Auswirkungen der Datenschutz-Revisionen auf Treuhänder

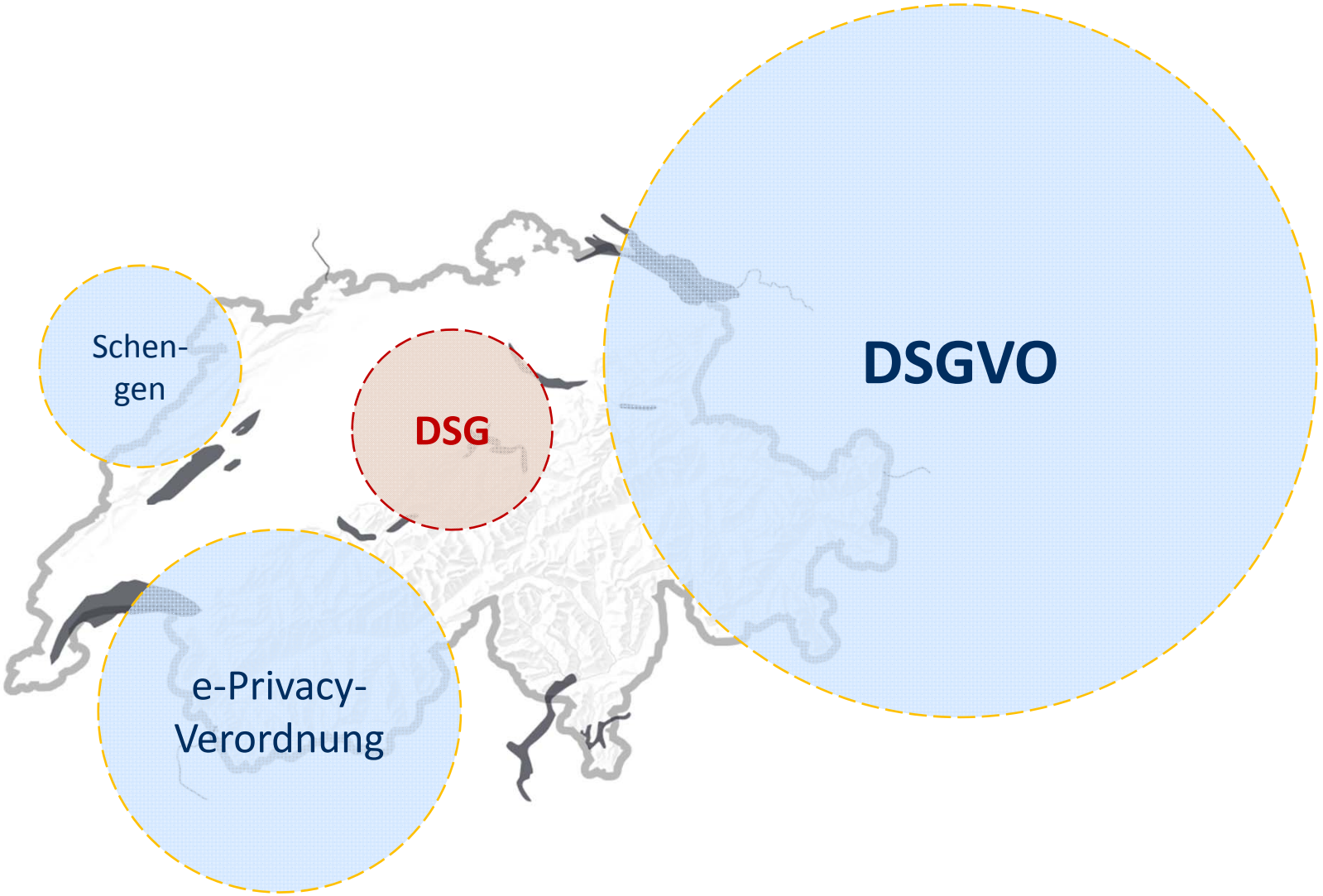
TREUHAND | SUISSE

David Vasella • 23. Oktober 2018

walderwyss rechtsanwälte

Umfeld, Anwendung der DSGVO

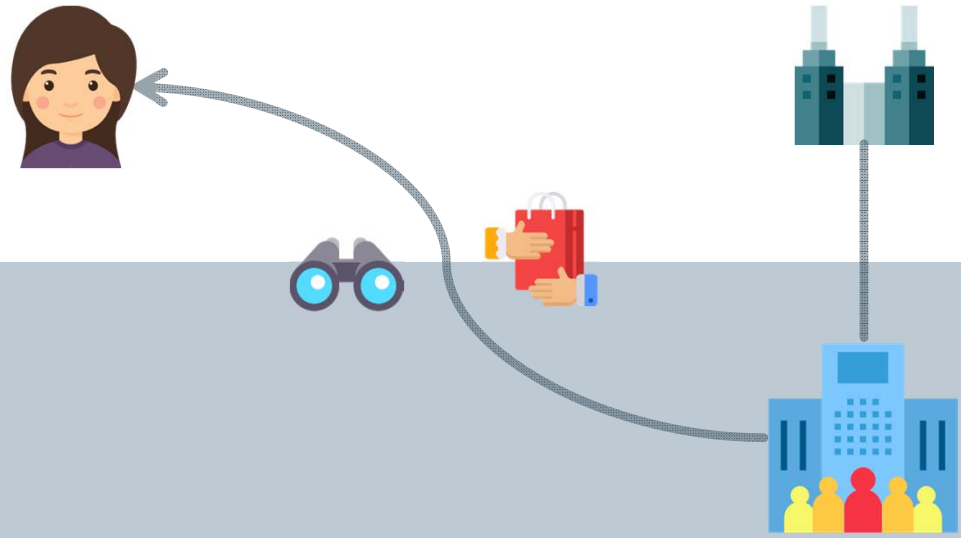
Umfeld



Stand der Revisionen im Bereich Datenschutz



Anwendungsbereich der DSGVO



1. Niederlassung im EWR
2. gezielte Angebote in den EWR
3. Beobachtung von Verhalten im EWR
4. zivilrechtliche Ansprüche: Personen mit gewöhnlichem Aufenthalt in der EU/im EWR

Angebotsausrichtung

Voraussetzungen:

– nur *gezielte* Angebote…

– an *natürliche Personen* mit Aufenthalt im EWR – nicht erfasst: B2B-Geschäft

Indizien: Sprache der Website, Ausgestaltung des Angebots, AGB, Lieferbedingungen etc.

Beispiele: Online-Bewerbung von Angeboten an Grenzgänger oder Personen im Ausland

unklare Fälle (Auswahl):

– allgemein-internationale Angebote

– weitere/fortgesetzte Angebote an Bestandskunden

Rechtsfolge: Anwendung der DSGVO auf Datenbearbeitungen *«im Zusammenhang»* mit dem Angebot, inkl. Direktwerbung und Vertragsabwicklung – aber nicht auf das Unternehmen generell

