
DSGVO: Vordringliche Umsetzungsmassnahmen

LITS: Lucerne LAW & IT Summit
1. Februar 2018

David Vasella

walderwyss rechtsanwälte

Europa:

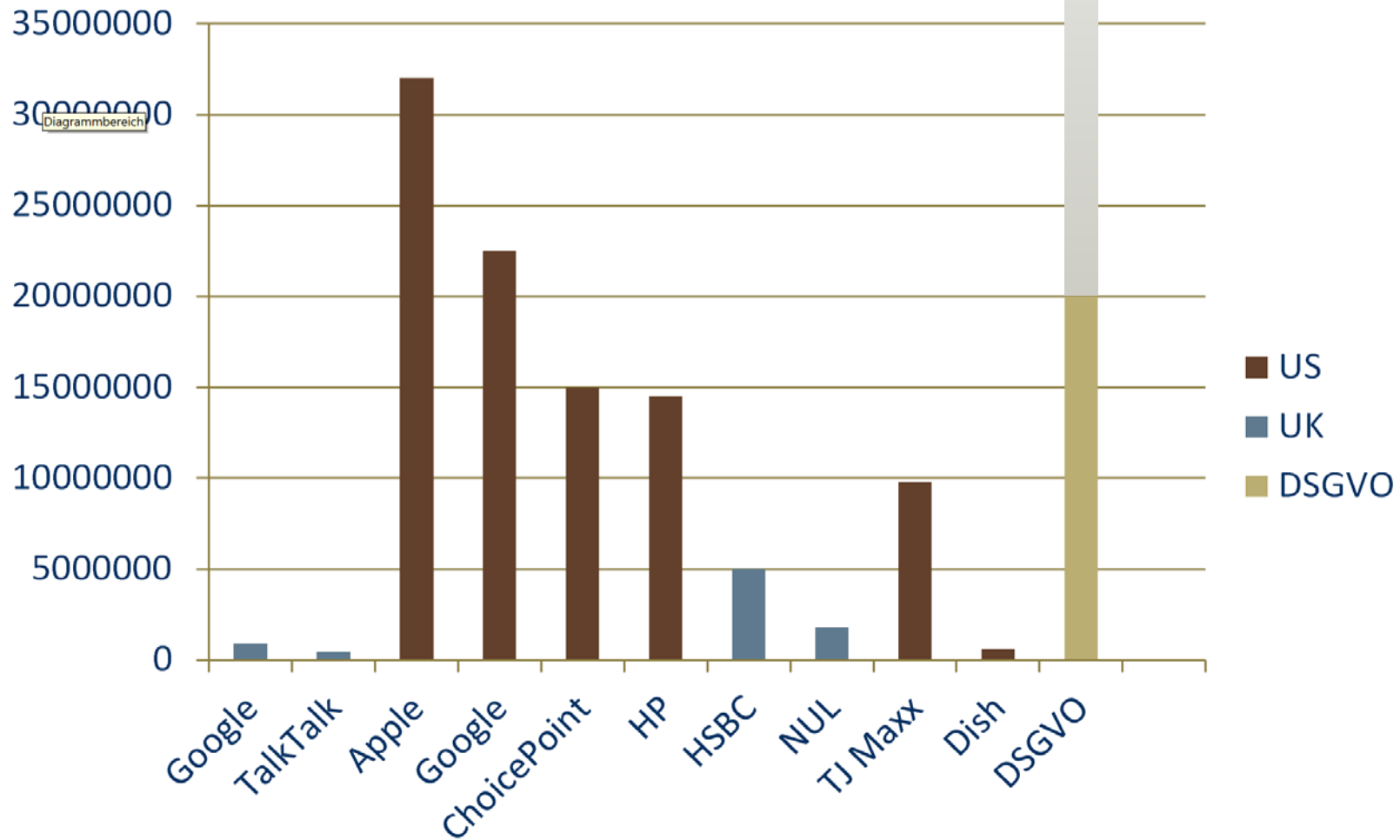
- DSGVO: 25. Mai 2018
- e-Privacy-Verordnung:
 - Konkretisierungen und Abweichungen von der DSGVO (als *lex specialis*), z.B. zur Rechtmässigkeit oder Speicherbegrenzung
 - genauer Inhalt und Zeitpunkt noch unklar

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 Öffnungsklauseln
- 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 dann das genau? → Übersicht über die Anforderungen gewinnen

Was mached mer dann überhaupt hüt so? → Dokumentation

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

Was müend mer dann 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 (Prozessanpassungen, 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.

- | | |
|---|--|
| <input type="checkbox"/> Employees | <input type="checkbox"/> Persons making a report/complaint |
| <input type="checkbox"/> Applicants | <input type="checkbox"/> Investigators, authorities |
| <input type="checkbox"/> Superiors of employees | <input type="checkbox"/> Shareholders and/or their banks |
| <input type="checkbox"/> Website | <input type="checkbox"/> The following group company/-ies: |
| <input type="checkbox"/> Mobile App | <input type="checkbox"/> The following master data system: |
| <input type="checkbox"/> Data broker | <input type="checkbox"/> The following public source: |
| | <input type="checkbox"/> 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).

