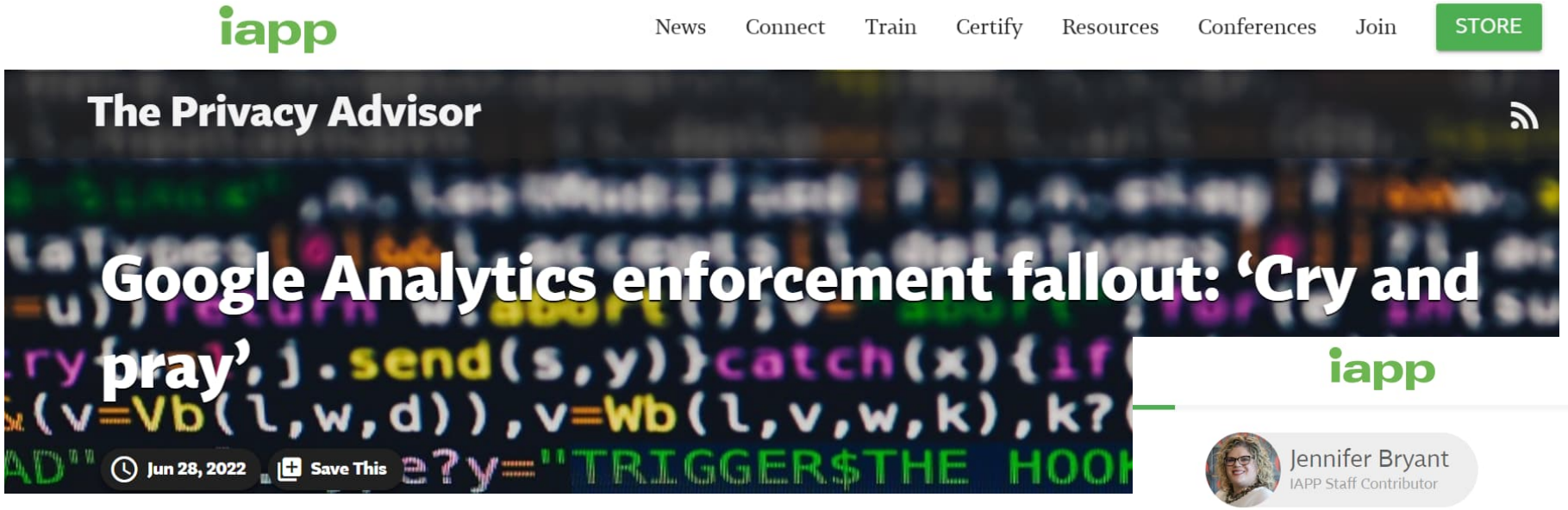
Auftragsdaten-bearbeitung mit Auslandstransfer

Schrems II: Problemstellung und Lösungsansätze für Beschaf-fungsstellen

Anselm Filliger und Vinzenz Ernst, SBB AG

24. August 2022

«Cry and pray» - Schrems II und seine Folgen



GDPR violation. The rulings come in response to 101 complaints filed across EU member states by advocacy group NOYB following the "Schrems II" decision that invalidated the EU-U.S. Privacy

iapp News Connect Train Certify

Jennifer Bryant
IAPP Staff Contributor

Three EU privacy authorities have determined Google Analytics unlawfully transfers data to the United States, leaving companies with little to no alternatives and privacy professionals debating how to react as continued similar decisions are anticipated.

"Cry and pray. I think that's the only thing we can do — is cry and pray," Fox Rothschild Partner Odia Kagan, CIPP/E, CIPP/US, CIPM, FIP, PLS, said. "Companies are really in a bind with no real good solutions."

Agenda

1. Auftragsdatenbearbeitung nach Schrems II (AF)
2. Handlungsbedarf bei Unternehmen/Behörden und Lösungsansätze (VE)
3. Diskussion (AF/VE)

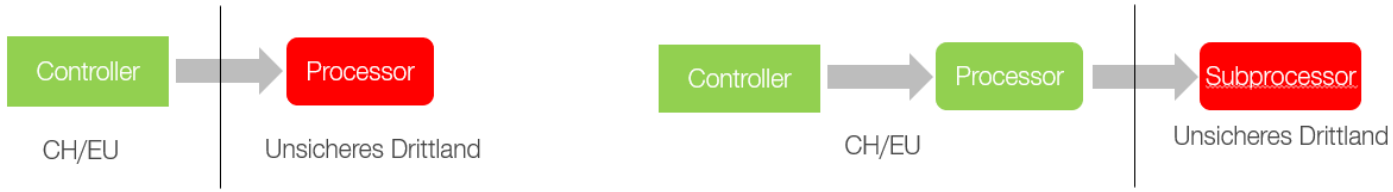
Ausgangslage: Wann findet Auslandstransfer i.d.R. statt?

