Anforderungen und Umsetzung der DSGVO und des revidierten DSG

Datenschutz Compliance Roundtable

Dr. Jürg Schneider; Dr. David Vasella

Zürich, 28. März 2017/6. April 2017 und Bern, 30. März 2017

walderwyss rechtsanwälte

Inhaltsübersicht

I. Einführung in die Thematik

II. Anforderungen

III. Praktische Umsetzung

Einführung in die Thematik

Einführung in die Thematik

Gegenwärtige Gesetzgebung

Schweiz	EU
• Europaratskonvention Nr. 108 (ERK 108) • Datenschutzgesetz vom 19. Juni 1992 (Stand 1. Januar 2014) (SR 235.1) • (Umsetzung des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 über den Schutz von Personendaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen [Schengen-Besitzstand])	• Europaratskonvention Nr. 108 (ERK 108) • RL 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (OJ L 281) • Nationale Gesetzgebung • (Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen [Schengen-Besitzstand])

– Technische Entwicklung
– Mangelnde Transparenz über Verwendung persönlicher Daten
– Verlangen nach Stärkung der Kontrollrechte

Einführung in die Thematik

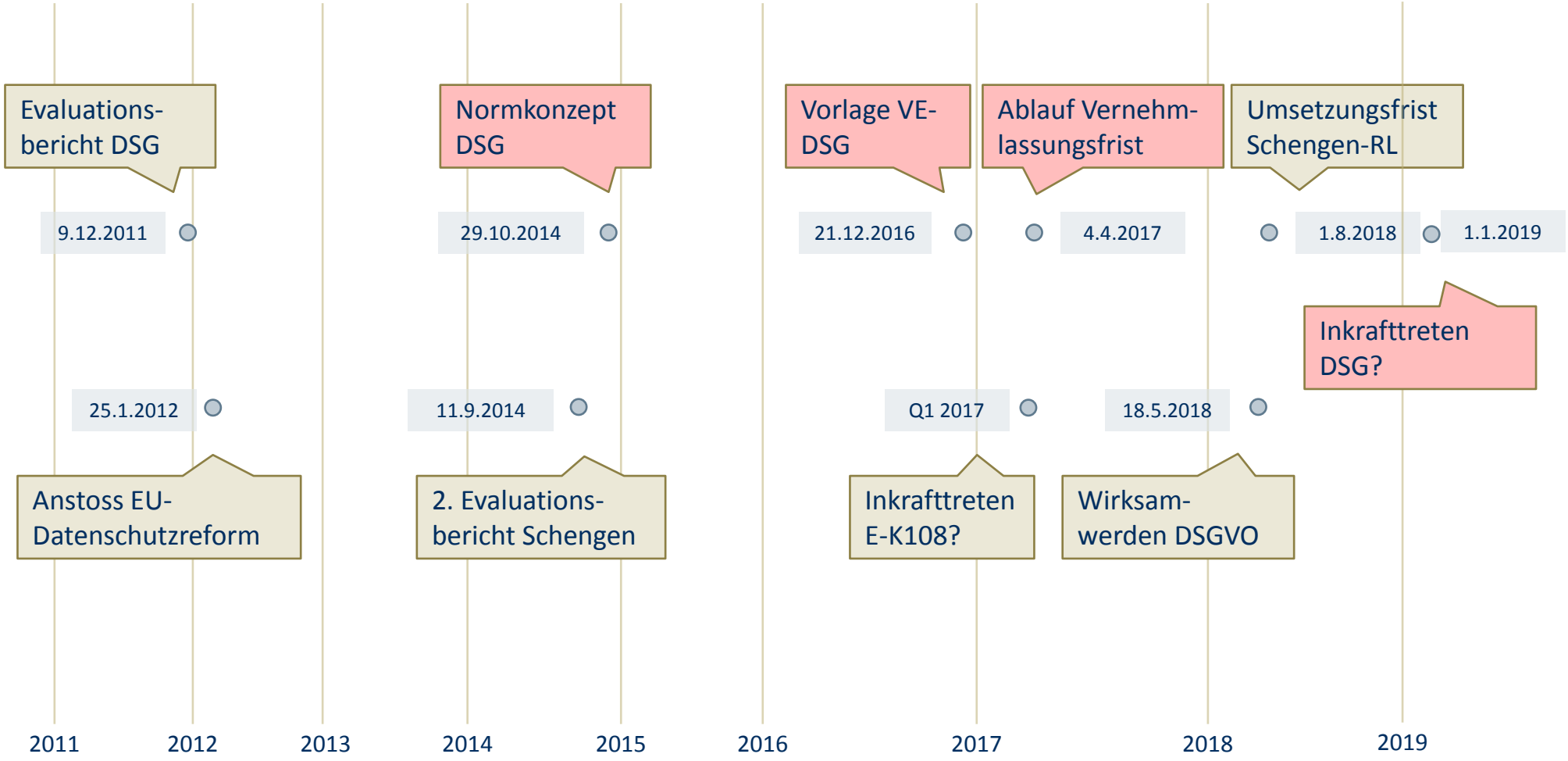
Revision

Schweiz	EU

• Entwurf rev. ERK 108
• VE-DSG vom 21. Dezember 2016
  • Vernehmlassung bis 4. April 2017
  • Inkrafttreten vermutungsweise 2019
• Unter Umständen Anwendbarkeit der DSGVO
• (Umsetzung der Schengen RL 2016/680 vom 1. September 2016)
	• Entwurf rev. ERK 108
	• Datenschutzgrundverordnung vom 27. April 2016 (DSGVO) (OJ L 119)
	  • Ersetzt RL 95/46/EG per 25. Mai 2018
	  • Harmonisiert das EU Datenschutzrecht
	  • Direkt anwendbar
	• (Schengen RL 2016/680 vom 1. September 2016)

