4. DATENSCHUTZRECHTSTAGUNG

Das neue DSG

8. September 2020, 13:45 – 18:00 Uhr

Universität Zürich, Raum KOL-G-201 (Aula)

Rämistrasse 71, 8006 Zürich

Nachdem die DSGVO während Jahren im Zentrum der Diskussion stand, liegt der Fokus derzeit auf der Revision des Schweizer Rechts. Die 4. Datenschutzrechtstagung des SF-FS widmet sich deshalb vertieft dem neuen DSG. Noch sind ein paar allerletzte Differenzen zu bereinigen, die wesentlichen Züge des künftigen Rechts sind aber doch schon klar erkennbar. Parallel zu den Revisionsarbeiten hat sich auch in der schweizerischen und europäischen Praxis einiges bewegt.

Die ersten beiden Referate vermitteln deshalb einen Überblick über die jüngsten Entscheidungen und Entwicklungen in der Schweiz und der EU. Längst ist auch ausserhalb Europas vieles in Bewegung geraten, nicht zuletzt in den USA. Für global tätige Unternehmen sind die raschen und teilweise tiefgreifenden Veränderungen der Rechtslage und die (weiterhin) beträchtlichen Unterschiede zwischen den einzelnen Staaten eine grosse Herausforderung. Mit diesen befasst sich das dritte Referat des ersten Teils, das Strategien und Perspektiven eines Global Players aufzeigt.

Der zweite Teil der Tagung widmet sich dann ganz dem neuen DSG. Das erste Referat geht auf die zentralen materiellen Neuerungen ein; im Vordergrund stehen dabei Fragen wie die neuen Informationspflichten (und ihre Ausnahmen!), Profiling (spielt es überhaupt eine Rolle?) und das Strafbarkeitsrisiko (und wie bedrohlich die Strafen wirklich sind). Das zweite Referat fokussiert auf die neuen Anforderungen an die Governance: Was muss verzeichnet und dokumentiert werden, ist jede falsch versandte Mail meldepflichtig und wie weit muss ein Betrieb bei einer Datenschutz-Folgenabschätzung gehen – der EDÖB erklärt, was er künftig erwartet. Der erste und zweite Teil der Tagung enden jeweils mit einer Panel- und Plenumsdiskussion. Diese bieten den Teilnehmenden die Möglichkeit, brennende Fragen zum geltenden Recht und zum neuen DSG aufzuwerfen 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
Upddate DSG
ROLAND MATHYS, Rechtsanwalt Zürich

14:30 – 15:00
Das neue DSGVO
Dr. MARIE LOUISE GÄCHTER-ALGE, Leiterin Datenschutzstelle,
Fürstentum Liechtenstein

15:00 – 15:30
Strategien und Perspektiven eines Global Players
Dr. ANNA ZEITER, Chief Privacy Officer eBay

15:30 – 16:00
Panel und Plenumsdiskussion

15:30 – 16:00 - Pause

16:30 – 17:00
Das neue DSG: Fokus materielles Recht
DAVID ROSENTHAL, Rechtskonsulent Zürich

17:00 – 17:30
Das neue DSG: Fokus Governance
Dr. ADRIAN LOBSIGER, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

17:30 – 18:00
Panel und Plenumsdiskussion

ab 18:00 Apéro

4. DATENSCHUTZRECHTSTAGUNG

Das neue DSG

Update DSG

ROLAND MATHYS, Rechtsanwalt, Zürich

SF-FS: 4. Datenschutzrechtstagung

Update Datenschutz

Roland Mathys, LL.M.

Zürich, 8. September 2020

1

Einleitung (1): Update Datenschutz?

2

Einleitung (2): Update Datenschutz!

Schellenberg Wittmer

Agenda

- Einleitung
- Arbeitsverhältnis
- Datenschutz in der Cloud
- Biometrische Daten
- Leading Cases
- Internationales Verhältnis
- Fazit

Schellenberg Wittmer

Arbeitsverhältnis (1): Art. 328b OR und DSG

- Art. 328b OR: Datenschutzrechtliche Sonderbestimmung im Arbeitsverhältnis
- Einschränkung der zulässigen Bearbeitungszwecke
  - Eignung für das Arbeitsverhältnis
  - Durchführung des Arbeitsvertrags
- Im Übrigen gilt DSG
  - Insbesondere Rechtfertigungsgründe (Art. 13 DSG)
  - Vorbehalt bei Zustimmung (wegen Art. 362 OR)
  - So auch OGer ZH (LA180002 vom 20.03.2018)
- Neuere Rechtsprechung des OGer ZH (LA180019 vom 15.03.2019, LA180031 vom 20.03.2019)
  - Jede Datenbearbeitung ohne genügenden Arbeitsplatzbezug unzulässig
  - Keine Rechtfertigungsmöglichkeiten

Schellenberg Wittmer

Arbeitsverhältnis (2): Covid-19

- Ausgangslage
  - Gesundheitsdaten als besonders schützenswerte Daten
  - Eingeschränkte Bearbeitungszwecke im Arbeitsverhältnis (Art. 328b OR)
  - Fürsorgepflicht des Arbeitgebers (Art. 328 OR)
  - Privates Interesse des Arbeitgebers
  - Öffentliches Gesundheitsinteresse
- Einhaltung der datenschutzrechtlichen Grundsätze, insbesondere
  - Zweckbindung
  - Transparenz
  - Verhältnismässigkeit (Eignung und Notwendigkeit)
- Konkrete Anwendungsfälle

Schellenberg Wittmer

Datenschutz in der Cloud (1)

- Datenschutz: Cloud Computing als Auftragsbearbeitung i.S.v. Art. 10a DSG
  - Cloud Provider kein «Dritter»
  - Voraussetzungen
    - Kein Verbot wegen gesetzlicher/vertraglicher Geheimhaltungspflicht
    - Gewährleistung der Datensicherheit
- Personendaten vs Berufsgeheimnisse
  - Insbesondere Bankgeheimnis, Arztgeheimnis, Anwaltsgeheimnis
  - 2019: Frage der Zulässigkeit als Gegenstand diverser Gutachten
    - Cloud-Leitfaden der Schweizerischen Bankiervereinigung
    - Gutachten des Schweizerischen Anwaltsverbands)
  - Cloud Provider als Hilfsperson/Beauftragter des Geheimnisträgers
  - BGer: In beschränktem Umfang zulässig (BGE 145 II 229)

Schellenberg Wittmer

Datenschutz in der Cloud (2)

- Cloud ausserhalb der Schweiz
  - Datenschutz: Art. 6 DSG
  - Berufsgeheimnis: Kein Herausgabe-/Aussageverweigerungsrecht des ausländischen Cloud Providers
  - Technische, organisatorische und vertragliche Massnahmen zur Gewährleistung der Datensicherheit
- Auswirkungen US CLOUD Act:
  Mögliche Ausdehnung auf Schweizer Cloud Provider mit US-Bezug
- Exkurs: Herausgabe im Konkurs des Cloud Providers
  - De lege lata: Auskunftsrecht (Art. 8 DSG)
  - De lege ferenda: Zugangsrecht (Art. 242b E SchKG)

Schellenberg Wittmer

Biometrische Daten (1): PostFinance

- Projekt von PostFinance zur Authentifizierung von Anrufern mit Stimmerkennung
- Stimmaufzeichnung als biometrische Daten
- Frage: Biometrische Daten als besonders schützenswerte Daten, womit allfällige Einwilligung explizit erfolgen muss?
  - DSGVO und revidiertes DSG: Ja
  - Geltendes DSG: Nicht ausdrücklich
    - EDÖB: Erhöhter datenrechtlicher Schutz notwendig
    - PostFinance: Keine gesetzliche Regelung
    - Stimmaufzeichnung als Gesundheitsdaten?
- Umsetzung
  - Schweiz: Opt-Out
  - Ausland: Opt-In

Schellenberg Wittmer

Biometrische Daten (2): Clearview

- Gesichtserkennungssoftware
- Einsatz zur massenhaften Beschaffung und Bearbeitung von Gesichtsdaten über das Internet
  - Quelle: z.B. aus sozialen Netzwerken
  - Bearbeitungszweck: z.B. Gesichtserkennung, Verbrechensbekämpfung
- Einschätzung EDÖB
  - Keine besonders schützenswerten Daten (?)
  - Verstoss gegen Grundsätze der Transparenz, Zweckbindung und Verhältnismässigkeit
  - Gesetzliche Grundlage (bei Behörden) bzw. Einwilligung (bei Privaten) notwendig

Schellenberg Wittmer

Biometrische Daten (3): Wildtrack

- Datenbank mit Videoaufzeichnungen sich bewegender Menschen
- Zweck: Training von Methoden zur Personenerkennung (z.B. für Einsatz bei selbstfahrenden Autos)
- Forschungsprojekt der ETHZ/EPFL
  - 7 Kameras auf Polyterrasse
  - Aufnahme von Studierenden, Lehrpersonal, Passanten
  - Gesichter gut erkennbar, Tonaufnahmen
  - Spärliche Information und Opt-Out
  - Freie Nutzung im Internet zu «Forschungszwecken»

Unsere Bilder tragen zur Überwachung bei

Quelle: NZZ 11. März 2020, S. 15/16

Schellenberg Wittmer

Leading Cases (1): Internationale Amtshilfe

- Hintergrund
  - Amtshilfeersuchen des US IRS an die ESTV
  - Praxis ESTV
    - Schwärzung nur derjenigen Namen, die mit Verfahren «überhaupt nichts» zu tun haben, nicht aber von sonstigen Drittpersonen (z.B. Bankmitarbeitende)
    - Keine vorgängige Information sonstiger Drittpersonen
  - Anderslautende Empfehlung des EDÖB von ESTV und EFD abgelehnt
- BVGer (Urteil A-5715/2018 vom 11.09.2019)
  - Nicht direkt betroffene Personen (Drittpersonen): Restriktiv auszulegen
  - Drittpersonen sind vorgängig zu informieren, sobald ihre Daten «voraussichtlich relevant» sind
- Beschwerde der ESTV vor BGer hängig (sistiert)

Schellenberg Wittmer

Leading Cases (2): Dashcams

- Aufnahmen von Dashcams als Beweismittel
- BGer: Urteil vom 26.09.2019 (6B_1188/2018)
  - Grobe Verkehrsregelverletzungen durch anderen Verkehrsteilnehmer mittels Dashcam aufgezeichnet
  - (Geheime) Aufzeichnung als Verstoss gegen Transparenzgebot (Art. 4 Abs. 4 DSG), evtl. auch gegen Verhältnismässigkeit
  - Möglichkeit der Rechtfertigung?
    - Keine Interessenabwägung gemäss Art. 13 Abs. 1 DSG
    - Stattdessen Analogie zu Art. 141 Abs. 2 StPO: Verwertung unrechtmässiger erlangter Beweismittel nur bei schweren Straftaten, woran es vorliegend fehlte
- Urteil im Einklang mit Empfehlungen des EDÖB, aber abweichend vom Entscheid des OGer ZG vom 11.05.2017 (GVP 2017, 195)

