21. Symposium on Privacy and Security
Zürich, 31. August 2016

Datenschutzbeauftragter des Kantons Basel-Stadt

Universität Basel

Uff!

Europas Datenschutzreformen und ihre Auswirkungen auf den öffentlichrechtlichen Datenschutz in der Schweiz

Beat Rudin

Prof. Dr. iur., Advokat, Titularprofessor an der Universität Basel, Datenschutzbeauftragter des Kantons Basel-Stadt, Basel

Was erwartet Sie?

Ein Blick auf das **grosse Bild**: Wo sind wir jetzt?

Ein Rückblick auf **überholte Ausnahmen**: Was muss weg (oder war – richtig verstanden – gar nie notwendig)?

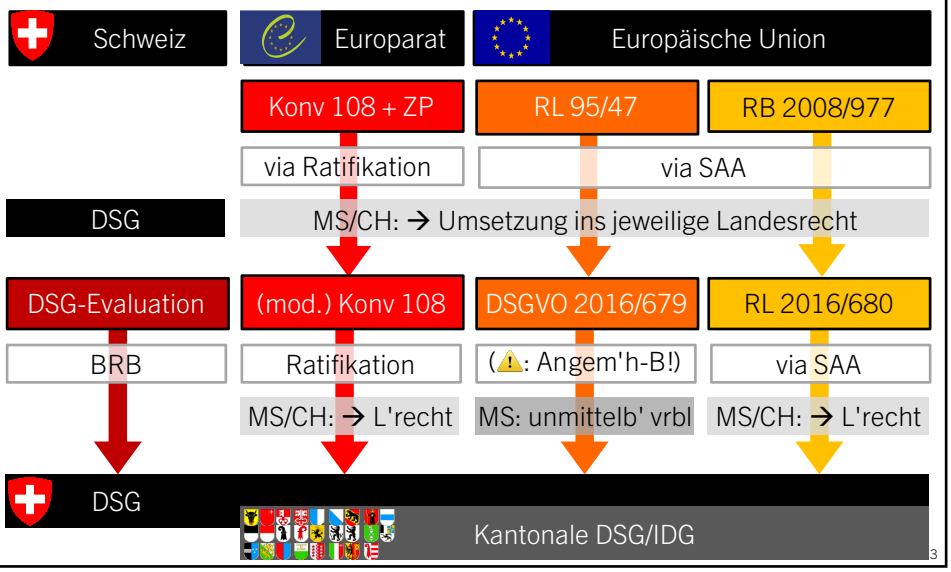
Ein Ausblick auf die **wichtigsten Anpassungen**: Was ist zu tun (oder zu lassen)?

Ein trauriger Anblick: Wie muss die **Aufsicht** aufgestellt sein (oder müsste schon lange so sein)?

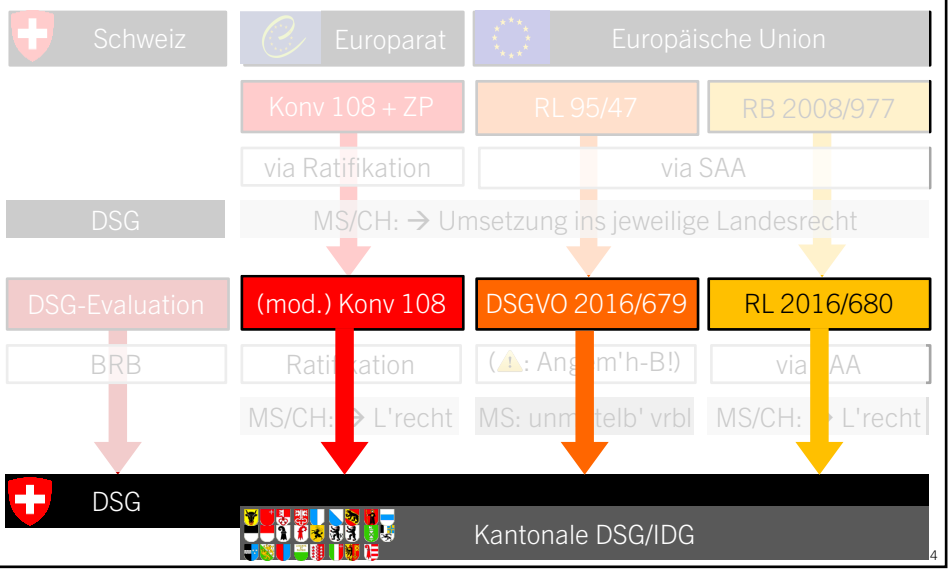
Ein letzter Blick voraus: Was sind die **Herausforderungen**?

