DSGVO: Vordringliche Umsetzungsmassnahmen

LITS: Lucerne LAW & IT Summit
1. Februar 2018

David Vasella

walderwyss rechtsanwälte

Europa:

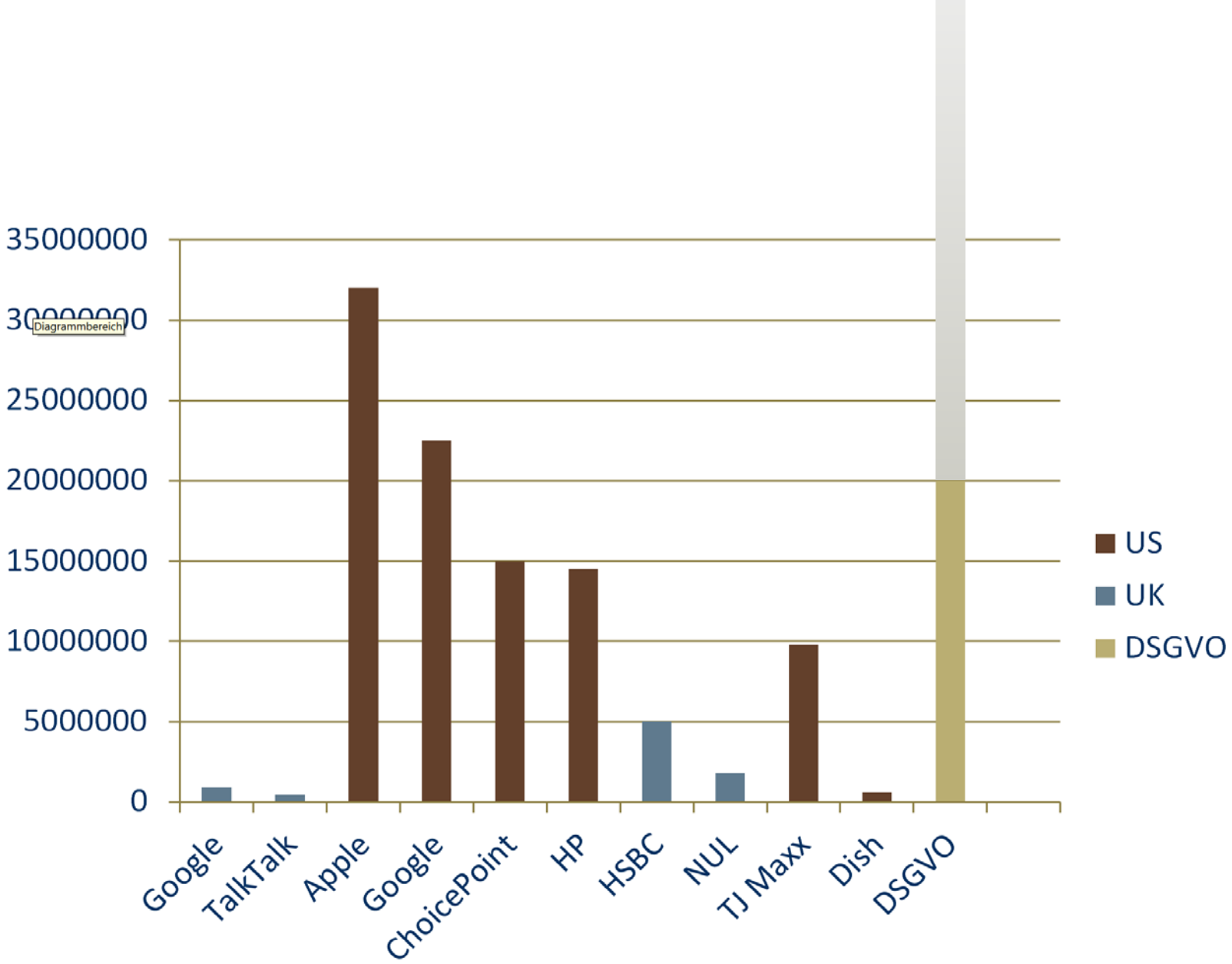
- DSGVO: 25. Mai 2018
- e-Privacy-Verordnung:
  - Konkretisierungen und Abweichungen von der DSGVO (als lex specialis), z.B. zur Rechtmässigkeit oder Speicherbegrenzung
  - genauer Inhalt und Zeitpunkt noch unklar

