

# «Last Minute Datenschutz»

Lunch and Law

Winterthur, 16. März 2023



# Einführung

# «Last Minute Datenschutz»

- BGH Urteil vom 17.06.1999 (Az.: I ZR 149/97):

«Insofern enthält der Begriff "Last-Minute-Reise" mehrere Aussagen. Er vermittelt beim angesprochenen Verkehr nicht nur den Eindruck einer gewissen **Kurzfristigkeit** [...], sondern ruft [...] auch die Vorstellung einer besonderen **Preisgünstigkeit** des Angebots hervor [...].»

- *Es ist höchste Zeit!*
- *Es ist machbar!*
- *Unnötige Risiken und Kosten vermeiden!*

# Inhalt der heutigen Veranstaltung

- Warum sollten Sie sich mit dem neuen Datenschutzrecht auseinandersetzen?
- Was muss mindestens getan werden?
- Wie gehen Sie das am einfachsten an?

# Datenschutzteam



**Julia Bhend**  
Rechtsanwältin, Partnerin



**Kaj Seidl-Nussbaumer**  
Rechtsanwalt



**Dr. Claudia Marti**  
Rechtsanwältin



**Dr. Michael Widmer**  
Rechtsanwalt, Konsulent

# Warum sollte Sie das neue DSG interessieren?

# DSG Revision: Hintergrund und Entwicklung



# DSG erhält Zähne

- Ausbau der Ressourcen, Kompetenzen und Befugnisse des EDÖB
- **Neu:** Kostenlosigkeit von zivilrechtlichen Verfahren wegen Verletzung Persönlichkeit
- **Neu:** Bussen bis CHF 250'000
  - Täter ist grundsätzlich eine natürliche Person (Leitungsperson / Geschäftsführung)
  - Nur vorsätzliche Pflichtverletzungen, aber Eventualvorsatz genügt
  - Voraussichtlich nicht gedeckt durch Versicherungen



# Was sollten Sie tun?

# Was sollten Sie tun?

- Inventar erstellen
  - Kenntnis der Bearbeitungen als Grundlage für weiteres Vorgehen
- Allgemeine Informationspflicht erfüllen
  - Grundsatz: *"Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist"*
  - **Datenschutzerklärungen** gewinnen an Wichtigkeit
- Verträge mit Dienstleistern aktualisieren oder abschliessen (Auftragsbearbeitung)
- Bekanntgabe ins Ausland: Voraussetzungen prüfen

**strafbar**

**strafbar**

**strafbar**

# Was sollten Sie tun?

- Datensicherheit
  - Mindestanforderungen erfüllen
  - Risikobasierter Ansatz
  - Technische und organisatorische Massnahmen / allenfalls Protokollierung und Bearbeitungsreglement
  - Spezialisten beiziehen
- Sensibilisierung und Organisation u.a. betr.
  - Betroffenenrechte wie Auskunft, Datenherausgabe und -übertragung
  - Meldung von Verletzungen der Datensicherheit
  - Löschung/Anonymisierung