 2

Einführung ins Thema: «Big Picture»



Einführung ins Thema: «Big Picture»: Gegenstand in diesem Referat



Einordnung

Woher? Quellen des umzusetzenden europäischen Rechts:

- (modernisierte) Europaratskonvention 108
  - via Ratifikation
- Richtlinie 2016/680
  - via Schengen-Assoziierungs-Abkommen SAA, weil schengenrevevant
- Verordnung 2016/679
  - nicht schengenrelevant, aber die Umsetzung ist Gegenstand der Angemessenheitsprüfung

Wohin? Anzupassende Gesetze:

- «Öffentlichrechtlicher Datenschutz» → DSG/Bund und DSG/Kantone

Bis wann?
Richtlinie 2016/680 wurde der Schweiz im August 2016 notifiziert → Umsetzung innert zweier Jahr, also bis August 2018

 5

Geltungsbereich 1

Bisher: keine Geltung des DSG/IDG (u.a.):

- in hängigen Verfahren des Zivil- und Strafprozesses
- in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit (Art. 2 Abs. 2 DSG/Bund und z.B. § 2 Abs. 2 IDG/BS)
- für öffentliche Register des Privatrechtsverkehrs (Art. 2 Abs. 2 DSG/Bund)

Die **Ausnahmen** sind **nicht mehr vorgesehen** – waren aber im Grunde genommen bisher schon **nicht erforderlich**.

 6

Geltungsbereich 2

Datenschutzgesetze = Grundsätze (sog. «*formelles Datenschutzrecht*»)

Anknüpfung an der Person des *Datenbearbeiters*: Bundesorgane → DSG/Bund, kantonale öffentliche Organe → kantonales DSG/IDG

Grundsätze: z.B. Personendaten-bearbeiten setzt gesetzliche Grund-lage voraus (Art. 17 DSG/Bund, § 9 IDG/BS)

Diese gesetzliche Grundlage findet sich in den ...

Fachgesetze = bereichsspezifische Datenbearbeitungsregeln (sog. «*materielles Datenschutzrecht*»)

Anknüpfung an der *Regelungskom-petenz*: Bundeskompetenz → BG (auch beim Bearbeiten durch kan-tonale öffentliche Organe!), kantonale Kompetenz → kant. G

z.B. im IVG und ATSG für die Invaliden-versicherung, im Schulgesetz für die Bildungsbehörden, im StGB und in der StPO für die Strafverfolgungsorgane, im ZGB und in der ZStV für das Zivilstands-amt ...

© 2016 B. Rudin 7

Geltungsbereich 3

Also – auch **ohne Geltungsbereichs-Ausnahme**:

- Die Bundesanwaltschaft findet die in Art. 17 (oder 19) DSG/Bund geforderte gesetzliche Grundlage in der StPO – *wie bisher!*
- Die Staatsanwaltschaft findet die vom kantonalen DSG/ IDG geforderte gesetzliche Grundlage in der StPO – *wie bisher!*
- Das von ihr zur Aushändigung von Akten aufgeforderte kantonale öffentliche Organ (z.B. die IV-Stelle) findet die vom kantonalen DSG/ IDG geforderte gesetzliche Grundlage in der StPO (Art. 194 StPO = Bekanntgabepflicht) – *wie bisher!*
- Dasselbe gilt für die öffentlichen Register des Privatrechts-verkehrs (Zivilstandsregister, Handelsregister, Grundbuch usw.): Die konkreten Datenbearbeitungsregeln finden sich im entsprechenden Registerrecht – *wie bisher!*

Also alles kein Problem? Kein Unterschied zu bisher? Doch ...

© 2016 B. Rudin 8

Geltungsbereich 4

Begründung für die Ausnahme war die Gefahr des Widerspruchs zwischen StPO und DSG/IDG – z.B. bezüglich der **Rechte und Ansprüche der Betroffenen**.

Lösung: Ausdrückliche Regelung im DSG/IDG:

«Die Rechte und Ansprüche der betroffenen Personen richten sich in hängigen Verfahren der Zivil- und Strafrechtspflege und der Verfassungs- und Verwaltungsgerichtsbarkeit ausschliesslich nach dem anwendbaren Verfahrensrecht.»

 9

Geltungsbereich 5

Verbleibender Unterschied: **(Datenschutz-)Aufsicht** neu (zusätzlich) durch Datenschutzbeauftragte – wenig sinnvoll.

