5. DATENSCHUTZRECHTSTAGUNG

Neue Regeln, weniger Spielräume?

8. September 2021, 13:45 – 18:00 Uhr

Universität Zürich, Raum RAA-G-01 (Aula)

Rämistrasse 59, 8001 Zürich

Mit der Verabschiedung des neuen DSG im September 2020 ist der jüngste Regulierungsschub im Datenschutzrecht in Europa an einem (vorläufigen) Endpunkt angelangt. Ausstehend ist nur noch die Revision der Verordnungen zum DSG. Diese Arbeiten werden wohl wiederum Anlass zu Kontroversen geben. Mit den neuen, meist strikteren Regeln stellt sich zudem die Frage, welche Spielräume bei der Umsetzung (noch) bestehen. Diese Frage steht im Zentrum der diesjährigen Datenschutztagung.

Seit Abschluss der Revisionsarbeiten am DSG hat sich in der schweizerischen und europäischen Praxis einiges bewegt. Die ersten beiden Referate vermitteln einen Überblick über die jüngsten Entscheidungen und Entwicklungen in der Schweiz und der EU. Das dritte Referat gibt einen Einblick in den Stand der Arbeiten an den Verordnungen, soweit dies im Zeitpunkt der Tagung möglich ist. Ziel des ersten Teils der Tagung ist, die Teilnehmenden auf den neusten Stand zu bringen.

Der zweite Teil der Tagung widmet sich zunächst der zentralen Frage, welche Möglichkeiten zur Anonymisierung von Personendaten bestehen, wie diese umgesetzt werden und wie der erfolgte Grad an Anonymisierung gemessen werden kann. Die weiteren Referate untersuchen die neuen Spielräume und datenschutzrechtlichen Grenzen in zwei Sektoren. Ein erstes Referat fokussiert auf den Bereich der Medien. Die Cookie-Ära neigt sich allmählich dem Ende zu – neue Konzepte und Methoden sind gefragt, um die Affinitäten der Leserinnen und Leser besser zu erfassen, ihre Interessen genauer zu ermitteln und trotz allem nicht zum verpönten „Datenstaubsauger“ zu werden. Ein zweites Referat geht der Frage nach, in welchem Umfang, mit welchen Mitteln und unter welchen Voraussetzungen Arbeitnehmende an ihrem Arbeitsplatz überwacht werden dürfen. Die Pandemie hat hier mit dem Siegeszug des home office einen Kulturwandel eingeläutet, der Anlass für eine vertiefte Analyse ist. Die Tagung schliesst mit einer Panel- und Plenumsdiskussion. Diese bietet den Teilnehmenden die Möglichkeit, brennende Fragen zu den Entwicklungen in Europa und der Schweiz und zu den näher untersuchten Herausforderungen zu stellen und mit den Referierenden erste Antworten zu finden.

Programm

13:45 – 14:00
Einführung
Prof. Dr. FLORENT THOUVENIN, Tagungsleiter, Universität Zürich
DAVID ROSENTHAL, Tagungsleiter, Rechtskonsulent, Zürich

14:00 – 14:30
Update DSG
Dr. STEFAN BRINK, Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Baden-Württemberg

14:30 – 15:00
Update DSG
JULIA BHEND, Rechtsanwältin Winterthur

15:00 – 15:30
Update DSV
DAVID ROSENTHAL, Rechtskonsulent Zürich

15:30 – 16:00 - Pause

16:00 – 16:30
Anonymisierung: so wird sie gemacht und gemessen
Dr. MATTHIAS TEMPL, Dozent für statistische Datenanalyse, ZHAW

16:30 – 17:00
Datenschutz in den Medien: Spielräume und Grenzen
CHANTAL IMFELD-MATYASSY, Head of Data Protection & Data Protection Officer, Ringier Group

17:00 – 17:30
Überwachung am Arbeitsplatz: was geht?
Dr. DAVID VASELLA, Rechtsanwalt Zürich und Dr. IRENE SUTER-SIEBER, Rechtsanwältin, Zürich

17:30 – 18:00
Panel und Plenumsdiskussion

5. DATENSCHUTZRECHTSTAGUNG

Neue Regeln, weniger Spielräume?

Update DSGVO:
Dr. STEFAN BRINK, Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Baden-Württemberg

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Update DSGVO 2021

Dr. Stefan Brink
LfDI Baden-Württemberg

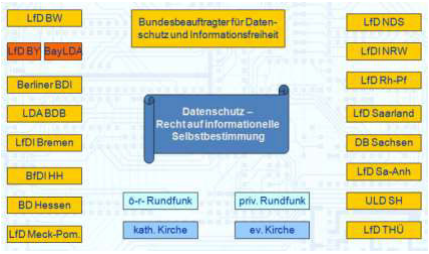
5. Datenschutzrechtstagung
SF SF Schweizer Forum für Kommunikationsrecht - Zürich

1

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Datenschutz damals

27 Aufsichtsbehörden in der EU und zusätzlich (mind.)
18 Aufsichtsbehörden in Deutschland

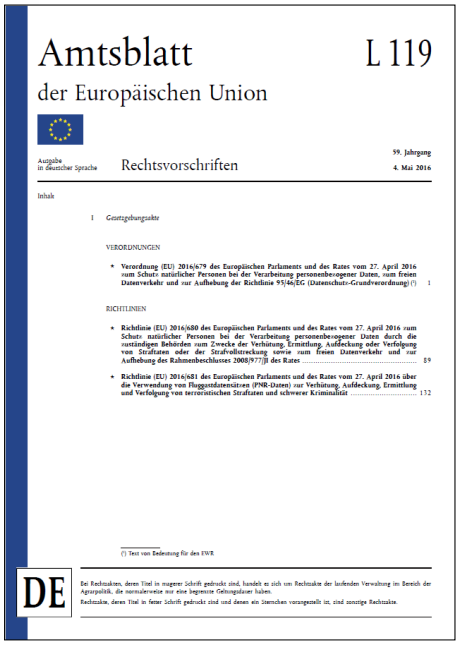


2

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Datenschutz heute

Datenschutz-Grundverordnung (DS-GVO)
und
JI-Richtlinie 2016/680
verkündet im
Amtsblatt der Europäischen Union
Vom 4. Mai 2016



Amtsblatt L 119
der Europäischen Union

Ausgabe in deutscher Sprache — Rechtsvorschriften — 59. Jahrgang, 4. Mai 2016

Inhalt

I Gesetzgebungsakte

VERORDNUNGEN

- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (1) 1

RICHTLINIEN

- Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates 89
- Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität 132

(1) Text von Bedeutung für den EWR.

DE

Bei Rechtsakten, deren Titel in magerer Schrift gedruckt sind, handelt es sich um Rechtsakte der laufenden Verwaltung im Bereich der Agrarpolitik, die normalerweise nur eine begrenzte Geltungsdauer haben.
Rechtsakte, deren Titel in fetter Schrift gedruckt sind und denen ein Sternchen vorangestellt ist, sind sonstige Rechtsakte.

3

Vorteile der DS-GVO

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- Einheitliches Recht für ganz Europa
- Einheitlich angewendet durch die nationalen Aufsichtsbehörden
- Ausweitung der Geltung der DS-GVO auf außereuropäische Mitbewerber (Marktortprinzip)

⇒ Vorteile für (international ausgerichtete) Gewerbebetriebe

⇒ Hauptproblem: Keine ausreichende Differenzierung zwischen Internetkonzernen und KMU/Vereinen

4

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Wie „gut“ ist die DS-GVO?

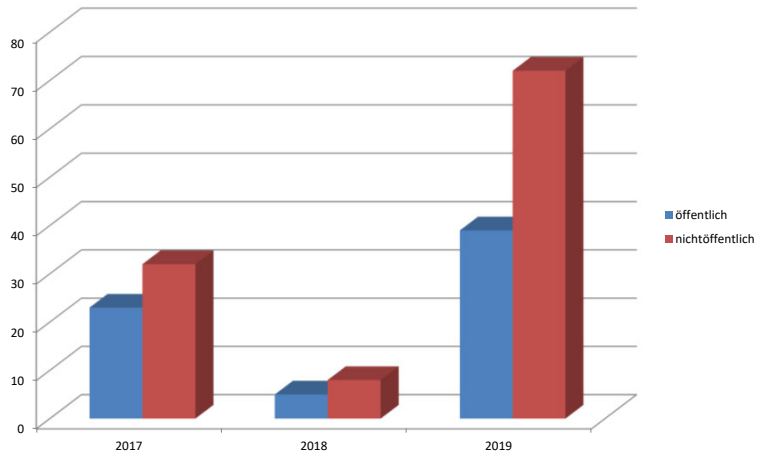
Das kommt uns **weniger bekannt** vor:

- Aufzehrende Sanktionen (Art. 83 DS-GVO)
- Dokumentations-/Rechenschaftspflichten (Art. 5 Abs. 2 DS-GVO)
- Keine Schonung von KMU/Vereinen

5

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Durchgeführte Kontrollen



6

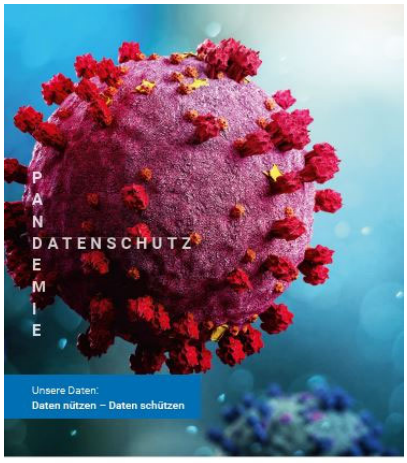
Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

1. Fazit der DS-GVO

#DS-GVO wirkt!

- Sanktionen wirken präventiv u. repressiv (Art. 83/82/58 DS-GVO)
- DS-GVO wirkt international (Vorbild/Marktregulierung)
- Europäische Koordination beginnt …
- Aufsichtsbehörden als Beratungsinstanz

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg



Tätigkeitsbericht
Datenschutz 2020

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

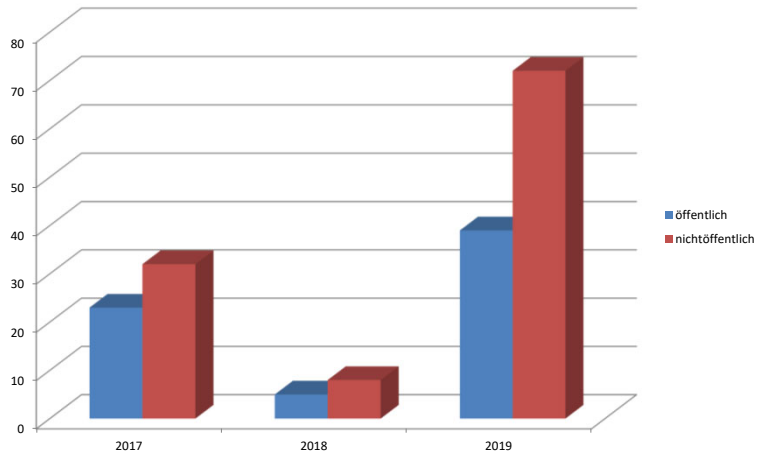
Datenschutz 2020/2021

Gesellschaftliche Reaktionen auf Pandemie

- Bargeldloses Bezahlen
- Kollektiv-Verhalten: Mehrheit respektiert Minderheitenrechte nicht mehr
  => Druck auf Meinungsfreiheit, Versammlungsfreiheit, DatenschutzGR
- Glaube an „Problemlöser Digitalisierung“
  => naiver Glaube an Stand und Möglichkeiten der Digitalisierung
  => Überwachungsüberschuss digitaler Techniken
  => Rückholbarkeit von Entscheidungen nach der Pandemie?