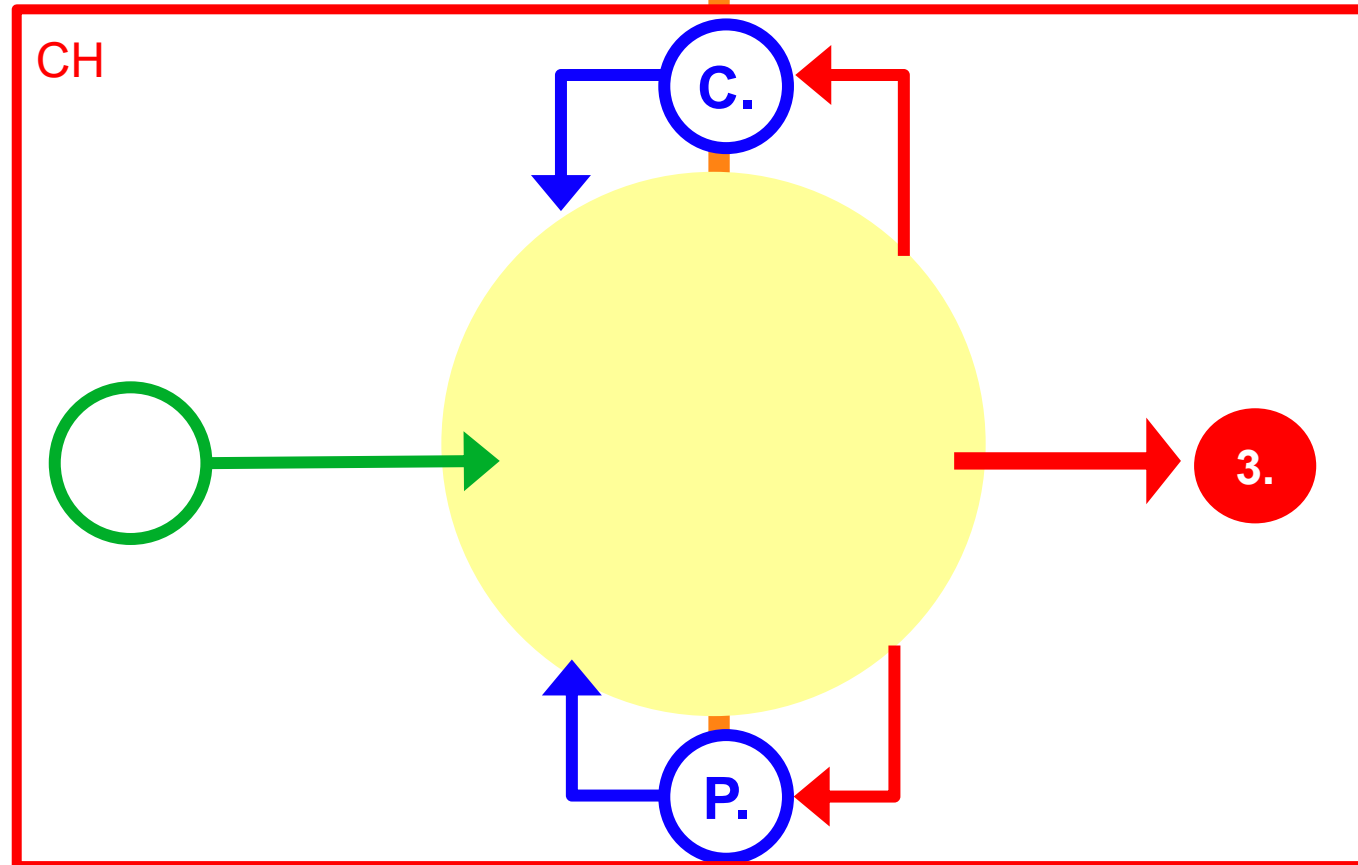
*strafbar*

# Wie angehen?

# Inventar – Was läuft bei mir bezüglich Personendaten?

Unsichere Drittländer (z.B. USA, China)

