Vorentwurf des neuen DSG

Ausgewählte Aspekte

10. Tagung zum Datenschutz, 8. Februar 2017, Kongresshaus Zürich

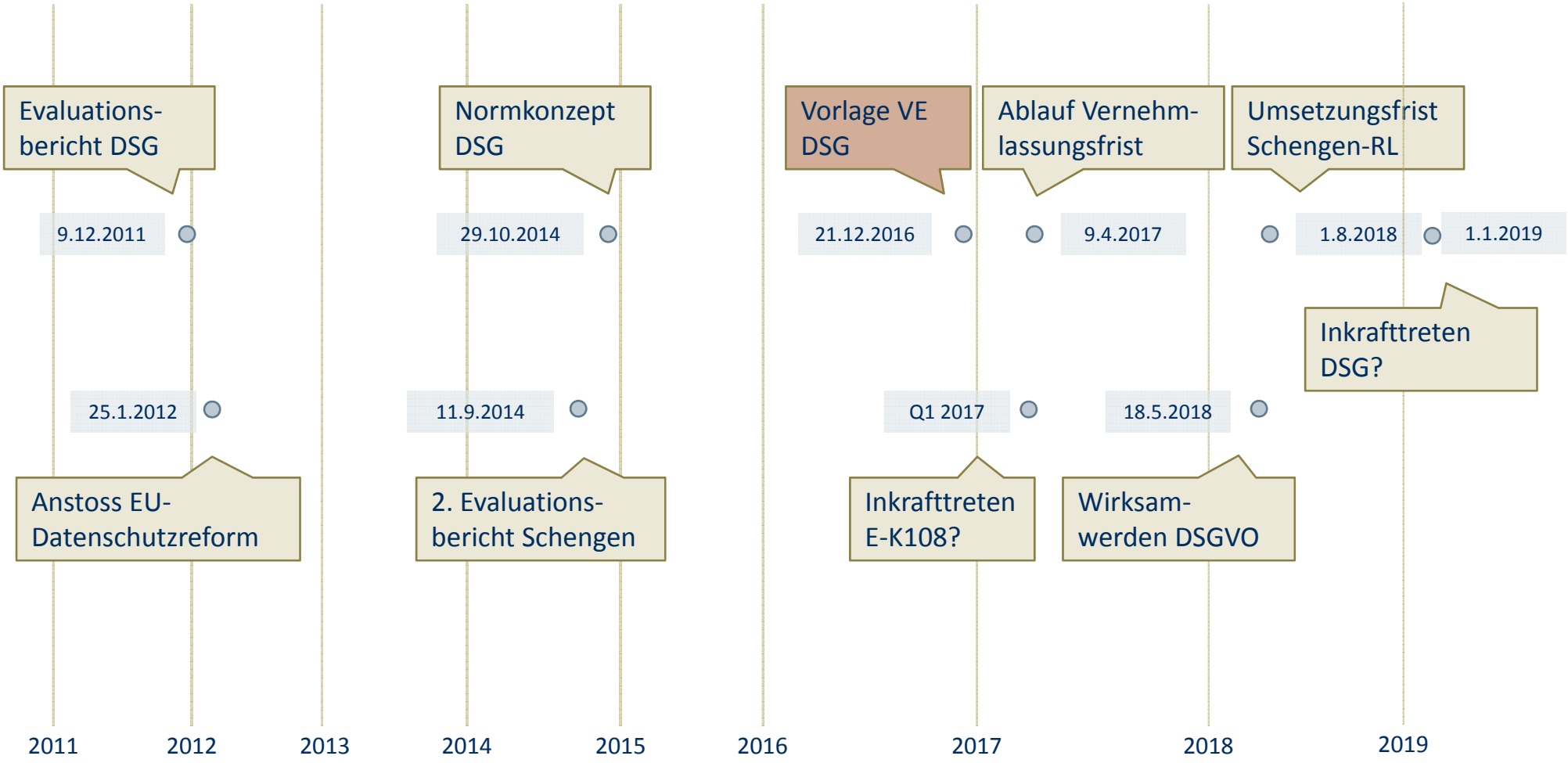
David Vasella

walderwyss rechtsanwälte

Vorbemerkungen

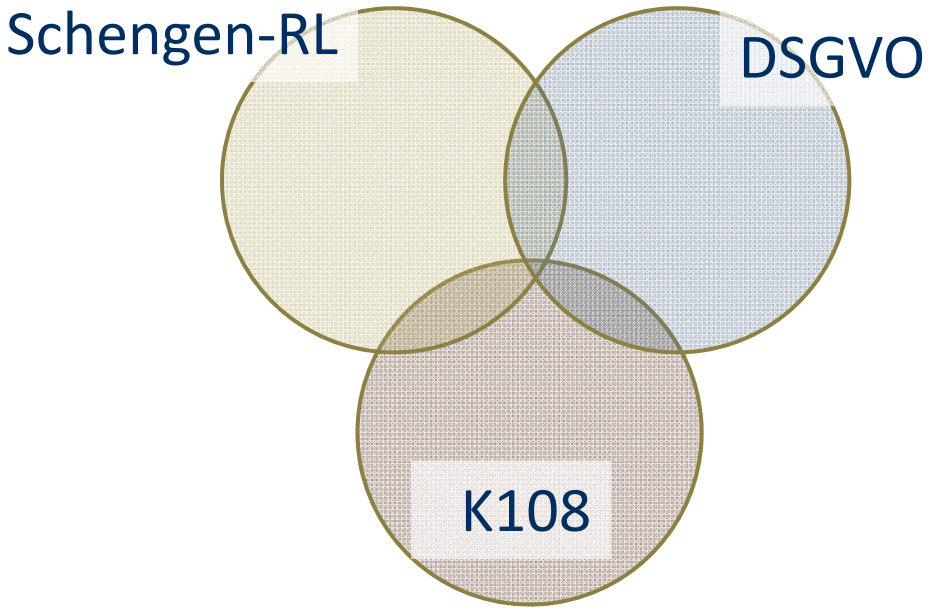
- Chronologie
- Kontext

Chronologie



Das internationale Umfeld

Schengen-RL: als Teil des Schengen-Acquis verbindlich
- für Behörden
- im Bereich der Verbrechens-bekämpfung und des Strafverfahrens



auf viele CH-Unternehmen anwendbar, aber Umsetzung im VE nicht zwingend (nicht Teil des Schengen-Acquis)