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Durchgeführte Kontrollen 2020/2021



Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Bußgeldpraxis in der EU

1. Ankündigungen durch ICO (GB)

- 183,39 Mio. £ gg. **British Airways** wg. Verstoß gg. Art. 32 DS-GVO (durch Cyberattacke wurden pb Daten von 500T Besuchern abgegriffen) [22 Mio. €]
- 99,2 Mio. £ gg. **Marriott International Inc.** wg. Verstoß gg. Art. 32 DS-GVO (durch Hackerangriff wurden Daten von 339M Kunden abgegriffen) [20 Mio. €]

2. LfDI Berlin: 14,5 Mio. € Bußgeld gg. Deutsche Wohnen SE

- Verstoß gegen Art. 5 und 25 DS-GVO (unzulässige Datenspeicherung)
- 2. Instanz Berlin

3. BfDI

- Bußgeld gegen 1&1 TelkomDienstleister 9,55 Mio € (telefon. Authentifizierungsverfahren unzureichend)
- LG Bonn

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Bußgelder 2020

Bußgeldkonzept

- Erhöhung von 50% im Vergleich zum Vorjahreszeitraum
- Bußgeld in Höhe von 100.000,- Euro gegen ein mittelständisches Lebensmittelhandwerksunternehmen
- Bußgeld gegen AOK BaWü
  1.2 Mio € für rw Werbemaßnahmen
  => Anknüpfung Bußgeldhöhe an Umsatz
  => Bußgelder gegen ö. Stellen

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Daten“Oasen“

A (lila): Strenge Gesetze gegen Zugriffe durch staatliche Behörden, strenge Regeln zum Datenschutz
B (grün): Gesetze gegen Zugriffe durch staatliche Behörden, Datenschutzregeln in Kraft
C (orange): Minimale Regulierung des staatlichen Zugriffs, eingeschränkte Regeln zum Datenschutz
D (rot): Vernachlässigbare Regeln gegen staatlichen Zugriff, Datenschutzregeln nicht existent
F (türkis) Keine Regulierungen, keine Datenschutzgesetze

Intralinks, 2018

13

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

DS-GVO und der Rest der Welt

DS-GVO als offensive Rechtsordnung

- **Räumlicher Anwendungsbereich (Art. 2 Abs. 2)**
  => Marktortprinzip
- **Datenexport in Drittländer (Art. 44 ff.)**

  - Angemessenheitsbeschluss EU-KOM (Art. 45)

  - Geeignete Garantien (Art. 46)
  => Standarddatenschutzklauseln

  - BCR (Art. 47)

  - Ausnahmetatbestände (Art. 49)

14

14

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

EuGH vor (Schrems II): Schrems I

EuGH äußert sich zu

- **EU-U.S. Safe Harbor (Oktober 2015)**
  - nationales U.S.-Recht schränkt Datenschutz ein

  →insbesondere: Zugang U.S.-Behörden wegen „nationaler Sicherheit“

  ⇒ kein mit EU vergleichbares Schutzniveau

  ⇒ keine justiziablen Rechte für Betroffene
  - **ungültig**

15

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

EuGH C-311/18 (Schrems II): Inhalt

EuGH äußert sich zu

- **EU-U.S. Privacy Shield (Juli 2016)**
  - nationales U.S.-Recht schränkt Datenschutz ein

  →insbesondere: Zugang U.S.-Behörden wegen „nationaler Sicherheit“

  ⇒ kein mit EU vergleichbares Schutzniveau

  ⇒ keine justiziablen Rechte für Betroffene
  - **ungültig**

16

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

17

17

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

OH LfDI vom 7.9.2020

- SCC
  - Änderungen/Ergänzungen („zusätzliche Garantien“)
    - Information des Betroffenen über Datenanforderung durch Behörde
    - Beschreiten des Rechtswegs gegen Datenanforderung
    - Entschädigungsklausel zu Lasten des Datenimporteurs
- Prüfung Ausnahmen Art. 49 (ErwG 111)
- Vorgehen LfDI: Auswahlermessen vor Untersagung
  => Kriterium: zumutbare Alternativangebote ohne Transferproblematik
  - beim selben Dienstleister (Verarbeitungsstandort EU/Verschlüsselung)
  - Wechsel des Dienstleisters
  - Zumutbarkeit: - Kosten / - Reichweite / - Verfügbarkeit

18

18

Zahlen & Fakten

19

Dienststellenstatistik

Bezeichnung	2016	2017	2018	2019	2020
Beschwerden	**2.048**	**3.058**	**3.902**	**3.757**	**4.782**
- öffentlicher Bereich	840	1186	1188	972	
- nicht-öffentlicher Bereich	1208	1872	2714	2785	
Kontrollen	**16**	**55**	**13**	**111**	**31**
- öffentlicher Bereich	12	23	5	39	
- nicht-öffentlicher Bereich	4	32	8	72	
Beratungen	**1.515**	**1.786**	**4.440**	**3.842**	**3.285**
- öffentlicher Bereich	878	991	1492	1289	
- nicht-öffentlicher Bereich	637	795	2948	2553	
Datenpannenmeldungen	**68**	**121**	**900**	**2.030**	**2.321**

20

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Nach dem #Twexit – Wie geht es beim LfDI weiter?

- Internetauftritt (täglich zwischen 5.000 und 8.000 Aufrufe).
- Newsletter (> 3.000 Abonnenten).
- Podcast „Datenfreiheit“
- Datenschutz- und IFG-Forum
- LfDI-App

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Dauerbrenner

- Datenschutz bei Gemeinden
- Datenschutz im Verein
- Unerwünschte Werbung
- Fotografieren „unter der DSGVO“
- Betroffenenrechte

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Fazit der DS-GVO 2021

#DS-GVO wirkt!

- Sanktionen wirken präventiv u. repressiv (Art. 83/82/58 DS-GVO)
- DS-GVO wirkt international (Vorbild/Marktregulierung)
- Europäische Koordination beginnt …
- Aufsichtsbehörden als Beratungsinstanz

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Vielen Dank für Ihre Aufmerksamkeit!

Weitergehende Informationen finden Sie unter
www.baden-wuerttemberg.datenschutz.de
und unter
https://twitter.com/lfdi_bw

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Vielen Dank für Ihre Aufmerksamkeit!

Weitergehende Informationen finden Sie unter

www.baden-wuerttemberg.datenschutz.de

und auf

Mastodon

@lfdi@bawü.social

5. DATENSCHUTZRECHTSTAGUNG

Neue Regeln, weniger Spielräume?

Update DSG

JULIA BHEND, Rechtsanwältin Winterthur

PROBSTPARTNER

Update DSG

SF-FS: 5. Datenschutzrechtstagung

Julia Bhend
Zürich, 8. September 2021

1

PROBSTPARTNER

Themen

- Datenbekanntgabe ins Ausland
- Auskunftsrecht
- Amtshilfe
- Anwendung DSG auf Private / Bundesorgane
- Datensparsamkeit
- Revision DSG

2

PROBSTPARTNER

Datenbekanntgabe ins Ausland

- Urteil EuGH in der Rechtssache C-311/18 (Schrems II)
  - Privacy Shield Framework kein genügender Schutz mehr für Datenexporte in USA
  - Auch Standardvertragsklauseln bieten nicht mehr *per se* einen genügenden Schutz
- Gleiche Schlussfolgerungen des EDÖB für die Schweiz

PROBSTPARTNER

Datenbekanntgabe ins Ausland (DSG 6 Abs. 2 lit. a)

- Neue Standardvertragsklauseln der EU-Kommission vom 4. Juni 2021
- 4 Module:

Importeur / Exporteur	Verantwortlicher in Drittstaat	Auftragsbearbeiter in Drittstaat
Verantwortlicher in EU	Modul 1	Modul 2
Auftragsbearbeiter in EU	Modul 4	Modul 3

- SCC decken auch Anforderungen an Auftragsdatenbearbeitung ab.
- SCC müssen unverändert übernommen werden, soweit eine Bestimmung nicht ausdrücklich als optional vorgesehen ist.

PROBSTPARTNER

Datenbekanntgabe ins Ausland (DSG 6 Abs. 2 lit. a)

- EDÖB anerkennt die neuen SCC als Grundlage für Übermittlung in Drittländer, verlangt aber Anpassungen für die Schweiz
  - Anpassungen betr. Aufsichtsbehörde, anwendbares Recht, Gerichtsstand, Verweise auf DSGVO, Daten juristischer Person (bis revDSG in Kraft)
  - Vgl. Mitteilung EDÖB vom 27. August 2021
- Übergangsfrist:
  - Anmeldungen mit bisherigen Musterverträgen bis 27. September 2021
  - Verwendung bis 31. Dezember 2022, sofern die Datenbearbeitung bzw. der Vertrag in der Zwischenzeit nicht wesentlich verändert wird.

PROBSTPARTNER

Datenbekanntgabe ins Ausland (DSG 6 Abs. 2 lit. a)

- SCC alleine genügen nicht
  - Einzelfallbezogene Prüfung, ob SCC tatsächlich eingehalten werden können und keine entgegenstehenden ausländischen Gesetze und Behördenzugriffe bestehen (vgl. Klausel 8 und 14 SCC).
  - Anleitung EDÖB vom Juni 2021 für die Prüfung zur Zulässigkeit von Datenübermittlungen ins Ausland nach Art. 6 Abs. 2 lit. a DSG
  - Wenn Grundrechtsgarantien in Bezug auf behördliche Zugriffe im Drittland und Rechte der Betroffenen nicht gewährleistet, sind neben SCC zusätzliche (insb. technische und organisatorische) Massnahmen nötig.
- p.m.: Meldepflicht nach Art. 6 Abs. 3 DSG

PROBSTPARTNER

Datenbekanntgabe ins Ausland (DSG 6 Abs. 2 lit. b-c)

- Stellungnahme EDÖB vom 25. Juni 2021 gegenüber US Securities and Exchange Commission zur Bekanntgabe von Personendaten von Schweizer Vermögensverwaltern an die US-Börsenaufsichtsbehörde

PROBSTPARTNER

Auskunftsrecht nach DSG 8

- Zweck:
  - Auskunftsanspruch darf nicht einzig dem Zweck der Beweismittelbeschaffung oder Abklärung der Prozessaussichten dienen
  - BGE 147 III 139 E. 1.7; BGer, 4A_227/2020
- Umfang:
  - Auch Angaben über Herkunft der Daten, sofern vorhanden; aber keine Pflicht zur Speicherung von Herkunftsangaben
  - Nur schriftlich bzw. «physisch» vorhandene und einsehbare Daten
  - Angaben über die Herkunft von Daten, die allenfalls im Gehirn gespeichert sein könnten, sind für Inhaber der Datensammlung nicht verfügbar und daher nicht erfasst
  - BGE 147 III 139 E. 3

