sein**

44

Wichtige Neuerungen durch die Richtlinie im Überblick

Artikel 9: Profiling und automatischer Datenverarbeitung

- Ausschließlich automatisierte Datenverarbeitung mit nachteiligen Rechtsfolgen oder erheblicher Beeinträchtigung Betroffener zum Zwecke der Bewertung einzelner Aspekte ihrer Person sind grundsätzlich verboten → vgl. Art 15 Richtlinie 95/46/EG (Datenschutzrichtlinie)
- Ausnahmen müssen ausdrücklich gesetzlich vorgesehen sein und Schutzgarantien enthalten
- **Keinesfalls aber hinsichtlich „besonderer Kategorien personenbezogener Daten" (Art 8)** – vgl. „sensible Daten" nach § 4 DSG

Artikel 11 – 16: Ausführlichere Regelung der Betroffenenrechte

- **Rechte auf Information, Auskunft und deren Ausnahmen**
- **Rechte auf Berichtigung und Löschung** (nicht neu) →
- **strafrechtliche Ermittlungen und Strafverfahren: Verweis nationales Strafprozessrecht**

Artikel 19: Datenschutz durch Technik und durch Voreinstellungen

- „Privacy by Design" – „Privacy by Default"
- Art. 14: Protokollierung von Erhebung, Veränderung, Abfrage, Weitergabe, Kombination oder Löschung - Zweck, Datum und Uhrzeit der Vorgänge und möglichst Identität des Verarbeiters
- **Artikel 27 – Datensicherheit: Detaillierte Vorschriften, verpflichtende Risikoanalyse**
- **Artikel 28 – Verständigungspflichten an Aufsichtsbehörde bei Datenschutzverletzungen**

45

research institute

Datenschutzgrundsätze (1/2)

- **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.
- **Grundsatz der Datenminimierung:** Reduktion der Verarbeitung personenbezogener Daten auf das Unvermeidbare

46

research institute

Datenschutzgrundsätze (2/2)

- **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**

47