E-K108: verbindlich (bei Ratifizierung)

Berücksichtigung im VE DSG

- **E-K108**: Umsetzung (vorweggenommen; noch keine definitive Fassung
- **Schengen-RL**:
  - differenzierte Umsetzung
  - generelle Umsetzung für Private, soweit E-K108 entsprechend (Erl Ber 27 f.)
- **DSGVO**:
  - terminologische «Annäherung» statt autonomer Nachvollzug - wirklich?
  - keine «DSGVO-konforme Auslegung» des neuen DSG (und auch nicht der K108)
  - eine Angst vor dem Verlust der Angemessenheit wäre unbegründet
- vgl. Konkordanztabelle des EDÖB

zur «Angemessenheit» des Schutzes gemäss DSGVO

- keine buchstabengetreue (oder artikelgetreue) Umsetzung erforderlich!
- verlangt ist lediglich angemessener Schutz durch Rechtsstaatlichkeit, gelebte Schutzmechanismen, Betroffenenrechte und unabhängige Aufsicht (Art. 45 Abs. 2 DSGVO)
- EuGH i.S. *Schrems* (6.10.2015, Rs. C-362/14):

  «… verlangt wird, dass das Drittland […] tatsächlich ein **Schutzniveau der Freiheiten und Grundrechte** gewährleistet, das dem in der Union aufgrund der Richtlinie 95/46 im Licht der Charta garantierten Niveau **der Sache nach gleichwertig** ist»
- Berücksichtigung insb. auch des Beitritts zur K108 (ErwGr 105)

Wesentliche Neuerungen des VE

- keine Anwendung auf juristische Personen (Art. 3 VE)
- Wegfall des «Inhabers»; stattdessen der «Verantwortliche» (Art. 3 VE)
- Wegfall der «Datensammlungen» (Art. 3 VE)
- Änderungen bei der Übermittlung ins Ausland (Art. 5 f. VE)
- Selbstregulierung durch Codes of Conduct (Art. 8 f. VE)
- Ausbau der Transparenz (Informationspflicht, Auskunftsrecht) (Art. 13 f., 20 VE)
- automatisierte Einzelfallentscheidungen (Art. 15 VE)
- Data breach notifications (Art. 17 VE)
- Privacy by design / by default (Art. 18 VE)
- Dokumentationspflicht (Art. 19 VE)
- Verfügungsmacht des EDÖB (Art. 37 ff. VE)
- strafrechtliche Sanktionen (Art. 51 ff. VE)

Konzept des VE DSG

- Mantelerlass mit zwei Teilen:
- 1. Totalrevision des DSG, Anpassungen in weiteren Bundesgesetzen
- 2. Änderungen weiterer Bundesgesetze zur Umsetzung der Schengen-RL
  - Art. 349a ff. StGB (Amtshilfe im Polizeibereich)
  - Art. 95a, 98 Abs. 2 StPO (Bearbeitung von Personendaten durch Polizeibehörden)
  - Art. 11b ff. IRSG (Datenschutz bei int. Strafrechtshilfe)
  - weitere Bestimmungen

aktive Informationspflicht

- Art. 13-14 VE
- Art. 7bis E-K108
- Art. 13 Schengen-RL
- Art. 12-14 DSGVO

Aktive Informationspflicht

- Erweiterung der **aktiven Informationspflicht** nach Art. 14 DSG auf die Beschaffung nicht-sensibler Personendaten (Art. 13 VE); aktives Informieren («mitteilen»)
- Pflicht des **Verantwortlichen**
- **Katalog** mitteilungsbedürftiger Punkte in Art. 13 Abs. 1 und 2 (Generalklausel und Pflichtangaben); Abs. 3 (Drittbekanntgabe) und Abs. 4 (Auftragsbearbeiter)
- Unterscheidung zwischen Direkterhebung beim Betroffenen und indirekter Erhebung (Art. 13 Abs. 5 VE; vgl. Art. 13 und Art. 14 DSGVO); Information je nachdem (i) bei Beschaffung oder (ii) Speicherung oder Bekanntgabe
- (Informationspflicht ggü. Empfängern bei Berichtigung, Löschung etc., Art. 19 lit. b VE; unabhängig von Grund und Interessenlage)

Art und Weise der Information

- kein Formerfordernis
- Information muss «leicht zugänglich» und «verständlich» sein (Erl Ber 56; vgl. Art. 12 Abs. 1 DSGVO)
- aber: datenschutzrechtliche Transparenz, nicht empfangsbedürftige Erklärung
- im Einzelfall oder allgemein vorab, z.B. in AGB oder DSE über gut sichtbaren und verständlichen Link (zumindest bei Direkterhebung über die Website)
- Zusammenfassung, klare Überschriften, Icons etc. können sinnvoll sein

Zeitpunkt der Information

- Direkterhebung: spätestens bei der Beschaffung (d.h. der Entgegennahme der Daten)
- indirekte Erhebung:
  - direkt nach der Beschaffung («Speicherung»)
  - oder spätestens bei Bekanntgabe an Dritte
  - strenger als Art. 14 Abs. 3 DSGVO:
    - spätestens nach einem Monat
    - bei Kommunikation mit dem Betroffenen: spätestens dann
    - bei Offenlegung an andere: spätestens dann

Ausnahmen der Informationspflicht

- Ausnahmen (Art. 14 VE):
  - bereits bekannte Angaben
  - Unmöglichkeit/Unzumutbarkeit (aber nur bei indirekter Beschaffung!)
  - überwiegende Interessen des Verantwortlichen (aber nur falls keine Drittbekanntgabe – anders als nach Art. 14 Abs. 5 lit. b DSGVO)
  - gesetzlich geregelte Bearbeitung
    - indirekte Erhebung: ausdrückliche Grundlage für die Bearbeitung genügt
    - Direkterhebung: formellgesetzliche Grundlage für die Verweigerung erforderlich
  - Nachholpflicht (Art. 14 Abs. 5 VE)

Gegenstand der Transparenz

I: Information
A: Auskunft
I**: wie vom MGS vorgesehen
I*: nur falls konkret erforderlich
DPA: Aufsichtsbehörde