PROBSTPARTNER

Bekanntgabe nach Art. 19 Abs. 1 lit. a DSG

BGer, 2C_1039/2018 / 2C_1052/2018 und 2C_1040/2018 / 2C_1051/2018 (zur Publ. vorgesehen):

- Einsicht in WEKO-Untersuchungen gestützt auf Art. 19 Abs. 1 lit. a DSG
- Zur Erfüllung der gesetzlichen Aufgabe unentbehrlich
  - Insb. Prüfung Schadenersatzansprüche
  - Erfüllung der gesetzlichen Aufgabe muss nur möglich sein. Kein Nachweis nötig, dass mit den Daten die gesetzliche Aufgabe tatsächlich erfüllt werden kann.
  - Einsichtsgesuche setzen weder rechtskräftigen Abschluss des Sanktionsverfahrens noch die Feststellung eines Kartellrechtsverstosses voraus.
  - Zweckbindung

PROBSTPARTNER

DSG: Privatbereich / Bundesorgane

BVGer, A-5921, Urteil vom 29. Juli 2021 (SwissPass):

- Art. 54 Abs. 1 PBG: je nach öffentlich- oder privatrechtlichem Handeln des Transportunternehmens sind Bestimmungen im DSG für Bundesorgane oder für private Personen massgebend
- Geltungsbereich DSG für Bundesorgane ist beschränkt auf Datenbearbeitung im Rahmen eines öffentlich-rechtlichen Verhältnisses
- Personentransportvertrag ist privatrechtlicher Natur und damit auch die damit zusammenhängende Datenbearbeitung
- Datenschutzrechtliche Ansprüche gegen privatrechtlich handelnde Bundesorgane richten sich nach Art. 15 DSG und sind auf dem Zivilweg durchzusetzen (Art. 23 DSG)

PROBSTPARTNER

Datensparsamkeit

BGer 1C_273/2020 (Funkwasserzähler; zur Publ. vorgesehen):

- Speicherung Stundenwerte während 252 Tagen und Aussenden über Funk alle 30 Sek.
- Datensicherheit rechtfertigt nicht notwendige Datenbeschaffung nicht.
- «Der Grundsatz der Erforderlichkeit bzw. Datenvermeidung und Datensparsamkeit bezweckt jedoch, dass nicht notwendige Daten gar nicht erst erhoben und bearbeitet werden. In diesem Sinne ist auch ihr Schutz besser gewährleistet: nicht existente Daten können nicht missbraucht werden.»

PROBSTPARTNER

Revision DSG

- Neues Bundesgesetz über den Datenschutz vom 25. September 2020
- Inkrafttreten 2. Hälfte 2022 geplant
- Stellungnahme EDÖB zu neuem DSG (Februar 2021)
- Vernehmlassung zum E-VDSG Juni bis Oktober 2021
- Aufstockung Stellen bei EDÖB

PROBSTPARTNER

Fragen und Anregungen

Julia Bhend
Probst Partner AG, Zürich/Winterthur
julia.bhend@probstpartner.ch
052 269 14 00
www.swissdataprotectionlaw.ch

5. DATENSCHUTZRECHTSTAGUNG

Neue Regeln, weniger Spielräume?

Update DSV

DAVID ROSENTHAL, Rechtskonsulent, Zürich

VISCHER

Revision DSG

Update Entwurf Verordnung zum DSG (E-VDSG)

David Rosenthal
8. September 2021

1

Wo stehen wir?

- **Vernehmlassung** zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)
  - Entwurf vom 23. Juni 2021, mit "erläuterndem Bericht"
  - Vernehmlassungsfrist bis **14. Oktober 2021**
- VDSG soll zeitgleich mit dem revidierten DSG in Kraft treten
  - Offiziell "in der zweiten Jahreshälfte 2022"
  - EDÖB: 1. Januar 2023

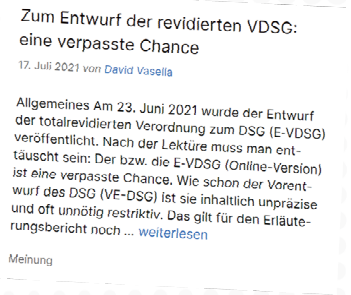
"Zahlreiche Bestimmungen im nDSG müssen auf Verordnungsebene konkretisiert werden. Bevor das Gesetz in Kraft treten kann, sind deshalb die entsprechenden Ausführungsbestimmungen in der VDSG grundlegend anzupassen." (Medienmitteilung)

2

VISCHER

Was wurde gemacht?

- Bereits innerhalb der Verwaltung sehr **umstrittene Vorlage**
- Ein Entwurf in Anlehnung an die bisherige VDSG, aber mit
  - Groben **Fehlern**
  - **Alten Zöpfen**, die abgeschnitten gehören
  - **Praxisfremden** Regelungen
  - Zahlreichen Bestimmungen **ohne Rechtsgrundlage**
- Erläuterungsbericht mit vielen **fachlichen Fehlern**
- Was tun? **Zurück an Absender** oder zahlreiche Bestimmungen streichen und anpassen



Zum Entwurf der revidierten VDSG: eine verpasste Chance

17. Juli 2021 von David Vasella

Allgemeines Am 23. Juni 2021 wurde der Entwurf der totalrevidierten Verordnung zum DSG (E-VDSG) veröffentlicht. Nach der Lektüre muss man enttäuscht sein: Der bzw. die E-VDSG (Online-Version) ist eine verpasste Chance. Wie schon der Vorentwurf des DSG (VE-DSG) ist sie inhaltlich unpräzise und oft unnötig restriktiv. Das gilt für den Erläuterungsbericht noch ... weiterlesen

Meinung

VISCHER

Was darf ein Verordnungsgeber?

BGE 141 II 169, E. 3.3:

«Die Kompetenz zum Erlass gesetzesvertretender Verordnungen setzt eine entsprechende Delegationsnorm im Gesetz voraus (Art. 164 Abs. 2 BV). Auch wenn der Gesetzgeber davon abgesehen hat, der Exekutive derartige (beschränkte) Legislativfunktionen zu übertragen, obliegt es dem Bundesrat, die Gesetzgebung zu vollziehen (Art. 182 Abs. 2 BV). Der Anwendungsbereich von Ausführungs- und Vollziehungsverordnungen ist indes darauf beschränkt, die Bestimmungen des betreffenden Bundesgesetzes durch Detailvorschriften näher auszuführen und mithin zur verbesserten Anwendbarkeit des Gesetzes beizutragen. Ausgangspunkt sind Sinn und Zweck des Gesetzes; sie kommen in grundsätzlicher Weise durch die Bestimmung im formellen Gesetz zum Ausdruck.»

VISCHER

Thema "Datensicherheit"

- Strafbar ist, wer vorsätzlich die "**Mindestanforderungen** an die Datensicherheit" nicht einhält, die der Bundesrat nach Art. 8 Abs. 3 erlassen hat
- Datensicherheit = Vertraulichkeit, Integrität und Verfügbarkeit
- Datensicherheit ≠ Bearbeitungsgrundsätze, Betroffenenrechte
- **E-VDSG** sieht dazu vor
  - Grundsätze
  - Schutzziele
  - Protokollierung
  - Bearbeitungsreglement

VISCHER

Datensicherheit: Grundsätze

Anpassen

- Datensicherheit darf **risikobasiert** erfolgen
- Wie kann eine Gesetzesnorm dem gerecht werden, gleichzeitig "Mindestanforderungen" definieren und trotzdem **bestimmt genug sein**, um Art. 1 StGB zu genügen?
- Die definierten Grundsätze tun es jedenfalls **nicht**
  - Legen Kriterien zur Beurteilung der Angemessenheit fest (z.B. Zweck, Art, Umfang der Datenbearbeitung, Stand der Technik, Risiko, Implementierungskosten)
  - Bisherige Liste wurde etwas ausgebaut
  - Definition von Risiko verwechselt Ursache und Wirkung
  - Überprüfung in "angemessenen Abständen"

VISCHER

Datensicherheit: Schutzziele

Streichen

- Die bereits bekannte Liste von Schutzzielen (Zugangskontrolle, Datenträgerkontrolle, Speicherkontrolle etc.) wurde erweitert
- Veraltetes Konzept – Giesskannenprinzip
- Schutzziele müssen "erreicht" werden: 100 Prozent Schutz?
- Besser wäre das Konzept von Art. 32 Abs. 1 DSGVO, welche Bestimmungen mögliche Massnahmen erwähnt, aber nicht zwingend vorgibt und auch nicht abschliessend ist

VISCHER

Datensicherheit: Protokollierung

Streichen

- Pflicht zur Einführung eines **Audit-Trails** für Bearbeitungen mit "hohem Risiko" für die Persönlichkeit oder die Grundrechte
- **Hoher Aufwand**, massive Datenbearbeitung
  - Jeder Benutzer wird bei jedem Schritt überwacht
  - Audit Trails für zwei Jahre aufbewahren
  - Aufbewahrung in vom operativen System getrennten Systemen
  - Protokolle dürfen nur für Datenschutzzwecke benutzt werden
- **Rechtsgrundlage fehlt**, Swiss Finish
  - Hier geht es nicht um Datensicherheit, sondern Datenschutz
  - Bundesrat hat auf Einführung einer Dokumentationspflicht im revDSG – ausser beim Inventar – bewusst verzichtet

VISCHER

Datensicherheit: Bearbeitungsreglement

Streichen

- Pflicht zur Führung eines "Bearbeitungsreglements" wenn **"umfangreich" besonders schützenswerte Personendaten** bearbeitet werden oder ein Profiling mit hohem Risiko besteht
  - Mindestangaben werden definiert (z.B. "Massnahmen, die zur Datenminimierung getroffen wurden", "Angaben zur Herkunft der Personendaten und zur Art ihrer Beschaffung")
- **Hoher Aufwand**
  - Ein weiteres, separates Dokument, das zu unterhalten ist …
- **Rechtsgrundlage fehlt**, Swiss Finish
  - Hier geht es nicht um Datensicherheit, sondern Datenschutz
  - Bundesrat hat auf Einführung einer Dokumentationspflicht im revDSG – ausser beim Inventar – bewusst verzichtet

VISCHER

Thema "Auftragsbearbeitung"

Streichen

- "Der Verantwortliche, der die Bearbeitung von Personendaten einem Auftragsbearbeiter überträgt, bleibt für den Datenschutz **verantwortlich**."
  - Kausalhaftung? Art. 41 ff. OR genügen …
- "Er muss **sicherstellen**, dass die Daten **vertrags- oder gesetzesgemäss** bearbeitet werden."
  - Gesetzliche Gewährleistung? Pflicht zur Vertragsdurchsetzung?
- Pflicht, "**gleichwertigen Datenschutz** [zu] gewährleisten" wenn der Auftragsbearbeiter dem DSG nicht untersteht
  - Verhältnis zu Art. 16 f. revDSG? Kausalhaftung?
- **Rechtsgrundlage fehlt**, Swiss Finish

VISCHER

Thema "Bekanntgabe ins Ausland"

Überarbeiten

- Inhaltliche **Vorgaben für Datenschutzklauseln** zum Schutz von Personendaten in unsicheren Drittländern
  - Wie z.B. Einhaltung der Bearbeitungsgrundsätze, die Namen der Staaten der Empfänger, Rechte der betroffenen Personen, Anforderungen an die Aufbewahrung von Daten
  - Keine Unterscheidung nach Controller und Processor
  - Keine vertragliche Meldepflicht für Data Breaches
- Pflicht **"sicherzustellen"**, dass der Empfänger im Ausland diese Datenschutzklauseln auch **einhält**
  - Nicht erfüllbar; DSGVO kennt keine solche Regelung

VISCHER

Thema "Informationspflicht"

Überarbeiten bzw. streichen

- Informationspflicht soll **auch für Auftragsbearbeiter** gelten
- Praxisfremde Erläuterungen (z.B. Empfehlung, am Telefon den Link zur Datenschutzerklärung zu nennen)
- Keine Klarstellung, dass Datenschutzerklärung auf Website in der Regel genügt – im Gegenteil
- Datenschutzerklärung muss "präzis" sein – noch genauere Angaben über die Datenbeschaffungen?
- Piktogramme "müssen" **maschinenlesbar** sein, obwohl es keinen Standard gibt, sie freiwillig sind und sie einem anderen Zweck dienen
  - Keine gesetzliche Grundlage; Strafbarkeit möglich?