Schellenberg Wittmer

Leading Cases (3): Helsana+

- Sachverhalt
  - Helsana+: App-gestütztes Bonusprogramm der Helsana Zusatzversicherungen AG
  - Einholung der Zustimmung, Daten von der obligatorischen Krankenpflegeversicherung der Helsana-Gruppe zur Zusatzversicherung zu übertragen
  - EDÖB: Einwilligung ungültig, Übertragung hat zu unterbleiben
- BVGer (Urteil vom 19.03.2019; A-3548/2018)
  - Keine Tätigkeit der Zusatzversicherung als Bundesorgan
  - Datenbeschaffung und -bearbeitung durch Zusatzversicherung von Einwilligung im Rahmen der Registrierung abgedeckt
  - Rechtmässige Beschaffung bedingt rechtmässige Bekanntgabe
  - Datenbekanntgabe durch Grundversicherung setzt schriftliche Einwilligung im Einzelfall voraus, an der es vorliegend fehlt

Schellenberg Wittmer

Internationales Verhältnis (1): Brexit

- Brexit
  - Austritt des Vereinigten Königreichs aus der EU am 31.01.2020
  - Wegfall von Unionsrecht (EU-DSGVO)
  - Frage der Adäquanz aus Sicht der Schweiz/EU
- Datenschutzniveau im Vereinigten Königreich weiterhin angemessen
  - Staatenliste EDÖB
  - DSGVO während Übergangsphase bis 31.12.2020 weiterhin anwendbar, danach Überführung in nationales Recht geplant
  - Adäquanzentscheid der EU bis Ende 2020 erwartet
  - EDÖB beobachtet Entwicklungen aktiv

Schellenberg Wittmer

Internationales Verhältnis (2): Privacy Shield

- Rahmenabkommen zum Datentransfer von der EU / Schweiz in die USA
- EuGH-Urteil i.S. Schrems II vom 16.07.2020 (C-311/18)
  - Aufhebung EU / US Privacy Shield
  - Erhöhte Anforderungen an Standardvertragsklauseln
- Auswirkungen auf die Schweiz?
  - EDÖB: «Urteil für die Schweiz nicht direkt anwendbar»
  - Swiss / US Privacy Shield nicht aufgehoben
  - Keine Anpassung der Staatenliste durch EDÖB
- Handlungsbedarf für Schweizer Unternehmen?
  - Bestehende Transfers: Nicht unmittelbar
  - Künftige Transfers: Prüfung Alternativen
  - Bei Anwendbarkeit DSGVO: Rasche Umsetzung Alternativen

Schellenberg Wittmer

Internationales Verhältnis (3): Adäquanz DSG

- DSG als Gesetzgebung mit angemessenem Schutzniveau gemäss EU (Entscheid vom 26.07.2000)
- Neubeurteilung der Angemessenheit unter DSGVO
- Angemessenheitsbeschluss mehrfach verschoben, zuletzt am 24.06.2020
  - Laufende Revision DSG
  - Kein Entscheid vor EuGH-Urteil i.S. Schrems II (16.07.2020)
  - Bis heute kein Entscheid
- Weitreichende Folgen eines allfälligen Negativentscheids
  - Datentransfers in die Schweiz massiv erschwert
  - Akzentuiert durch Schrems II (Standardvertragsklauseln)
- Swiss / US Privacy Shield als zusätzliche Hürde?

Schellenberg Wittmer

Vielen Dank.

Roland Mathys, LL.M.
roland.mathys@swlegal.ch

Schellenberg Wittmer AG / Rechtsanwälte
Löwenstrasse 19 / Postfach 2201 / 8021 Zürich / Schweiz
T +41 44 215 5252 / F +41 44 215 5200
www.swlegal.ch

Schellenberg Wittmer

4. DATENSCHUTZRECHTSTAGUNG

Das neue DSG

Update DSGVO

Dr. MARIE-LOUISE GÄCHTER-ALGE, Leiterin Datenschutzstelle, Fürstentum Liechtenstein

4. Datenschutzrechtstagung

Update DSGVO

8. September 2020

Dr. Marie-Louise Gächter
Leiterin Datenschutzstelle Liechtenstein

Erster Bericht der EU-Kommission zur DSGVO (Juni 2020)

- **Zweck**: Überprüfung der Wirkungsweise der DSGVO (Art. 97 DSGVO)

- **Insgesamt positive Bilanz, aber auch einiger Handlungsbedarf:**
  - Aufsichtsbehörden müssen enger kooperieren und erforderliche gemeinsame Untersuchungen vornehmen, um Harmonisierung der DSGVO zu stärken
  - unterschiedliche nationale Reglungen stellen eine Herausforderung für den Verantwortlichen dar (vgl. etwa Altersbestimmungen)
  - DSGVO = Herausforderung für kleinere und mittlere Unternehmen (KMU) – Behörden sind gefordert!
  - Anwendung DSGVO auf neue Technologien (etwa Blockchain oder KI)
  - Angemessenheitsbeschlüsse, Überprüfung bestehende + neu GB (Brexit)

Anwendbarkeit der DSGVO in Drittstaaten

- **Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO (Artikel 3) Version 2.0 12. November 2019**
  - Niederlassungskriterium sehr weit gefasst (auch Zweigniederlassungen oder Filialen)
  - Aber: blosse Tatsache, dass eine Website in der EU abrufbar sei, reicht nicht zur Begründung einer Niederlassung aus
  - Tätigkeit der Niederlassung und die fragliche Datenverarbeitung müssen im konkreten Einzelfall untrennbar miteinander verbunden sein
  - **Targeting-Kriterium**: Entscheidend ist der aus Sicht des Verantwortlichen anzunehmende Standort der betroffenen Personen in dem Moment, in dem die Angebotsausrichtung oder die Verhaltensbeobachtung erfolgt
  - Vertreter in EU: gilt nicht als Niederlassung; darf nicht gleichzeitig Datenschutzbeauftragter sein; befreit Verantwortlichen nicht von seiner Verantwortung/Rechenschaftspflicht
  - **Fazit**: viele hilfreiche Klarstellungen, nichtsdestotrotz bleiben Fragen offen

Anwendbarkeit der DSGVO in Drittstaaten

- **Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO (Artikel 3) Version 2.0 12. November 2019**

Beispiel 16: Eine Schweizer Universität in Zürich leitet ihr Auswahlverfahren für den Master-Abschluss mit der Bereitstellung einer Online-Plattform ein, auf der Bewerber ihren Lebenslauf und das Anschreiben sowie ihre Kontaktdaten hochladen können. Das Auswahlverfahren steht allen Studierenden mit ausreichenden Kenntnissen der deutschen und englischen Sprache und einem Bachelor-Abschluss offen. Die Universität wirbt nicht speziell um Studierende an EU-Universitäten und nimmt Zahlungen lediglich in Schweizer Währung entgegen.

Die Schweizer Universität bietet auch Sommerkurse in internationalen Beziehungen an und wirbt speziell für dieses Angebot an deutschen und österreichischen Hochschulen, um möglichst viele Teilnehmer an den Kursen zu gewinnen.

Privacy Shield gekippt: Auswirkungen des EuGH-Urteils Schrems II

«Der Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes ist ungültig.»

«Die Prüfung des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG […] hat nichts ergeben, was seine Gültigkeit berühren könnte.»

***ABER**: «Folglich obliegt es dem Verantwortlichen bzw. Auftragsverarbeiter, in jedem Einzelfall – gegebenenfalls in Zusammenarbeit mit dem Empfänger der Übermittlung – zu prüfen, ob das Recht des Bestimmungsdrittlands nach Maßgabe des Unionsrechts einen angemessenen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet, und erforderlichenfalls mehr Garantien als die durch diese Klauseln gebotenen zu gewähren.»*

Privacy Shield gekippt: Auswirkungen des EuGH-Urteils Schrems II

Eine schnelle Analyse des Quellcodes von europäischen Webseiten zeigt, dass diese einen Monat nach dem Urteil des Europäischen Gerichtshofs (EuGH) immer noch Google Analytics oder Facebook Connect verwenden - obwohl beide Unternehmen eindeutig unter die US-amerikanischen Überwachungsgesetze fallen, wie etwa FISA 702. Keines der beiden Unternehmen scheint eine rechtliche Grundlage für die Übertragung zu haben. Google behaupten immer noch, sich auf den "Privacy Shield" zu verlassen - einen Monat, nachdem er für ungültig erklärt wurde. Facebook nutzt weiter die "SCCs" obwohl der EuGH festgehalten hat, dass diese gegen US-Überwachungsgesetzen keinen ausreichenden Schutz bringen und daher nicht genutzt werden dürfen.

- Link zur Liste aller 101 *noyb-Beschwerden* und Unternehmen (Englisch)
- Googles Information weiter Privacy Shield zu nutzen und auf SCCs "überzugehen"
- Facebooks Information weiterhin Standardvertragsklauseln zu verwenden

Cookies – Was gilt beim Einsatz von Cookies auf Internetseiten?

Erst der EuGH, jetzt auch der BGH:
Bundesgerichtshof zur Einwilligung in telefonische Werbung und Cookie-Speicherung vom 28. Mai 2020

Der EuGH und aktuell auch der BGH haben entschieden, dass der Nutzer bei einer Zustimmung bei allen nicht unbedingt erforderlichen Cookies aktiv einwilligen muss. Ein «Durch Weitersurfen akzeptieren Sie alle Cookies» - Banner ohne direkte Zustimmung (zum Beispiel ein Klick auf OK) reicht nicht aus. Auch eine schon ausgewählte Checkbox ist nicht erlaubt.

Oft unterschätzt: «Cookies-Grundsätze» auch auf andere Technologien übertragbar!

Corona: IT-Herausforderungen

Homeoffice ist mit der COVID-19-Pandemie Teil des Arbeitsalltags geworden.

Die grössten Herausforderungen aus Sicht des Datenschutzes:

- Erhöhtes Bedrohungspotential aufgrund unternehmensexterner Geräte, die mit der Infrastruktur verbunden sind;
- Nicht standardisierte Lösungen stellen eine Gefahr für das Unternehmen dar;
- Unischere häusliche Umgebung;
- Erhöhtes Risiko für Datenlecks;
- Etc.