Einführung in die Thematik

Chronologie



Anforderungen

Anforderungen

Anwendbarkeit der DSGVO auf Unternehmen in der Schweiz

- Verarbeitung von Personendaten durch Unternehmen in der Schweiz, wenn sie
  - Waren oder Dienstleistungen betroffenen Personen in der EU anbieten oder (Art. 3 Abs. 2 lit. a DSGVO)
  - Das Verhalten betroffener Personen beobachten, soweit das Verhalten in der EU erfolgt (Art. 3 Abs. 2 lit. b DSGVO)

Anforderungen

Anwendbarkeit der DSGVO auf Unternehmen in der Schweiz

- Auftragsdatenbearbeitung von Personendaten eines Unternehmens in der Schweiz durch ein Unternehmen in der EU (?) (Art. 3 Abs. 1 DSGVO)
- Auftragsdatenbearbeitung in der Schweiz für Unternehmen in der EU (Art. 3 Abs. 3 DSGVO)

Anforderungen

Anwendbarkeit der DSGVO auf Unternehmen in der Schweiz

- Einhaltung der DSGVO, doch was gilt?
- Regeln zur Bearbeitung von Personendaten, Betroffenenrechte und Organisationsvorschriften(?)
- Benennung eines EU-Vertreters (Art. 27 DSGVO)
  - Verpflichtung des Verantwortlichen und des Auftragsbearbeiters
  - Niederlassung in der EU
  - Ansprechperson für betroffene Personen und Aufsichtsbehörden
- Benennung eines Datenschutzbeauftragten (Art. 37 ff. DSGVO)
  - Verpflichtung des Verantwortlichen und des Auftragsbearbeiters
    - Kerntätigkeit sind Datenbearbeitungsvorgänge, die umfangreiche regelmässige und systematische Überwachung betroffener Personen erfordern; oder
    - Kerntätigkeit ist umfangreiche Verarbeitung sensitiver Personendaten
  - Qualifizierte und unabhängige Ansprechperson für das Unternehmen, betroffene Personen und die Aufsichtsbehörde

Anforderungen

Wesentliche Neuerungen VE-DSG und DSGVO

- Informations- und Auskunftspflicht
  (Art. 13 f., 20 VE-DSG; Art. 13-15 DSGVO)
- Datenschutzfolgenabschätzung
  (Art. 16 VE-DSG; Art. 35 f. DSGVO)
- Privacy by design / by default (Art. 18 VE-DSG; Art. 25 DSGVO)
- Dokumentationspflicht (Art. 19 lit. a VE-DSG; Art. 30 DSGVO)
- Meldepflichten
- Sanktionen (Art. 50 ff. VE-DSG; Art. 83 f. DSGVO)

Anforderungen

Wesentliche Neuerungen

VE-DSG

- Wegfall (Art. 3 VE-DSG)
  - Anwendung auf juristische Personen
  - «Inhaber»; stattdessen der «Verantwortliche»
  - «Persönlichkeitsprofil»; stattdessen «Profiling»
  - «Datensammlungen» (und Registrierung)
  - Interner Datenschutzbeauftragter
- Änderungen bei der Übermittlung ins Ausland (Art. 5 f. VE-DSG)
- Selbstregulierung durch Codes of Conduct (Art. 8 f. VE-DSG)
- Verfügungsmacht des EDÖB (Art. 37 ff. VE-DSG)

DSGVO

- Höhere Anforderungen an die Wirksamkeit der Einwilligung (Art. 7 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Benennung eines EU-Vertreters (Art. 27 DSGVO)
- Benennung eines Datenschutzbeauftragten (Art. 37 ff. DSGVO)

Informationspflicht

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

Informationspflicht

Pflicht zur aktiven Information

- Stärkung der Informationspflichten durch **aktives** Informieren (Art. 13 f. VE-DSG; Art. 13 f. DSGVO) seitens des Verantwortlichen
- Sowohl bei Beschaffung bei der betroffenen Person als auch bei Dritten
- Erweiterung der **aktiven Informationspflicht** auf die Beschaffung nicht-sensibler Personendaten (Vgl. Art. 14 DSG und Art. 13 VE-DSG)
- Datenschutzrechtliche Transparenz
  - nicht empfangsbedürftige Erklärung
  - «leicht zugänglich» und «verständlich» (Erl Ber 56; vgl. Art. 12 Abs. 1 DSGVO)
  - im Einzelfall oder allgemein vorab, z.B. in AGB oder Datenschutzerklärungen über gut sichtbaren und verständlichen Link (zumindest bei Direkterhebung über die Website)
  - bei der Beschaffung (d.h. der Entgegennahme der Daten) oder Speicherung (Art. 13 Abs. 2 und Art. 13 Abs. 5 VE-DSG); bei der Beschaffung oder spätesten nach einem Monat (Art. 13 Abs. 1 und Art. 14 Abs. 3 lit. a DSGVO)
- Verletzung sanktioniert