VISCHER

Thema "Mitteilungspflichten"

Streichen

- Bei der Bekanntgabe von Personendaten muss der Empfänger über **Aktualität, Zuverlässigkeit und Vollständigkeit** der bekanntgegebenen Daten informiert werden
  - Sogar ein Auftragsbearbeiter wird verpflichtet
  - Nicht praktikabel
  - (Noch immer) keine gesetzliche Grundlage; Swiss Finish
- Verantwortliche haben **Empfänger** "unverzüglich" über Berichtigung, Löschung oder Vernichtung sowie Einschränkung der Bearbeitung von Personendaten **zu informieren**
  - War im Entwurf des revDSG vorgesehen, wurde jedoch vom Parlament gestrichen
  - Keine gesetzliche Grundlage

VISCHER

Thema "Dokumentationspflichten"

Streichen

- **Datenschutzfolgenabschätzung** muss "schriftlich" erfolgen
  - Textform muss jedoch genügen
  - Sie muss während zwei Jahren nach Beendigung der Datenbearbeitung aufbewahrt werden
- **Meldungen der Verletzungen der Datensicherheit**
  - Keine De-Minimis-Regelung, dafür Unnötiges (z.B. Erlaubnis, schrittweise zu informieren, wenn es nicht anders geht)
  - Sie müssen für drei Jahre dokumentiert werden (nur die meldepflichtigen?) mit allen "zusammenhängenden Tatsachen"
- Dokumentationspflichten haben **keine gesetzliche Grundlage**
  - Aufbewahrungsfristen erscheinen zufällig …

VISCHER

Thema "Auskunftsrecht"

Überarbeiten bzw. streichen

- **Nutzlose Regelungen** (im Sinne von "wenn alle einverstanden sind, darf die Auskunft auch mündlich begehrt werden")
- Ungenügende **Fristenregelung** und zu tiefe Kostenbeteiligung
- Pflicht, die Auskunft so zu erteilen, dass **die nachfragende Person sie versteht**
  - Was muss z.B. dem Teilnehmer einer medizinischen Studie erklärt werden, der alle von ihm erhobenen Daten haben will?
  - Geht viel zu weit; DSG sieht den subjektiven Ansatz nicht vor
- **Dokumentation** der Gründe für Einschränkung der Auskunft muss beim Verantwortlichen für drei Jahre dokumentiert sein
  - Auch hier: Keine gesetzliche Grundlage

VISCHER

Thema "Datenschutzberater"

Überarbeiten

- **Fehlende Abstimmung** zwischen Gesetz und Verordnung
  - Pflichtenheft wurde nicht aus dem Gesetz übernommen, sondern der bisherigen Verordnung (im bisherigen DSG gab es nichts)
  - Braucht es wirklich eine Regelung in der VDSG?
  - Gesetz: Schulung, Beratung, Mitwirkung an der Compliance
  - E-VDSG: Prüfung (aller?) Bearbeitungen und Empfehlung von Korrekturen, wo die Datenschutzvorschriften verletzt werden
- Aufgaben sind als persönliche **gesetzliche Pflicht** formuliert
  - Welche **Haftungsfolgen** hat dies für ihn/sie?

VISCHER

Thema "Verzeichnis"

Klarstellen

- Bundesrat kann Ausnahme von der Inventarpflicht vorsehen bei Unternehmen mit weniger als 250 Mitarbeitern und "deren Datenbearbeitung ein **geringes Risiko**" mit sich bringt
- Ausnahme soll dann nicht gelten, wenn ein "Profiling mit hohem Risiko" durchgeführt wird oder **umfangreich besonders schützenswerte Personendaten** bearbeitet werden
- Bedeutet dies im Umkehrschluss, dass nur diese beiden Fälle ein hohes Risiko mit sich bringen? Gilt dieser Massstab auch bei der Frage, wann es eine Datenschutz-Folgenabschätzung braucht?
- Ist die Ausnahme bei einer Datenbearbeitung nicht erfüllt, muss dann das Inventar für alle Aktivitäten gemacht werden?

VISCHER

Das bringt uns zur Schlussfrage:

Wie weiter?

VISCHER

Danke für Ihre Aufmerksamkeit!

Fragen: drosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

www.vischer.com

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

5. DATENSCHUTZRECHTSTAGUNG

Weniger Regeln, neue Spielräume?

Anonymisierung: so wird sie gemacht und gemessen

Dr. MATTHIAS TEMPL, Dozent für statistische Datenanalyse, ZHAW

Anonymisierung: so wird sie gemacht und gemessen

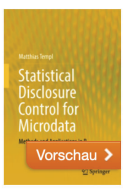
Matthias Templ

Institut für Datenanalyse und Prozessdesign
School of Engineering
Zürcher Hochschule für Angewandte Wissenschaften

5. DATENSCHUTZRECHTSTAGUNG, Universität Zürich, 08.09.2021

Mein Hintergrund in Anonymisierung

- Projekte in/mit Statistik Austria, OECD, IHSN, Weltbank, EU, Helsana, Swisscom, ESTHER/MEIRU, SBB, Stadt und Kanton Zürich, Beratungen für BAG, Workshops, ...
- Publikationen, z.B. im Journal of Statistical Software (sdcMicro, simPop)
- Springer-Book Statistical Disclosure Control



© 2017

Statistical Disclosure Control for Microdata

Methods and Applications in R

Autoren: **Templ**, Matthias

- LVA *Statistical Disclosure Control* an der Freien Univ. Berlin, Uni Bamberg und Uni Trier (2019, 2020, 2021).

Einige Eigenschaften

Online/Offline

- Online: Anonymisierung (oder Vorhersage) dynamisch, sobald eine Abfrage gestellt wird. Offline: Anonymisierung a-priori

Einige Eigenschaften

Online/Offline

- Online: Anonymisierung (oder Vorhersage) dynamisch, sobald eine Abfrage gestellt wird. Offline: Anonymisierung a-priori

Additivität:

- Z.B. ausgegebene Totals = Summe der Einzelwerte.

Einige Eigenschaften

Online/Offline

- Online: Anonymisierung (oder Vorhersage) dynamisch, sobald eine Abfrage gestellt wird. Offline: Anonymisierung a-priori

Additivität:

- Z.B. ausgegebene Totals = Summe der Einzelwerte.

Konsistenz:

- Erneute idente Abfrage/Analyse/Vorhersage → gleiche Ergebnisse.

Einige Eigenschaften

Online/Offline

- Online: Anonymisierung (oder Vorhersage) dynamisch, sobald eine Abfrage gestellt wird. Offline: Anonymisierung a-priori

Additivität:

- Z.B. ausgegebene Totals = Summe der Einzelwerte.

Konsistenz:

- Erneute idente Abfrage/Analyse/Vorhersage → gleiche Ergebnisse.

Hohe Utility:

- Analyse mit anonymisierter Information ist im wesentlichen ident mit der nicht-anonymisierten Version

Einige Eigenschaften

Online/Offline

- Online: Anonymisierung (oder Vorhersage) dynamisch, sobald eine Abfrage gestellt wird. Offline: Anonymisierung a-priori

Additivität:

- Z.B. ausgegebene Totals = Summe der Einzelwerte.

Konsistenz:

- Erneute idente Abfrage/Analyse/Vorhersage $\rightarrow$ gleiche Ergebnisse.

Hohe Utility:

- Analyse mit anonymisierter Information ist im wesentlichen ident mit der nicht-anonymisierten Version

Disclosure Risk:

- Beurteilt wie hoch das Re-identifizierungsriskio einer Person im Datensatz ist

Arten sicher mit Personendaten umzugehen (1/2)

Privacy Preserving Computation

Generell: online, nicht-additiv, nicht-konsistent, low risk and utility
User sieht Daten nicht. Modellparameter werden trainiert und Vorhersagen von sensibler Information einer Person getätigt

- differential privacy: Füge Noise zu Ergebnissen hinzu
- federated learning: Daten auf versch. Servern mehrerer Clients

Anwendung vor allem in der Medizin und Banking. User machen keine detail. Analysen, sondern begnügen sich mit Vorhersage.

Arten sicher mit Personendaten umzugehen (1/2)

Privacy Preserving Computation

Generell: online, nicht-additiv, nicht-konsistent, low risk and utility
User sieht Daten nicht. Modellparameter werden trainiert und Vorhersagen von sensibler Information einer Person getätigt

- differential privacy: Füge Noise zu Ergebnissen hinzu
- federated learning: Daten auf versch. Servern mehrerer Clients

Anwendung vor allem in der Medizin und Banking. User machen keine detail. Analysen, sondern begnügen sich mit Vorhersage.

Query servers

Zugriff auf aggregierter Form der Daten.

- differential privacy (Generell: online, nicht-additiv, nicht-konsistent, low risk and utility): Füge Noise zu Abfrageergebnissen hinzu
- Methoden der Zellsperrung (offline, additiv, konsistent, risk and utility depends), uva. . . .

Anwendungsgebiet: Dashboards und Query Server

Arten sicher mit Personendaten umzugehen (2/2)

Synthetische Datenerzeugung

Statt den Originaldaten werden synthetische "Zwillings' 'daten bereitgestellt, welche mit ML-Methoden generiert werden.
Einsatzgebiete: Training- und Schulungsdaten. Public-Use-Files und schnelle Datenweitergabe zur Voranalyse.

Arten sicher mit Personendaten umzugehen (2/2)

Synthetische Datenerzeugung

Statt den Originaldaten werden synthetische "Zwillings' 'daten bereitgestellt, welche mit ML-Methoden generiert werden.
Einsatzgebiete: Training- und Schulungsdaten. Public-Use-Files und schnelle Datenweitergabe zur Voranalyse.

Anonymisierung durch Veränderung der Daten

- Information von Personen mit erhöhtem Riskio werden gezielt verändert.
- Ziel: Daten mit möglichst hoher Utility zur Verfügung zu stellen

Einsatzgebiet: überall dort wo detailierte (aber anonymisierte) Daten für genauere Analysezwecke verteilt werden.
Diese Methoden wollen wir im Anschluss besprechen.

Fragestellungen

- Wer ist der Nutzerkreis der Daten?
- Wie hoch ist das **Re-Identifizierungsrisiko**?
- Wie ist das **Re-Identifizierungsrisiko** jeder einzelnen Person zu quantifizieren?
- Wie viel Anonymisierung ist notwendig?
- Welche Anonymisierungsmethoden sind zu wählen?
- Wie gut ist die Datenqualität nach Anonymisierung?