Angebotsausrichtung



NGEN

NGEN

ERTUNGEN

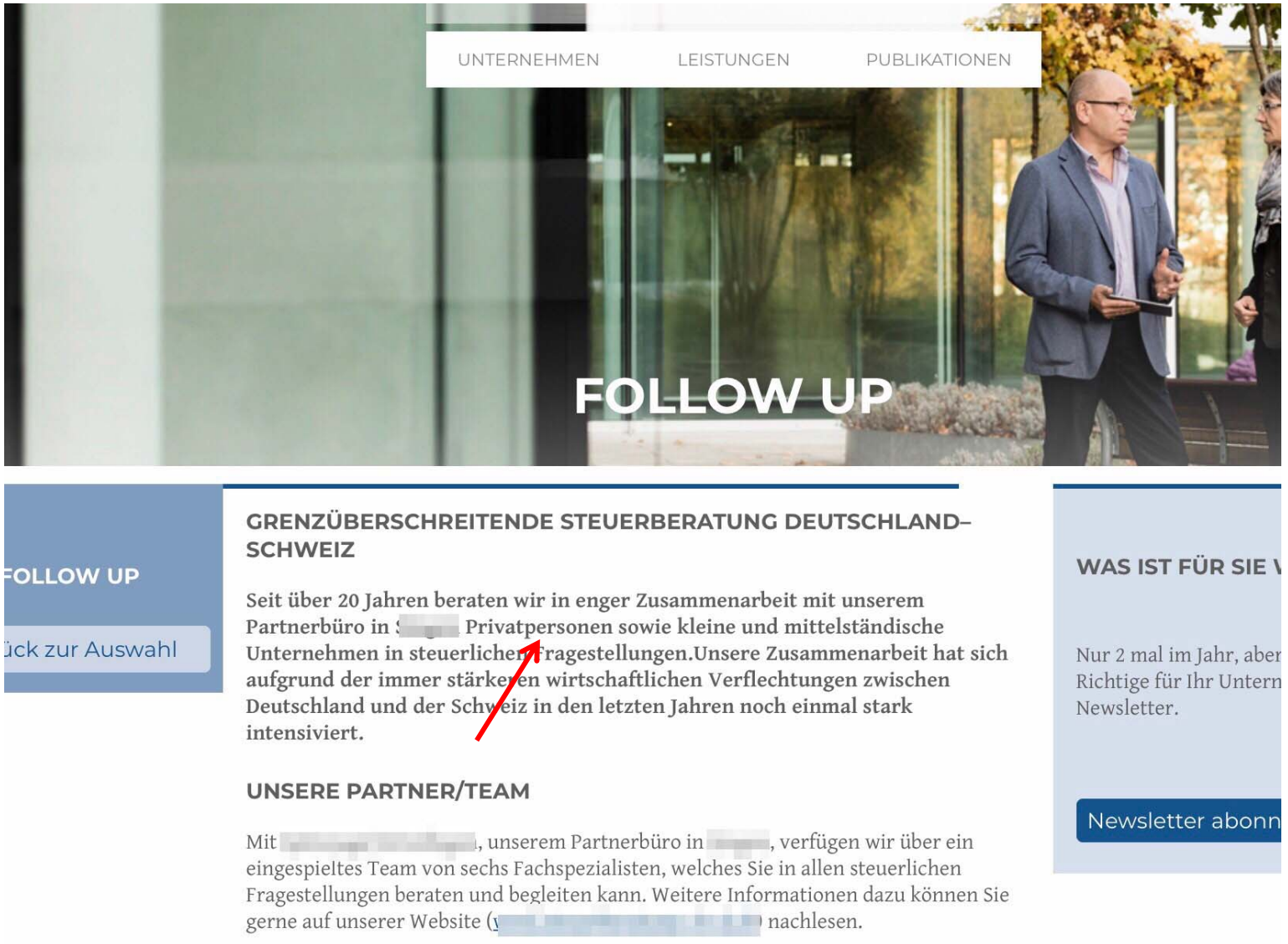
Steuern

Wachsen Sie mit uns.