- | |
|--|
| <input type="checkbox"/> For the following duration: |
| <input type="checkbox"/> In accordance with the following logic/criteria: |
| <input type="checkbox"/> In accordance with the following retention/deletion/storage policy: |
| <input type="checkbox"/> 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.

- | |
|---|
| <input type="checkbox"/> The following <i>departments</i> , for the following reasons: |
| <input type="checkbox"/> The following <i>group companies</i> as other controllers, for the following reasons: |
| <input type="checkbox"/> The following <i>group-internal service providers</i> , for the following reasons: |
| <input type="checkbox"/> The following <i>third-party service providers</i> , for the following reasons: |
| <input type="checkbox"/> The following third parties, for the following reasons, for the following reasons: |
| <input type="checkbox"/> The following <i>authorities</i> , for the following reasons, for the following reasons: |
| <input type="checkbox"/> The <i>public</i> 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 [Processor] [Processor] [Processor] [Processor]	Vetting/selection [vetting/selection] [vetting/selection] [vetting/selection] [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 [Recipient] [Recipient] [Recipient]	Data received and task or role [data, Task/role] [data, Task/role] [data, Task/role]	Purpose of access [purpose] [purpose] [purpose]
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 [Recipient/access] [Recipient/access] [Recipient/access]	Country [country] [country] [country]	Which data? [data] [data] [data]

Security

Compliance Assessment

[RECOMMENDATION/REMEDY]

[1-3]

Purpose and purpose limitation

Q27 **Purpose definition** (art. 5(1)(b) GDPR) Yes
 Unclear
 No
[\[please explain\]](#)

Q28 **Purpose limitation** (art. 5(1)(b) GDPR) Yes
 Unclear
 No
[\[please explain\]](#)

Q29 **Purpose compatibility** (art. 5(1)(b) GDPR) Yes
 Unclear
 No
[\[please explain\]](#)

Q30 **Information about new purpose(s)** (art. 13(3) GDPR; WP 250) 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% 25% 50% 75% 100%
not compliant Need for substantial improvements Improvements recommended Improvements possible Full compliance

Recommendation/remedy: **Priority (1-3):**

Datenschutz-Folgenabschätzung

implementiert

Assess residual risk considering the mitigating measures confirmed for implementation:

Im	2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/>
	1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/>
		1	2	3
		Likelihood		

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]

Impact	4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/>
	3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/>
	2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/>
	1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/>

[Document classification, for example internal / confidential]

Page 8 of :

Datenschutz-Erklärungen

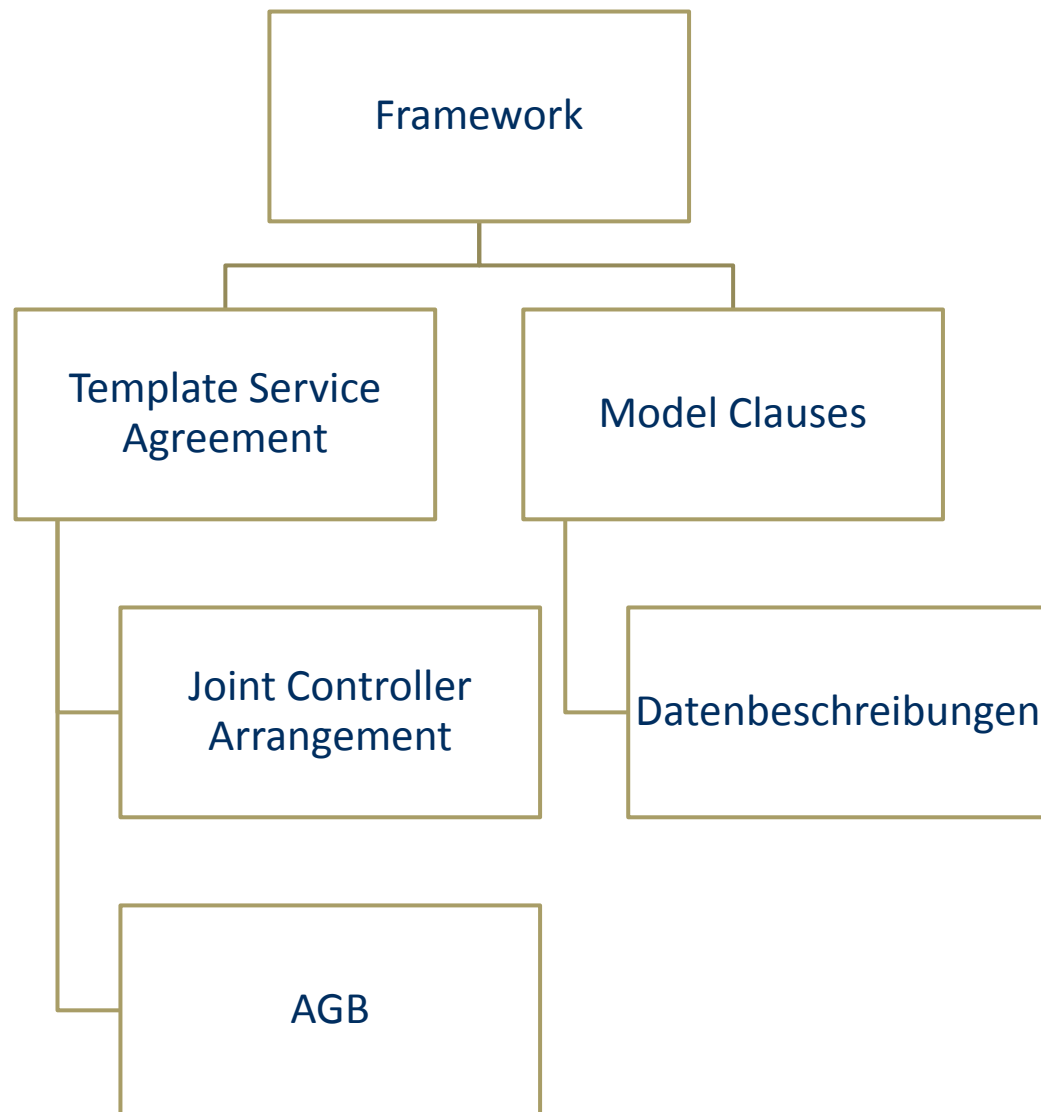
- Wer: Endkunden; Mitarbeiter; ggf. weitere
- Gegenstand:
 - gemäss Art. 13 DSGVO, u.a. Verantwortlicher und Rechtsgrundlage
 - Zusatzangaben gemäss WP260: Konsequenzen der Verarbeitung, existierende DSFA
- Sprache: sehr konkret; keine bloss in Zukunft möglichen Verarbeitungszwecke
- One size will not 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):



Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung;

- b) im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt;

Datenschutz...

(36) Die Hauptniederlassung eines Verantwortlichen sollte der Ort seiner Hauptverwaltung in der Union sein, es sei denn, dass Entscheidungen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten in einer anderen Niederlassung des Verantwortlichen in der Union getroffen werden; in diesem Fall sollte die letztgenannte als Hauptniederlassung gelten. Zur Bestimmung der Hauptniederlassung eines Verantwortlichen in der Union sollten objektive Kriterien herangezogen werden; ein Kriterium sollte dabei die effektive und tatsächliche Ausübung von Managementtätigkeiten durch eine feste Einrichtung sein, in deren Rahmen die Grundsatzentscheidungen zur Festlegung der Zwecke und Mittel der Verarbeitung getroffen werden. Dabei sollte nicht ausschlaggebend sein, ob die Verarbeitung der personenbezogenen Daten tatsächlich an diesem Ort ausgeführt wird. Das Vorhandensein und die Verwendung technischer Mittel und Verfahren zur Verarbeitung personenbezogener Daten oder Verarbeitungstätigkeiten begründen an sich noch keine Hauptniederlassung und sind daher kein ausschlaggebender Faktor für das Bestehen einer Hauptniederlassung. Die Hauptniederlassung des Auftragsverarbeiters sollte der Ort sein, an dem der Auftragsverarbeiter seine Hauptverwaltung in der Union hat, oder — wenn er keine Hauptverwaltung in der Union hat — der Ort, an dem die wesentlichen Verarbeitungstätigkeiten in der Union stattfinden. Sind sowohl der Verantwortliche als auch der Auf-

...awareness

...akzeptanz

...verständnis

...kultur

nen Verfahren der Zusammenarbeit teilnehmen. Auf jeden Fall sollten die Aufsichtsbehörden des Mitgliedstaats oder der Mitgliedstaaten, in denen der Auftragsverarbeiter eine oder mehrere Niederlassungen hat, die betroffene Aufsichtsbehörden betrachtet werden, wenn sich der Bescheid nur auf den Verantwortlichen bezieht. Wird die Verarbeitung der Daten durch eine Unternehmensgruppe vorgenommen, so sollte die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten, es sei denn, die Zwecke und Mittel der Verarbeitung werden von einem anderen Unternehmen festgelegt.

17. „Vertreter“ eine in der Union niedergelassene natürliche Person, die im Namen des Verantwortlichen oder Auftragsverarbeiters bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung übertragenen Aufgaben vertritt;

18. „Unternehmen“ eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, die in einem Mitgliedstaat registriert ist, oder eine natürliche Person, die in einem Mitgliedstaat eine wirtschaftliche Tätigkeit nachgehen;

19. „Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;

(37) Eine Unternehmensgruppe sollte aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen bestehen, wobei das herrschende Unternehmen dasjenige sein sollte, das zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann. Ein Unternehmen, das die Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, sollte zusammen mit diesen als eine „Unternehmensgruppe“ betrachtet werden.

20. „verbindliche interne Datenschutzvorschriften“ Maßnahmen zur Verarbeitung personenbezogener Daten, zu deren Einhaltung sich ein Unternehmen im Gebiet eines Mitgliedstaats niedergelassener Verantwortlicher verpflichtet.

- 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

walderwyss rechtsanwälte