Keine 08/15 und standardisierten Lösungen

Jede Anonymisierung muss sehr **daten- und anwendungsfallspezifisch** gemacht werden.

Breite Perspektive

- alle verfügbaren Ressourcen müssen berücksichtigt werden, d.h. **alle** denkbaren **Angriffe müssen berücksichtigt werden**.
- **Datenqualität**: (übermässige) Anonymisierung kann Daten für die Analyse unbrauchbar machen. Es muss darauf geachtet werden, dass die Datenqualität durch die Anonymisierung nicht leidet.
- **Sensibilität**: Einfache Anonymisierungen können ausreichen, um eher uninteressante Daten zu liefern, während sie für hochsensible Daten unzureichend sein können.

de-fakto Anonymität

Wenn der Aufwand zur Re-Identifizierung von Daten höher ist als der Nutzen, sprechen wir von de-fakto Anonymität.

Anonymisierung in der Praxis: Grober Ablauf

1) **RISK** Messung des Risikos 

- Stichprobe oder Grundgesamtheit? Mikrodaten oder tabellarische Daten?
- Welche Datenquellen mit sich überschneidenden Grundgesamtheiten gibt es auf dem *Markt*?
- Bestimmung eines sogenannten **Disclosure-Szenarios**.
- Individuelles Risiko (jeder einzelnen Person) und globales Risiko

Anonymisierung in der Praxis: Grober Ablauf

1) **RISK** Messung des Risikos 

- Stichprobe oder Grundgesamtheit? Mikrodaten oder tabellarische Daten?
- Welche Datenquellen mit sich überschneidenden Grundgesamtheiten gibt es auf dem *Markt*?
- Bestimmung eines sogenannten **Disclosure-Szenarios**.
- Individuelles Risiko (jeder einzelnen Person) und globales Risiko

2)  Anonymisierung 

- Traditionelle Methoden oder synthetische Datengenerierung?
- Kategoriale Variablen und/oder kontinuierliche Variablen?
- Sind Cluster und hierarchische Strukturen in den Daten vorhanden?

Anonymisierung in der Praxis: Grober Ablauf

1) **RISK** Messung des Risikos 

- Stichprobe oder Grundgesamtheit? Mikrodaten oder tabellarische Daten?
- Welche Datenquellen mit sich überschneidenden Grundgesamtheiten gibt es auf dem *Markt*?
- Bestimmung eines sogenannten **Disclosure-Szenarios**.
- Individuelles Risiko (jeder einzelnen Person) und globales Risiko

2)  Anonymisierung 

- Traditionelle Methoden oder synthetische Datengenerierung?
- Kategoriale Variablen und/oder kontinuierliche Variablen?
- Sind Cluster und hierarchische Strukturen in den Daten vorhanden?

3)  Messung des Nutzens der anonymisierten Daten 

Arten von Merkmalen in Daten (1/2)

1. **Löschen** global eindeutiger (z. B. Versicherungsnummer) und **direkter Identifikatoren** (z. B. genaue Adresse oder Name) oder **Pseudo-Anonymisierung** dieser (mit bereichs- und projektspezifischen *Salts* und *Hashes*)

Arten von Merkmalen in Daten (1/2)

1. **Löschen** global eindeutiger (z. B. Versicherungsnummer) und **direkter Identifikatoren** (z. B. genaue Adresse oder Name) oder **Pseudo-Anonymisierung** dieser (mit bereichs- und projektspezifischen *Salts* und *Hashes*)
2. **Quasi-Identifikatoren** (z. B. Postleitzahl, Alter, Geschlecht), abgekürzt QIDs: Attribute, die zur Re-Identifizierung verwendet werden können; werden auch als auch **Schlüsselvariablen**, *Indirekte Identifikatoren* oder *Implizite Identifikatoren* bezeichnet. Salopp: Diejenigen Variablen, die sich mit anderen auf dem Markt verfügbaren Populationen (oder Stichproben) überschneiden.

Arten von Merkmalen in Daten (1/2)

1. **Löschen** global eindeutiger (z. B. Versicherungsnummer) und **direkter Identifikatoren** (z. B. genaue Adresse oder Name) oder **Pseudo-Anonymisierung** dieser (mit bereichs- und projektspezifischen *Salts* und *Hashes*)
2. **Quasi-Identifikatoren** (z. B. Postleitzahl, Alter, Geschlecht), abgekürzt QIDs: Attribute, die zur Re-Identifizierung verwendet werden können; werden auch als auch **Schlüsselvariablen**, *Indirekte Identifikatoren* oder *Implizite Identifikatoren* bezeichnet. Salopp: Diejenigen Variablen, die sich mit anderen auf dem Markt verfügbaren Populationen (oder Stichproben) überschneiden.

Ein **Schlüssel** definiert eine Kombination von Werten der QIDs (z.B. Alter $= 10$, Geschlecht $=$ M, Region $=$ ZH)

Beispiel: Abgleich von Schlüsselvariablen (1)

Bereitgestellte Datensätze (QIDs und Schlüssel) Wohnsitz $\times$ Beruf $\times$ Geschlecht)

name	Wohnsitz	Beruf	Geschlecht	# $\{1, .., n\} \in$ key	Einkom
x	Stadel	Prof	M	1	176456
x	Winterthur	architect	M	18	143111
x	...	...	...	...	...

Externer Datensatz (das externe Wissen des Eindringlings)

name	Wohnsitz	Beruf	Geschlecht	# $\{1, .., n\} \in$ key	...
Max Muster	Stadel	Prof	M	1	...
Jo Johann	Winterthur	architect	M	18	...
Nils Nilson	Winterthur	architect	M	18	...
...	...	...	...	...	...

Beispiel: Abgleich von Schlüsselvariablen (1)

Beobachtungen linked (QID's und Schlüssel Wohnsitz × Beruf × Geschlecht)

Name	Wohnsitz	Beruf	Geschlecht	# $\{1, .., n\} \in$ key	Einkor
Max Muster	Stadel	Prof	M	1	17645
x	Winterthur	architect	M	18	14311
x	...	...	...	...	...

Externer Datensatz (das externe Wissen des Angreifers)

Name	Wohnsitz	Beruf	Geschlecht	# $\{1, .., n\} \in$ key	...
Max Muster	Stadel	Prof	M	1	...
Jo Johann	Winterthur	architect	M	18	...
Nils Nilson	Winterthur	architect	M	18	...
...	...	...	...	...	...

Beispiel: Abgleich von Schlüsselvariablen (1)

Beobachtungen linked (QID's und Schlüssel Wohnsitz × Beruf × Geschlecht)

Name	Wohnsitz	Beruf	Geschlecht	# $\{1, .., n\} \in$ key	Einkor
Max Muster	Stadel	Prof	M	1	17645
x	Winterthur	architect	M	18	14311
x	...	...	...	...	...

Externer Datensatz (das externe Wissen des Angreifers)

Name	Wohnsitz	Beruf	Geschlecht	# $\{1, .., n\} \in$ key	...
Max Muster	Stadel	Prof	M	1	...
Jo Johann	Winterthur	architect	M	18	...
Nils Nilson	Winterthur	architect	M	18	...
...	...	...	...	...	...

→ Max Muster ist eindeutig zuzuordnen.

Types of characteristics in data (2/2)

3. **Sensitive attributes** (e.g. sickness status, costs, late payments, mental disorder, ...): Informationen, mit denen man nicht in Verbindung gebracht werden möchte.
4. ... there are more (hierarchische Strukturen, Clusters, linked variables, sampling weights, event dates, longitudinal information, trajectories, ...)

Re-identifizierungsrisiko, allgemein

Der **wichtigste und komplizierteste Teil** ist nicht die Anwendung von Anonymisierungsmethoden, sondern **die Messung des Re-Identifizierungsrisikos** von Personen.

- bei Grundgesamtheiten ist die Risikobestimmung einfacher.
- nicht trivial für Erhebungsstichproben und/oder für Daten mit fehlenden Werten

Re-identifizierungsrisiko, allgemein

Der **wichtigste und komplizierteste Teil** ist nicht die Anwendung von Anonymisierungsmethoden, sondern **die Messung des Re-Identifizierungsrisikos** von Personen.

- bei Grundgesamtheiten ist die Risikobestimmung einfacher.
- nicht trivial für Erhebungsstichproben und/oder für Daten mit fehlenden Werten

2 Schritte:

1. Bestimmung des **Disclosure-Szenarios** (Was sind die Schlüsselvariablen?) = welche überlappenden Variablen sind in zugänglichen externen Datensätzen enthalten und können für das Matching verwendet werden (GfK-Daten, BFS-Daten, Social Media-Daten, ...)
2. **Risikomessung** mit math. Methoden des *Statistical Disclosure Control*

Grundbegriffe Offenlegungsrisiko für Populationen

Begriff der **Einzigartigkeit**:

- Durch die Kombination mehrerer Variablen (der QIDs) kann ein Individuum eindeutig im Datensatz identifiziert werden.
- Ein Schlüssel ist eindeutig, wenn seine Häufigkeit 1 ist (nur eine Person hat die durch den Schlüssel definierte Merkmalskombination. Beispiel: der Schlüssel Postleitzahl **8404**, Staatsbürgerschaft **Österreich**, **Mann**, **Alter 45**)

Grundbegriffe Offenlegungsrisiko für Populationen

Begriff der **Einzigartigkeit**:

- Durch die Kombination mehrerer Variablen (der QIDs) kann ein Individuum eindeutig im Datensatz identifiziert werden.
- Ein Schlüssel ist eindeutig, wenn seine Häufigkeit 1 ist (nur eine Person hat die durch den Schlüssel definierte Merkmalskombination. Beispiel: der Schlüssel Postleitzahl **8404**, Staatsbürgerschaft **Österreich**, **Mann**, **Alter 45**)

Konzept k-**Anonymität**:

- Jede Kombination von Schlüsselvariablen enthält mindestens k Beobachtungen
- Oft wollen wir 3-Anonymität sicherstellen

Risikobewertung - Überblick

- Bestimmung des Identifizierungsrisikos für **jede** Person
- Risikoeinschätzung: Unterscheidung zwischen **kategorialen** Schlüsselvariablen (wie Alter, Geschlecht, Region, . . .) und **kontinuierlichen** Schlüsselvariablen (wie Kosten, Einkommen, . . .)

Risikobewertung - Überblick

- Bestimmung des Identifizierungsrisikos für **jede** Person
- Risikoeinschätzung: Unterscheidung zwischen **kategorialen** Schlüsselvariablen (wie Alter, Geschlecht, Region, ...) und **kontinuierlichen** Schlüsselvariablen (wie Kosten, Einkommen, ...)

Daten der gesamten **Bevölkerung** (z.B. Daten von allen Personen mit diagnostizierter psychischer Störung im Kanton Zürich)

- Konzept der Einzigartigkeit, k-Anonymität
- l-Diversität, ...
- *Einzigartigkeit auf Teilmengen* (SUDA)

Risikobewertung - Überblick

- Bestimmung des Identifizierungsrisikos für **jede** Person
- Risikoeinschätzung: Unterscheidung zwischen **kategorialen** Schlüsselvariablen (wie Alter, Geschlecht, Region, ...) und **kontinuierlichen** Schlüsselvariablen (wie Kosten, Einkommen, ...)