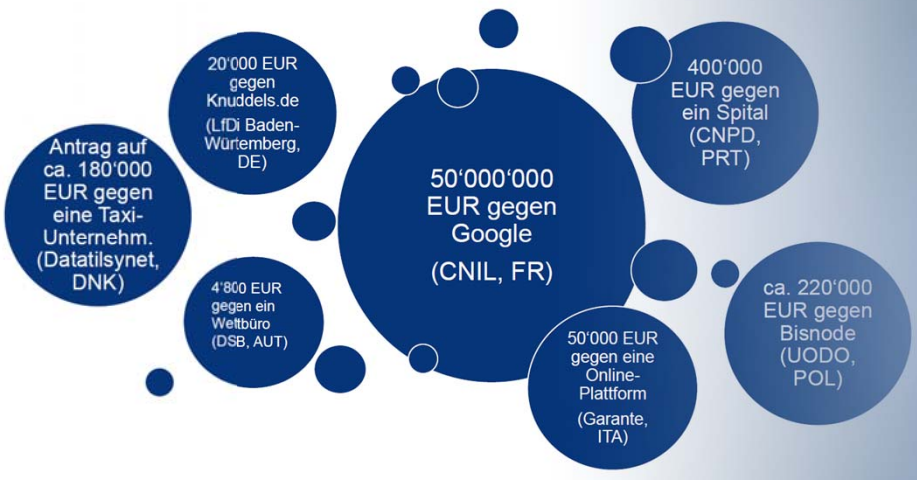
Corona: Herausforderungen für die Privatsphäre

Verfahren und Sanktionen

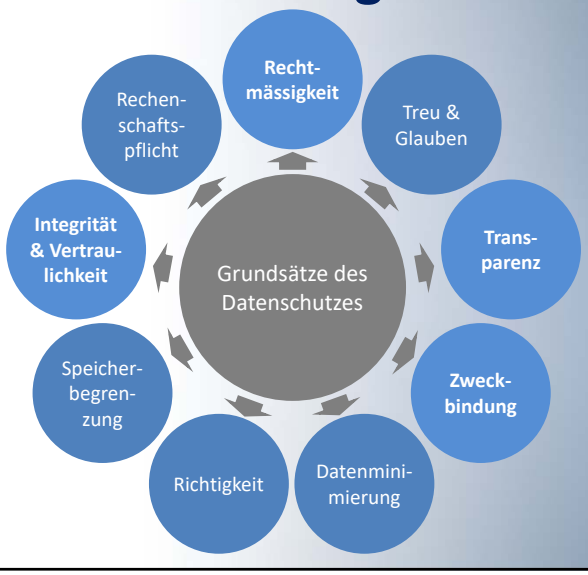
- Insgesamt sehr aktive Datenschutz-Aufsichtsbehörden in Europa
- Viele offene Fragen in Bezug auf nationale und europäische Verfahren(srechte) und Verhängung von Geldbussen
- Vehemente Kritik an Irischer Aufsichtsbehörde («*hochgradig ineffizient und teilweise kafkaesk*»…Zitat noyb

- Max Schrems: «**Die DSGVO ist nur so stark wie ihre schwächste Aufsichtsbehörde**.»

Sanktionen



Nicht alles ist neu: Grundsätze für die Datenverarbeitung



Grundsätze für die Datenverarbeitung

Es finden sich zu allen Dingen Grundsätze, allein dabei muss es nicht verbleiben, sondern man muss sich bemühen, über diese Sache selbst zu denken, auch sie fleissig üben, um in diesen Grundsätzen geschickt und geläufig zu werden.

Friedrich II. der Grosse

MTBF

Personal Firewall

Phishing

OSI-Schichtenmodell

Darknet

Verantwortlicher

WhatsApp

Byte

Megabyte

Cache

Netzwerk

TSR

Operating System

Administrator

Cookie

ePrivacy

Spam

Makro

Fast Ethernet

File-System

Gateway

Hoax

Q-Bus

Proxy

Digitale Signatur

ROM

Datenträger

RAID

Makrovirus

Firmware Upgrade

Notfallkonzept

Spyware

Pseudonymisierung

TOM

FTP

Authentifizierung

Direktwerbung

Anonymisierung

BIOS

Boot-Viren

Auftragsverarbeitung

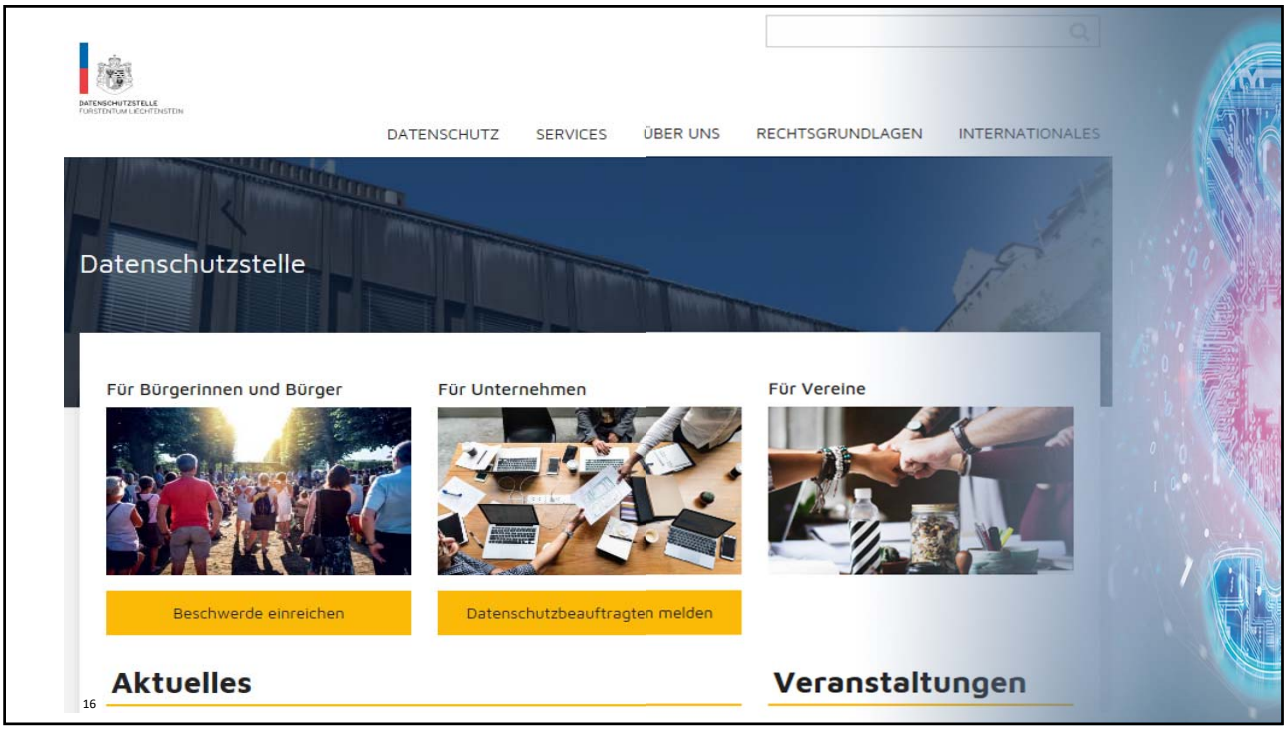
IPSec

IP-Adresse

Keylogger

Router

15



16

Datenschutzstelle
Städtle 38
Postfach 684
9490 Vaduz
Liechtenstein

T +423 236 60 90
info.dss@llv.li
www.datenschutzstelle.li

4. DATENSCHUTZRECHTSTAGUNG

Das neue DSG

Strategien und Perspektiven eines Global Players Dr. ANNA ZEITER, Chief Privacy Officer eBay Inc.

Strategien und Perspektiven eines Global Players

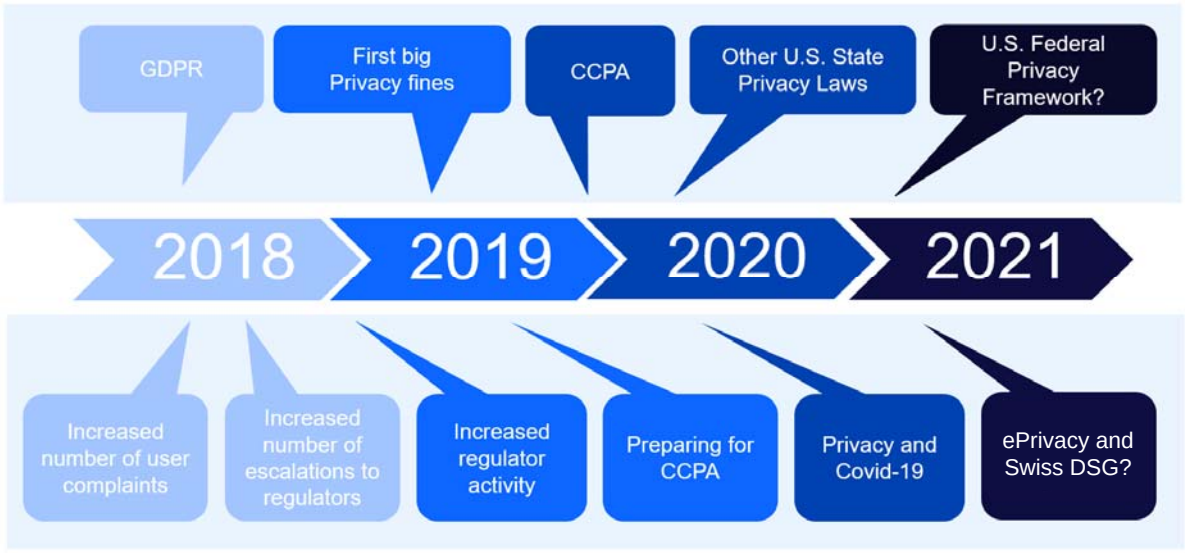
Dr. Anna Zeiter, LL.M.
Chief Privacy Officer, eBay Inc.
September 2020

AGENDA

- Globale Entwicklungen im Datenschutz – eine kurze Zeitreise
- DSGVO – Was sehen wir nach 2,5 Jahren?
- CCPA, CPRA & Co. – Datenschutzentwicklungen in den USA
- LGPD & PIPA – Datenschutzentwicklungen in LATAM & APAC
- Wie werden neue datenschutzrechtliche Anforderungen umgesetzt?
- Q&A

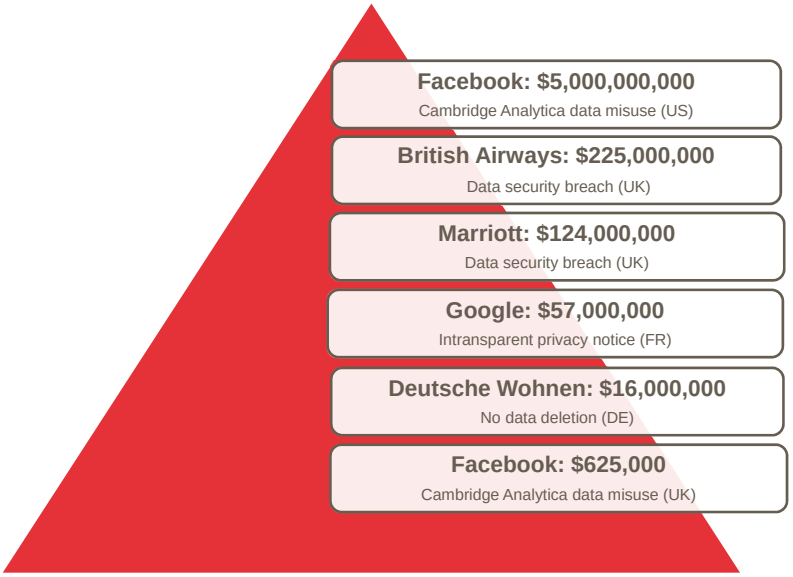
GLOBALE ENTWICKLUNGEN IM DATENSCHUTZ

Globale Entwicklungen im Datenschutz – eine kurze Zeitreise



DSGVO – WAS SEHEN WIR NACH 2,5 JAHREN?