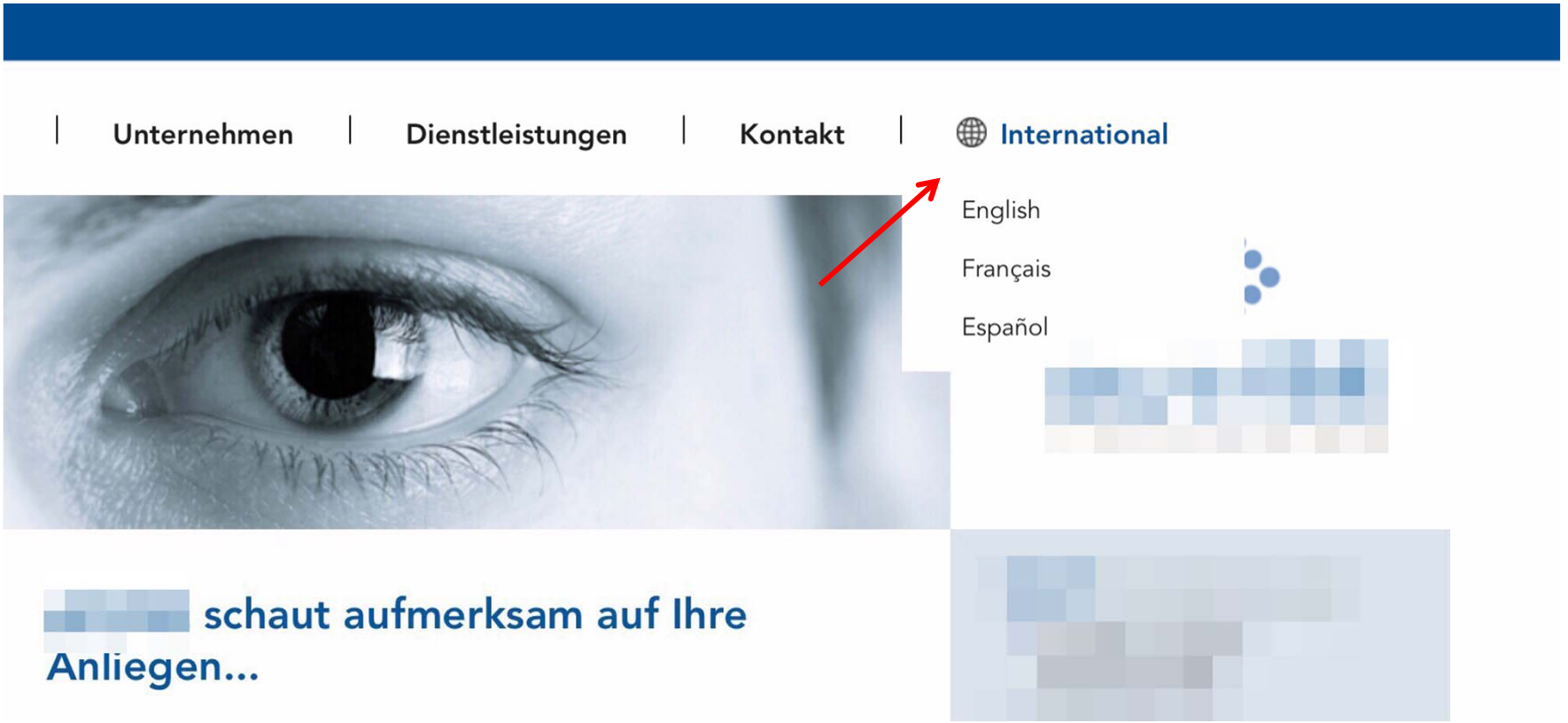
Gerne erledigen wir für Sie sämtliche Steuerangelegenheiten

- Erstellen von Steuererklärungen für natürliche und juristische Personen
- Prüfung von Steuerveranlagungen
- Bearbeitung von Steuereinsprachen
- Steuerplanung und Steueroptimierung
- Steuerberatung in sämtlichen Steuerarten
- Einkommens-, Vermögens-, Verrechnungs-, Grundstückgewinn-, Liegenschafts-, Erbschafts- und Schenkungssteuern
- Steuerberatung bei Gesellschaftsgründung und Gesellschaftsumwandlung Sanierungen und Liquidation
- Mehrwertsteueranmeldungen / -abmeldungen in der Schweiz, Deutschland und Österreich
- Erstellen von Mehrwertsteuerabrechnungen der Schweiz, Deutschland und Österreich

Angebotsausrichtung



Angebotsausrichtung



Verhaltensbeobachtung

- «**Beobachtung**»: Anforderungen unklar; setzt aber eine gewisse Intensität und Dauer voraus
- Nur im **Internet**?
  Erwägungsgrund 24: «Internetaktivitäten»)
- bereits durch **Analysedienste** wie z.B. Google Analytics?
- **Rechtsfolge**: Anwendung der DSGVO auf Datenbearbeitungen «im Zusammenhang» mit der Beobachtung, nicht auf das Unternehmen generell