EU/EWR und sonstige sichere Drittländer



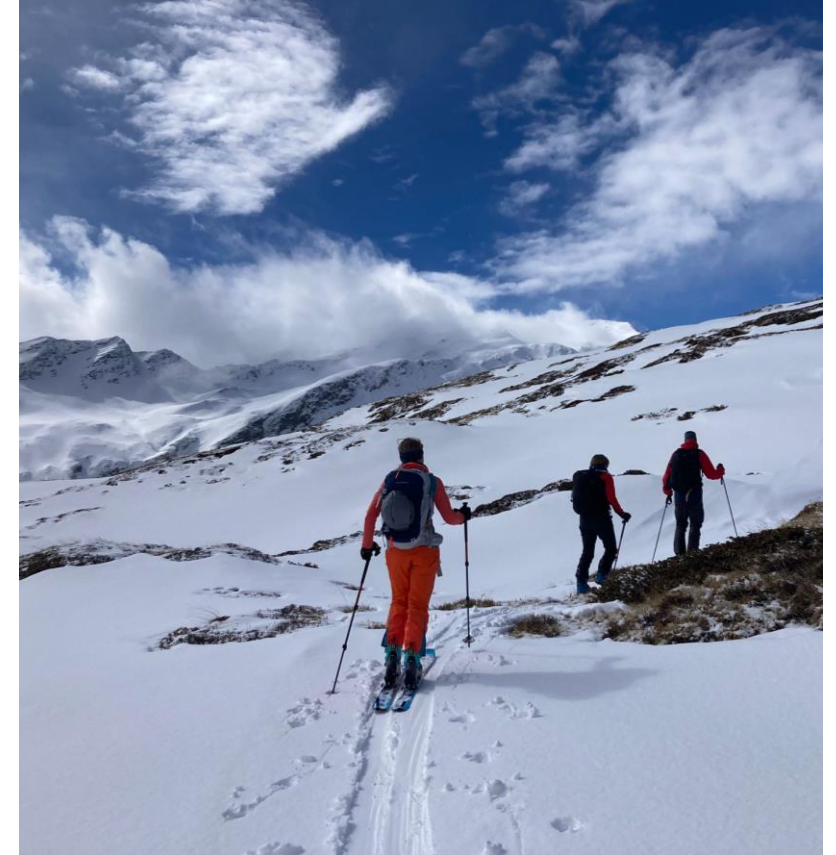
# Inventar

- Grundsätzlich **Pflicht**, aber mit KMU Ausnahme:
  - weniger als 250 MA
  - nicht in grossem Umfang besonders schützenswerte Personendaten
  - kein Profiling mit hohem Risiko
- *Viele KMU fallen unter die Ausnahme*
- **Unabhängig von Pflicht:** Wichtiges Werkzeug im Bereich Datenschutz, das Ableitung der nötigen Massnahmen erlaubt und Umsetzung erleichtert
- **Vorfrage:**
  - Welches Recht: DSGVO oder DSG?
  - Vorbefassung

Bearbeitungstätigkeit	Zwecke der Bearbeitung	Kategorien der Personendaten	besonders schützenswerte Personendaten	Kategorien der betroffenen Personen	Herkunft der Daten	Kategorien der Empfänger	Aufbewahrungsdauer oder Kriterien zu deren Festlegung	Gewährleistung der Datensicherheit	bei Auslandstransfer: Zielländer und Garantien	Bemerkungen
<b>Personal</b>										
Personaladministration	Durchführung Arbeitsverhältnis	Name und Vorname, Adresse, E-Mailadresse, AHV-Nummer, Lohn, Beschäftigungsgrad, Geburtsdatum, Familie, Zivilstand, Geschlecht, Nationalität/Heimatort, Aufenthaltsbewilligung, Kontoangaben, Eintritts-/Austrittsdatum, Ausbildung, Berufliche Funktion, Beurteilungen, Zeiterfassung, Krankentaggelder, Arztzeugnisse, Zugriffsrechte IT.	Gesundheitsdaten (Krankentaggelder, Arztzeugnisse, behinderungsbedingte Arbeitsplatzanpassungen)	Mitarbeiter; Angehörige Mitarbeiter (Notfallkontakte, Versicherungsleistungen)	Mitarbeiter; Muster AG; Dritte (z.B. Referenzen)	Auftragsbearbeiter (IT-Provider und Saläradministration); Behörden; Neue Arbeitgeber (Referenzauskünfte)	längstens 10 Jahre nach Beendigung Arbeitsverhältnis	siehe Datensicherheitskonzept Muster AG	Deutschland (sicheres Drittland)	
Bewerberprozess	Durchführung Bewerberprozess	Bewerbungsdossier, Referenzen	Gesundheitsdaten (allfällige Beeinträchtigungen)	Bewerber	Bewerber frühere Arbeitgeber (Referenzen) Dritte (Head Hunter)	Auftragsbearbeiter (IT-Provider); frühere Arbeitgeber (Referenzen).	bis Abschluss Arbeitsvertrag oder Absage; mit Zustimmung Bewerber länger.	siehe Datensicherheitskonzept Muster AG	Deutschland (sicheres Drittland)	
Ehemaligennetzwerk	Pflege des Kontakts zu ehemaligen Mitarbeitern	Name, Adresse, E-Mailadresse, Kontaktdaten; Eintritts-/Austrittsdatum.	n.a.	ehemalige Mitarbeiter	ehemalige Mitarbeiter	n.a.	bis zur Abmeldung durch Mitarbeiter	siehe Datensicherheitskonzept Muster AG	n.a.	
<b>Newsletter</b>										
<b>Lieferantenmanagement</b>										
<b>Strategische Partner (Verein "Ich-Tauchen-so-gern")</b>										
Vermittlung Tauchkurse	Vermittlung zwischen freien Instruktoren und Kursteilnehmern	Name und Vorname, E-Mailadresse	Gesundheitsdaten (Tauchfähigkeit)	Instruktoren des Vereins "Ich-tauchen-so-gern" Kursteilnehmer	Instruktoren, Kursteilnehmer, Dritte (Arztzeugnis Tauchfähigkeit)	Kursteilnehmer, Instruktoren, Hallenbad Musterthur	längstens 10 Jahre nach Vermittlung	siehe Datensicherheitskonzept Muster AG	n.a.	