DSGVO – Was sehen wir nach 2,5 Jahren?



https://www.enforcementtracker.com/

DSGVO – Was sehen wir nach 2,5 Jahren?

Erste grosse Sanktionen / Geldbussen wurden verhängt

Grösseres Datenschutzbewusstsein bei Kunden und Mitarbeitern

Grössere Bedeutung von Datenschutz in Unternehmen

DSGVO hat weltweiten Datenschutz-Standard gesetzt

Unterschiedlich ausgeprägte Aktivitäten von verschiedenen Aufsichtsbehörden

Stark von einander abweichende DSGVO-Auslegungen und Handlungsempfehlungen

Probleme beim Kohärenzverfahren und bei der Zusammenarbeit der Aufsichtsbehörden

CCPA, CPRA & CO. – DATENSCHUTZENTWICK-LUNGEN IN DEN USA

CCPA, CPRA & Co. – Datenschutzentwicklungen in den USA

Januar 2020

- Im Januar 2020 ist der California Consumer Privacy Act (CCPA) in Kraft getreten
- Dieser Act enthält diverse strenge Anforderungen, teilweise sogar strenger als die DSGVO
- Erste ‚Enforcement Letters' wurden im Juli 2020 an Unternehmen versendet

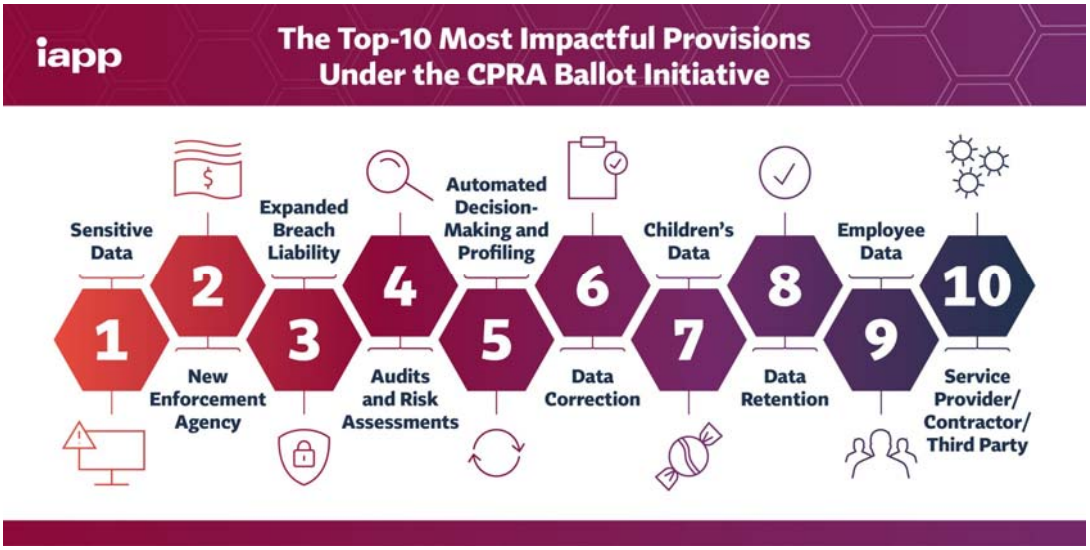
November 2020

- Der CCPA ist der Privacy Activist Group ‚Californians for Consumer Privacy' unter Alastair Mactaggart jedoch nicht weitgehend genug
- Die Aktivisten-Gruppe will im November 2020 in Kalifornien ein noch strengeres Datenschutzgesetz zur Abstimmung bringen, den California Consumer Privacy Rights Act (CPRA)

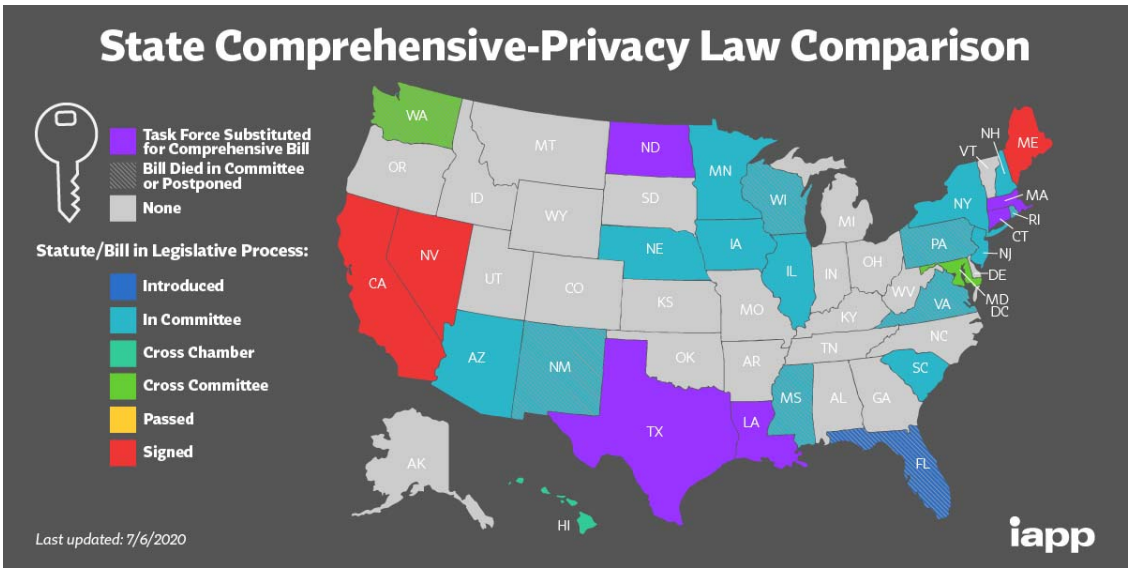
Januar 2023

- Falls die Initiative Erfolg haben sollte, würde der CPRA im Januar 2023 in Kraft treten
- Der CPRA enthält diverse neue und insbesondere strengere Anforderungen
- Außerdem soll eine Kalifonische Aufsichtsbehörde etabliert werden, die California Privacy Protection Agency (CPPA)

CCPA, CPRA & Co. – Datenschutzentwicklungen in den USA



CCPA, CPRA & Co. – Datenschutzentwicklungen in den USA

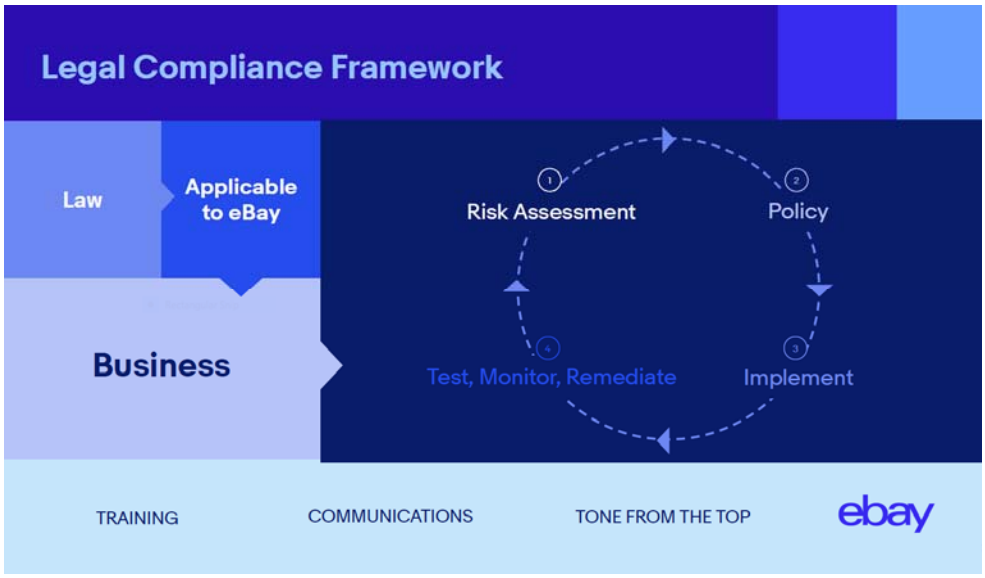


LGPD & PIPA – DATENSCHUTZENTWICK-LUNGEN IN LATAM & APAC

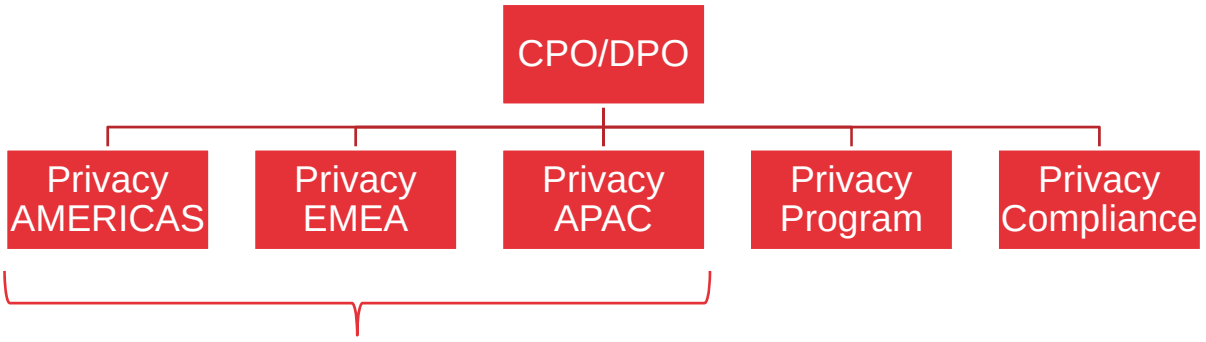
LGPD & PIPA – Datenschutzentwicklungen in LATAM & APAC

WIE WERDEN NEUE DATENSCHUTZRECHTLICHE ANFORDEGUNGEN UMGESETZT?

Wie werden datenschutzrechtliche Anforderungen umgesetzt?



Wie werden datenschutzrechtliche Anforderungen umgesetzt?