Auftragsdatenbearbeitung:

- Controller (Auftraggeber) / Processor (Auftragnehmer)
- Auftragsdatenbearbeitungsvertrag (ADV)
- Prüfungspflicht

Auslandstransfer:

- Zielland: angemessener/unangemessener Datenschutz (sicheres/unsicheres Drittland)
- Art der Bekanntgabe: Speicherung/Zugriffe
- Subjekt des Exporteurs: direkter/indirekter Transfer



- Garantien für Export (unsichere Drittländer): **Standard Contract Clauses** (SCC) / Privacy Shield

Neues DSG: Neue Risiken

- **Inkrafttreten:** 1. September 2023

- **Strafbestimmungen:** Bussen von bis zu CHF 250’000 für die intern verantwortliche Person bei (eventual)vorsätzlicher Verletzung:
  - der Informationspflichten,
  - der Regeln über Auslandtransfer und
  - der Regeln über die Auftragsdatenbearbeitung

- **Eventualvorsatz:** «Mir doch egal»

- **Datenschutzgesetz (DSG):** risikobasierter Ansatz

Schrems II: Neue Anforderungen

- **EUGH** erklärt im Urteil "Schrems II" den Privacy Shield für ungültig und die **SCC für ungenügend**.

- **EU-Kommission** erlässt als Folge im Hinblick auf den Auslandtransfer in unsichere Drittstaaten **neu strukturierte SCC**:

  - **Modularer Aufbau:** Direkter Transfer (Modul 2) / Indirekter Transfer (Modul 3)

  - **Abschluss der SCC allein genügt nicht**, es braucht zusätzlich ein **Transfer Impact Assessment („TIA“)** = Abklärung, ob im Zielland die rechtsstaatlichen Garantien eingehalten werden.

  - Falls es im Zielland keine oder ungenügende rechtsstaatlichen Garantien gibt, muss der Exporteur **zusätzliche Massnahmen** zum Schutz der Daten **treffen** und **dokumentieren**.