Schweiz:

- rev. DSG:
  - genauer Inhalt noch offen, aber wohl nahe bei der DSGVO
  - Zeitpunkt nicht klar; Inkrafttreten nicht vor 2019

DSGVO: Kurzübersicht

- «einheitliche» Neuregelung des Datenschutzes in der EU: Verordnung mit Öffnungs-klauseln
- Anwendungsbereich: Unternehmen in der EU/im EWR, oft aber auch ausserhalb
- Ablauf der Übergangsfrist: 25. Mai 2018 (Art. 99(2) DSGVO)
- keine konzeptionelle Neufassung, aber:
  - Fokus auf Verantwortung des Unternehmens («Accountability»)
  - mehr, detailliertere und schärfere Regelungen
  - schärfere Sanktionen (4%/EUR 20 Mio.)



Datenquelle: IAPP

Geltung der DSGVO

- Verarbeitung durch eine **Niederlassung** in der EU
  - Tochter in D
  - ZN in F
- Ausrichtung auf den **(Endkunden-)Markt** in der EU
  - B2C-SaaS-Angebot in DACH
  - Onlineshop für antiquarische Bücher (auch) in D
- **Verhaltensbeobachtung** in der EU
  - Online-Tracking (bei Personenbezug)
  - Cloud-Freemium-Angebot
- nicht: grenzüberschreitendes Outsourcing
- … Anwendung jeweils auf **Verarbeitungen**, nicht Unternehmen

EU: inkl. EWR

Hauptanforderungen

- **Dokumentation** (Art. 30 DSGVO)
- **Grundsätze**: v.a. Rechtmässigkeit, Zweckbindung, Minimierung, Richtigkeit (Art. 5 ff. DSGVO)
- **Information** der betroffenen Personen (Art. 12 ff. DSGVO)
- Wahrung der **Betroffenenrechte** (Art. 12 ff., 16 ff., 21 f. DSGVO)
- Auswahl und Einbindung von **Auftragsverarbeitern** (Art. 28 DSGVO)
- **Datensicherheit** und Folgenabschätzung (Art. 24, 32 ff. DSGVO)
- Meldung von **Verletzungen** (Art. 33 f. DSGVO)
- **Organisation** (Vertreter; DPO) (Art. 27, 37 ff. DSGVO)

Umsetzung in Arbeitspakete

Was heisst dänn das genau? ⟶ Übersicht über die Anforderungen gewinnen

Was mached mer dänn überhaupt hüt so? ⟶ Dokumentation

Tärfed mer das no? ⟶ Anforderungs- und Gap-Analyse

Was müend mer dänn konkret mache?

⟶ Ausarbeitung von Richtlinien, Prozessdefinitionen; Datenschutzerklärung(en), Einwilligungen, Korrespondenz

⟶ Verträge für/mit Auftragsverarbeitern, Regelung der Auslandsübermittlung (intern und intern)

Aber wer cha das mache? ⟶ Projektplanung und Datenschutzorganisation

Und nochär isch äs verbi? ⟶ nein! Prozessabläufe, Schulung etc.

Mögliche Prioritäten

1. ggf. Abklärungen und Grundentscheidungen
2. **Mapping** und (selektive) **Gap-Analyse**
   1) Endkundendaten
   2) Mitarbeiterdaten und heiklere Verarbeitungen (z.B. CMS)
   3) alles andere
3. **Aussenauftritt**
   - Datenschutzerklärungen und AGB
   - Auskunftsprozess
   - Korrespondenz
4. **Richtlinien** und Prozessbeschreibungen
5. weitere **Dokumentation**:
   - Verträge mit Auftragsverarbeitern
   - ggf. sonstige Verträge
6. **konzerninterner Datenverkehr**
   - Auslandsübermittlung
   - Shared Services
7. **Schulungsmaterial**

Risikobasierter Ansatz

Unternehmenssicht:

- Risiken für das Unternehmen (Reputation, Sanktionen)
- Sichtbarkeit gegen aussen
- Umsetzungsaufwand («quick wins»)

Sicht des Datenschutzes:

- Risiken für die betroffenen Personen
- grösste Lücken in der Compliance
- Zeitbedarf und Aufwand zur Umsetzung (Prozess-anpassungen, Anpassungen der IT)

Risikobasierter Ansatz beim Mapping

- 1. Stufe: generelles, einfaches Mapping

  Minimum nach Art. 30 DSGVO

  + Compliance-Fragen

  + Risikofragen

- 2. Stufe: risikobasiert selektives, genaueres Mapping («Deep Dive»)

- 3. Stufe: Compliance Assessment (Gap-Analyse) auf Basis Deep Dive

- 4. Stufe: Datenschutz-Folgenabschätzung

  - bei «hohen Risiken» (Risikokumulation)
  - für bestehende Verarbeitungen i.d.R. optional, aber ggf. sinnvoll

«Einfaches» Mapping

Q8	**Source (origin) of the data** Please indicate where the data specified in Q5 is collected or received from.	☐ Employees ☐ Applicants ☐ Superiors of employees ☐ Website ☐ Mobile App ☐ Data broker	☐ Persons making a report/complaint ☐ Investigators, authorities ☐ Shareholders and/or their banks ☐ The following group company/-ies: ☐ The following master data system: ☐ The following public source: ☐ The following third party/-ies:
Q9	**Storage time** Please indicate the duration of storage of the data specified in Q5 or the criteria that decide on the duration of the storage (ignore backup and archival copies for this question).	☐ For the following duration: ☐ In accordance with the following logic/criteria: ☐ In accordance with the following retention/deletion/storage policy: ☐ No storage time defined	
Q10	**Data recipients** Is personal data given to – or make accessible for – any person within the group or outside of the group? Please indicate the names of the recipients, if possible, and the reason for the transfer/disclosure.	☐ The following *departments*, for the following reasons: ☐ The following *group companies* as other controllers, for the following reasons: ☐ The following *group-internal service providers*, for the following reasons: ☐ The following *third-party service providers,* for the following reasons: ☐ The following third parties, for the following reasons, for the following reasons: ☐ The following *authorities*, for the following reasons, for the following reasons: ☐ The *public*, for the following reasons:	

«Deep Dive»

		[Processor]	[data, Task/role]		[Contract]
Q24	**Data processors (2)** Please describe how the processor(s) indicated above have been vetted or selected (process and main criteria).	**Processor**	**Vetting/selection**		
		[Processor]	[vetting/selection]		
		[Processor]	[vetting/selection]		
		[Processor]	[vetting/selection]		
		[Processor]	[vetting/selection]		
Q25	**Other data recipients** Is personal data given to – or make accessible for – any person within the group or outside of the group, other than to the data processors indicated in Q19 above? What is the reason for such a transfer/disclosure?	**Recipient**	**Data received and task or role**	**Purpose of access**	**Contra**
		[Recipient]	[data, Task/role]	[purpose]	[Contra
		[Recipient]	[data, Task/role]	[purpose]	[Contra
		[Recipient]	[data, Task/role]	[purpose]	[Contra
Q26	**Data transfers abroad** Is personal data transferred to a recipient abroad, or can personal data be accessed by anyone abroad, other than as indicated above in Q18 and Q19? If yes: Who are the recipients or the person having access, where are they located (indicate all countries), and what is the purpose of the transfer?	**Recipient/person with access**	**Country**	**Which data?**	**Safegu**
		[Recipient/access]	[country]	[data]	[safegu
		[Recipient/access]	[country]	[data]	[safegu
		[Recipient/access]	[country]	[data]	[safegu
Security					

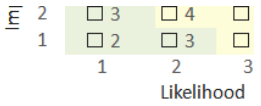
Compliance Assessment

[Recommendation/remedy:] [1-3]