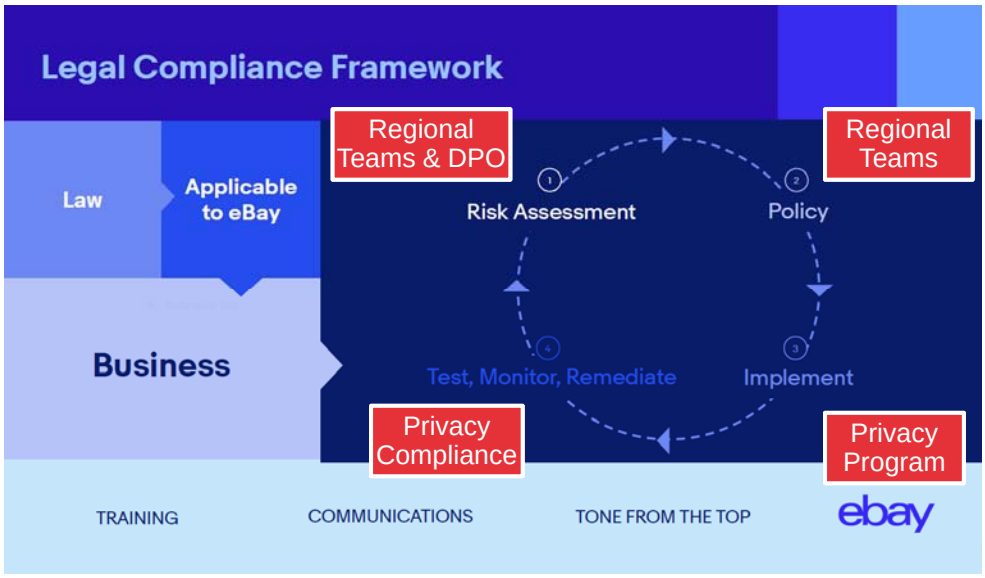


- Regional Privacy Advice
- Regional Privacy Inquiries / Complaints / Investigations
- Regulatory Affairs
- Privacy Policy / Governmental Relations
- PR / Communication

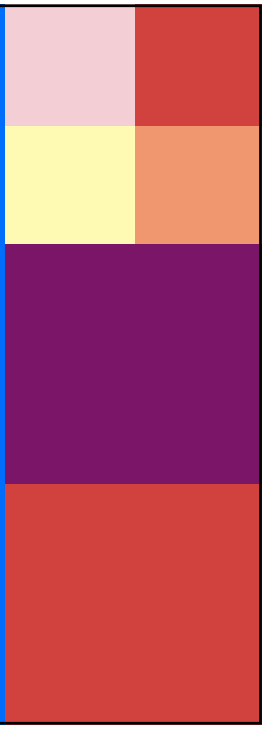
- PMO
- Implementation of new laws
- Operations
- DPIAs / PIAs / LIAs
- Policies

- Compliance Checks
- BCRs Checks
- Recommenda-tions
- Mitigations

Wie werden datenschutzrechtliche Anforderungen umgesetzt?



FRAGEN?



4. DATENSCHUTZRECHTSTAGUNG

Das neue DSG

Fokus materielles Recht

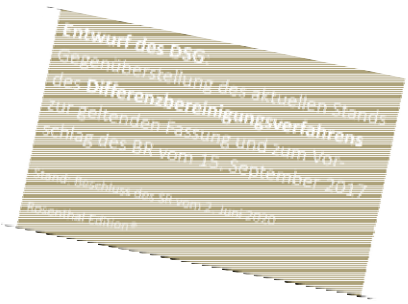
DAVID ROSENTHAL, Rechtskonsulent, Zürich

VISCHER

Das neue DSG:
Fokus materielles Recht

David Rosenthal
8. September 2020

Überblick



- Eine unendliche Geschichte …
  - Konsolidierter Überblick: https://bit.ly/3jD96A3 (von datenrecht.ch)
- Differenzbereinigung nach wie vor im Gange
  - Vorschlag der SPK-N (https://bit.ly/2QMpeTd) zu Profiling und zum Rechtfertigungsgrund der Kreditwürdigkeitsdaten
  - Herbstsession (7.–25. September 2020)
  - Verabschiedung in der Wintersession?
  - Inkraftsetzung im zweiten Halbjahr 2021 oder auf Anfang 2022?
  - Übergangsfristen sind unklar (eigentlich wurden sie gestrichen)

(DSG-Referenzen beziehen sich auf gegenwärtigen Entwurf)

VISCHER

Ausgewählte materielle Aspekte

- Räumlicher Geltungsbereich
- Bearbeitungsgrundsätze
- Einwilligung
- Profiling
- Informationspflicht
- Automatisierte Einzelentscheide
- Privacy by Design, Privacy by Default
- Auftragsbearbeitung
- Strafbestimmungen, inklusive Schweigepflicht

VISCHER

Räumlicher Geltungsbereich

- Unterscheidung zwischen öffentlich-rechtlichen, privatrechtlichen und strafrechtlichen Bestimmungen
- Territorialitätsprinzip, inkl. Auswirkungsprinzip
  - Bei öffentlich-rechtlichen Regeln (z.B. Art. 17, 20, 22)
  - Greift, sobald ein relevanter Teil des Sachverhalts in der Schweiz stattfindet
  - Handlung in der Schweiz in Bezug auf geregelten Sachverhalt (z.B. Beschaffung, Bearbeitung, Data Breach)
    - z.B. Art. 11: Verantwortlicher in der Schweiz muss auch ausländische Bearbeitungen verzeichnen
  - Auswirkung in der Schweiz
- Privatrecht: Wahlrecht nach Art. 139 IPRG

Art. 2a Räumlicher Geltungsbereich

[1] Dieses Gesetz ist auf Sachverhalte anwendbar, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden.

[2] Für privatrechtliche Ansprüche gilt das Bundesgesetz vom 18. Dezember 1987 über das internationale Privatrecht. Vorbehalten bleiben zudem die Bestimmungen zum räumlichen Geltungsbereich des Strafgesetzbuches.

VISCHER

Bearbeitungsgrundsätze

- Bearbeitungsgrundsätze
  - Anpassung bei Zweckbindung an das Konzept der «Zweckkompatibilität»
    - Analog der DSGVO
    - Keine wesentliche Veränderung
  - Auf ersten Blick fehlt das Transparenzgebot …
    - Ist im Grundsatz von Treu und Glauben enthalten
    - Gilt als privatrechtliche Norm (während Art. 17 öffentlich-rechtlicher Natur ist)
- Grundkonzept bleibt: Wenn ein Grundsatz verletzt ist, der Betroffene widerspricht oder besonders schützenswerte Daten weitergegeben werden, ist eine Rechtfertigung nötig

Art. 5 Grundsätze

[1] Personendaten müssen rechtmässig bearbeitet werden.
[2] Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein.
[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.
[4] Sie werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.
[5] Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Die Angemessenheit der Massnahmen hängt namentlich ab von der Art und dem Umfang der Datenbearbeitung sowie von den Risiken, welche die Bearbeitung für die Persönlichkeit und Grundrechte der betroffenen Personen mit sich bringt.
[…]

VISCHER

Einwilligung

- Einwilligung weiterhin nicht per se erforderlich
  - Auch nicht für besonders schützenswerte Personendaten (oder Profiling → siehe Slides hinten)
  - Aber: Falls eine Einwilligung gelten soll, muss sie bei solchen Personendaten [und ggf. Profiling] ausdrücklich sein
- Anforderungen an eine Einwilligung ändern sich nicht
- Ausdrücklich ist eine Einwilligung dann, wenn
  - ein aktives Verhalten oder ein solches vorliegt, das als affirmativ vereinbart wurde (z.B. mittels einer AGB-Klausel, wonach ein Schweigen auf eine AGB-Änderung hin als Zustimmung gilt) und
  - die Bedeutung dieses affirmativen Verhaltens sich direkt auf die betreffende Datenbearbeitung bezieht

Art. 5 Grundsätze

[…]

[6] Ist die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie für eine oder mehrere bestimmte Bearbeitungen nach angemessener Information freiwillig erteilt wird.
[7] Die Einwilligung muss ausdrücklich erfolgen für:
a. die Bearbeitung besonders schützenswerten Personendaten;
b. ein Profiling mit hohem Risiko durch eine private Person; oder
c. ein Profiling durch ein Bundesorgan.

Abs. 7 noch offen

VISCHER

Profiling

Art. 4 Begriffe

f. Profiling: jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

- Profiling beginnt dort, wo das Persönlichkeitsprofil aufhört …
  - Persönlichkeitsprofil: Sammlung der Daten, welche die Beurteilung bestimmter Aspekte der Person erlaubt
  - Profiling: Vorgang der Bewertung solcher Aspekte durch eine Maschine (wenn auch durch vorprogrammierte Parameter)
  - Profiling ist weder der Input noch der Output
  - Nur Bearbeitungen, die eine Interpretation, d.h. eine Wertung erfordern (≠ blosse Feststellung eines Sachverhalts)

VISCHER

Profiling

- Wo ist Profiling im neuen DSG überhaupt rechtlich relevant?
  - [Ggf.] Anforderungen an eine Einwilligung
  - [Ggf.] Rechtfertigungsgrund der Kreditwürdigkeitsprüfung
  - Erfordernis einer formellen Rechtsgrundlage beim Profiling durch Bundesorgane
  - Nicht mehr: Automatisierte Einzelentscheide, DSFA
- Aber: Grundsatz der Verhältnismässigkeit bzw. dessen Verletzung kann eine Rechtfertigung beim Profiling erfordern
  - z.B. beim Einsatz von detaillierten Profilen einer identifizierten Person für Marketingzwecke
- Der «gefühlte Datenschutz» kann eine Einwilligung erfordern

VISCHER

Profiling

- Offene Punkte in der Revision / Anträge der SPK-N
  - Kein Profiling mit hohem Risiko definieren
  - Minderheit: Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt
  - Keine Ausdrücklichkeit der Einwilligung bei Profiling mit hohem Risiko (Minderheit will hingegen das Erfordernis der Ausdrücklichkeit)
  - Minderheit: Bei Profiling soll ein neues Widerspruchsrecht eingeführt werden (siehe Kasten)

[8] Gegen jede Form des Profilings steht der betroffenen Person ein Widerspruchsrecht zu. Die betroffene Person muss auf dieses Widerspruchsrecht hingewiesen werden. Ist Widerspruch eingelegt, dürfen die Daten nicht weiter verarbeitet werden; im Einzelfall kann die Verarbeitung fortgesetzt werden, wenn bei erhöhtem Risiko zwingende schutzwürdige Gründe die weitere Verarbeitung erfordern. Entscheidung und Gründe sind der betroffenen Person mitzuteilen.

https://bit.ly/2QMpeTd

VISCHER

Informationspflicht

- Nur im Falle einer «Beschaffung»
  - Erfordert Planmässigkeit
  - Gilt neben dem Transparenzgebot nach Art. 5
  - Über Änderungen muss nicht informiert werden, nur über neue Zwecke (ist eine indirekte Beschaffung)
- Mindestinformationen nach Abs. 2, 3 und 4 (sowie nach Art. 9 und 12a)
  - Zweck muss nicht ausführlich sein (es gelten die AGB-Auslegungsregeln)
  - Ländernennung: Auch «weltweit», «Europa»
  - Weitergehende Angaben nur ausnahmsweise

Art. 17 Informationspflicht bei der Beschaffung von Personendaten

[1] Der Verantwortliche informiert die betroffene Person angemessen über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden.

[2] Er teilt der betroffenen Person bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist; er teilt ihr mindestens mit:

a. die Identität und Kontaktdaten des Verantwortlichen;
b. den Bearbeitungszweck;
c. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden.

[3] Werden Daten nicht bei der betroffenen Person beschafft, so teilt er ihr zudem die Kategorien der bearbeiteten Personendaten mit.

[4] Werden die Personendaten ins Ausland bekanntgegeben, so teilt er der betroffenen Person auch den Staat oder das internationale Organ und gegebenenfalls die Garantien nach Artikel 13 Absatz 2 oder die Anwendung einer Ausnahme nach Artikel 14 mit.

[5] Werden die Daten nicht bei der betroffenen Person beschafft, so teilt er ihr die Informationen nach den Absätzen 2–4 spätestens einen Monat, nachdem er die Daten erhalten hat, mit. Gibt der Verantwortliche die Personendaten vor Ablauf dieser Frist bekannt, so informiert er die betroffene Person spätestens im Zeitpunkt der Bekanntgabe.