- EDÖB anerkannte die SCC umgehend -> sie müssen **ab sofort** verwendet werden

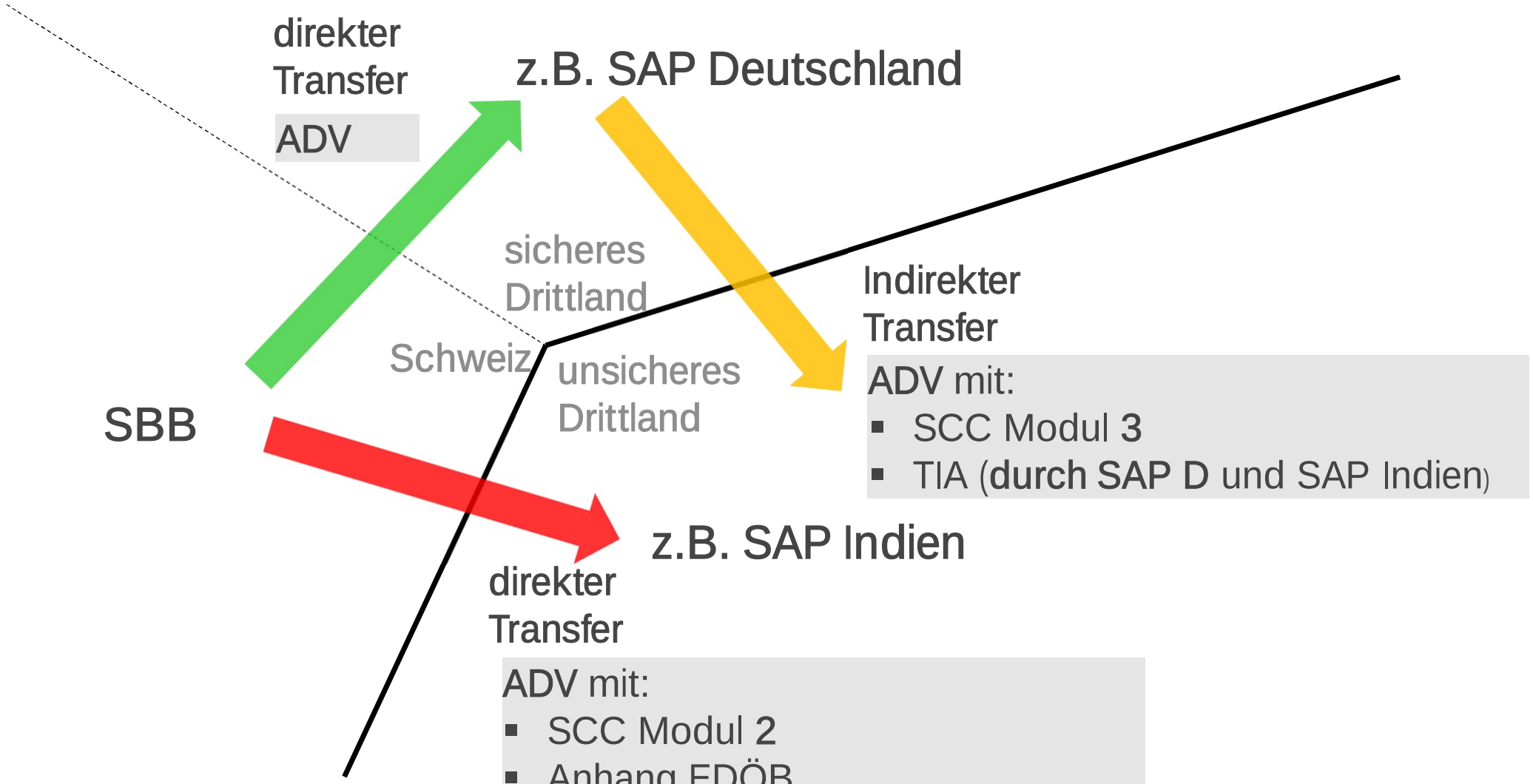
Aufwand für Vertragsmanagement und Risiko von Rechtsverletzungen steigen markant

Unsichere Rechtsentwicklung: von Schrems II zu Google I, II, III und …

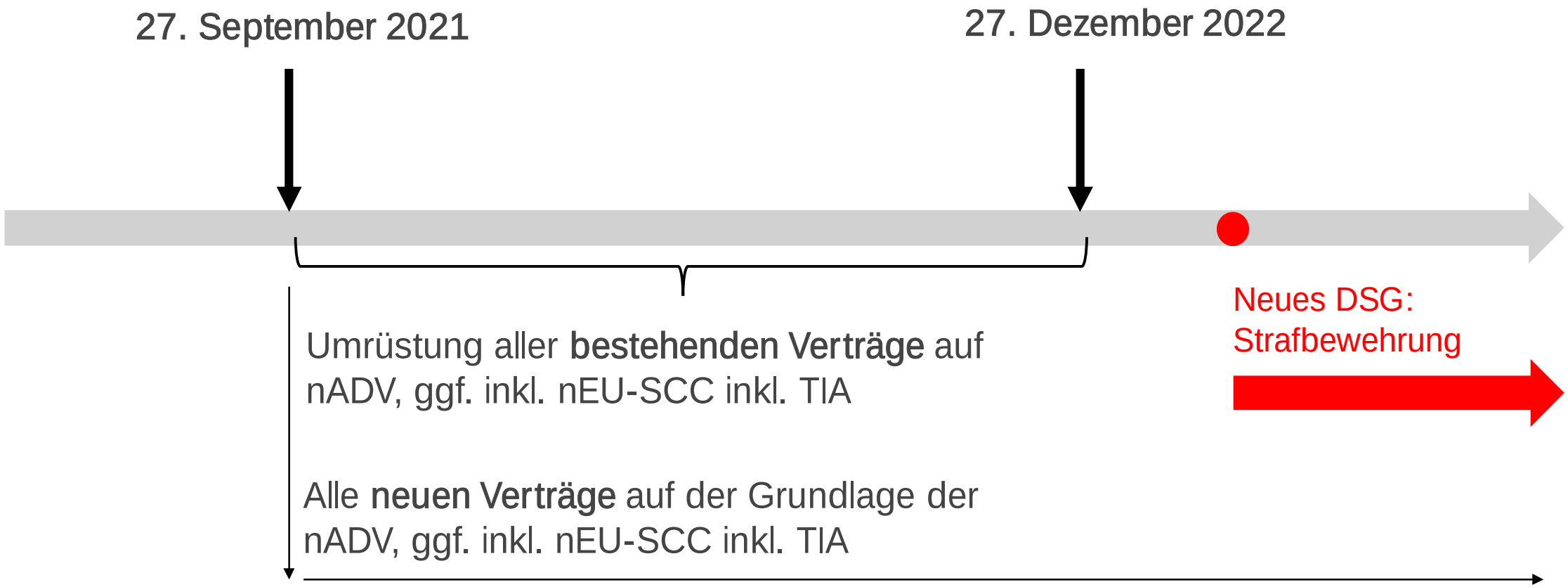
- Umsetzung und die Folgen der Grundsatzurteile bereiten in der Praxis grosse Schwierigkeiten
- Entscheidend ist, ob **„risk-based“** oder **„right-based“**
- Rechtsprechung:
  - Google Analytics Entscheide („cry and pray…“)
  - Vergabekammer Baden-Württemberg