Informationspflicht

Pflicht zur aktiven Information

- Katalog mitteilungsbedürftiger Punkte, aber mit Generalklausel (Art. 13 Abs. 2 VE-DSG):
  - Identität und Kontaktdaten des Verantwortlichen (plus Vertreter, DSGVO)
  - bearbeitete Daten oder Kategorien (DSGVO: nur sofern bei Dritten beschafft)
  - Bearbeitungszwecke (plus Rechtsgrundlage, DSGVO)
- zusätzliche Angaben je nach Situation:

VE-DSG	DSGVO
Angabe der Empfänger im In- und Ausland bzw. Kategorien bei Bekanntgabe an Dritte (Art. 13 Abs. 3 VE-DSG) Angabe von Identität und Kontaktdaten der Auftragsbearbeiter (!) (Art. 13 Abs. 4 VE-DSG)	Angabe der Empfänger im In- und Ausland bzw. Kategorien bei Bekanntgabe an Dritte (Art. 13 Abs. 1 lit. f) Bei Übermittlung in ein Drittland Information über das Fehlen eines Angemessenheitsbeschlusses • Verweis auf die rechtfertigende Garantie • Kopie der Garantie

- … und alles, was sonst noch «erforderlich» ist!

Auskunftspflicht

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

Auskunftspflicht

- Pflicht auf Anfrage der betroffenen Person über die Bearbeitung von deren Personendaten zu informieren
- Information über **alle** Entscheidungen, die auf Grund einer Datenbearbeitung gefällt werden, nicht nur automatisierte Einzelfallentscheidungen
  (Art. 20 Abs. 3 VE-DSG)
  - Überschiessende Pflicht: Ergebnis, Zustandekommen und Auswirkungen
  - Sinnvoll nur bei relevanten Eingriffen - Beschränkung auf automatische Einzelfallentscheidung
  - Risiko: Offenbarung von Geschäftsgeheimnissen
  - DSGVO: «nur» Information über automatische Einzelfallentscheidungen und Profiling
    (Art. 15 Abs. 1 lit. h DSGVO)
- Pflicht des Verantwortlichen (subsidiär des Auftragsbearbeiters)
- Verletzung sanktioniert

Datenschutz-Folgenabschätzung

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

Datenschutz-Folgenabschätzung

- In der Sache nichts Neues: Art. 7 DSG/Art. 8 VDSG; Art. VDSG 20 Abs. 2 für Bundesorgane bei automatisierter Bearbeitung
- Geplante Datenbearbeitung mit voraussichtlichem Risiko
  - «erhöht» (Art. 16 Abs. 1 VE-DSG) vs. «hoch» (Art. 35 Abs. 1 DSGVO)
  - VE-DSG: Empfehlungen der guten Praxis; EU: Positiv- und Negativlisten der Aufsichtsbehörden
- Inhalt (VE-DSG): Umschreibung der geplanten Bearbeitung, Risiken für Persönlichkeit, Massnahmen zur Risikoverhinderung (Art. 16 Abs. 2 VE-DSG)
- VE-DSG verpflichtet auch den Auftragsbearbeiter (!), die DSGVO nicht
- Verletzung sanktioniert

Privacy by design und by default

- Art. 18 VE-DSG
- Art. 8bis Abs. 3 E-K108
- (Art. 20 Schengen-RL)
- Art. 25 DSGVO

Privacy by design und by default

- Datenschutzmassnahmen bereits ab Zeitpunkt der Planung der Datenbearbeitung
- Durch Voreinstellungen sicherstellen, dass nur diejenigen Personendaten bearbeitet werden, die für den Verwendungszweck erforderlich sind
  - Bereits durch das Erfordernis der Datensicherheit abgedeckt (Art. 11 VE-DSG)
  - VE-DSG verpflichtet auch den Auftragsbearbeiter (!), die DSGVO nicht
- Verletzung sanktioniert

Dokumentationspflicht

- Art. 19 lit. a VE-DSG
- (Art. 24 Schengen-RL)
- Art. 24 und 30 DSGVO

Dokumentationspflicht

- VE-DSG
- Pflicht trifft
  - **jeden** Verantwortlichen (Art. 19 lit. a VE-DSG)
  - **jeden** Auftragsbearbeiter (Art. 19 lit. a VE-DSG)
- Umfang: unklar