VISCHER

Informationspflicht

- Mehrstufige Information nicht vorgeschrieben
  - Angabe, wo die Datenschutzerklärung zu finden ist (z.B. auf Website)
  - Medienbruch erlaubt
  - Kann erwartet werden, dass Betroffene das Internet nutzen um sich zu informieren?
    - Normalerweise ja; der Staat tut das ja auch
- Vorsätzliche Verletzung ist strafbewehrt

Art. 17 Informationspflicht bei der Beschaffung von Personendaten

[1] Der Verantwortliche informiert die betroffene Person angemessen über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden.

[2] Er teilt der betroffenen Person bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist; er teilt ihr mindestens mit:

a. die Identität und Kontaktdaten des Verantwortlichen;
b. den Bearbeitungszweck;
c. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden.

[3] Werden Daten nicht bei der betroffenen Person beschafft, so teilt er ihr zudem die Kategorien der bearbeiteten Personendaten mit.

[4] Werden die Personendaten ins Ausland bekanntgegeben, so teilt er der betroffenen Person auch den Staat oder das internationale Organ und gegebenenfalls die Garantien nach Artikel 13 Absatz 2 oder die Anwendung einer Ausnahme nach Artikel 14 mit.

[5] Werden die Daten nicht bei der betroffenen Person beschafft, so teilt er ihr die Informationen nach den Absätzen 2–4 spätestens einen Monat, nachdem er die Daten erhalten hat, mit. Gibt der Verantwortliche die Personendaten vor Ablauf dieser Frist bekannt, so informiert er die betroffene Person spätestens im Zeitpunkt der Bekanntgabe.

VISCHER

Ausnahmen

- Keine Information …
  - Über das, was die Person schon weiss
  - Soweit aus Umständen hervorgeht, dass die Person auf die Information verzichtet hat oder kein Interesse daran hat (vgl. BBl 2017 7053)
  - Über gesetzlich vorgesehene Bearbeitungen (!)
- Unmöglichkeit meint …
  - Identifizierung und Lokalisierung
  - Ist mit verhältnismässigen Mitteln nicht möglich

Art. 18 Ausnahmen von der Informationspflicht und Einschränkungen

[1] Die Informationspflicht nach Artikel 17 entfällt, wenn eine der folgenden Voraussetzungen erfüllt ist:

a. Die betroffene Person verfügt bereits über die entsprechenden Informationen;
b. Die Bearbeitung ist gesetzlich vorgesehen;
c. Es handelt sich beim Verantwortlichen um eine private Person, die gesetzlich zur Geheimhaltung verpflichtet ist;
d. Die Voraussetzungen nach Artikel 25 sind erfüllt.

[2] Werden die Personendaten nicht bei der betroffenen Person beschafft, so entfällt die Informationspflicht zudem, wenn eine der folgenden Voraussetzungen erfüllt ist:

a. Die Information ist nicht möglich;
b. Die Information erfordert einen unverhältnismässigen Aufwand.

[3] Der Verantwortliche kann die Mitteilung der Information in den folgenden Fällen einschränken, aufschieben oder darauf verzichten:

a. Überwiegende Interessen Dritter erfordern die Massnahme;
b. Die Information vereitelt den Zweck der Bearbeitung;
c. Der Verantwortliche ist eine private Person und die folgenden Voraussetzungen sind erfüllt:
   1. Überwiegende Interessen des Verantwortlichen erfordern die Massnahme;
   2. Der Verantwortliche gibt Personendaten nicht Dritten bekannt.
d. Der Verantwortliche ist ein Bundesorgan und eine der folgenden Voraussetzungen ist erfüllt:
   1. Die Massnahme ist wegen überwiegender öffentlicher Interesse, insbesondere der inneren oder der äusseren Sicherheit der Schweiz erforderlich.
   2. Die Mitteilung der Information kann eine Ermittlung, eine Untersuchung oder ein behördliches oder gerichtliches Verfahren gefährden.

[4] Die Voraussetzungen nach Absatz 3 Buchstabe c Ziffer 2 gilt als eingehalten, wenn die Bekanntgabe von Personendaten zwischen Unternehmen stattfindet, die von derselben juristischen Person kontrolliert werden.

VISCHER

Ausnahmen

- Abs. 3 erfordert eine Interessenabwägung
  - Vereitelung: Angestrebte Zielerreichung durch Info ernsthaft gefährdet und das Ziel erscheint wichtiger
  - Auftragsbearbeiter, gemeinsame Verantwortliche und Gruppengesellschaften sind keine Dritten

Art. 18 Ausnahmen von der Informationspflicht und Einschränkungen

[1] Die Informationspflicht nach Artikel 17 entfällt, wenn eine der folgenden Voraussetzungen erfüllt ist:
- a. Die betroffene Person verfügt bereits über die entsprechenden Informationen;
- b. Die Bearbeitung ist gesetzlich vorgesehen;
- c. Es handelt sich beim Verantwortlichen um eine private Person, die gesetzlich zur Geheimhaltung verpflichtet ist;
- d. Die Voraussetzungen nach Artikel 25 sind erfüllt.

[2] Werden die Personendaten nicht bei der betroffenen Person beschafft, so entfällt die Informationspflicht zudem, wenn eine der folgenden Voraussetzungen erfüllt ist:
- a. Die Information ist nicht möglich;
- b. Die Information erfordert einen unverhältnismässigen Aufwand.

[3] Der Verantwortliche kann die Mitteilung der Information in den folgenden Fällen einschränken, aufschieben oder darauf verzichten:
- a. Überwiegende Interessen Dritter erfordern die Massnahme;
- b. Die Information vereitelt den Zweck der Bearbeitung;
- c. Der Verantwortliche ist eine private Person und die folgenden Voraussetzungen sind erfüllt:
  1. Überwiegende Interessen des Verantwortlichen erfordern die Massnahme;
  2. Der Verantwortliche gibt Personendaten nicht Dritten bekannt.
- d. Der Verantwortliche ist ein Bundesorgan und eine der folgenden Voraussetzungen ist erfüllt:
  1. Die Massnahme ist wegen überwiegender öffentlicher Interesse, insbesondere der inneren oder der äusseren Sicherheit der Schweiz erforderlich.
  2. Die Mitteilung der Information kann eine Ermittlung, eine Untersuchung oder ein behördliches oder gerichtliches Verfahren gefährden.

[4] Die Voraussetzungen nach Absatz 3 Buchstabe c Ziffer 2 gilt als eingehalten, wenn die Bekanntgabe von Personendaten zwischen Unternehmen stattfindet, die von derselben juristischen Person kontrolliert werden.

VISCHER

Automatisierte Einzelentscheide

- AEE = Entscheid and aufgrund einer Bearbeitung von Personendaten and Bewertung and vollautomatisch and (Rechtsfolge für Person or erhebliche Beeinträchtigung)
  - Verweis auf Profiling wurde gestrichen – relevant?
- Folgen nach erfolgtem Entscheid
  - Information (aber keine weiteren Vorgaben)
  - «Menschliches Gehör»

Art. 19 Informationspflicht bei einer automatisierten Einzelentscheidung

[1] Der Verantwortliche informiert die betroffene Person über eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt.

[2] Er gibt der betroffenen Person auf Antrag die Möglichkeit, ihren Standpunkt darzulegen. Die betroffene Person kann verlangen, dass die Entscheidung von einer natürlichen Person überprüft wird.

[3] Die Absätze 1 und 2 gelten nicht, wenn:
- a. die Entscheidung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person steht und ihrem Begehren stattgegeben wird; oder
- b. die betroffene Person ausdrücklich eingewilligt hat, dass die Entscheidung automatisiert erfolgt.

[4] Ergeht die automatisierte Einzelentscheidung durch ein Bundesorgan, so muss es die Entscheidung entsprechend kennzeichnen. Absatz 2 ist nicht anwendbar, wenn die betroffene Person nach Artikel 30 Absatz 2 des Verwaltungsverfahrensgesetzes vom 20. Dezember 1968 oder nach einem anderen Bundesgesetz vor dem Entscheid nicht angehört werden muss.

VISCHER

Automatisierte Einzelentscheide

- Gilt nicht, wenn:
  - Einwilligung der Person, dass sie betreffende Entscheide automatisiert erfolgen → hinreichende Information über Entscheid erforderlich
  - Entscheid für Abschluss oder Abwicklung erforderlich und es wurde dem Begehren stattgegeben (z.B. Gutheissung eines Versicherungsclaims)

Art. 19 Informationspflicht bei einer automatisierten Einzelentscheidung

1 Der Verantwortliche informiert die betroffene Person über eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt.

2 Er gibt der betroffenen Person auf Antrag die Möglichkeit, ihren Standpunkt darzulegen. Die betroffene Person kann verlangen, dass die Entscheidung von einer natürlichen Person überprüft wird.

3 Die Absätze 1 und 2 gelten nicht, wenn:

a. die Entscheidung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person steht und ihrem Begehren stattgegeben wird; oder

b. die betroffene Person ausdrücklich eingewilligt hat, dass die Entscheidung automatisiert erfolgt.

4 Ergeht die automatisierte Einzelentscheidung durch ein Bundesorgan, so muss es die Entscheidung entsprechend kennzeichnen. Absatz 2 ist nicht anwendbar, wenn die betroffene Person nach Artikel 30 Absatz 2 des Verwaltungsverfahrensgesetzes vom 20. Dezember 1968 oder nach einem anderen Bundesgesetz vor dem Entscheid nicht angehört werden muss.

VISCHER

Privacy by Design & Default

- «Privacy by Design» war bisher Teil von Art. 7 DSG
  - Massnahmen gegen unbefugtes Bearbeiten
- Art. 6 ist kein Bearbeitungsgrundsatz (mehr)
  - Richtet sich nur an Verantwortliche, keine Sanktion
  - Keine Rechtfertigungsmöglichkeit
- Erfasst «Datenschutzvorschriften», d.h. alles, was die Bearbeitung der Daten oder Betroffenenrechte betrifft
  - Nicht das Inventar, DSFA, Data Breach Notification

Art. 6 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

1 Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze nach Artikel 5. Er berücksichtigt dies ab der Planung.

2 Die technischen und organisatorischen Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie den Risiken, welche die Bearbeitung für die Persönlichkeit und Grundrechte der betroffenen Personen mit sich bringt, angemessen sein.

3 Der Verantwortliche ist verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt.

VISCHER

Privacy by Design & Default

- «Privacy by Default» gilt nur, wo es «Einstellungen» gibt, nicht für jede Einwilligungs- oder Opt-out-Möglichkeit
  - Verwendungszweck bezieht sich auf Gesamtheit der Bearbeitungen, nicht den Zweck der Dienstleistung
  - Betrifft nur Voreinstellung, nicht eine initiale Einwilligung

Art. 6 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

1 Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze nach Artikel 5. Er berücksichtigt dies ab der Planung.

2 Die technischen und organisatorischen Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie den Risiken, welche die Bearbeitung für die Persönlichkeit und Grundrechte der betroffenen Personen mit sich bringt, angemessen sein.