Gegenstand	VE-DSG Information	E-K108	Schengen-RL	DSGVO
Angaben zum Verantwortlichen	I, A	I, A	I	I
bearbeitete Daten bzw. Kategorien	I, A	I, A	A	I, A
Bearbeitungszweck(e)	I, A	I, A	I, A	I, A
ggf. Empfänger (Dritte, Auftragsbearbeiter)	I, A	I, A	I*, A	I, A
ggf. Auslandsübermittlung				I
Rechtsgrundlage			I**, A	I
Datenquelle	A	A	A	I*, A
Speicherdauer oder -logik	A	A	I*, A	I*, A
ggf. AEFE	A	A		I*, A
ggf. Angaben zu Entscheidungen (ohne AEFE)	A	A		
ggf. Breach notification	DPA/Betroffener	nur DPA	DPA/Betroffener	DPA/Betroffener
Beschwerderecht			I, A	I*, A
Aufklärung über Betroffenenrechte		I, A	I, A	I*, A
ggf. weitere (Generalklausel)	I	I, A	I**	I*

Mögliche weitere Informationspunkte:

- Rechteausübung durch die Betroffenen (vgl. Schengen-RL 13 I d; E-ERK 7bis I; DSGVO 13 II b/14 I c)
- Widerruflichkeit einer Einwilligung (vgl. Art. 13 Abs. 2 lit. c/Art. 14 Abs. 1 lit. d DSGVO)
- Beschwerderecht beim EDÖB (vgl. Art. 13 Abs. 1 lit. d Schengen-RL; Art. 13 Abs. 2 lit. d/Art. 14 Abs. 2 lit. e DSGVO)
- Freiwilligkeit der Datenbekanntgabe und ggf. die Folgen der Verweigerung (vgl. Art. 13 Abs. 2 lit. e DSGVO)
- eigenen Interessen bei Rechtfertigung durch überwiegende Interessen (vgl. Art. 13 Abs. 1 lit. f/Art. 14 Abs. 2 lit. b DSGVO bei der direkten Beschaffung)
- Übermittlung ins Ausland (vgl. DSGVO 13 I f/14 I f)

Transparenz?

«Allerdings hat die Minderheit der Fachpersonen sich auch dahingehend geäussert, **dass durch die umfassende Information nicht mehr Transparenz geschaffen würde, sondern es einfach zu einem Mehr an Information kommen würde**, was letztlich der Transparenz zuwider liefe (**Informationsüberflutung**) und kontraproduktiv wäre […]»

Regulierungsfolgenabschätzung, 28

Auskunftspflicht

- Art. 20 f. VE
- Art. 8 Abs. 1 lit. b und c E-K108
- Art. 14 Schengen-RL
- Art. 15 DSGVO

Auskunftsrecht

- wie heute: unverzichtbares Recht auf kostenlose Auskunft über Bearbeitungen und bearbeitete Daten
- aber keine Beschränkung mehr auf Datensammlungen (bei nicht erschliessbaren Datenbeständen: ggf. Aufschub, Einschränkung oder Verweigerung)
- Pflicht des Verantwortlichen (subsidiär des Auftragsbearbeiters)
- Anwendung auch in kantonalen Verfahren (Art. 2 Abs. 3 VE)
- keine zeitlichen und formellen Vorgaben im VE
- keine Pflicht zu Vollständigkeitsbestätigungen
- Verletzung sanktioniert

Gegenstand des Auskunftsrechts

Gegenstand	VE-DSG Information	E-K108	Schengen-RL	DSGVO
Angaben zum Verantwortlichen	•	•		
bearbeitete Daten bzw. Kategorien		•	•	•
Bearbeitungszweck(e)	•	•	•	•
ggf. Empfänger (Dritte, Auftragsbearbeiter)	•	•	•	•
ggf. Auslandsübermittlung				
Rechtsgrundlage			•	
Datenquelle	•	•	•	•
Speicherdauer oder -logik	•	•	•	•
ggf. Vorliegen einer AEFE	•	•		•
ggf. Angaben zu Entscheidungen (ohne AEFE)	•	•		
Beschwerderecht			•	•
Angaben zu Betroffenenrechten		•	•	•

Auskunftsrecht über «Entscheidungen»?

- Art. 20 Abs. 3 VE:

  *«Wird aufgrund einer Datenbearbeitung eine **Entscheidung** gefällt, insbesondere eine automatisierte Einzelentscheidung, erhält die betroffene Person Informationen über das Ergebnis, das Zustandekommen und die Auswirkungen der Entscheidung.»*

- stammt aus Art. 8 Abs. 1 lit. c E-K108:

  "Every individual shall have a right: … c. to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her;»

- jedenfalls nur bei relevanten Eingriffen (Bsp. im Draft Expl Rep: Credit Scoring)
- Beschränkung auf AEFE wäre besser (so auch in Art. 15 Abs. 1 lit. h DSGVO)
- Pflicht zur Information in groben Zügen; keine Offenbarung von Geschäftsgeheimnissen

Einschränkung des Auskunftsrechts

- Regelung der Einschränkung (verweigern, einschränken oder aufschieben) im Grundsatz gleich wie im heutigen Recht
- Gründe wie beim Informationsrecht bei Direkterhebung:
  - bereits bekannte Angaben
  - gesetzlich geregelte Bearbeitung
  - überwiegende Interessen des Verantwortlichen (falls keine Drittbekanntgabe)
- Einschränkung durch Medienschaffende (Art. 22 VE) wie heute geregelt (Art. 10 DSG)
- ebenfalls wie heute (Art. 9 Abs. 5 DSG) Begründungspflicht des Auskunftspflichtigen (Art. 21 Abs. 2 VE)

Breach Notification

- Art. 17 VE
- Art. 30 Schengen-RL
- Art. 7 Abs. 2 E-K108
- Art. 22 DSGVO

Breach Notification

- Instrument der Datensicherheit und der Transparenz
- eigentlich heute schon vorhanden (Art. 4 Abs. 3 und Art. 7 DSG)?
- Grundsatz: Mitteilungspflicht…
  - des Verantwortlichen
  - ggf. auch des Auftragsbearbeiters ggü. dem Verantwortlichen
  - bei jeder unbefugten Bearbeitung
  - an den EDÖB und ggf. den Betroffenen
- Ausnahme: voraussichtlich kein Risiko für die betroffenen Personen

Breach Notification

«**Unbefugte Bearbeitung**»:

- unbefugte Bearbeitung (vgl. Art. 7 Abs. 1 DSG)
- nur effektiv erfolgte Bearbeitung (folgenlose Verletzungen der Datensicherheit z.B. durch versehentliches Zugänglichmachen sind nicht erfasst)

Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person:

- das durch die Verletzung bewirkte Risiko
- Ausschluss von Bagatellmeldungen: Meldung nur (i) bei relevanten Risiken (ii) mit gewisser Eintretenswahrscheinlichkeit

Meldung an den EDÖB (Art. 17 Abs. 1 VE)

- «unverzüglich», d.h. ohne unbegründete Verspätung
- kein Formerfordernis
- Gegenstand:
  - relevante Angaben zur erfolgten Datenschutzverletzung
  - Bewertung des daraus folgenden Risikos

Meldung an den Betroffenen (Art. 17 Abs. 2 VE)

- bei hohem Risiko (Art. 31 Abs. 1Schengen-RL/Art. 34 Abs. 1 DSGVO)
  - sofern es zum Schutz der betroffenen Person erforderlich ist (wenn die betroffene Person das verbleibende Risiko sinnvoll reduzieren kann), oder
  - auf Verlangen des EDÖB
- Wegfall/Einschränkung der Informationspflicht
  - bei überwiegenden Drittinteressen (z.B. Sicherheit der Personendaten anderer Betroffener)
  - bei eigenen überwiegenden Interessen, sofern keine Drittbekanntgabe erfolgt (Art. 14 Abs. 3 und 4 VE)
- Gegenstand:
  - erfolgte Datenschutzverletzung
  - Risikominderungsmassnahmen
- kein Formerfordernis – ggf. auch durch öffentliche Information (nicht grds. empfangsbedürftig

Breach Notification

- Meldepflicht des Auftragsbearbeiters (Art. 17 Abs. 4 VE): unklarer Umfang
- Sanktionsrisiken
  - des Verantwortlichen (Art. 50 Abs. 1 lit. b Ziff. 1 und Art. 50 Abs. 2 lit. d* VE)
  - des Auftragsbearbeiters (Art. 50 Abs. 3 lit. b VE)

* falsche Nummerierung (lit. e) im VE

Automatisierte Einzelfallentscheidungen

- Art. 15 VE
- Art. 11 Schengen-RL
- Art. 8 lit. a E-K108
- Art. 22 DSGVO

Automatisierte Einzelfallentscheidung

- Anspruch auf «menschliches Gehör» bei einschneidenden Entscheidungen
- keine Rechtfertigungsbedürftigkeit (ausser bei Profiling, Art. 24 VE; anders Art. 22 Abs. 1 DSGVO)
- kein Verbot der AEFE...
  - gestützt auf besonders schützenswerte Personendaten (anders Art. 22 Abs. 4 DSGVO, ausser bei Einwilligung)
  - bei Kindern (anders ErwGr 71)
- … aber Informations- und Anhörungspflicht des Verantwortlichen

Was ist eine AEFE?

- Entscheidung im Einzelfall
- automatisiert: Ablauf der Bearbeitung bis zur konkreten Entscheidung ohne menschliches Zutun (aber auch ohne Profiling)
- mit rechtlichen Wirkungen…
  - Begründung, Aufhebung oder Änderung einer Rechtsposition
- …oder erheblichen Auswirkungen
  - z.B. Verweigerung eines Vertrags (kein Einfluss auf eine Rechtsposition), relevant daher nur bei Erheblichkeit
  - Anlehnung an BGE 129 III 35 (Post/VgT): Normalbedarf?

Informationspflicht bei der AEFE

- aktive Information über die AEFE selbst – unklar ist der Umfang der Informationspflicht
- vorab oder im Nachhinein (z.B. mit Mitteilung des Ergebnisses)
- Information über die Auswirkungen und Zustandekommen: nur auf Gesuch (Art. 20 Abs. 3 VE)

Äusserungsrecht bei der AEFE

- Anhörung zur Entscheidung und zur Datengrundlage
- vorab oder im Nachhinein
- keine Formerfordernisse und keine Reaktionspflicht (anders Art. 22 Abs. 3 DSGVO)
- aber Pflicht zur «Berücksichtigung» (Art. 8 Abs. 1 lit. a E-K108): Möglichkeit des Eingreifens in die Entscheidung

sinnvolle Neuerung?

- Recht auf «menschliches Gehör» zur Verbesserung der Datenqualität: Konsumentenschutz im Gewand des Datenschutzrechts
  - Einmischung in den zivilrechtlichen Willensbildungsvorgang
  - Richtigkeitsgebot hätte genügt
- automatisierte Entscheidung wohl meistens gleich und manchmal besser als «menschliche» Entscheidung
- … aber vorgegeben durch Art. 8 Abs. 1 lit. a E-K108
- aber: zu weitgehendes Äusserungsrecht (auch zur Entscheidung selbst, über Datengrundlage hinaus)

Datenschutz-Folgenabschätzung

- Art. 16 VE
- Art. 8bis Abs. 2 E-K108
- Art. 27 f. Schengen-RL
- Art. 35 f. DSGVO

Datenschutz-Folgenabschätzung

- «Privacy Impact Assessment»: Instrument zur Erkennung und Minderung erhöhter Datenschutzrisiken
- in der Sache nichts Neues: Art. 7 DSG/Art. 8 VDSG; Art. VDSG 20 Abs. 2 für Bundesorgane
- inhaltliche und formelle Vorgaben: Textform; Beschreibung der Bearbeitung, der Risiken und ggf. der Massnahmen zur Minderung (Art. 16 Abs. 2 VE)

Aufgreifkriterien der DSFA

- vorgesehene Datenbearbeitung mit «voraussichtlich» «erhöhtem» Risiko
  - keine Pflicht bei unvorhersehbaren oder bereits bekannten Risiken («voraussichtlich»)
  - «erhöht» müsste «hoch» heissen (Art. 27 Abs. 1 Schengen-RL; Art. 35 Abs. 1 DSGVO; Erl Ber 61: Potential «erheblicher» Einschränkungen; vgl. Art. 35 Abs. 3/ErwGr 91 DSGVO)
  - Risikofaktoren: Zahl der potentiell betroffenen Personen; Umfang und Art der Daten; Zugriffsberechtigte; Profilierung; Übermittlung in Drittstaaten ohne angemessenen Schutz; Risiken bei Datenlecks
  - Risiko auch für Grundrechte: DSG als Einfallstor für direkte Drittwirkung?
  - VE: Empfehlungen der guten Praxis (Art. 8 f. VE); EU: Positiv- und Negativlisten der Aufsichtsbehörden (DSGVO 35 Abs. 4/5)