Daten der gesamten **Bevölkerung** (z.B. Daten von allen Personen mit diagnostizierter psychischer Störung im Kanton Zürich)

- Konzept der Einzigartigkeit, k-Anonymität
- l-Diversität, ...
- *Einzigartigkeit auf Teilmengen* (SUDA)

Daten aus komplexen **Erhebungen** (z.B. Umfrage zum sozialen Kontaktverhalten in Covid-19 Zeiten)

- Ansatz des individuellen Risikos
- globales Risiko über log-lineare Modelle

k-Anonymität und l-Diversity

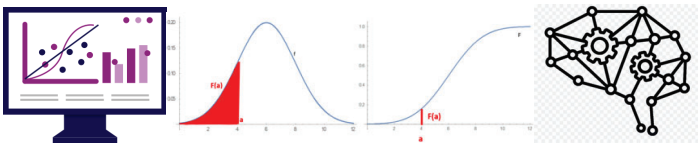
Beispiel: k-Anonymität und l-Diversität

	key variables		f_k	sensitive variable	distinct l-diversity
	gender	age group		stage of dementia	
1	male	30s	3	3	2
2	male	30s	3	0	2
3	male	30s	3	0	2
4	female	20s	3	1	1
5	female	20s	3	1	1
6	female	20s	3	1	1

Methoden zur Anonymisierung von Daten

Verschiedene Gruppen von Methoden:

- Methoden, die Werte Verallgemeinern oder Unterdrücken. Beispiele sind Umkodierung oder lokale Unterdrückung
- Methoden, die Daten *verändern*. Beispiele sind Hinzufügen von Rauschen, Post-Randomisierungsmethode (PRAM), Mikroaggregation und Shuffling.
- Methoden zur Erzeugung synthetischer Daten



Umkodierung

Umkodierung von kategorialen Schlüsselvariablen:

- Anonymität durch Zusammenlegung/Verallgemeinerung von Kategorien erreichen
  - Beispiel: Zusammenlegung/Verallgemeinerung mehrerer Postleitzahlen (8400, 8401, 8402, 8403, 8404 zu 840x)
  - Beispiel: Von Y/M/D zu Y/M für Geburtsdatum

Umkodierung kontinuierlicher Variablen

- bedeutet, die Variable zu diskretisieren
  - Beispiel: Genaues Alter einer Person in Alterskategorien

Lokale Unterdrückung

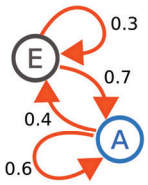
Problemstellung: Einige Personen haben nach Anwendung voriger Methoden immer noch ein erhöhtes Risiko. Würden weitere Informationen vergröbert oder umkodiert werden → Utility zu klein. Ausweg:

Lokale Unterdrückung

- **Ziel**: So wenig Werte wie möglich zu unterdrücken um z.B. k-Anonymität zu gewährleisten (ein optimales Unterdrückungsmuster zu finden)
- Wird typischerweise **nach** einer Umkodierung eingesetzt, um das Restrisiko zu minimieren.
- Heuristische **Optimierungsmethoden**, um bestimmte Muster in kategorialen Schlüsselvariablen zu finden. Ersetzen Sie dieses Muster durch fehlende Werte.
- Weitere Komplexität: Häufigkeiten von Schlüsseln mit fehlenden Werten.
- Gewichtung der Variablen nach ihrer Wichtigkeit

Post Randomization (PRAM)

- Werte zwischen Kategorien einer Variablen mit gegebenen Übergangswahrscheinlichkeiten vertauschen.
  - Beispiel: mit einer Wahrscheinlichkeit von 0.1 wird der Wohnort Oberwinterthur mit dem Wohnort Winterthur-Hegi vertauscht.
  - In der Praxis meist innerhalb von Schichten (z.B. Vertauschen der Postleitzahl einer Person nur innerhalb eines Kantons).
- Der Angreifer kann nie sicher sein, ob ein Wert wahr ist oder vertauscht wurde.
- In der Praxis häufig verwendet: Austausch von geografischen Informationen mit PRAM



Anonymisierung von kontinuierlichen Schlüsselvariablen

- **Mikroaggregation**: Finden ähnlicher Beobachtungen (Clustering-Problem) und Ersetzen der Werte durch ein Aggregat (z. B. arithm. Mittelwert)
  - garantieren, dass z.B. mindestens k Beobachtungen die gleichen Werte aufweisen
- **Zufügen von Rauschen**
  - zufälliges Rauschen z.B. zum Geburtsjahr hinzufügen ...
- **Shuffling**: komplexere Methode, die ein statistisches (Regressions-)Modell verwendet, jedoch mit einigen Mängeln.
- ...

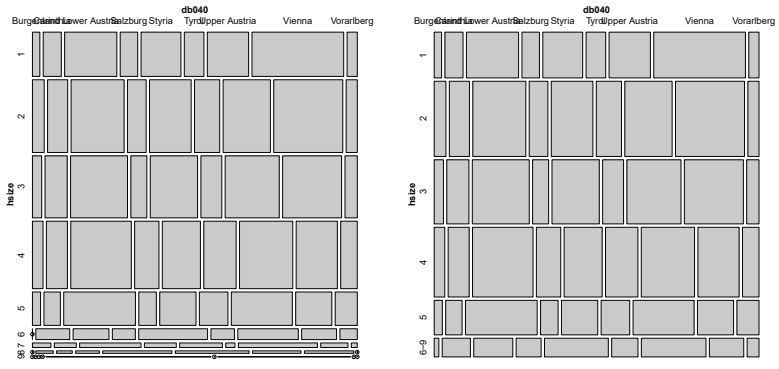
Utility

- Nach der Anonymisierung von Daten ist es wichtig, den Informationsverlust und die Datenqualität zu bewerten.
- Vergleich von Ergebnissen aus ursprünglichen und anonymisierten Daten (Tabellen, Regressionsmodelle, Verteilungen, . . .)
- Vergleich von Indikatoren
- Propensity-Score-Matching-Methoden
- Etc.

Wenn die Utility klein ist, sollte eine andere Anonymisierung in Betracht gezogen werden.

Trade-Off und iterativer Ansatz (Anonymisierung $\leftrightarrow$ Nutzen)

Utility Bsp einer (von vielen mögl.) Visualisierung(en)



Mosaikplot von Geschlecht (`rb090`) $\times$ Staatsangehörigkeit (`pb220a`) $\times$ Haushaltsgröße (`hsize`) mit den ursprünglichen Stichprobenhäufigkeiten (linkes Diagramm) und den Stichprobenhäufigkeiten aus den anonymisierten Daten (rechtes Diagramm).

Software

 **sdcMicro** (Templ et al., Journal of Statistical Software, 2016)

- state-of-the-art Software
- kann komplexere Daten verarbeiten
- mit Klick-App (für den Browser)
- ist sehr effizient programmiert (C++-Code, paralleles Rechnen)

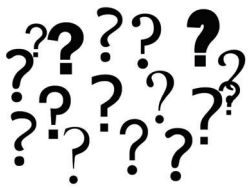
 **simPop** (Templ et al., Journal of Statistical Software, 2017)

- für die Erstellung von synthetischen Datensätzen
- kann im Gegensatz zu anderer Software auch komplexere Datenstrukturen verarbeiten

 **sdcTable** and **cellKey** (Author: B. Meindl)

- Für die Anonymisierung von aggregierter Information

Schwierigkeiten in der Praxis



- Leider gibt es keine allgemeine Lösung und kein standardisiertes Verfahren.
- Anonymisierungsmethoden sind an sich fast trivial, aber deren Anwendung (inklusive Risikomessung und Messung der Utility) in der Praxis ist höchst komplex, da:
- Die Anonymisierung und Wahl der Methoden variieren von Fall zu Fall $\Longrightarrow$ stark daten- und fallabhängig.
- Langjährige Erfahrung erforderlich.

Zukünftiges

Fellowship DIZH *Anonymisierung und Abschätzung des Re-Identifizierungsrisikos von personenbezogenen Daten*, Kompetenzzentrum Datenanonymisierung.

- Start Fellowship: Sept. 2020.
- Das Kompetenzzentrum für Datenanonymisierung wird noch dieses Jahr gegründet.

Zukünftiges

Fellowship DIZH *Anonymisierung und Abschätzung des Re-Identifizierungsrisikos von personenbezogenen Daten*, Kompetenzzentrum Datenanonymisierung.

- Start Fellowship: Sept. 2020.
- Das Kompetenzzentrum für Datenanonymisierung wird noch dieses Jahr gegründet.

Matthias Templ Anonymisierung: so wird sie gemacht und gemessen 26 / 26

Zukünftiges

Fellowship DIZH *Anonymisierung und Abschätzung des Re-Identifizierungsrisikos von personenbezogenen Daten*, Kompetenzzentrum Datenanonymisierung.

- Start Fellowship: Sept. 2020.
- Das Kompetenzzentrum für Datenanonymisierung wird noch dieses Jahr gegründet.

Haben Sie weitere Fragen zum Inhalt dieser Präsentation oder zum Thema im Allgemeinen?

→ matthias.templ@zhaw.ch

5. DATENSCHUTZRECHTSTAGUNG

Neue Regeln, weniger Spielräume?

Datenschutz in den Medien: Spielräume und Grenzen

CHANTAL IMFELD-MATYASSY, Head of Data Protection & Data Protection Officer,
Ringier Group

Ringier

We inform.
We entertain.
We connect.

06. September 2021

Chantal Imfeld-Matyassy
Head of Data Protection & Data Protection Officer Ringier Gruppe

Datenschutz in den Medien: Spielräume und Grenzen

Agenda

1. Wer sind wir und was tun wir?
2. Der wilde “Westen”
3. Das Ende der Cookie-Ära?
4. Ausblick - Was tun wir bei Ringier?

We are into media – ever since 1833!

Die Entwicklung auf einen Blick...and it goes on!

1833 | 1915 | 1970 | 1987 | 2003 | 2007 | 2015

1833
Pastor's son Johann Rudolf Ringier buys a printing house in Zofingen.

1911
The first edition of the *Schweizer Illustrierte Zeitung* is published.

1921
The first edition of *L'illustré* is published. Ringier Romandie goes into business.

1959
The first edition of *Blick* is published.

1974
Ringier launches the first Swiss School of Journalism at Römerhalde.

1978
Opening of the Ringier Pressehaus in Zurich.

1987
First business operations in China (printing house in Hong Kong).

1989
The newspaper *Cash* revolutionises financial reporting. Ringier expands into Eastern Europe, starting with the Czech Republic.

2007
Takeover of *Energy* radio and beginning of involvement in Scout24 Schweiz AG.

2008
Launch of the free commuter newspaper *Blick am Abend*.

2010
First newsroom in Switzerland for the *Blick* Group.

2011
First business operations in Africa.

2012
Ringier steps up its diversification: *DeinDeal*, *Geschenkidee*, *Anibis.ch*, etc.

2015
Founding of Admeira, the joint-venture between Ringier, SRG and Swisscom

2016
New joint-venture Ringier Axel Springer Schweiz AG.

Die Entwicklung auf einen Blick...and it goes on!