3 Der Verantwortliche ist verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt.

VISCHER

Auftragsbearbeitung

- Abgrenzung Controller-Processor: Wie DSGVO*
  - Processors sind teilweise auch Controller, nicht alle Dienstleister sind Processors
- Was braucht der Vertrag?
  - Weisungsrecht, das auch ausgeübt werden muss (frei oder standardisiert)
  - Gpf. Pflicht zur Mitwirkung bei Erfüllung des DSG
  - Möglichkeit zur Kontrolle, nicht zwingend Auditrecht
  - Regelung zu Subprocessors, Daten-Rückgabe und Datensicherheit gemäss Art. 28 DSGVO
  - Auslandsdatentransfer (nicht Teil von Art. 8 DSG)
- Busse bei Verletzung von Abs. 1+2 durch Auftraggeber

Art. 8 Datenbearbeitung durch Auftragsbearbeiter

1 Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:
   a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und
   b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

2 Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

3 Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.

4 Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.

* Dazu: http://www.rosenthal.ch/downloads/Rosenthal-ControllerProcessor.pdf

VISCHER

Strafbestimmungen

- Bisherige Strafnorm bleibt (Art. 54), aber mit verschärfter Bussendrohung (CHF 250k)
- Höhere Strafdrohung als Art. 292 StGB bei Missachtung von Verfügungen des EDÖB (CHF 250k, Art. 57)
- Verletzung von «Sorgfaltspflichten» auf Antrag betraft
  - Verbotener Auslandsexport
  - Unzulässige Auftragsbearbeitung, aber nicht betreffend Subprocessor-Regelung; gilt nur für Verantwortliche
  - Verletzung der Datensicherheitsvorgaben des BR

Art. 55 Verletzung von Sorgfaltspflichten

Mit Busse bis zu 250 000 Franken werden private Personen auf Antrag bestraft, die vorsätzlich:

a. unter Verstoss gegen Artikel 13 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 14 erfüllt sind, Personendaten ins Ausland bekanntgeben;
b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 8 Absätze 1 und 2 erfüllt sind;
c. die Mindestanforderungen an die Datensicherheit, die der Bundesrat nach Artikel 7 Absatz 3 erlassen hat, nicht einhalten.

Art. 56 Verletzung der beruflichen Schweigepflicht

1 Wer geheime Personendaten vorsätzlich offenbart, von denen sie oder er bei der Ausübung ihres oder seines Berufes, der die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat, wird auf Antrag mit Busse bis zu 250 000 Franken bestraft.

2 Gleich wird bestraft, wer vorsätzlich geheime Personendaten offenbart, von denen sie oder er bei der Tätigkeit für eine geheimhaltungspflichtige Person oder während der Ausbildung bei dieser Kenntnis erlangt hat.

3 Das Offenbaren geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.

VISCHER

Strafbestimmungen

- Erweiterte berufliche Schweigepflicht (heute Art. 35 DSG)
  - Geheime Personendaten and nötig für den Beruf and gegenüber Unberufenen offenbart and vorsätzlich
  - Ist es eher ein Berufsgeheimnis oder eher eine datenschutzrechtliche Norm?
    - Relevant für die Frage, ob eine gemäss DSG erlaubte Offenbarung eine Verletzung sein kann (z.B. im Falle eines überwiegenden Interesses)
  - Hilfspersonen ebenfalls erfasst

Art. 55 Verletzung von Sorgfaltspflichten

Mit Busse bis zu 250 000 Franken werden private Personen auf Antrag bestraft, die vorsätzlich:

a. unter Verstoss gegen Artikel 13 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 14 erfüllt sind, Personendaten ins Ausland bekanntgeben;
b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 8 Absätze 1 und 2 erfüllt sind;
c. die Mindestanforderungen an die Datensicherheit, die der Bundesrat nach Artikel 7 Absatz 3 erlassen hat, nicht einhalten.

Art. 56 Verletzung der beruflichen Schweigepflicht

1 Wer geheime Personendaten vorsätzlich offenbart, von denen sie oder er bei der Ausübung ihres oder seines Berufes, der die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat, wird auf Antrag mit Busse bis zu 250 000 Franken bestraft.

2 Gleich wird bestraft, wer vorsätzlich geheime Personendaten offenbart, von denen sie oder er bei der Tätigkeit für eine geheimhaltungspflichtige Person oder während der Ausbildung bei dieser Kenntnis erlangt hat.

3 Das Offenbaren geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.

VISCHER

Danke für Ihre Aufmerksamkeit!

Bei 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

4. DATENSCHUTZRECHTSTAGUNG

Das neue DSG

Fokus Governance
Dr. ADRIAN LOBSIGER, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Das neue DSG
Fokus Governance

4. Datenschutzrechtstagung in Zürich
Schweizer Forum für Kommunikationsrecht
8. September 2020

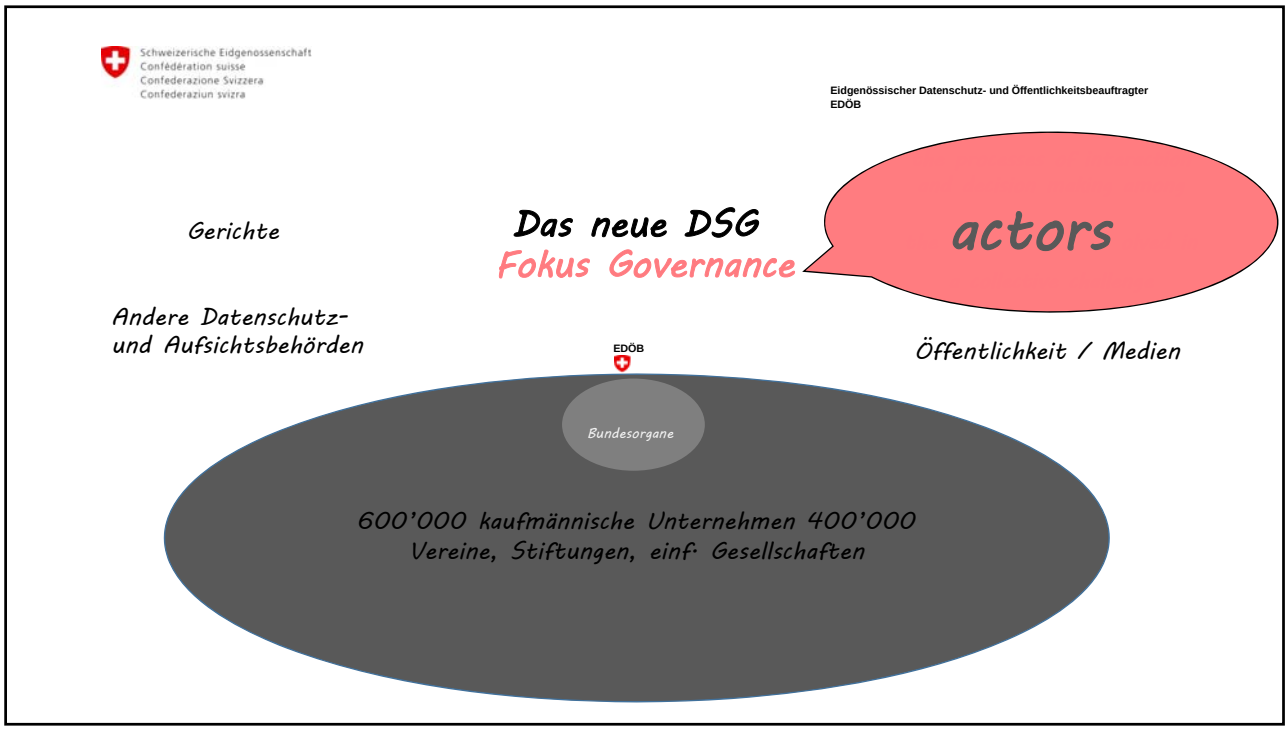
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

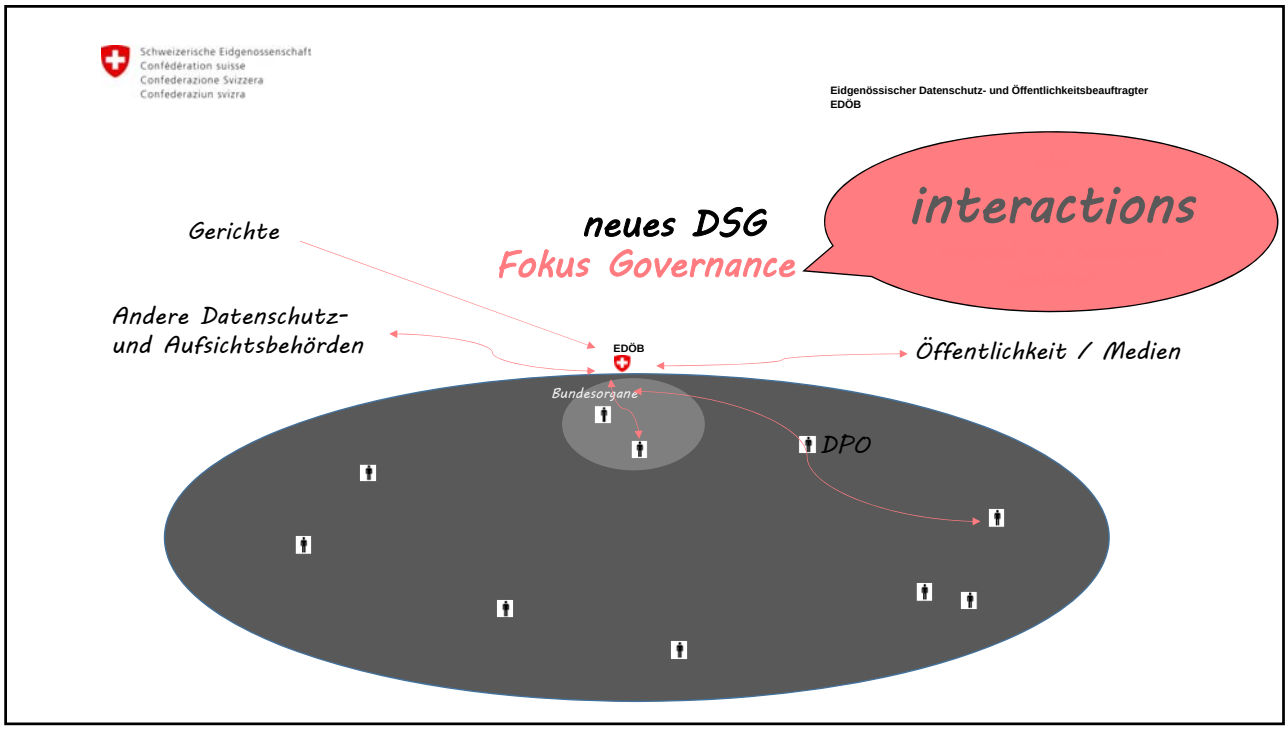
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Das neue DSG
Fokus Governance

the processes of **interaction and decision making** among the actors involved in a collective challenge

Bundesorgane


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB
Gerichte
Das neue DSG
Fokus Governance
actors
Andere Datenschutz- und Aufsichtsbehörden
Öffentlichkeit / Medien
EDÖB
Bundesorgane
600'000 kaufmännische Unternehmen 400'000 Vereine, Stiftungen, einf. Gesellschaften


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB
Gerichte
neues DSG
Fokus Governance
interactions
Andere Datenschutz- und Aufsichtsbehörden
EDÖB
Öffentlichkeit / Medien
Bundesorgane
DPO

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

regulation

neues DSG
VDSG

~~Schengen DSG für fedpol GWK i.K. 1.2019~~

D S G

EDÖB

Gesetz und Verordnungen umsetzen
Merkblätter, Musterklauseln etc. auf Webseite

alle Beschwerden behandeln ?
- Priorisierung
- Opportunitätsprinzip

Verzeichnisse
- Datenschutzerklärungen

Musterklauseln
- Anhänge

Gebühren erheben
- Gebührenverordnung
- Stundenansätze

Verfügungen

Sanktionen
- Natürliche Personen
- Vorsatz
- Minimale technische Vorkehren

DPO und Vorlagepflichten

Praxis zu neuen Begrifflichkeiten
- Datenbearbeitung mit hohem Risiko
- Profiling mit hohem Risiko
- Portabilität
- Biometrische Daten, die Person eindeutig identifizieren
- Verletzung der Datensicherheit
- etc.