- **Folgen in der Schweiz**
  - Grundsätzlich: DSG baut auf dem „risiko-basierten“ Ansatz auf
  - Stellungnahmen EDÖB (Auslandstransfer / Office 365 (Suva))
  - Zürcher Regierungsrat (Office 365)
  - Kant. Staatsanwaltschaften

Handlungsbedarf und Lösungsansätze: **Übersicht**



Handlungsbedarf und Lösungsansätze: **Zeitachse**



Schritt 1: Analyse Vertragslandschaft Altverträge
Lead: Projektleitung; Einbezug Vertragsinhaber, Einkauf, Legal, IT-Security

1. Übersicht über die Vertragslandschaft gewinnen

   a) Verträge mit Personendaten erkennen

   b) (Auslands)transfers erkennen:
      - was (Bearbeitung: Datenkategorien, Speicherung/Zugriff)
      - wohin (Transfer: sicher/unsicher)
      - wie (Transfer in unsicheren Drittstaat: direkt/indirekt)

Schritt 2: Personendaten definieren (betr. Alt- und Neuverträge)
Lead: Legal / IT-Security

2. Sensitivitätsstufen der Personendaten je für Mitarbeiter- und Kundendaten

	Mitarbeiterdaten (Bsp.)	Kundendaten (Bsp.)
D1	Mitarbeiternummer; Log-Daten	Kundennummer, Log-Daten
D2	Privatadresse. Zivilstand, Geburtsdatum,	Standortdaten, Aufnahmen (Video, Telefon, etc.)
D3	Personalbeurteilung, Lohn, Steuern,	Finanzielle Verhältnisse wie z.B. Betreibungen