# Datenschutzerklärungen

- **Erforderliche Informationen:**
  - Identität und Kontaktdaten des Verantwortlichen (und des Datenschutzberaters)
  - Bearbeitungszweck
  - Konkrete Empfänger oder Kategorie der Empfänger
  - Bei Beschaffung von Dritten: Kategorien der Personendaten
  - Staat und Garantien/Ausnahme bei Auslandsbekanntgabe
  - Ggf. automatisierte Einzelentscheidung



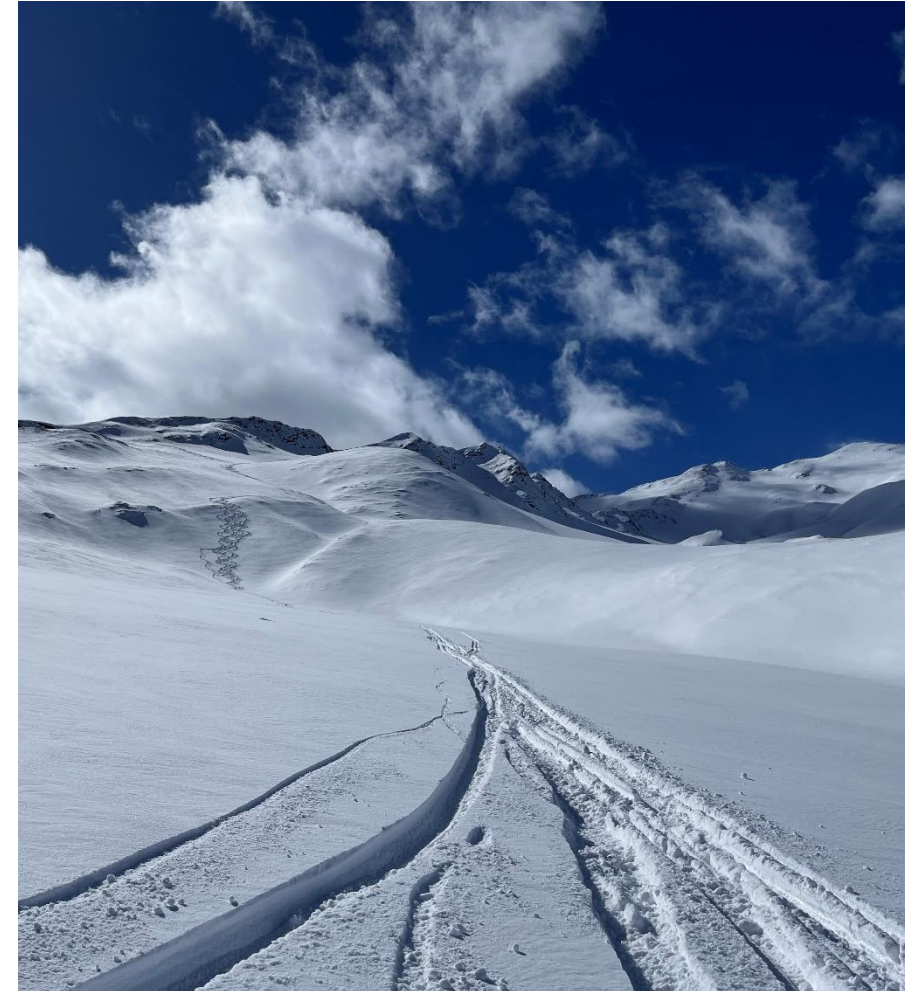


# Datenschutzerklärungen

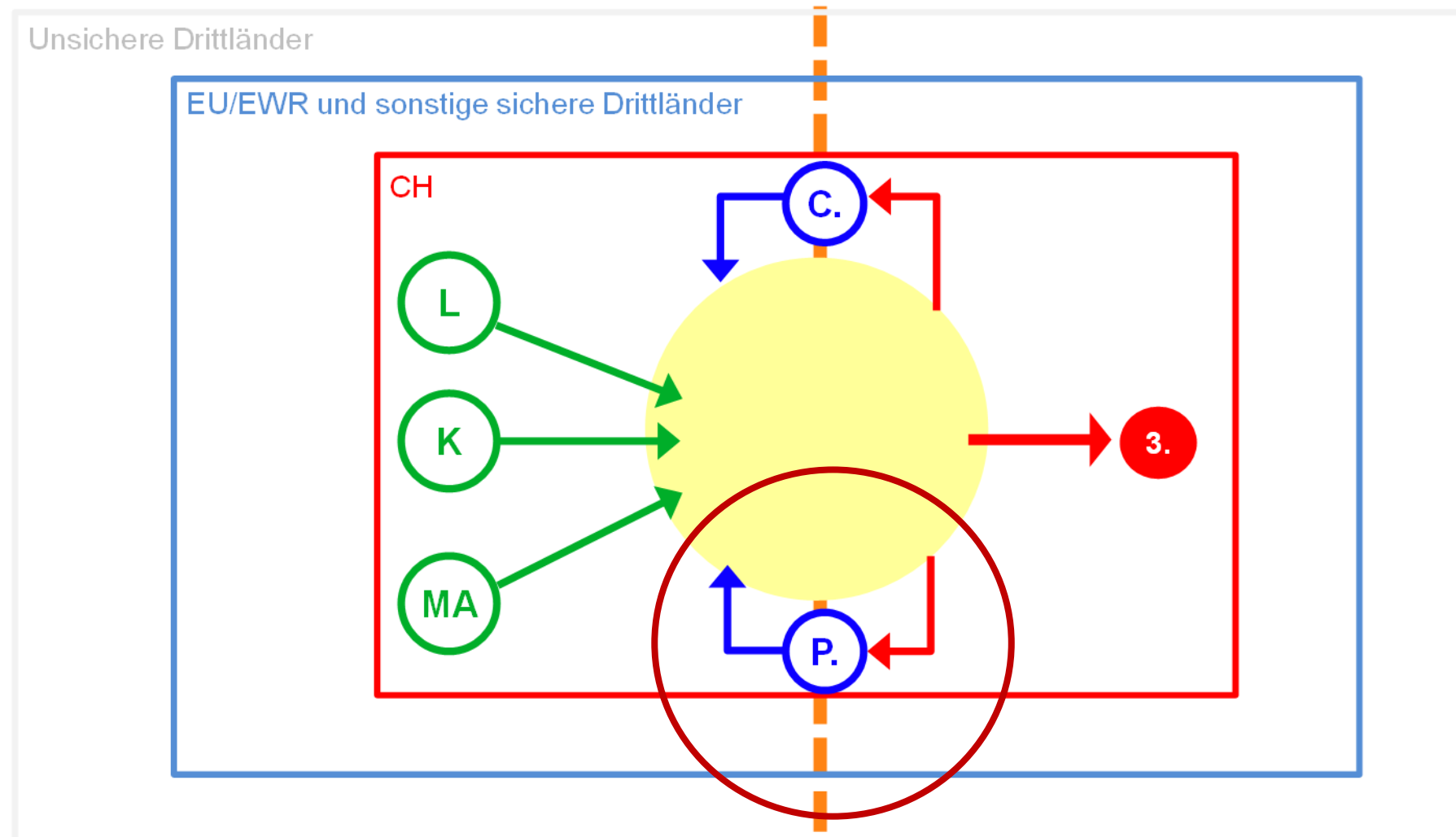
- Nicht erforderlich, aber **üblich**: Rechtaufklärung, wie
  - Auskunft, Berichtigung, Löschung oder Vernichtung
  - Datenherausgabe oder Datenübertragung
  - Widerruf einer allfälligen Einwilligung
  - Beschwerde beim EDÖB
- Nicht erforderliche und **nicht übliche** Inhalte:
  - Rechtsgrundlage
  - Aufbewahrungsdauer
  - Herkunftsangaben

# Datenschutzerklärungen

- **Form:**
  - präzise, transparent, verständlich, leicht zugänglich
  - Üblicherweise auf Webseite
- **Ausnahmen:** im Einzelfall zu klären