- DSGVO
- Pflicht trifft
  - Verantwortlichen (Art. 30 Abs. 1 DSGVO) und Auftragsbearbeiter (Art. 30 Abs. 2 DSGVO), sofern (Art. 30 Abs. 5 DSGVO):
  - **mindestens 250 Mitarbeiter, oder**
  - **(erhebliches) Risiko** für die betroffenen Personen, **oder**
  - Bearbeitung erfolgt **nicht nur gelegentlich**; **oder**
  - es werden **sensible Personendaten** bearbeitet
- Umfang: Liste

Verletzung sanktioniert

Meldepflichten

Meldepflichten

- Verletzungen des Datenschutzes
  - Meldung **jeder** Verletzung (Art. 17 Abs. 1 VE-DSG) an den EDÖB vs. Meldung der Verletzung der Datensicherheit an Aufsichtsbehörde (Art. 33 Abs. 1 DSGVO)
  - Meldung an die betroffene Person sofern erforderlich (Art. 17 Abs. 2 VE-DSG) vs. Meldung an die betroffene Person bei einem hohen Risiko (Art. 34 Abs. 1 DSGVO)
  - Nemo tenetur
  - Achtung: auch Meldepflicht des Auftragsbearbeiters an den Verantwortlichen (Art. 17 Abs. 4 VE-DSG und Art. 33 Abs. 2 DSGVO)

- Datenschutz-Folgenabschätzung
  - Meldung **jeder** Datenschutz-Folgenabschätzung, inkl. Ergebnis und der geplanter Massnahmen an den EDÖB (Art. 16 Abs. 3 VE-DSG) vs. Konsultation der Aufsichtsbehörde nur bei erheblichen Restrisiken (Art. 36 Abs. 1 DSGVO)
  - Frist für Einwände: EDÖB drei Monate (Art. 16 Abs. 4 VE-DSG) vs. Aufsichtsbehörde 8 Wochen (Art. 36 Abs. 2 DSGVO)

Meldepflichten

- Auslandübermittlung
  - Neu: Entscheid Bundesrat, dass Gesetzgebung einen angemessenen Schutz gewährleistet (d.h. verbindliche Länderliste) (Art. 5 Abs. 2 VE-DSG)
  - Auslandübermittlung und deren Rechtsgrundlage (spezifische sowie standardisierte Garantien, BCR und Ausnahmefälle)
  - Genehmigungspflicht der BCR durch EDÖB (Art. 5 Abs. 3 lit. d Ziff. 1 VE-DSG)
  - Frist für Einwände: EDÖB sechs Monate (Art. 5 Abs. 5 VE-DSG), 30 Tage gemäss geltendem Recht (Art. 6 Abs. 5 VDSG)
- Verletzung sanktioniert
- Swiss Finish: Administrativaufwand für EDÖB, wirtschaftsfeindlich für Unternehmen

Sanktionen

- Art. 50 ff. VE-DSG
- Art. 10 E-K108
- Art. 57 Schengen-RL
- Art. 83 DSGVO

Sanktionen

VE-DSG (Art. 50 VE-DSG)

- **Strafrechtliche** Sanktionen gegen den Einzelnen
- Bussen bis CHF 500’000, bei Fahrlässigkeit bis CHF 250’000
- Subsidiäre Bestrafung von Unternehmen
  - Busse bis CHF 100’000 möglich
  - Unverhältnismässiger Ermittlungsaufwand
  - Schafft falsche Anreize

DSGVO (Art. 83 DSGVO)

- Unternehmenstrafen - **Verwaltung**sbussen
- Bussen bis EUR 20 Mio. oder 4% des weltweiten Jahresumsatzes

«Nulla poena sine lege» und Verhältnismässigkeit

vs.

Wirkung und Abschreckung

Umsetzung

praktische Hinweise

Ausgangslage

Ist:

- Ein Risikobewusstsein fehlt, weil es an Risiken fehlt
- Es fehlt internes Knowhow
- Datenbearbeitungen werden nicht systematisch und nicht an der Quelle erfasst – Datenschutz taucht erst als Randthema der Compliance auf
- Konzerninterne Datenströme sind nicht abgesichert
- Verträge mit Zulieferern und Kunden sind datenschutzrechtlich nicht geprüft

Soll:

- Es bestehen ein Bewusstsein für Datenschutz und ein Gefühl für relevante Risiken
- Die Kommunikation im Bereich Datenschutz ist eingespielt
- Guter Datenschutz ist als Wettbewerbsfaktor etabliert
- Eine Dokumentation existiert und wird à jour gehalten
- Konzerninterne Datenströme sind rechtskonform
- Es gibt etablierte interne Prozesse (Auskunftsbegehren, DSFA etc.)
- Verträge und Datenschutzerklärungen sind geprüft

Schritte zur Datenschutz-Compliance

Typisches Vorgehen

1. Vorbereitung: Bestimmung der Projektorganisation, Budgetierung

2. Mapping: systematische Erfassung der Bearbeitungen und Personendaten

3. Gap-Analyse: Bestimmung der Anforderungen und Abgleich mit dem Ist-Zustand, Priorisierung der Massnahmen

4. Implementierung: Umsetzung der Massnahmen, Schaffung von Strukturen, Gestaltung von Prozessen; Schulungen, Trainings, Überwachung der Einhaltung

vgl. z.B. CNIL, Leitfaden / 6. Schritte (www.datenrecht.ch)