	Purpose and purpose limitation	
Q27	**Purpose definition** (art. 5(1)(b) GDPR) Is the purpose/are the purposes of the Activity clearly defined before/at the time of collection and recorded in a data inventory?	☐ Yes ☐ Unclear ☐ No [please explain]
Q28	**Purpose limitation** (art. 5(1)(b) GDPR) Is data processed only as reasonably required for the purpose(s) indicated to the subjects (original purpose)? Cf. Q31 et seq.	☐ Yes ☐ Unclear ☐ No [please explain]
Q29	**Purpose compatibility** (art. 5(1)(b) GDPR) If the answer to Q28 is "no" or "unclear": Is the purpose/are the purposes compatible with the original purpose? Make an assessment based on the criteria set out in art. 6(4) GDPR.	☐ Yes ☐ Unclear ☐ No [please explain]
Q30	**Information about new purpose(s)** (art. 13(3) GDPR; WP 250) When data is processed for new, compatible purposes and in case of other changes, the subjects must be notified in accordance with WP 250.	Is there an option to inform (interface with) data subjects if their data is processed for new purp given earlier changes? ☐ Yes [please explain and/or include reference] ☐ No
R3	**Compliance assessment and recommendation**	Overall assessment of the level of compliance with the requirements under this Section: ☐ 0% not compliant ☐ 25% Need for substantial improvements ☐ 50% Improvements recommended ☐ 75% Improvements possible ☐ 100% Full compliance **Recommendation/remedy:** Priority (1-3):

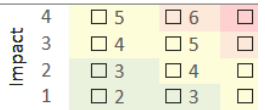
Datenschutz-Folgenabschätzung

	Assess residual risk considering the mitigating measures confirmed for implementation:	implemented]



Storage limitation: Risk of failure to erase or anonymize persona data in due course

Q27	**Threats** Please describe scenarios where personal data might be kept for longer than necessary for the purpose of the Activity or to comply with applicable laws.	[...]
Q28	**Potential harm** Please describe potential harm for data subjects in the event that a threat described above materializes:	☐ Physical harm [describe possible impact] ☐ Loss of liberty or freedom [describe possible impact] ☐ Financial loss [describe possible impact] ☐ Other tangible loss [describe possible impact] ☐ Intangible distress [describe possible impact] ☐ Embarrassment, anxiety [describe possible impact] ☐ Other intangible loss [describe possible impact]
Q29	**Risk assessment** Assess the risk for the data subjects. The risk is the	[Make an assessment of the risk for data subjects in relation with the use of personal data for incompatible purposes]