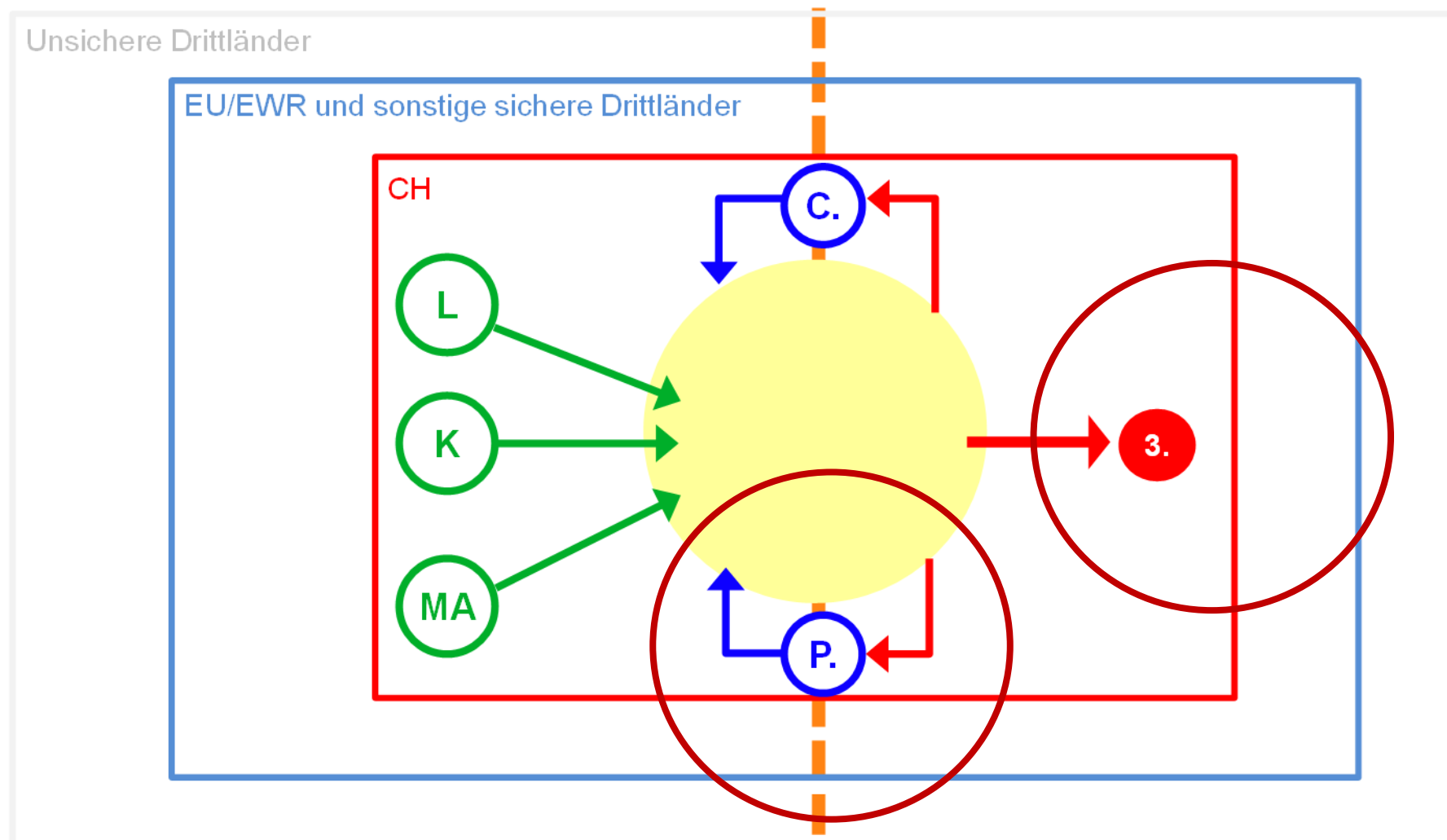
# Verträge mit Dienstleistern



# Verträge mit Dienstleistern

- Alle Auslagerungen brauchen Bearbeitungsvertrag, am besten schriftlich
  - Gesetzlicher Mindestinhalt vorgegeben, wichtigste Änderungen:
    - Subunternehmer nur mit vorgängiger Genehmigung
    - Meldung bei Datenschutzverletzungen vertraglich verankern
  - Hauptproblem in der Praxis: Dokumentation
- 
- *Liste aufstellen, für welche Prozesse Dienstleister beigezogen sind*
  - *Überprüfen, ob/welche Verträge bereits bestehen*
  - *Aktualisieren gem. neuen Anforderungen*