Verhaltensbeobachtung



Hauptanforderungen nach DSGVO und E-DSG

an Treuhandunternehmen bzw. ihre Kunden

Übersicht

Anforderungen	DSGVO	E-DSG
Bearbeitungsverzeichnis	•	•
Datenschutzerklärung(en)	•	•
ggf. Bestellung eines EU-Vertreters	•	
ggf. Bestellung eines DPO	•	
Verträge mit (IT-)-Dienstleistern	•	•
Verträge mit Kunden («Auftragsbearbeitung)»: je nach Vertragsgegenstand	•	•
interne Richtlinien, Anleitungen, Weisungen etc.	•	(•)
Rechtsgrundlage; u.U. Einwilligung einholen (ggf. in AGB)	•	
Meldung von Datenschutz-Verletzungen	•	•
ggf. Datenschutz-Folgenabschätzungen	•	•
Betroffenenrechte	•	•

… etc.

Bearbeitungsverzeichnis

- Verzeichnis (Inventar) von Datenbearbeitungstätigkeiten
- Pflicht von Verantwortlichen und Auftragsverarbeitern (inhaltliche Unterschiede; DSGVO: beschränkte KMU-Ausnahme)
- auf Verlangen an Behörden herauszugeben
- Kopie durch den EU-Vertreter aufzubewahren

Bearbeitungsverzeichnis

Nr.	Bezeichnung der Verarbeitungstätigkeit	gemeinsam Verantwortliche	Zweck	Kategorien betroffener Personen	Kategorien personenbezogene Daten
#	Name der betreffenden Verarbeitung	allenfalls mit dem Verantwortlichen gemeinsam verantwortliche Unternehmen	Was soll mit der Verarbeitung erreicht werden? Z.B. "Personalmanagement", „Lohnbuchhaltung", „Direktmarketing", „Abwicklung von Kundenverträgen", „Führung eines Aktienbuchs	Welche Personengruppen sind betroffen?	Welche Arten von Personend betroffen (Datenfelder)? Z.B „Kunden" oder „Angestellte" Kategorien von Personendat „Kontaktangaben", „Gesundheitsdaten", „Einkau
1	Salärverwaltung				
2	Arbeitszeiterfassung				
3	Stellenbewerbung				
4	Geschäftsreisen				
5	Kundendatenverwaltung				
6	Beschaffung				
7	Verwaltung der Website				
8	Direktmarketing				
9					
10					
11					

Bestellung eines EU-Vertreters

EU-Vertreter:

- «EU-Vertreter»: natürliche oder juristische Person
- in einem EWR-Staat mit betroffenen Personen
- Anlaufstelle für Behörden und Betroffene

Pflicht zur Bestellung:

- Verantwortliche/Auftragsverarbeiter ohne Niederlassung im EWR
- Ausnahme: nur gelegentliche Bearbeitung ohne nicht umfangreiche Bearbeitung besonderer Daten und voraussichtlich ohne relevantes Risiko

Bestellung:

- Vertrag mit dem Vertreter
- diverse Dienstleistungsangebote verfügbar (z.B. in D oder FL)
- in der Datenschutzerklärung anzugeben (aber keine Meldung ggü. Behörden)