Gegenstand der DSFA

- Art. 16 Abs. 2 VE:
  - geplante Bearbeitung (betroffene Daten und Systeme; Bearbeitungszwecke; Abläufe)
  - Risikobewertung
  - Risikominderungsmassnahmen (Art der Massnahmen, z.B. Privacy by design/default; erwartete Wirkung)
  - Interessenabwägung, akzeptierte Restrisiken

Ablauf der DSFA

- Pflicht (nur) des Verantwortlichen (trotz Art. 16 Abs. 1 VE – Präzisierung wäre sinnvoll)
- Prüfschritt bei internen Abläufen, sobald ausreichende Klarheit besteht
- Einbezug interner Stellen (Fachverantwortliche)
- keine Pflicht zum Einbezug potentiell betroffener Personen (vgl. Art. 35 Abs. 9 DSGVO)
- Festhalten des Ergebnisses (Meldepflicht)

Meldepflicht ggü. dem EDÖB

- unterschiedslose Mitteilung des Ergebnisses und der geplanten Massnahmen an den EDÖB (Art. 16 Abs. 3):
  - zu weit – Art. 36 DSGVO: Konsultation nur bei erheblichen Restrisiken (vgl. ErwGr 84)
  - erheblicher Eingriff
  - zweck- und wirkungslos
- EDÖB: (zu lange) Dreimonatsfrist für Einwände (Art. 16 Abs. 4; aber weder Sperrwirkung noch Präjudiz, da Konsultation, nicht Genehmigungserfordernis)

Sanktionierung

- Strafbarkeit (Art. 51 Abs. 1 d VE) ist hier angesichts der Unbestimmtheit besonders stossend
- Strafbarkeit nur der unterlassenen Meldung?

Kompetenzen des EDÖB

- Art. 36 ff. VE
- Art. 12bis E-K108
- Art. 41 ff. Schengen-RL
- Art. 51 ff. DSGVO

Übersicht

Information des EDÖB:

- Verwendung spezifischer Garantien
- Verwendung standardisierter Garantien
- im Ausland genehmigte BCR
- durch u.a. Vertragsabwicklung oder ausländisches Verfahren gerechtfertigte Übermittlung ins Ausland
- Ergebnis der DSFA
- Breach Notification

Genehmigung durch den EDÖB:

- standardisierte Garantien und BCR
- Empfehlungen der guten Praxis

Untersuchungen

- Untersuchung bei jeder Datenschutzverletzung möglich (Art. 41 Abs. 1 VE; auch ohne «Systemfehler»)
- Vorgabe von Art. 12bis Abs. 2 lit. a E-K108
- Untersuchung trotzdem nur bei grösserer Zahl Betroffener (Erl Ber 78)
- Mitwirkungspflichten wie nach geltendem Recht, nun aber sanktioniert (Art. 50 Abs. 2 lit. c VE)
- bei Verletzung neu auch Recht auf Hausdurchsuchungen

Verfügungskompetenz

- neu: Verfügungskompetenz des EDÖB ohne Umweg über das BVGer (Art. 43 VE), zur Erfüllung der Schengen-Anforderungen
- Verhältnismässigkeit: ggf. genügt Beratung i.S.v. Art. 41 Abs. 4 VE
- auch vorsorgliche Massnahmen (Art. 42 VE)
- keine Befugnis zu Verwaltungssanktionen
- Recht zur Information der Öffentlichkeit (Art. 48 Abs. 2 VE), sofern es das öffentliche Interesse verlangt (und i.d.R. nur anonymisiert) – nur bei Verletzungen mit besonderer Bedeutung und branchenweiter Bedeutung?

Verfügungskompetenz

- Verfahren und Beschwerderecht nach VwVG (Art. 44 VE)
- keine Parteirechte der betroffenen Person (Art. 44 Abs. 2 VE)
- umfassende Anzeigepflicht des EDÖB bei Offizialdelikten (Art. 45 VE):
- weitergehend als nach Art. 22a BPG, Art. 12^{bis} Abs. 1 lit. d E-K108, Art. 47 Abs. 5 Schengen-RL und Art. 58 Abs. 5 DSGVO: Recht, nicht Pflicht zur Anzeige)
- Amtshilfe: Art. 46 f. VE

Strafrechtliche Sanktionen

- Art. 50 ff. VE
- Art. 10 E-K108
- Art. 57 Schengen-RL
- Art. DSGVO

Allgemeine Punkte

- keine Verwaltungsbussen des EDÖB, sondern strafrechtliche Sanktionen – Entlastung des EDÖB, aber Sanktion gegen die verantwortliche **natürliche** Person!
- mehrheitlich Übertretungen:
  - keine Anstiftung (Art. 24 Abs. 1)
  - Versuch und Gehilfenschaft hier nicht strafbar (105 Abs. 2 StGB)
- Antragsdelikte (ausser bei Pflichten ggü. dem EDÖB)
- Bussen bis CHF 500’000, bei Fahrlässigkeit bis CHF 250’000 (gleich wie bei Art. 47 BankG)
- Bestrafung des Unternehmens bei Bussen bis CHF 100’000 möglich bei «unverhältnismässigem» Ermittlungsaufwand

Übertretungen (Übersicht)

Pflichten gegenüber der **betroffenen Person**:

- Information über direkte oder indirekte Beschaffung
- Information und Anhörung bei AEFE
- Breach notification

Pflichten gegenüber dem EDÖB:

- Mitteilung Ergebnis der DSFA
- Meldung bei Übermittlung auf Grundlage spezifischer Garantien
- Vorlage eigener standardisierter Garantien oder BCR
- Meldung bei Übermittlung auf Grundlage standardisierte Garantien und BCR
- Korrekte Angaben und Mitwirkung bei Untersuchung
- Breach notification
- Einhalten von Verfügungen des EDÖB

Übertretungen (Übersicht)

Pflichten gegenüber **Dritten**:

- Mitteilungen an Datenempfänger (Art. 19 lit. b VE)
- Information des Verantwortlichen durch Auftragsbearbeiter bei unbefugter Bearbeitung

Sonstige Pflichten :