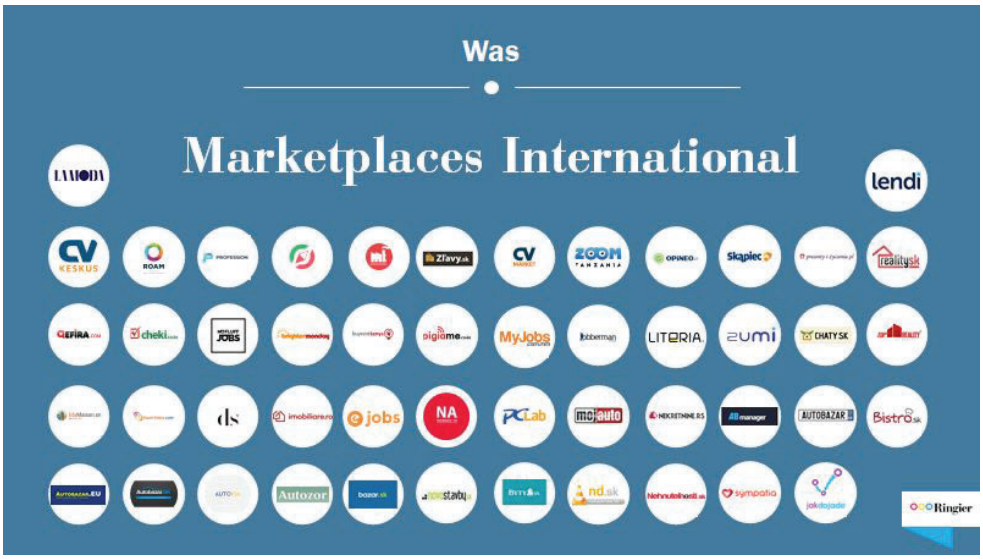
Ringier Group - Heute

6

Ringier Group - Heute

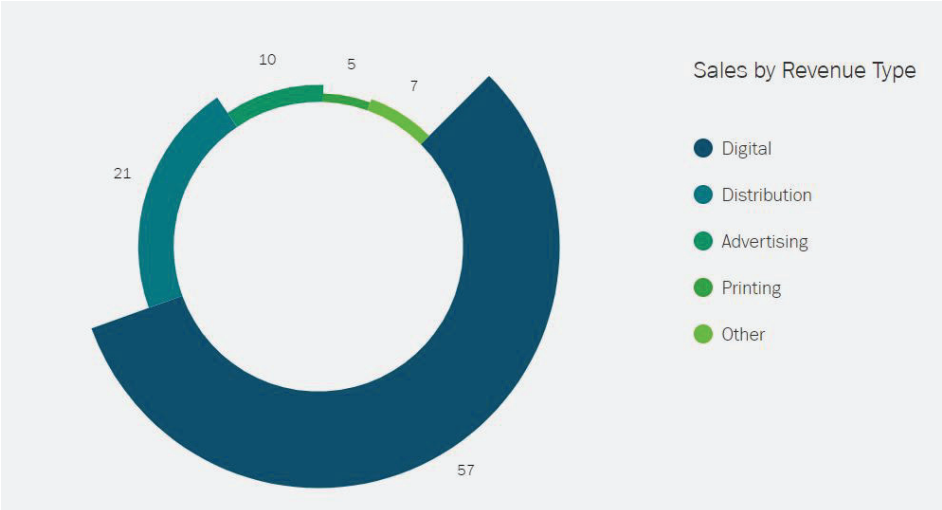
Ringier Group - Heute

Ringier Group - Heute

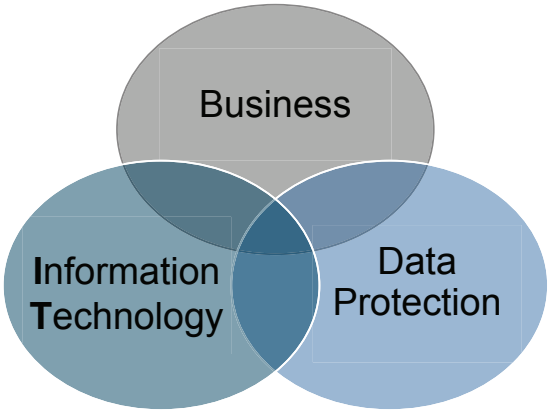


9

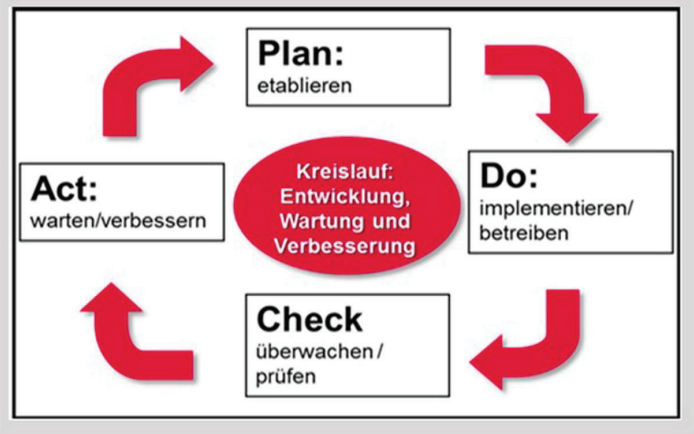
Ringier Group - Heute



Data Protection is a process and not a product!



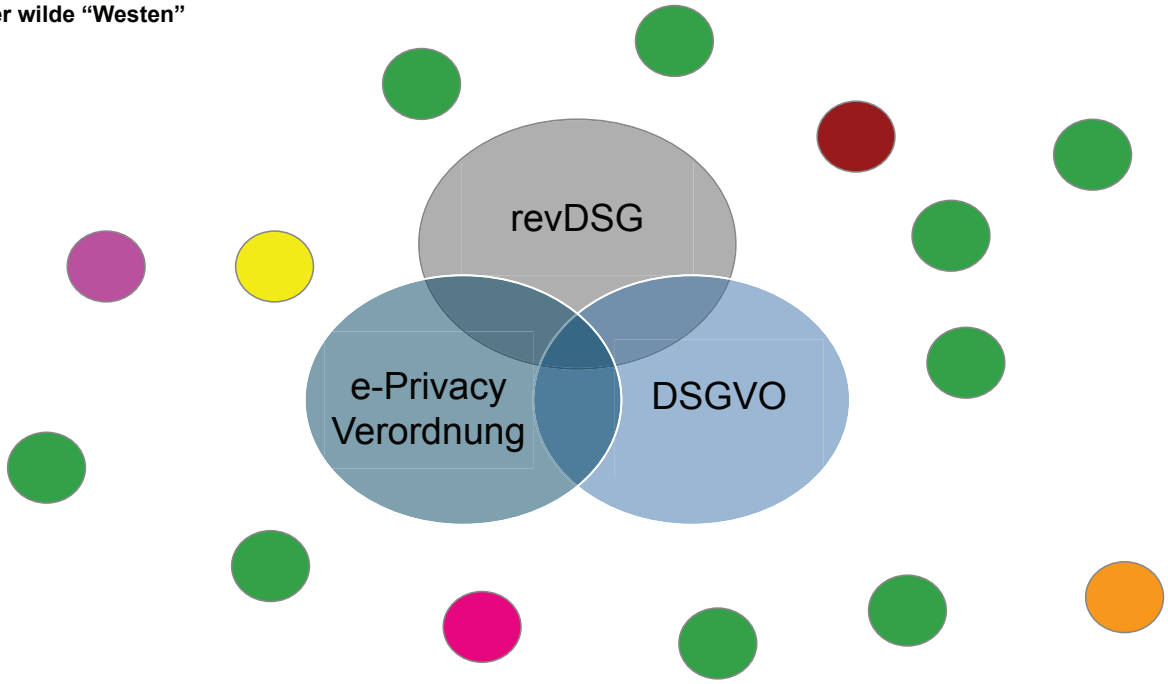
Data Protection must be agile!



Der wilde “Westen”

©Samuel John Carter

Der wilde “Westen”



Das Ende der Cookie-Ära?

Ausblick - was tun wir bei Ringier?

© ra2studio / iStock

Ringier

We inform.
We entertain.
We connect.

Vielen Dank für Ihre Aufmerksamkeit

5. DATENSCHUTZRECHTSTAGUNG

Weniger Regeln, neue Spielräume?

Überwachung am Arbeitsplatz: was geht?

Dr. DAVID VASELLA, Rechtsanwalt, Zürich und Dr. IRENE SUTER-SIEBER, Rechtsanwältin
Zürich

Überwachung am Arbeitsplatz: Was geht?

8. September 2021 • Schweizer Forum für Kommunikationsrecht (SF-FS) • Datenschutzrechtstagung
Irène Suter-Sieber und David Vasella

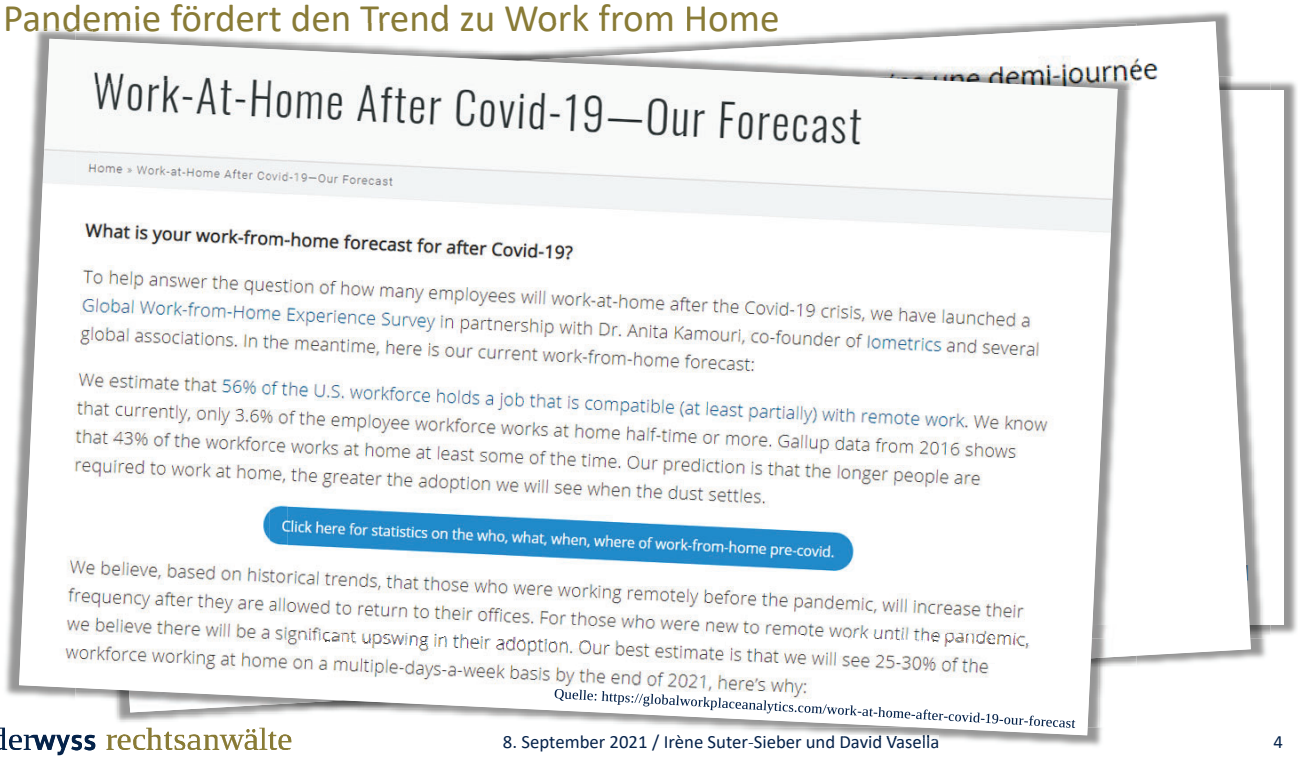
walderwyss rechtsanwälte

Übersicht

1. Intro
2. Motive
3. Rechtsgrundlagen
4. Risiken
5. Empfehlung
6. Zum Schluss

Intro

Die Pandemie fördert den Trend zu Work from Home



Work-At-Home After Covid-19—Our Forecast

Home » Work-at-Home After Covid-19—Our Forecast

What is your work-from-home forecast for after Covid-19?