Datenschutzerklärungen

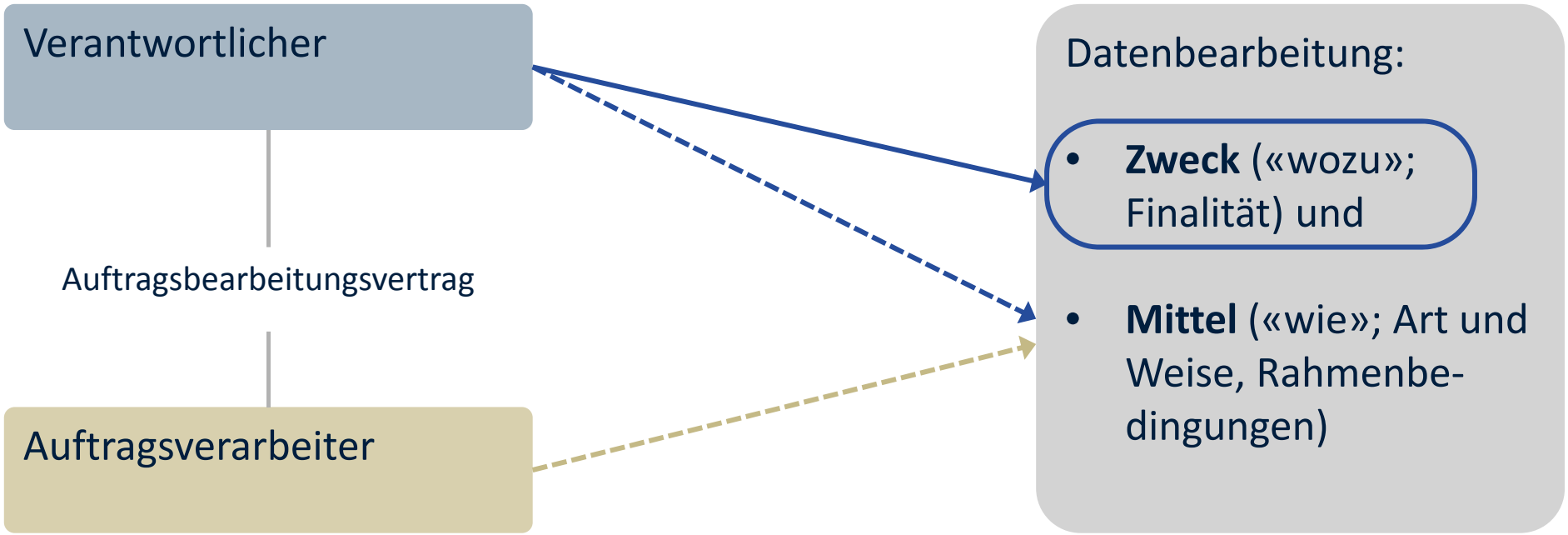
Anforderungen:

- aktive Information bei grds. jeder Datenbeschaffung
- Mindestinhalte nach DSGVO/E-DSG

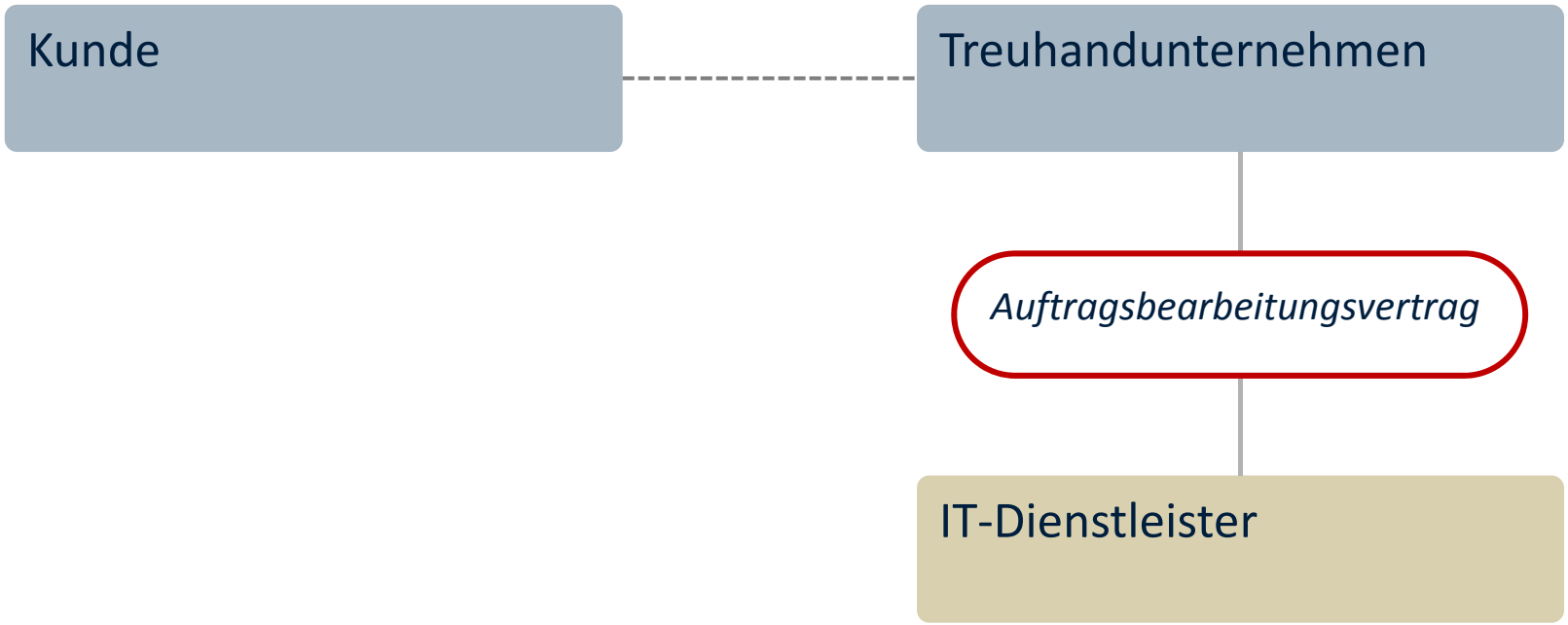
Umsetzung (Bsp./Vorschlag):