# Bekanntgabe ins Ausland



# Bekanntgabe ins Ausland

- Häufige Fälle:
  - Dienstleister im Ausland / Cloud
  - Gruppengesellschaften im Ausland
  - Strategische Partnerschaften
- Triage: sicheres / unsicheres Ausland
- Bei unsicherem Ausland: zusätzliche Schutzmassnahmen nötig, z.B.
  - Einwilligung (nur in Ausnahmefällen praktikabel)
  - Standardvertragsklauseln mit Einzelfallanpassung + Transfer Impact Assessment
- *Aufwändig; nur sinnvoll, wenn Bekanntgabe schwer verzichtbar (z.B. Toolwechsel)*
- *Generell: Anbieter mit Sitz in CH/EU/EWR nehmen, Serverstandort CH/EU/EWR wählen wo möglich*

# Sensibilisierung und Organisation

- Sensibilisierung für Datenschutz im Unternehmen, z.B. durch Schulung, Handbuch
- Zuständigkeiten festlegen für Datenschutzfragen, insb.
  - DSGVO-Fragen allgemein
  - Beantwortung von Auskunftsbefehlen
  - Datensicherheitsverletzungen
  - Datensicherheit
- Externe Unterstützung holen

# Sensibilisierung und Organisation

*Grüezi,*

*Ich bitte Sie, mir alle meine Daten herauszugeben und mir per E-Mail an [jonasmueller@gmail.com](mailto:jonasmueller@gmail.com) zuzustellen.*

*Ich erwarte die Daten bis am 25. März 2023.*

*Mit freundlichen Grüssen*

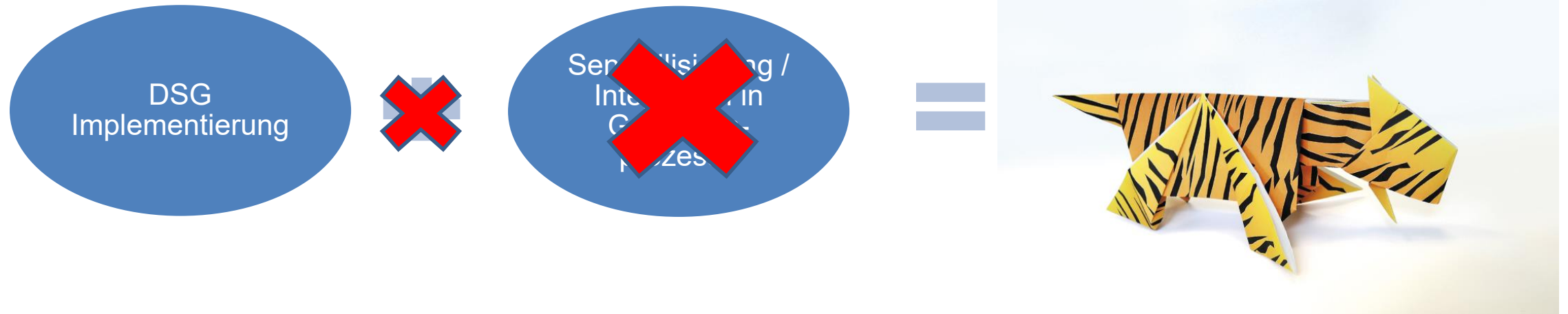
*Heidi Muster*



# Sensibilisierung und Organisation

- Datenschutz in Geschäftsprozesse integrieren
  - Erfassung von Personendaten
  - Auswahl von Produkten / Systemen
  - Aufbewahrungsdauer und Löschung

# Sensibilisierung und Organisation



# Abschluss



Vermeiden Sie unnötige Risiken und Kosten!



Wer «seine Hausaufgaben» gemacht hat, geht in aller Regel kein Bussgeldrisiko ein.



Beginnen Sie mit der Umsetzung!



Es ist machbar!

# Take aways

- Inventar erstellen
- Datenschutzerklärungen entwerfen
- Verträge mit Dienstleistern und Auslandsbekanntgaben prüfen
- Datensicherheit sicherstellen

# bei weiteren Fragen

Probst Partner AG, Zürich/Winterthur  
+41 52 269 1400

[www.probstpartner.ch](http://www.probstpartner.ch)

<https://swissdataprotectionlaw.ch/>