Schritte zur Datenschutz-Compliance

1. Vorbereitung

Ziele:

- interne Beschlussfassung
- Budgetierung und zeitliche Planung der ersten Schritte (Mai 2018 als Zieldatum?)
- Klarheit in der Projektorganisation
- interne Kommunikation, Kick-off

Herausforderungen:

Unklare Zuständigkeiten

- braucht Teamwork und Führung

Unsicherheit des Projektverlaufs:

- Scoping
- Budgetierung und Planung in Etappen,
- Aufteilung in (für sich jeweils verwendbare) Teilprojekte (Mapping, Gap-Analyse etc.)

Widerstand auf Seiten des Business:

- Sponsoring auf VR/GL-Stufe
- gute Kommunikation
- ggf. Training/Schulung zu Beginn
- Aufsetzen auf bestehenden Strukturen und Prozessen

Schritte zur Datenschutz-Compliance

1. Vorbereitung: «Abholen»

Data Inventory – FAQ and Introductions

Frequently Asked Questions (FAQ)

1. Why you are reading this document

This document includes instructions and FAQs about the Data Inventory. Please see below for information about the contents of the Data Inventory and about completing it.

There are two reasons why the Data Inventory is of importance and a strategic initiative on a group level:

- **Data Master File**: We need to have a group-wide, complete picture of all personal data processing activities. That includes data we create ourselves, data we receive or collect from employees, business partners or other third parties and data we transfer within the group or to third parties.

- **Compliance with laws**: The legal framework is changing rapidly. The European Union (EU) and other regions and countries (including Switzerland) are introducing much stricter rules for personally identifiable information, sometimes with massive sanctions. EU law that is set to enter into force in May 2018, for example,

Begleitmassnahmen:

- Schulung von «Privacy Champions»
- Dokumentation, z.B. FAQ, Anleitung, Glossar etc.

Schritte zur Datenschutz-Compliance

2. Datenerfassung («Mapping»)

Ziele:

- **Hauptziel**: Erfassung der existierenden Daten(schutz)landschaft
- **Nebenziele**:
  - Schaffung einer ersten Kommunikationsbasis und der erforderlichen internen Beziehungen
  - Vorbereitung der Dokumentation

Schritte zur Datenschutz-Compliance

2. Datenerfassung («Mapping»)

Herausforderungen:

Widerstand des Business, negative Kompetenzkonflikte:

- braucht frühzeitige Planung, gute Kommunikation
- Opportunitäten zeigen

potentiell grosser Aufwand, Gefahr des Ausuferns:

- klar abgesteckten Scope
- Ausgehen vom Bekanntem (Applikationen, Use Cases)
- Verzicht auf Perfektion
- angepasstes Vorgehen (Pilot; gestuftes Vorgehen; Questionnaire(s); Interviews etc.)

Schritte zur Datenschutz-Compliance

2. Datenerfassung («Mapping»): Bsp. detaillierte Erfassung

Data subjects (affected by data processing)

Indicate or describe the categories of persons affected by data processing (e.g., employee, customer, contact person at supplier, etc.)

Personal Data Processing?

yes

Will personally identifiable information be collected, used, transmitted or otherwise processed through the Application for this Purpose (y/n)?

Indicate or describe the categories of personal data (e.g., employee data, supplier data, customer data, etc.)

select:

Will special categories of data or data about criminal sanctions be processed for this Purpose?

Pseudonymization/anonymization: Will pseudonymized or anonymized data be used for the Purpose? Please specify.

Users and Access Rights

Schritte zur Datenschutz-Compliance

2. Datenerfassung («Mapping»): Bsp. detaillierte Erfassung

Regulatory Requirements for Personal Data

Legislation

Indicate the legislation that applies to the processing for the Purpose (eg., GDPR, local laws)

Registration and Notification Requirements

select:

Register the Application, or a data base used for the Purpose, with the local Data Protection Authority

select:

Notify the Data Protection Authority of the Purpose (or any related processing activities)

select:

Obtain approval from the Data Protection Authority for the Purpose

select:

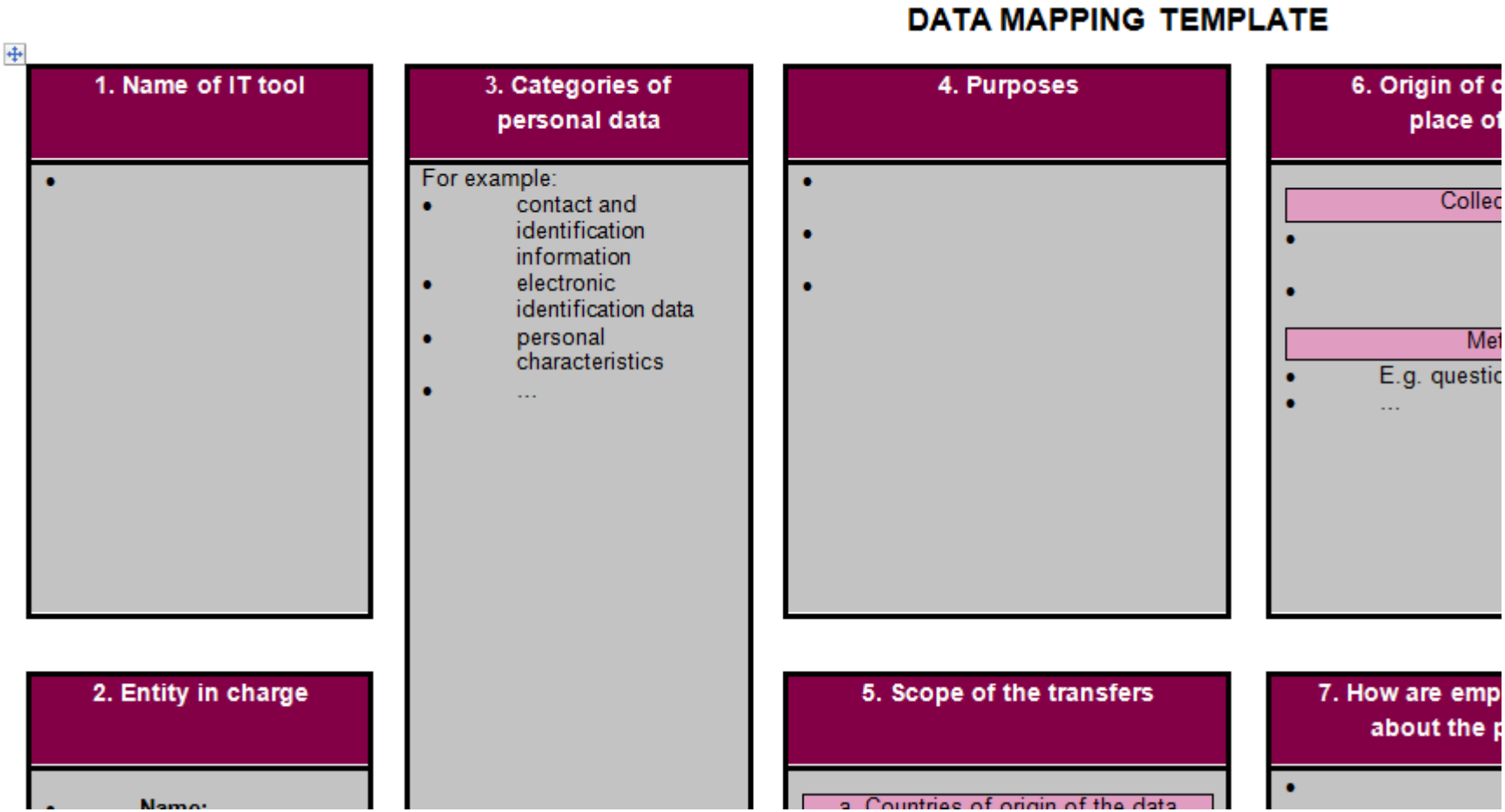
Obligation to appoint a Data Protection Officer

Data Subjects' Rights

Are you able to provide access to the data processed for this purpose, or rectify errors or delete the data, on request, in due course?

Schritte zur Datenschutz-Compliance

2. Datenerfassung («Mapping») Bsp. weniger detaillierte Erfassung



DATA MAPPING TEMPLATE

1. Name of IT tool	3. Categories of personal data	4. Purposes	6. Origin of c… place of…
•	For example: • contact and identification information • electronic identification data • personal characteristics • …	•	Collec… •
		•	•
		•	Met… • E.g. questio… • …

2. Entity in charge	5. Scope of the transfers	7. How are emp… about the p…
• Name:	a. Countries of origin of the data	•

Schritte zur Datenschutz-Compliance

2. Datenerfassung («Mapping»): Muster CNIL

Fiche de registre	ref-ooo					
Description du traitement						
Nom / sigle						
N° / REF	ref-ooo					
Date de création						
Mise à jour						
Acteurs	Nom	Adresse	CP	Ville	Pays	Te
Responsable du traitement						
Délégué à la protection des données						
Représentant						
Responsable(s) conjoint(s)						
Finalité(s) du traitement effectué						
Finalité principale						
Sous-finalité 1						
Sous-finalité 2						
Sous-finalité 3						
Sous-finalité 4						
Sous-finalité 5						
Mesures de sécurité						
Mesures de sécurité techniques						
Mesures de sécurité organisationnelles						

Catégories de données personnelles concernées	Description	Délai d'effacement
Etat civil, identité, données d'identification, images...		
Vie personnelle (habitudes de vie, situation familiale, etc.)		