- unerlaubte Übermittlung ins Ausland
- unzulässiger Beizug von Auftragsbearbeitern
- Unterlassung der "notwendigen" Massnahmen zur Datensicherheit
- Unterlassung von DSFA
- Verletzung der Grundsätze von Privacy by design/default
- Verletzung der Dokumentationspflicht

Vergehen (Übersicht

VE:

Art. 52 (Verletzung der beruflichen Schweigepflicht):

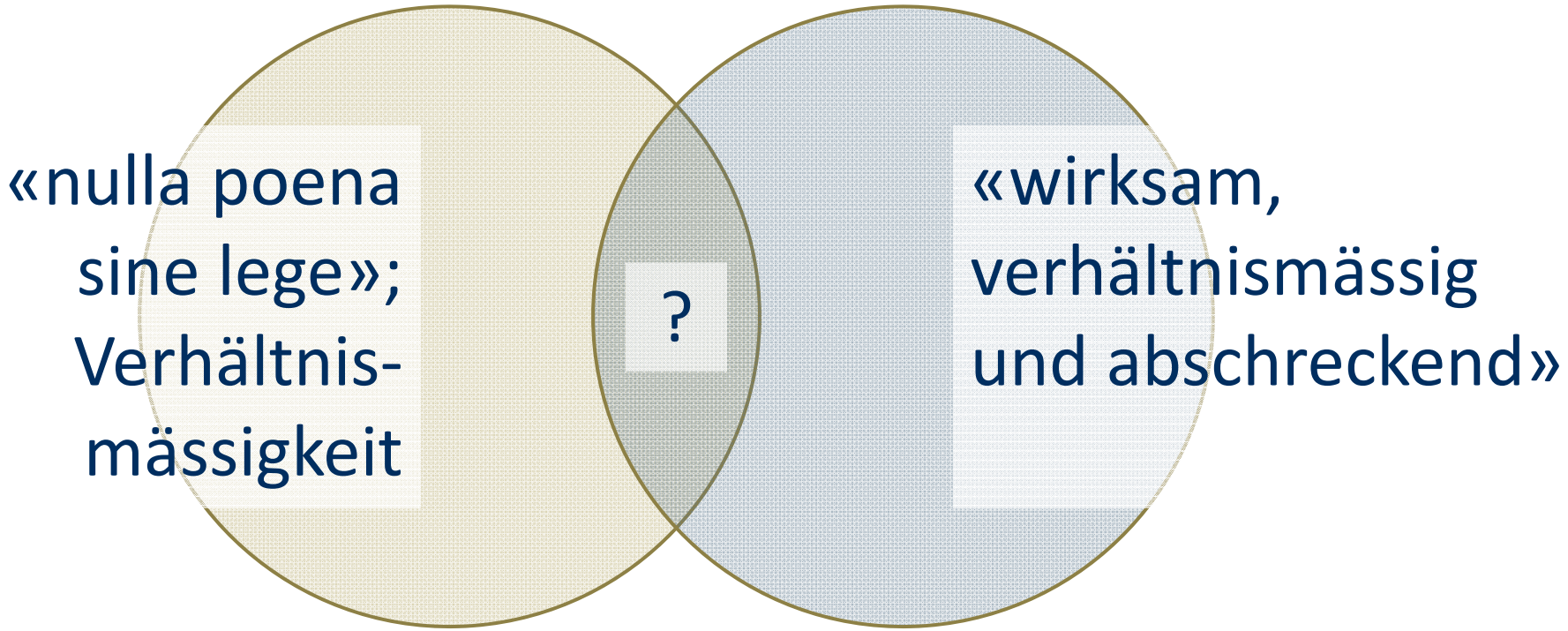
– Anwendung auf bestimmte Bekanntgaben beliebiger Personendaten (anders heute Art. 35 DSG); auf Antrag Freiheitsstrafe bis 3 Jahre oder Geldstrafe

StGB:

– Art. 179^{novies} (Unbefugtes Beschaffen von Personendaten): Anwendung auf alle Personendaten; auf Antrag Freiheitsstrafe bis 3 Jahre oder Geldstrafe

– Art. 179^{decies} (**neu**: Identitätsmissbrauch zwecks Erlangung eines unrechtmässigen Vorteils); auf Antrag Freiheitsstrafe bis 1 Jahr oder Geldstrafe

Handlungsspielraum des Gesetzgebers



Linderungsmöglichkeiten

- Verwaltungsbussen durch den EDÖB
- Überdenken der Strafwürdigkeit einzelner Tatbestände
- klarere Umschreibung der Tatbestände
- Erhöhung der subsidiären Unternehmensstrafbarkeit auf z.B. CHF 250’000
- korrigierende Anwendung durch die Gerichte (analog zu Art. 3 Abs. 1 lit. a UWG?)

Weitere Punkte (Auswahl)

Geltungsbereich (Art. 2 VE)

- keine Anwendung mehr auf juristische Personen
  - sinnvolle Klarstellung bei der Auslandsübermittlung (bereits heute meist keine besonderen Anforderungen)
  - Wegfall des datenschutzrechtlichen Auskunftsanspruchs juristischer Personen
  - Erweiterung des Zugangsrechts nach BGÖ (vgl. Art. 9 und 11 ff. BGÖ; aber weiterhin Geltung von Art. 7 Abs. 3 und – neu – Abs. 3 BGÖ)
- Anpassung beim Anwendungsausschluss für laufende Verfahren (aber sehr weite Formulierung von Art. 2 Abs. 2 lit. c VE)
- keine Anwendungsausschluss mehr für Verfahren vor kantonalen Gerichten (!)
- Aufhebung der Ausnahme für öffentliche Register von Bundesbehörden im Privatverkehr (Art. 2 Abs. 2 lit. d DSG); dafür Art. 6 Abs. 1 lit. f VE (Auslandsübermittlung)

Geltungsbereich (Art. 2 VE)

- Was sind Personendaten?
- Grundsatzfrage: Heisst Personenbezug «Individualisierung» oder «Singularisierung»?