Datenschutz-Erklärungen

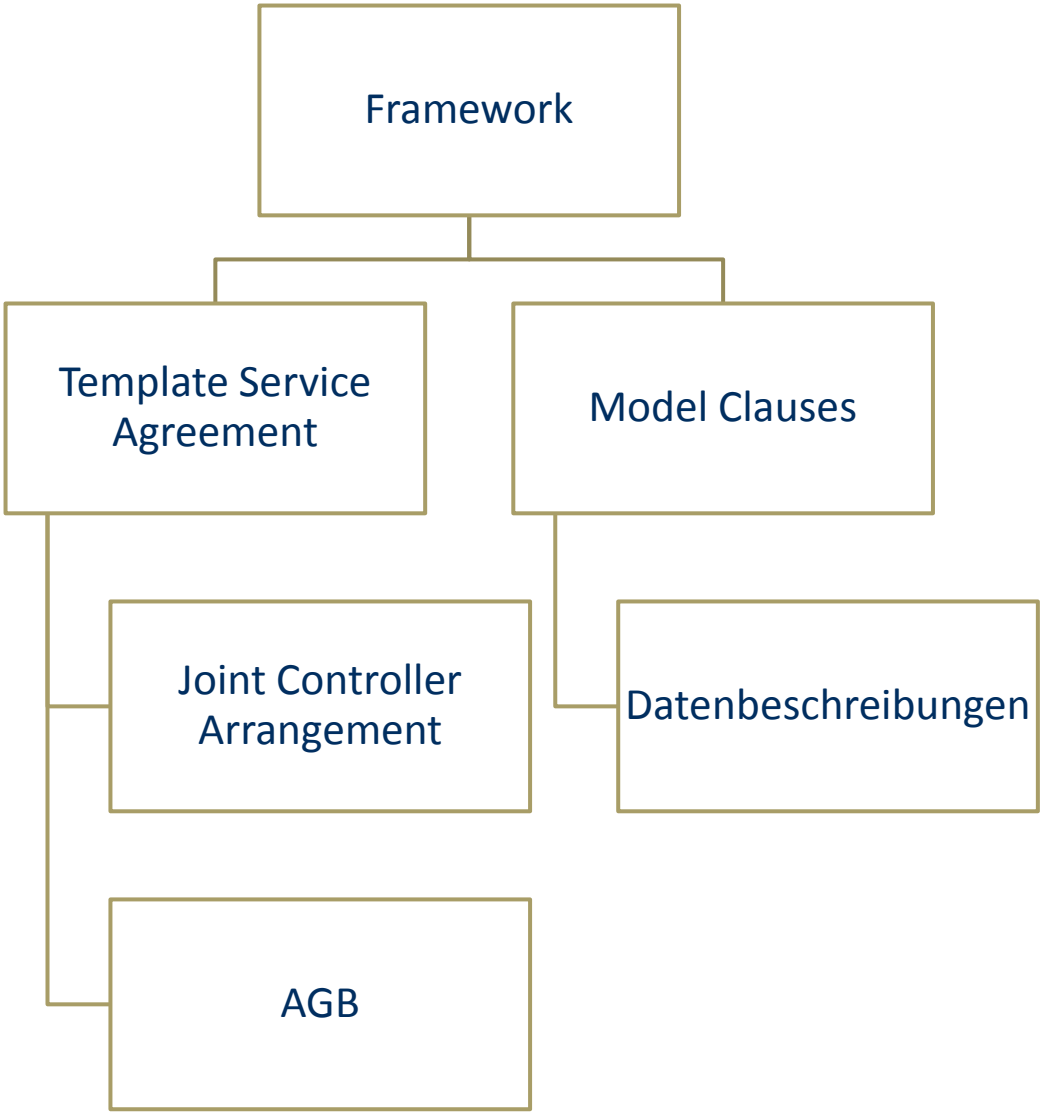
- Wer: Endkunden; Mitarbeiter; ggf. weitere
- Gegenstand:
  - gemäss Art. 13 DSGVO, u.a. Verantwortlicher und Rechtsgrundlage
  - Zusatzangaben gemäss WP260: Konsequenzen der Verarbeitung, existierende DSFA
- Sprache: sehr konkret; keine bloss in Zukunft möglichen Verarbeitungszwecke
- One size will not fit all!
- Medienbruch: nur im Notfall akzeptabel
- Angaben auf Websites: genügend nur bei Hinweis auf die Website (anders als in der Schweiz [?])
- empfohlen werden ebenfalls «layered»-Erklärungen
- in Apps: max. 2 Schritte entfernt (?)

Richtlinien und Prozessdefinitionen

- Datenschutzrichtlinie: mehr oder weniger zwingend
- weitere Richtlinien, z.B.:
  - Auskunft
  - Berichtigung
  - Löschung, Einschränkung
  - ggf. Datenübertragbarkeit
  - Profiling, automatisierte Einzelentscheidung
  - ggf. Privacy by Design, Privacy by Default
  - Meldung von Verletzungen
  - Datenschutzfolgenabschätzung
  - EU-Vertreter
  - Benennung von Datenschutzbeauftragten
  - Kontakt mit Behörden, Bestimmung One-Stop-Shop
- nicht zu detailliert

Konzerninterner Datenverkehr

Mögliches Vorgehen (mit Restrisiken):



Datenschutz…

…awareness

…akzeptanz

…verständnis

…kultur

- Awareness schaffen
- Datenmapping beginnen
- Organisation planen
- risikobasierte Gap-Analyse durchführen
- parallele Arbeit an Kerndokumentation

- vorerst entscheidend: ernsthafte (und richtig dokumentierte) Bemühungen mit Risikofokus
- «Rabbit Holes» und Perfektionismus vermeiden

Vielen Dank!

RA Dr. David Vasella
Walder Wyss AG

+41 58 658 52 87
+41 79 417 23 22
david.vasella@walderwyss.com