Lösung: (zulässige) Ausnahme im DSG/IDG:

«Der Kontrolle durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten unterstehen nicht:

x. Datenbearbeitungen in hängigen Verfahren der Zivil- und Strafrechtspflege und

y. Datenbearbeitungen in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit.»

 10

Begriffsdefinitionen – oder etwas mehr ... 1

Personendaten = Daten über bestimmte oder bestimmbare natürliche *und juristische* Personen (Art. 3 lit. a+b DSG/Bund)

Oder nicht mehr? Antwort des Bundesrates auf die Motion 16.3379 Beglé: «*Der Bundesrat erachtet es als wichtig, dem Stand des Datenschutzrechts im Rahmen des Europarates und der Europäischen Union Rechnung zu tragen. Deshalb ist vorgesehen, auf den Schutz der Personendaten juristischer Personen zu verzichten.*»

Auswirkungen im öffentlichrechtlichen Datenschutz?

In den kantonalen DSG/IDG belassen?

 11

Begriffsdefinitionen – oder etwas mehr ... 2

Besonders schützenswerte (besondere) Personendaten

Neu: **«Genetische Daten»**

Sicherstellen, dass diese bei den besonders schützens-werten Personendaten zweifellos mitverstanden werden

Neu: **«Biometrische Daten, die eine natürliche Person eindeutig identifizieren»**

Sicherstellen, dass diese bei den besonders schützens-werten Personendaten zweifellos mitverstanden werden

Definition klar? Fingerabdrücke, Iris-Scans. Gesichtsbilder, die durch Gesichtserkennungsprogramme generiert wurden – nicht aber «gewöhnliche» Fotos?

 12

Begriffsdefinitionen – oder etwas mehr … 3

«Profiling»

Jedes automatisierte Bearbeiten von Daten, unabhängig davon, ob sie sich auf eine Person beziehen oder nicht, bei dem diese Daten verwendet werden, um wesentliche persönliche Merkmale, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Sexualleben oder Ortswechseln, zu analysieren oder vorherzusagen.

Also nicht mehr eine Kategorie von (heiklen) Daten, sondern eine (heikle) **Art des Bearbeitens** → muss bei den Bearbeitungs-Voraussetzungen berücksichtigt werden, z.B.:

«Besonders schützenswerte Personendaten dürfen nur bearbeitet oder ein Profiling darf nur vorgenommen werden, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht oder wenn es für eine in einem Gesetz im formellen Sinn klar umschriebene Aufgabe unentbehrlich ist».

 13

Betonung der Verantwortung, Nachweis des «Compliant-Seins»

Die **Verantwortung** wird stärker betont → sie muss klar(er!) geregelt sein.

Von besonderer Bedeutung, wenn mehrere öffentliche Organe einen Informationsbestand gemeinsam bearbeiten *(«Datenpools»)* und bei der *Auftrags(daten)bearbeitung*.

Mehrfach wird auf die Pflicht hingewiesen, **nachweisen** zu können, dass die Datenschutzregeln eingehalten sind.

Mögliche Lösung: Datenschutz-Managementsystem (DSMS) oder Informationssicherheits-Managementsystem (ISMS)

Kriterien? Anforderungen?

 14

Datenschutz-Folgenabschätzung, Vorabkontrolle

Bisher: Vorabkontrolle: «Datenbearbeitungsvorhaben, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Personendaten besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich bringen können» → Vorlage an DSB

Neu: **Datenschutz-Folgenabschätzung** in der Verantwortung des Datenbearbeiters

- Beschreibung der geplanten Bearbeitungsvorgänge
- Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken
- Darstellung und Bewertung der geplanten Abhilfemassnahmen
- = *Vorbereitung der Vorabkontrolle durch das verantwortliche öffentliche Organ*

Vorabkontrolle bleibt:

- Prüfung der Risikoanalyse und der geplanten Massnahmen
- = *«Kontrolle» der Datenschutz-Folgenabschätzung*
- Empfehlungen

 15

Systemgestaltung

Verankerung von Prinzipien zur Systemgestaltung:

Privacy by design: datenschutzfreundliche Systemgestaltung

Privacy by default: datenschutzfreundliche Voreinstellungen

Umsetzung? → Referat Marc Langheinrich

 16

Transparenz: Informationspflicht, Verzeichnis der Datenbearbeitungstätigkeiten

Erhöhte Anforderungen an die Transparenz

Wechsel vom Erfordernis der blossen Erkennbarkeit einer Datenbeschaffung zur **Informationspflicht** darüber