Aufsicht

Objekt der Aufsichtstätigkeit

- Risiken / Verletzungen der Privatsphäre und informationellen Selbstbestimmung

Massstab der Beurteilung

- DSG, VDSG
- Rechtsprechung schweizerischer Gerichte
- Stellungnahmen des EDÖB
- Wahrung des angemessenen Datenschutzes mit EWR und weiteren Staaten ist dem EDÖB nach Massgabe der schweizerischen Rechtsordnung möglich, da davon auszugehen ist, dass Letztere dieses Schutzniveau gewährleistet

Handlungsformen

- Neu Verfügungen i.S.v. Art. 5 VwVG – Aufforderung, (nicht) zu bearbeiten, löschen, informieren, melden etc.
- Empfehlungen (Klagemöglichkeit ans BVGer fällt weg)
- Stellungnahmen auf Vorlage hin ist keine Genehmigung oder Bewilligung und kann Vorbehalte enthalten (Vertrauensschutz und Rechtsmittel mit Blick auf abstrakte Natur der Prüfung beschränkt)
- Spontane Stellungnahmen

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Spontane Stellungnahmen

Ambition des EDÖB – Softlaw – «race to the bottom/top» ?

- Im Fokus steht die riko-orientierte Sensibilisierung in der digitalen Realität, zwecks Erhöhung des Publikumsschutzes und der Rechtssicherheit
- EDÖB weist auf Risiken und Massnahmen zu deren Verhinderung hin
- Im Ereignisfall (Verletzung der Datensicherheit) erfolgt dann konkrete Beurteilung ex post

- Formalismen (Konventionen, Gesetze, Verordnungen abschreiben bringt nichts)

Vorlagepflichten

Verhaltenskodizes (Art. 10)

- Organisationen mit statutarischem Mandat der Branche
- Prüfpflicht des EDÖB
- Publikationspflicht des EDÖB – Abgrenzung zur eigenen Empfehlung der guten Praxis (Art. 52)

Datenschutz Folgenabschätzung (Art. 20)

- Vorlage an DPO oder an EDÖB
- Prüfpflicht des EDÖB
- Keine Publikationspflicht des EDÖB (Letzterer ist aber BGÖ unterworfen)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Verhaltenskodizes (Art. 10)

- Befreiung des Branchenmitgliedes von der Erstellung einer eigenen Datenschutz Folgenabschätzung
- Sinnvoll, soweit Kodex Risiken mit Blick auf die branchenspezifischen und unternehmerischen Besonderheiten des konkreten Falles anspricht und mit entsprechenden Massnahmen abdeckt
- Allgemein gehaltene Kodizes und Risikoanalysen vermögen Unternehmen nicht zu dispensieren bezüglich erkennbar hoher Risiken, die der Kodex unerwähnt lässt

Meldung Verletzung der Datensicherheit (Art. 22)

- Verletzung der Datensicherheit def. In Art. 4 DSG
- Meldung muss «so rasch als möglich» erfolgen
- Konkretisierung durch Praxis
- Keine Fristen in Gesetz und Verordnung vorgesehen wie nach DSGVO
- Keine Strafen vorgesehen bei Verletzung der unbestimmten Frist

- EDÖB berät ab Kenntnisnahme
- EDÖB kann Massnahmen verfügen (Bsp. Information der Betroffenen)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Profiling

Art. 4, 5, 27

Profiling

- Befürchtung, Entwurf BR zum Profiling sei ein Swissfinish, der CH Wirtschaft benachteilige → Kompromisslösung SR → erhöhter Schutz nur bei **«Profiling mit hohem Risiko»**:

  Art. 4 lit. fbis E-DSG:
  Profiling mit hohem Risiko: Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, namentlich 1. bei der systematischen Verknüpfung von Daten aus verschiedener Herkunft, die verschiedene Lebensbereiche einer natürlichen Person betreffen; oder 2. bei einer systematischen und umfangreichen Bearbeitung von Daten, um Rückschlüsse auf verschiedene Lebensbereiche einer natürlichen Person zu ziehen.

Profiling

- NR wünscht, dass nicht die Bearbeitungsmethode, sondern deren Resultat reguliert wird, und ändert Definition:

  Art. 4 lit. fbis E-DSG
  Profiling mit hohem Risiko: Profiling, welches zu besonders schützenswerten Personendaten führt.

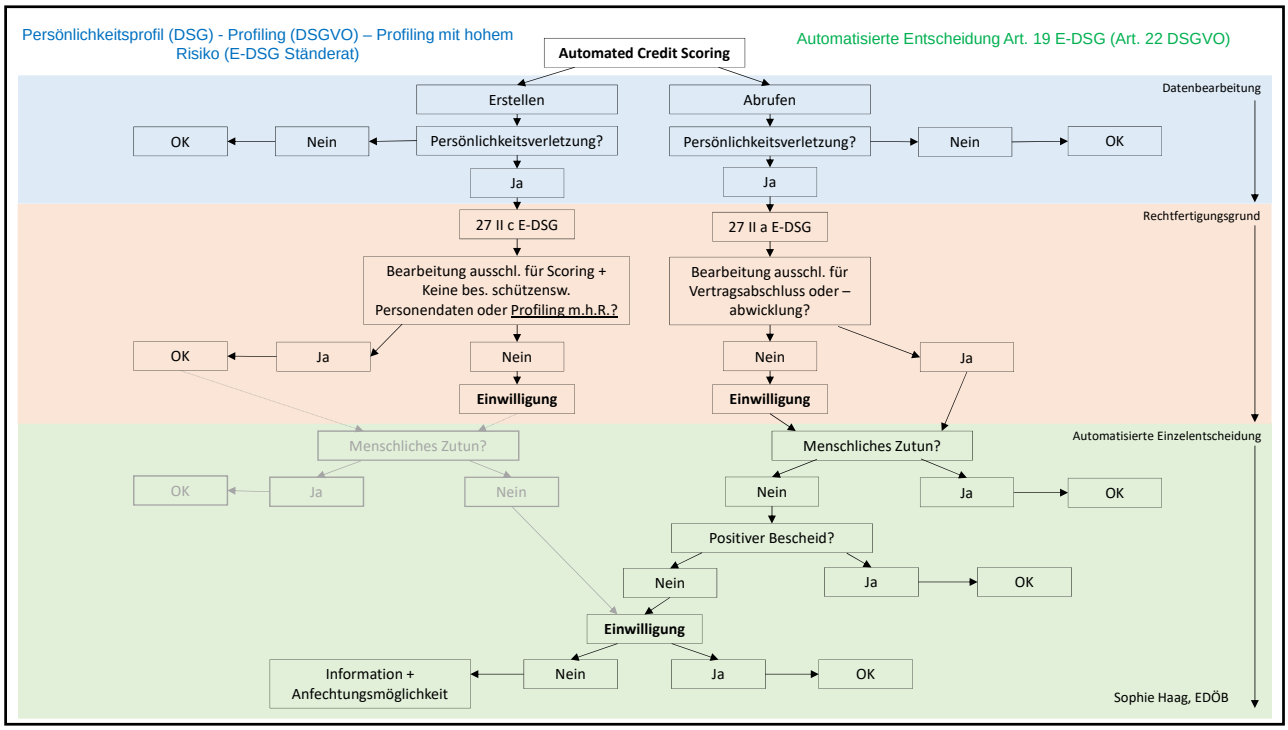
  → nebst Schutz vor Bearbeitung besonders schützenswerter Personendaten bietet diese Defintion den Bürgern keinen zusätzlicher Schutz vor Profiling (Regelung wirkungslos)

Profiling

- NR wird in Herbstsession als Zweitrat über letzte Differenzen entscheiden
- Mehrheit der nationalrätlichen Kommission beantragt gänzliche Streichung des Profiling mit hohem Risiko. Eine Minderheit befürwortet die Version des SR.

Profiling

- Wo würde sich der erhöhte Schutz beim Profiling auswirken?
  - Datenbearbeitungen durch Bundesorgane
    - Erfordern bei jeder Form des Profilings formell-gesetzliche Grundlage
  - Privatbereich:
    - Gestützt auf Rechtfertigungsgrund der Wirtschaftsauskunft und Bonitätsprüfung (ohne Einwilligung): Profiling mit hohem Risiko unzulässig (Art. 27 Abs. 2 lit. c Ziff 1 E-DSG)
    - Gestützt auf eine Einwilligung: nur wenn diese für das Profiling mit hohem Risiko ausdrücklich erfolgt (Art. 5 As. 6 und 7 E-DSG)
    - Minderheitsantrag: Spezielles Widerspruchsrecht mit Informationspflicht gegen jede Form des Profilings analog zu Art. 21 DSGVO der EU


Persönlichkeitsprofil (DSG) - Profiling (DSGVO) – Profiling mit hohem Risiko (E-DSG Ständerat)
Automated Credit Scoring
Automatisierte Entscheidung Art. 19 E-DSG (Art. 22 DSGVO)
Datenbearbeitung
Erstellen
Abrufen
Persönlichkeitsverletzung?
Persönlichkeitsverletzung?
Nein
OK
Nein
OK
Ja
Ja
Rechtfertigungsgrund
27 II c E-DSG
27 II a E-DSG
Bearbeitung ausschl. für Scoring + Keine bes. schützensw. Personendaten oder Profiling m.h.R.?
Bearbeitung ausschl. für Vertragsabschluss oder –abwicklung?
OK
Ja
Nein
Nein
Ja
Einwilligung
Einwilligung
Automatisierte Einzelentscheidung
Menschliches Zutun?
Menschliches Zutun?
OK
Ja
Nein
Nein
Ja
OK
Positiver Bescheid?
Nein
Ja
OK
Einwilligung
Information + Anfechtungsmöglichkeit
Nein
Ja
OK
Sophie Haag, EDÖB