  Erläuterungsbericht zur E-ERK (vgl. auch WP136 der Art.-29-Gruppe):

  17. The notion of 'identifiable' does not only refer to the individual's civil or legal identity as such, but also to what may allow to "individualise" or single out (and thus allow to treat differently) one person from others. This "individualisation" could be done, for instance, by referring to him or her specifically, or to a device or a combination of devices (computer, mobile phone, camera, gaming devices, etc.) on the basis of an identification number, a pseudonym, biometric or genetic data, location data, an IP address, or other

- dennoch: weiterhin Identifikation der Person selbst (durch eindeutigen Namen) erforderlich (vgl. auch ErwG 30 DSGVO)
- im Ergebnis keine Änderung des Begriffs des Personendatums

Legaldefinitionen (Art. 3 VE)

- Erweiterung der «besonders schützenswerten» Daten (lit. c)
  - genetische Daten
  - biometrische Daten: weitere Definition als nach Art. 4 Nr. 14 DSGVO (kein Erfordernis spezieller technischer Verfahren)
- «Profiling» statt Persönlichkeitsprofil:
  - keine ausdrücklichen Vorgaben an das Profiling (anders DSGVO ErwG 71)
  - Präzisierung wäre sinnvoll: Profiling nur bei Personenbezug des Ergebnisses
  - auch nicht-automatisiertes Profiling und Profiling mittels Sachdaten erfasst: entgegen europarechtlichen Vorgaben (Art. 3 Nr. 4 Schengen-RL; vgl. Art. 4 Nr. 4 DSGVO), überschiessend
  - besonders angesichts von Art. 23 Abs. 3 lit. d VE: Rechtfertigung nur mit (ausdrücklicher) Einwilligung oder auch durch Interessen?

Legaldefinitionen (Art. 3 VE)

- «Verantwortlicher: Entscheidung über «Zweck» und «Mittel», aber auch «Umfang» - Abweichung zu den europäischen Vorgaben
- Streichung von «Datensammlung» und «Inhaber»
  - Erweiterung der Pflichten des «Verantwortlichen»
  - Erweiterung der Pflichten auch der Auftragsbearbeiter
  - häufigere «joint controllership»

Bearbeitungsgrundsätze (Art. 4 VE)

- Zweckbindung:
  - «klare» Erkennbarkeit nur redaktionelle Anpassung (Erl Ber 46) – Präzisierung im Text wäre sinnvoll
  - Lockerung erlaubter Bearbeitung durch Kompatibilitätstest? Sinnvoll, auch als Ausgleich für Einschränkungen über Privacy by design/default-Grundsatz
- Klarstellung der Verhältnismässigkeit mit Bezug auf Speicherdauer
- «Richtigkeit» in Art. 4 integriert
- Präzisierungen bei der Einwilligung, aber keine Übernahme der DSGVO
  - kein Kopplungsverbot
  - keine besonderen Anforderungen bei Einwilligung in Textform
  - konkludente Einwilligung bleibt grds. möglich

Bekanntgabe ins Ausland (Art. 5 f. VE)

- Neufassung in Art. 5 (Übermittlung in sichere Staaten und aufgrund von Garantien) und Art. 6 (Freistellung in Ausnahmefällen)
- Kompetenz des Bundesrats zu verbindlichen, abschliessenden Angemessenheitsbeschlüssen
- zu weitgehende Genehmigungs- und v.a. Meldeerfordernisse (letzteres auch für Auftragsbearbeiter)
- (zu) lange Fristen für die Genehmigung standardisierter Garantien (z.B. Code of Conduct) und BCR als Leitbehörde
- keine Änderung bei der Einwilligung (Art. 6 Abs. 1 lit. a VE)

Bekanntgabe ins Ausland (Art. 5 f. VE)

- Übermittlung nun auch für ausländische Verwaltungsverfahren (Art. 6 Abs. 1 lit. c Ziff. 2 VE)
- zu eng bei der Übermittlung im Zusammenhang mit Verträgen (nur Daten des Vertragspartners; anders Art. 38 Abs. 1 lit. b Schengen-RL und Art. 49 Abs. 1 lit. c DSGVO)
- weiterhin fehlend: Übermittlung im eigenen überwiegenden Interesse (vgl. Art. 12 Abs. 4 lit. d E-K108 und 49 Abs. 1 DSGVO)
- übertriebene Meldepflicht: jede Übermittlung zur Vertragsabwicklung oder Durchsetzung von Rechtsansprüchen (Art. 6 Abs. 2 VE; vgl. Art. 12 Abs. 5 E-K108: Information nur auf Antrag)

Auftragsbearbeitung (Art. 7 VE)

- wie bisher grundsätzliche Zulässigkeit und Privilegierung
- unnötige und wenig praktikable Informationspflicht des Verantwortlichen bei der Weitergabe an Auftragsbearbeiter (Art. 13 Abs. 4 VE)
- unnötiges Erfordernis schriftlicher Zustimmung für Unteraufträgen (Art. 7 Abs. 3 VE) – immerhin: auch generisch und nicht unbedingt ausdrücklich
- strafrechtlich sanktionierte Pflicht zur Information des Verantwortlichen bei Data Breach (Art. 17 Abs. 4/50 Abs. 3 lit. b VE)

Empfehlungen der guten Praxis (Art. 8 f. VE)

- Korrektiv zur Unbestimmtheit
- Erarbeitung durch den EDÖB oder durch Branchen mit Genehmigung
- Einfallstor für die Übernahme von europäischen Codes of Conduct?
- Gefahr faktischer Verbindlichkeit trotz Art. 9 Abs. 2 (Strafrisiken)
- Safe Harbor bei Einhaltung… wirklich?

Daten Verstorbener (Art. 12 VE)

- teilweise Übernahme des heutigen Art. 1 Abs. 7 VDSG: Auskunftsrecht über Daten Verstorbener bei ausreichendem Interesse, insb. bei Verwandtschaft
- Erweiterung der Berechtigung durch Fiktion schutzwürdiger Interessen (Art. 12 Abs. 2 VE)
- Auskunftsrecht geht Berufsgeheimnissen vor (Art. 12 Abs. 3 VE)
- «digitaler Tod» (neu):
  - Verbotsrecht des Verstorbenen (zu Lebzeiten…; Art. 12 Abs. 1 lit. a VE)
  - Löschungsrecht jedes einzelnen Erben, unter Vorbehalt eines Verbots und einer Interessenabwägung («digitaler Tod»; Umsetzung eines parlamentarischen Vorstosses, 14.3782)

Daten Verstorbener (Art. 12 VE)