Schritte zur Datenschutz-Compliance

2. Datenerfassung («Mapping»)

Entity Inventory (Data Protection)

General Company Information			Contact for Data Protection					EU Representative informa		Processing Inventory		Certification		
Full legal (official) company name	Full Company Address	Strategic Business Units	Name	Full Address	Email address and/or phone	Registered DP Officer?	External DP Officer?	Appointed EU Representative?	Representative name or company and address	Existing processing inventory/-ies?	Please describe inventory (if applicable; e.g., scope, currentness, etc.)	Certified or ongoing?	ISO 27001	please d (scope, d company period o etc.)
		select:				select:	select:	select:		select:		select:	select:	
		select:				select:	select:	select:		select:		select:	select:	
		select:				select:	select:	select:		select:		select:	select:	
		select:				select:	select:	select:		select:		select:	select:	
		select:				select:	select:	select:		select:		select:	select:	
		t:				t:	t:	t:		t:		t:	t:	

Erfassungsformular Gesellschaften

Schritte zur Datenschutz-Compliance

3. Gap-Analyse

Ziele:

- Definition der Anforderungen und Abweichungen; «lebendes» Dokument zur Begleitung des Projekts
- Bestimmung der zu planenden Prozesse und erforderlichen Massnahmen

Herausforderungen:

Umfang der Anforderungen:

- risikobasiertes Vorgehen; Konzentration auf das Wesentliche

Unklarheiten bei den Anforderungen:

- Aufbau von Knowhow
- Verfolgen der Entwicklungen (Schweiz/EU; Gesetzgeber/Aufsichtsbehörden)
- Abstimmung mit Branche/vergleichbaren Unternehmen
- später: Regeln der Guten Praxis

Schritte zur Datenschutz-Compliance

3. Gap-Analyse: Entwicklungen verfolgen

EU GDPR | Regulatory Guidance

No°	Date	Authority/Issuer	Title	Short Summary
A.	**Germany**			
1.	May 2016	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) / Federal Data Protection Authority	Broschüre zum Thema EU DSGVO	High level overview on most relevai GDPR
2.	May 2016	Konferenz der unabhängigen Datenschutz-behörden des Bundes und der Länder / Conference of independent data protection authorities of the federal and state govern-ments	Entschließung: EU-Datenschutz-Grundverordnung erfordert zusätzliche Ressourcen für Datenschutz-behörden	Overview on rights of data subjects, es, consistency mechanism, legal re
3.	May 2016	Forum Privatheit und Selbstbestimmtes Leben in der Digitalen Welt	White Paper Datenschutz-Folgenabschätzung	Reasons and requirements for PIA
4.	May 2016	Berufsverbands der Datenschutzbeauftrag-ten Deutschlands (BvD) e.V.	Überblick über die EU DSGVO	Overview in 10 steps: PIA, legal clas troller-data processor relationships
5.	June 2016	Bayrisches Landesamt für Datenschutzauf-sicht (BayLDA) / Bavarian Data Protection Authority	Kurz-Papier: Zertifizierung – Art. 42 DSGVO	Overview on certification requirem GDPR, the applicable framework, cc
6.	June 2016	Bayrisches Landesamt für Datenschutzauf-sicht (BayLDA) / Bavarian Data Protection Authority	Kurz-Papier: Sicherheit der Verarbeitung – Art. 32 DS-GVO	Overview on protection objectives, resilience of processing systems
7.	July 2016	Bayrisches Landesamt für Datenschutzauf-sicht (BayLDA) / Bavarian Data Protection	Kurz-Papier: Videoüberwachung nach der DS-GVO	Overview on CCTV, legal consequer tions, practical recommendations

Schritte zur Datenschutz-Compliance

3. Gap-Analyse – mögliche Gliederung

1. Grundsätze

- Generelle Anforderungen (Bearbeitungsgrundsätze etc.); Einwilligung
- Sanktionen
- Einbindung Dritter

2. Betroffenenrechte

- Datenschutzerklärung, Einwilligung
- Rechtsausübung (Auskunft etc.)

3. Datenübermittlungen

- Auslandsübermittlung

4. Governance

- Dokumentation
- Policies
- Training

5. Datensicherheit

- Datensicherheitsmassnahmen

Schritte zur Datenschutz-Compliance

3. Gap-Analyse

Aktive Informationspflicht

Inhaltliche Anforderungen

Bereich	Anforderung (allgemein)	DSG	VE-DSG	DSGVO	konkrete Anforderungen	praktische Umsetzungsmöglichkeit	Compliance-Anforderungen (Prozesse, Dokumentation etc.)
aktive Information bei direkter Beschaffung	Information über -- Kontaktdaten des Verantwortlichen und seines Vertreters; -- Verarbeitungszweck; -- Kategorien der bearbeiteten Personendaten; -- Kategorien der Empfänger (inkl. Empfänger im Ausland); -- Information über automatisierte Entscheidfindung.	x	x	x	Schaffung von Transparenz mittels Information der betroffenen Personen über die Beschaffung ihrer Personendaten.		Prüfung der Dokumente, in welchen informiert wird (Datenschutzerklärung, AGB's, usw.), und wo notwendig Aufdatierung der bestehenden Dokumente, Webseiten usw. Dokumentation der Information über die Angabe der Datenbearbeitung.
	Entscheidfindung (VE-DSG nur wo keine gesetzliche Grundlage)		x	x			
	Kontaktdaten des Auftragsbearbeiters		x				
	Information über: -- Kontaktdaten des			x			