To help answer the question of how many employees will work-at-home after the Covid-19 crisis, we have launched a Global Work-from-Home Experience Survey in partnership with Dr. Anita Kamouri, co-founder of Iometrics and several global associations. In the meantime, here is our current work-from-home forecast:

We estimate that 56% of the U.S. workforce holds a job that is compatible (at least partially) with remote work. We know that currently, only 3.6% of the employee workforce works at home half-time or more. Gallup data from 2016 shows that 43% of the workforce works at home at least some of the time. Our prediction is that the longer people are required to work at home, the greater the adoption we will see when the dust settles.

Click here for statistics on the who, what, when, where of work-from-home pre-covid.

We believe, based on historical trends, that those who were working remotely before the pandemic, will increase their frequency after they are allowed to return to their offices. For those who were new to remote work until the pandemic, we believe there will be a significant upswing in their adoption. Our best estimate is that we will see 25-30% of the workforce working at home on a multiple-days-a-week basis by the end of 2021, here's why:

Quelle: https://globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast

Steigende Nachfrage nach HR-Analytics-Tools

- **Global demand** for employee monitoring software increased by:
  - **87% in April 2020** compared with monthly average prior to the pandemic, following an initial **7% bump in March**
  - **71% in May 2020** versus pre-pandemic levels
- **Second wave of demand:** 63% average increase since March 2021 compared to pre-pandemic average. This is a 24% increase compared to nine months prior.
- **New normal**: 58% more interest in employee surveillance since pandemic declared than before
- **Most popular surveillance tools:** Hubstaff, Time Doctor, FlexiSPY
- **Eight in 10** of the most in-demand companies incentivize long-term use

Quelle: https://www.top10vpn.com/research/covid-employee-surveillance/

Umfrage des Forschungsinstituts für Arbeit und Arbeitswelten der Universität St. Gallen 2020:

– Die Mehrheit der befragten Unternehmen investiert unabhängig von der Pandemie in sogenannte HR-Analytics-Tools.
– 10 Prozent der befragten Unternehmen haben seit dem Ausbruch von Covid-19 «stark» in den Ausbau von HR-Analytics-Tools investiert.

Motive

2

Motive der Überwachung (1/2)

- Kontrollpflichten *ex lege*:
  - Einhaltung des Gesundheitsschutzes durch Arbeitnehmer
    bspw. Arbeitsplatzeinrichtung im Homeoffice
  - Prüfung der Einhaltung der Arbeits- und Ruhezeiten durch Arbeitnehmer
    insb. Höchstarbeitszeit/Pausen/Verbot von Nacht- und Sonntagsarbeit
  - FINMA Rundschreiben 2013/8 – Marktverhaltensregeln
    Überwachung von Mitarbeitergeschäften
- Sicherheit und Unfallverhütung (Diebstahlschutz, Arbeitssicherheit)
  bspw. Videoüberwachung des Kassenraums
- Verbesserung von Arbeitsabläufen
  bspw. durch GPS-Tracker
- Kontrolle der Arbeitsleistung/-qualität
  bspw. Anzahl entgegengenommene Anrufe im Callcenter;
  Anzahl versendete E-Mails

Motive der Überwachung (2/2)

- Wissensmanagement
  bspw. Datenanalyse, um Know-how Träger auszumachen
- Compliance mit Gesetzen/Reglementen
  bspw. Analyse von Telefonaten/E-Mails auf Triggerworte
- Schutz vor sich selbst? Anleitung von Mitarbeitern zur besseren Selbstorganisation
  bspw. M365 – MyAnalytics

Rechtsgrundlagen

3

Rechtliche Rahmenbedingungen (1/2)

Quelle	Norm	Kurzbeschrieb
Strafrecht	Art. 179bis-179^{novies} StGB	Insb. (i) Verbot der Aufnahme eines nichtöffentlichen Gesprächs ohne die Einwilligung der Teilnehmer sowie (ii) Verbot der Aufnahme auf einen Bildträger einer Tatsache aus dem Geheimbereich eines andern oder einer nicht jedermann ohne weiteres zugänglichen Tatsache aus dem Privatbereich eines andern ohne dessen Einwilligung
Persönlichkeits-schutz	Art. 28 ff. ZGB	Achtung der Persönlichkeit
Datenschutzrecht	Art. 4 ff. DSG (Art. 6 ff. revDSG) (i.d.R. nicht DSGVO)	Bearbeitungsgrundsätze, insbesondere Verhältnismässigkeit und Transparenz/Zweckbindung

Rechtliche Rahmenbedingungen (2/2)

Quelle	Norm	Kurzbeschrieb
Arbeitsvertragsrecht	Art. 328/328b OR	Datenbearbeitung nur bei «Arbeitsplatzbezug»: Daten müssen die Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sein. D.h. die Bearbeitung rein privater Daten ist i.d.R. nicht erlaubt. Ob der Arbeitnehmer rechtsgültig in die Datenbearbeitung ohne Arbeitsplatzbezug einwilligen kann, ist höchstrichterlich nicht geklärt.
Gesundheitsschutzrecht	Art. 6 ArG i.V.m. Art. 26 ArGV1	Verbot von Verhaltenskontrollsystemen, die geeignet sind, die Gesundheit oder das Wohlbefinden der Arbeitnehmer zu beeinträchtigen (BGer 6B_536/2009 E. 3.6.2). Einwilligung *dagegen* ist nicht möglich.
Mitwirkungsrecht	Art. 6 Abs. 3 ArG i.V.m. Art. 6 Abs. 1/2 ArGV3 Art. 10 lit. a MitwG i.V.m. Art. 48 ArG	Mitspracherecht der Arbeitnehmer in Fragen des Gesundheitsschutzes, d.h. Anspruch auf Anhörung und Beratung sowie Begründung eines ablehnenden Entscheids. ABER: kein Recht auf Mitentscheidung.

Risiken

4

Und wenn die Überwachung zu weit geht?

- **Verwertungsverbot von Beweismaterial im Zivilprozess**

  Art. 152 Abs. 2 ZPO: «Rechtswidrig beschaffte Beweismittel werden nur berücksichtigt, wenn das Interesse an der Wahrheitsfindung überwiegt.»

- **Verwertungsverbot von Beweismaterial im Strafprozess**

  BGer 6B_1468/2019 E. 1.3.1: «Von Privaten rechtswidrig erlangte Beweismittel sind nur verwertbar, wenn sie von den Strafverfolgungsbehörden rechtmässig hätten erlangt werden können und kumulativ dazu eine Interessenabwägung für deren Verwertung spricht. […] Die Verwertung ist […] nur zulässig, wenn dies zur Aufklärung einer schweren Straftat unerlässlich ist […].»

- **Strafrechtliche Sanktionen**: Abhören und Aufnehmen fremder Gespräche und Verletzung des Geheim- und Privatbereichs durch Aufnahmegeräte

OGer ZH LA180031 vom 20.3.2019: Unverwertbarkeit der privaten WhatsApp Nachrichten mit ehrverletzendem Inhalt und Hinweisen auf Simulierung einer Arbeitsunfähigkeit. Fristlose Entlassung der Mitarbeiterin ungerechtfertigt.

BGer 6B_1468/2019 E. 1.3.1: Verwertbarkeit der Videoaufnahmen von vier Überwachungskameras eines Hotels (DSG-Grundsatz der Erkennbarkeit und von Treu und Glauben verletzt), die den Täter beim Landfriedensbruch zeigten.

Art. 179bis-179^{quater} StGB: Freiheitsstrafe bis zu 3 Jahren oder Geldstrafe (auf Antrag).

Und wenn die Überwachung zu weit geht?

- **Busse nach dem revDSG**
  Verletzung der Informationspflicht bzw. des Auskunftsrechts (Achtung: Generalklausel)
- **Arbeitsinspektorat prüft Gesundheitsschutz**
- **Reputation**
- **Arbeitnehmerzufriedenheit/Hiring Markt**
- **Schadenersatz und Genugtuung**

Art. 60 Abs. 1 revDSG: Busse bis CHF 250’000 für die verantwortlichen Personen.

BGer 8C_539/2015: Arbeitgeberin sichtete private Daten des Arbeitnehmers ohne Arbeitsplatzbezug. Klage des Arbeitnehmers auf Genugtuung (CHF 35’000) wegen Persönlichkeitsverletzung wurde abgewiesen, da nur leichte Verletzung. *Obiter*: Anders könnte es sein bei Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen.

Empfehlungen

5

Empfehlungen

1. Anonymisierte Überwachung als Ausgangspunkt
2. Personenbezogenes Vorgehen bei Verdacht
3. Bei personenbezogener Überwachung:
   a. Prüfung der Verhältnismässigkeit und der Transparenz
   b. Prüfung des Arbeitsplatzbezugs
   c. Prüfung einer möglichen Beeinträchtigung der Gesundheit und des Wohlbefindens der Arbeitnehmer
   d. Ton- und Videoaufnahmen grundsätzlich nur mit vorgängiger Einwilligung
4. Dokumentation der internen Weisungen und Überlegungen
5. Sorgfältige Redaktion von Datenschutzerklärungen und Auskunftsmitteilungen
6. Datenschutzfolgeabschätzung
7. Einbezug der Belegschaft vor Implementierung von präventiven Überwachungsmassnahmen

Zum Schluss

6

Thesen

- Klassische Überwachung: entspricht zunehmend dem Erwarteten
  - Mitarbeiter haben andere Erwartungen, aber Arbeitgeber können auch offener kommunizieren
- Neue Formen: «Nudging» im Spannungsfeld zwischen Entmündigung und Empowerment
  - Gesundheitsschutz ist nicht nur Datenschutz – Menschenrecht auf Ineffizienz? «Diffus bedrohliches Gefühl des Beobachtetseins» – BVerfG; «right to be left alone» (1890!)
- Datenschutz durch neue Technologien vielleicht weniger relevant als der Gesundheitsschutz: Art. 26 ArGV 3 als Grundnorm?

Vielen Dank!

RA Dr. iur. Irène Suter-Sieber, Fachanwältin SAV Arbeitsrecht
Irene.suter@walderwyss.com • +41 58 658 56 60

RA Dr. David Vasella, CIPP/E, CIPM
david.vasella@walderwyss.com • +41 58 658 52 87

www.walderwyss.com

walderwyss rechtsanwälte