- eigentlich kein datenschutzrechtliches Thema (E-K108, Schengen-RL und DSGVO auf Daten Verstorbener nicht anwendbar)
- vgl. laufende Revision des ZGB (Art. 601a E-ZGB, bit.ly/2kuhpDi: nicht datenschutzrechtlicher Informationsanspruch von Personen mit erbrechtlichen Ansprüchen)

Privacy by design/by default (Art. 18 VE)

- wohl nicht nur programmatische Grundsätze:
  - sanktioniert (Art. 51 Abs. 1 lit. e VE)
  - eigene Übergangsbestimmung (Art. 59 lit. b VE)
  - Planung ggf. durch DSFA
- eigentlich (bereits heute) Teil der Datensicherheit
- für alle Datenbearbeitungen anwendbar (nicht nur durch IT-Systeme)
- Pflicht zu «angemessenen Massnahmen», d.h. zur datenschutzkonformen Gestaltung von Systemen und Abläufen
- Berücksichtigung von Kosten und Nutzen und anderen Faktoren

Privacy by design/by default (Art. 18 VE)

- technisch und organisatorisch – es geht nicht nur um Systemdesign, sondern auch um den Umgang mit Systemen bspw. durch Weisungen und Standardprozesse
- Privacy by design: technische und organisatorische «Massnahmen» (Art. 18 Abs. 1) bzw. «Vorkehrungen» (Art. 59 lit. b) VE, z.B.
  - Datenminimierung (Anonymisierung, Pseudonymisierung)
  - Zugangsbeschränkungen z.B. durch Rollenkonzept
  - Löschkonzept, etc.

Privacy by design/by default (Art. 18 VE)

- für alle Datenbearbeitungen anwendbar (nicht nur durch IT-Systeme)
- Privacy by default (Art. 18 Abs. 2 VE):
  - durch den Nutzer beeinflussbare Voreinstellungen
  - beschränkt auf den Verwendungszweck
- Bedenken:
  - strafrechtliche Sanktionierung des Verhältnismässigkeitsgrundsatzes!
  - Masstab ist der «Zweck» - Eingriff in die Wirtschaftsfreiheit durch Zweckzensur infolge enger Auslegung (vgl. PostFinance-Schlussbericht)?

Dokumentationspflicht (Art. 19 VE)

- allgemeine Pflicht von Verantwortlichen und Auftragsbearbeitern zur Dokumentation ihrer «Bearbeitungen»
- Konkretisierung ggf. in einer Verordnung (vgl. Schengen-RL 24 I; DSGVO 30 I)
- Voraussetzung der Informations- und Meldepflichten; Dokumentation daher der entsprechenden Vorgänge

Dokumentationspflicht (Art. 19 VE)

- Freiheit im Format der Dokumentation
- ggf. mehrere Dokumentationen (bereits für das «Data Mapping»), bspw.
  - «Verarbeitungsverzeichnisse», d.h. Beschreibungen von Applikationen und entsprechenden Datenbearbeitungen – fragen Sie Ihren deutschen DPO
  - Verzeichnis besonderer Vorfälle wie Datenschutzverletzungen, DSFA etc.
  - freiwillig: Verzeichnis der Ländergesellschaften und entsprechenden Zusatzabgaben

Konzept; Rechtfertigung (Art. 23 f. VE)

- zu Recht keine Änderung im Grundsatz der Erlaubnis mit Verbotsvorbehalt statt (wie z.B. nach 6 Abs. 1 DSGVO Verbot mit Erlaubnisvorbehalt)
- willkommene Klarstellung: Rechtfertigung einer Verletzung der Bearbeitungsgrundsätze nicht nur «mit besonderer Zurückhaltung»
- keine grds. Änderung bei den Rechtfertigungsgründen und beim Rechtfertigungsbedarf
- Rechtfertigung des Profilings nur durch ausdrückliche Einwilligung (Art. 23 Abs. 2 lit. d VE): konzeptionell nicht überzeugend (vgl. Art. 28 Abs. 2 ZGB) und aufgrund der zu weiten Definition des Profilings übertrieben

Überwiegende private Interessen (Art. 24 Abs. 2 VE)

- Regelung ähnlich wie im geltenden Recht
- Regelbeispiele:
  - wie bisher Vertragspartnerdaten bei Vertragsabschluss und Abwicklung
  - Wettbewerbszwecke
  - Prüfung der Kreditwürdigkeit: wie bisher unter Ausschluss besonders schützenswerter Daten (durch die Streichung des Begriffs des „Persönlichkeitsprofils" allenfalls aber umfangreichere Datenbearbeitung) und nur für Vertragsanbahnung/-abschluss; neu aber nicht mehr bei Minderjährigen
  - Bearbeitung durch Medien für redaktionelle Inhalte
  - Forschung, Planung und Statistik: leichte Verschärfung
  - Personen des öffentlichen Lebens

Rechtsansprüche (Art. 25 VE)

- keine grundsätzlichen Änderungen
  - negatorische Ansprüche gemäss Art. 28 ff. ZGB
  - reparatorische Ansprüche gemäss Art. 41 ff. und 423 OR
  - Bestreitungsvermerk wie bisher (Art. 15 Abs. 2 DSG)
  - zu Recht keine Ausweitung des Schadensbegriffs (vgl. Art. 82 Abs. 1 DSGVO!)
  - Kodifikation des «Rechts auf Vergessen» (Art. 25 Abs. 1 lit. c VE; ohne inhaltliche Änderungen)
- neu: Bearbeitungsbeschränkung (Art. 25 Abs. 2 Satz 2 VE; gemäss Art. 16 Abs. 3 Schengen-RL)
  - Weiterbearbeitung der Daten nur zur Feststellung der Richtigkeit; i.d.R. durch technische Mittel umzusetzen)
  - bei bestrittener Richtigkeit (anders Art. 18 Abs. 1 DSGVO: weitere Tatbestandsalternativen)

Übergangsrecht

- Inkrafttreten des VE: völlig offen – Umsetzungsfrist für die Schengen-RL endet aber am 1. August 2018 (Erl Ber 27)
- anwendbar auf alle Bearbeitungen (inkl. Speicherung!) mit Inkrafttreten
- einzige Übergangsbestimmung (Art. 59 VE): zwei Jahre Zeit für:
  - Datenschutz-Folgenabschätzung
  - Legacy-Bearbeitungen: Privacy by design/default und Dokumentation

Kontakt

Dr. David Vasella
david.vasella@walderwyss.com
+41 58 658 52 87