Schritte zur Datenschutz-Compliance

3. Gap-Analyse

Datenschutz-Folgenabschätzung

Vorprüfung

Bereich	Anforderung (allgemein)	DSG	VE-DSG	DSGVO	konkrete Anforderungen	praktische Umsetzungsmöglichkeit	Compliance-Anforderunge Dokumentation etc.)
	Prüfung, ob eine DSFA erforderlich ist.		x	x	Prüfung muss vor dem Beginn der Datenverarbeitung erfolgen.	Prozessdefinition: Wann muss eine DSFA vorgenommen werden (z.B. Erarbeitung unter Verwendung neuer Technologien und Profiling)? Mitarbeiterschulung.	VE-DSG: 2 Jahre nach Ink Dokumentation der Prüf bei potentiell kritischer Projekten. Zusammenarbeit mit de Datenschutzverantwortl

Durchführung und inhaltliche Anforderungen

Bereich	Anforderung (allgemein)	DSG	VE-DSG	DSGVO	konkrete Anforderungen	praktische Umsetzungsmöglichkeit	Compliance-Anforderunge Dokumentation etc.)
Durchführung	Bei erhöhtem Risiko (VE-DSG) vs. Hohem Risiko (DSGVO).				Der VE-DSG verpflichtet (anders als die DSGVO) nicht nur den Verantwortlichen, sondern auch den Auftragsbearbeiter.		Zusammenarbeit mit de Datenschutzverantwortl Dokumentation.
inhaltliche Anforderungen	-- Wie soll die Datenbearbeitung vor sich gehen - systematische Beschreibung? -- Was sind die Risiken für betroffene Personen (allfällige negative Auswirkungen)? -- Was sind die geplanten Massnahmen zum Schutz der betroffenen Personen und zum Ausgleich der Risiken?		x	x	Verhältnismässigkeitsprüfung (Verarbeitungszweck und Interessen des Verantwortlichen vs. Risiken und Interessen der betroffenen Personen). Erörterung der möglichen Massnahmen zur Minimierung der Datenschutzrisiken.		Zusammenarbeit mit de Datenschutzverantwortl Dokumentation.

Mitteilung an die Aufsichtsbehörde

Bereich	Anforderung (allgemein)	DSG	VE-DSG	DSGVO	konkrete Anforderungen	praktische Umsetzungsmöglichkeit	Compliance-Anforderunge Dokumentation etc.)
EDÖB	Mitteilung der		x		Mitteilung *jeder*	Berücksichtigung der notwendigen Zeit	Mitteilung an den EDÖB

Schritte zur Datenschutz-Compliance

4. Implementierung

Ziele:

- Umsetzung der Anforderungen
- Implementierung der Compliance-Strukturen und -prozesse
- Ausarbeitung der erforderlichen Dokumentation (DSE, Policies, Verträge, ggf. Supplier DD, ggf. Betriebsratsvereinbarungen etc.)

Herausforderungen:

- Trägheit des Ist-Zustands – braucht Trainings und Kontrolle
- zentrale Anlaufstelle für datenschutzrechtliche Fragen definieren
- nicht nur Soll definieren, sondern Prozesse planen
- keine Theorie, sondern praktische Umsetzungsvarianten
- Standardisierungsbedarf und -möglichkeiten ausloten

Schritte zur Datenschutz-Compliance

4. Implementierung: erforderliche Prozesse (Auswahl)

- Verarbeitungsverzeichnis
- Zweckfestlegung und -änderung
- Datensicherheit
- „Privacy by design and by default“ (?)
- Recht auf Datenübertragbarkeit (EU)
- Breaches / notification
- Information bei Datenerhebung
- Auskunftsrecht
- Löschkonzepte
- „Recht auf Vergessenwerden“
- Recht auf Einschränkung der Verarbeitung
- Widerspruchsrecht
- Recht auf Berichtigung
- Datenschutz-Folgenabschätzung
- Auftragsverarbeitung
- Profiling
- Big Data-Analyse
- Übermittlung von Daten in Drittstaaten

Schritte zur Datenschutz-Compliance

Take-Aways

Projekt ernstnehmen:

- Ressourcen einplanen
- Business einbinden
- Datenschutzkultur verankern

mit Augenmass vorgehen:

- risikobasierter Ansatz
- Jedes Unternehmen ist gefordert, aber: one size does not fit all

keine Panik:

- Compliance-Projekte befinden sich generell noch im Anfangsstadium
- auch Aufsichtsbehörden brauchen Zeit
- vieles wird sich (erst) in den nächsten Monaten und Jahren klären

walderwyss rechtsanwälte

Kontakt

Dr. iur. Jürg Schneider
Seefeldstrasse 123
Postfach 1236
8034 Zürich

juerg.schneider@walderwyss.com
+41 58 658 55 71

Dr. iur. David Vasella
Seefeldstrasse 123
Postfach 1236
8034 Zürich

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

Weitere Informationen:
www.dataprotection.ch