- Datenschutzerklärungen online
  - Verwendung der Website
  - Bearbeitung im Zusammenhang mit Dienstleistungen
  - ggf. weitere Datenschutzerklärungen für Bewerber, Mitarbeiter und Dienstleister
- zusammenfassende Hinweise/Verweisung auf Website
  - in AGB
  - in der Antwort auf Bewerbungen
  - etc.

Kundenverträge



Kundenverträge



Umgang mit Datenschutzverletzungen

- **Verletzungen der Datensicherheit**: Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit (Verlust, Diebstahl, unbefugte/unabsichtliche Löschung, Veränderung oder Offenlegung)
- Meldepflicht ggü. **Behörden** (in der Schweiz: EDÖB)
  - E-DSG: bei hohen Risiken; möglichst rasch
  - DSGVO: bei Risiken; möglichst rasch; max. 72h
- Meldepflicht ggü. **betroffenen Personen**
  - E-DSG: falls nötig/vom EDÖB verlangt
  - DSGVO: bei hohen Risiken
- Meldepflicht des **Auftragsverarbeiters** ggü. dem Verantwortlichen
- **Umsetzung**: z.B. einer internen Weisung zur Feststellung, Eskalation und Meldung von Datenschutzverletzungen

Betroffenenrechte

- **Auskunftsrecht**: Recht auf Auskunft und Kopie der Personendaten
- **Berichtigungsrecht**: Recht auf Berichtigung bzw. Vervollständigung von Personendaten
- **Widerspruch** gegen die weitere Bearbeitung
- ggf. **Löschung** von Personendaten
- **Einschränkung** der Bearbeitung
- **Datenübertragung**

Umsetzung:

- ggf. interne Weisung(en), Prozessbeschreibung und Musterkorrespondenz
- Hinweise in Datenschutzerklärungen
- Einhaltung des Ablaufs im Einzelfall; rasche Bearbeitung
- Dokumentation (z.B. in einem «Log-Buch»)

Risiken bei Verletzungen

- zunehmende Aufmerksamkeit: Datenschutzverletzungen sind unvermeidbar, werden aber laufend besser erkannt und schneller moniert
- zunehmende Reputationsrisiken, v.a. in exponierten Branchen
- Datenschutz als Waffe und Instrument vor und bei Auseinandersetzungen – interne Kosten
- Sanktionsrisiken (EU: theoretisch Bussen bis EUR 20M/4%); CH: u.U. bis CHF 250’000 als Busse vorgesehen)
- Haftungsrisiken (z.B. immaterielle Schäden nach Art. 82 Abs. 1 DSGVO; u.U. solidarische Haftung nach Art. 82 Abs. 4 DSGVO)
- Risiko von indirekten Vertragsverletzungen («Compliance with laws»-Klauseln)

Vielen Dank.

Dr. David Vasella, CIPP/E

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