Nicht nur bei besonders schützenswerten Personendaten
- im DSG/Bund wie bisher – in den meisten Kantonen neu

Wechsel vom Register der Datensammlungen (häufig noch vom DSB geführt) zum **Verzeichnis der Datenbearbeitungstätigkeiten**, das vom verantwortlichen öffentlichen Organ geführt werden muss

 17

Transparenz: Meldung von Datenschutzverletzungen

Meldepflicht bei Datenschutzverletzungen («Data Breach Notification»)
- an DSB (ausser die Verletzung führt nicht zu einem Risiko für die Betroffenen)
- an die Betroffenen («wenn die Umstände es erfordern» – z.B. wenn von ihrer Seite Schutzmassnahmen getroffen werden können/müssen)
- mit Einschränkungen (wie bei der Informationspflicht)

Bei der Auftragsbearbeitung: unverzügliche Information des auftraggebenden öffentlichen Organs (das ja verantwortlich bleibt!)

 18

Datenschutzaufsicht 1

Aufgaben:
- Beratung
- Kontrolle
- Sensibilisierung, Öffentlichkeitsarbeit
- Verfolgung der Entwicklungen
- Kooperation mit anderen DSB
- Pflicht zur Behandlung von «Beschwerden» betroffener Personen (in der Schweiz wohl: «aufsichtsrechtliche Anzeige»)

Befugnisse:
- Weitgehende Ermittlungsbefugnisse
- Wirksame Einwirkungsbefugnisse
  - Beanstandungen, Empfehlungen, Anordnungen (bis hin zum befristeten oder vollständigen Untersagen bestimmter Datenbearbeitungen)
  - Umsetzung: formloser Hinweis / Empfehlung (mit Antwortpflicht des adressierten öffentlichen Organs) / Weisung (z.B. in Form einer anfechtbaren Verfügung)
- Anzeigerecht

 19

Datenschutzaufsicht 2

Ausnahme von der Aufsicht:
- Gerichtliche Verfahren

Unabhängigkeit als Voraussetzung für eine wirksame Aufsicht

Angemessene Ressourcen

Zusammengefasst:
- Kaum etwas, was nicht heute schon umzusetzen wäre ([alte] ER-Konv 108 und Zusatzprotokoll, EG-Richtlinie 95/46 via SAA).
- Vielerorts aber erhebliche Defizite – in einer Vielzahl von Kantonen zwischen praktisch inexistent und beschränkt wirksam.

 20

Umsetzung

Anpassungen auf **Stufe Bund**:
- allgemein: im DSG/Bund
  - → gilt nicht für kantonale öffentliche Organe!
- in den relevanten Gesetzen
  - AuG, AsylG, BGG, BPI, BWIS, IRSG, MG, RVOG, SIaG, StGB, StPO, VGG, VwVG, ZentG, ZNDG usw.
  - → gelten ggf. auch für kantonale öffentliche Organe

Anpassungen auf **Stufe Kanton**:
- allgemein: im DSG/IDG
- bereichsspezifisch: kantonale Gesetze?

Arbeitsgruppe von privatim

Arbeitsgruppe «Datenschutz» der BOSD (KdK)

 21

Herausforderung

Analyse des Handlungsbedarfs

Konkretisieren
- Abstrakte Formulierungen in der (modernisierten) ER-Konvention 108 → handhabbare Regelungen

Herunterbrechen
- EU-Recht reduzieren → verständliche, handhabbare Regelungen (das Erfordernis der Referendumstauglichkeit diszipliniert!)
- Einpassen ins bestehende Recht

Vereinfachen und nicht übertreiben («Musterschüler»-Vorwurf) – aber auch **keine Schlaumeiereien**!

Die Schweiz sieht sich als Hort der Freiheit – wirksamer Schutz der Grundrechte der Schweizerinnen und Schweizer in der digitalen Welt nur, weil und soweit es die EU verlangt?!?

 22

Fragen?

Datenschutzbeauftragter des Kantons Basel-Stadt

Universität Basel

Danke für Ihr Interesse!

N.B. Happy Birthday!

Beat Rudin
Prof. Dr. iur., Advokat, Titularprofessor an der Universität Basel
Datenschutzbeauftragter des Kantons Basel-Stadt
Henric Petri-Strasse 15, Postfach 205
4010 Basel
www.dsb.bs.ch
datenschutz@dsb.bs.ch

 23

 24