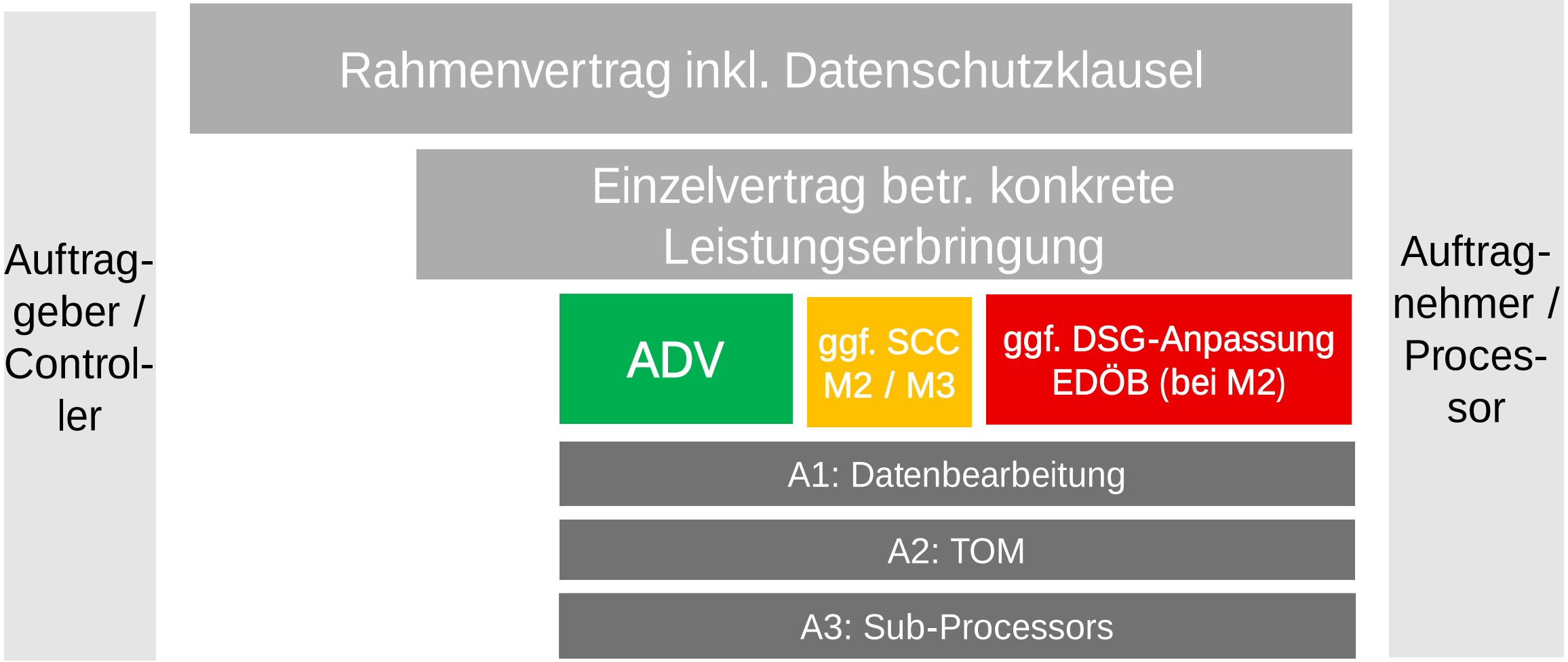
Schritt 3: Security / TOM definieren (betr. Alt- und Neuverträge)
Lead: Legal / IT-Security

3. Anforderungen an die Datensicherheit der Personendaten (TOM) definieren: je für Speicherort bzw. Zugriff

Transfer \ Datenkategorie			D1	D2	D3
wohin	zu Anbieter mit Speicherort in	unsicherem Drittstaat	TOM	TOM S+	TOM S++
		sicherem Drittstaat oder CH	(TOM)	TOM	TOM
	zu Anbieter mit Zugriff aus	unsicherem Drittstaat	TOM	TOM Z+	TOM Z++
		sicherem Drittstaat oder der CH	(TOM)	TOM	TOM

Schritt 4: Vertragsvorlagen erarbeiten (betr. Alt- und Neuverträge)
Lead: Legal / IT-Security

4. Template ADV inkl. fallbezogen zu konkretisierende Anhänge erstellen



Schritt 5: Aufarbeitung Altverträge

Lead: Projektleitung; Einbezug Vertragsinhaber, Einkauf, Legal, IT Security

6. Umsetzung erfolgt risikoorientiert gemäss der vorgenommenen Risikokategorisierung

7. Einkauf / Vertragsinhaber führt Verhandlungsprozess mit dem Lieferanten

8. Situativer Beizug Spezialisten Legal und IT-Security betr. ADV, TOM und TIA

9. Risikobeurteilung Verhandlungsergebnis: Vertragsinhaber

Schritt 6: Zielbild Neuverträge
Lead: Einkauf; Einbezug Vertragsinhaber, Legal, IT-Security

Shoring-Strategie
Beschaf-fungsde-sign (EK, TS)
Beschaf-fungsbe-dürfnis
Markt-angebot

	wie/wohin:	SCC	TIA	Verantwortung SBB für TIA	Methodik TIA
1.	in sichere Drittstaaten	n.a.	n.a.	n.a.	n.a.
2.	indirekter Transfer in unsichere Drittstaaten	nEU-SCC	TIA zwischen Processor und Subprocessor	kontrollieren	keine Vorgabe SBB
3.	direkter Transfer in unsichere Drittstaaten	nEU SCC mit DSG-Anpassung EDÖB	TIA zwischen Controller und Processor	miterstellen	Rosenthal (?)

Handlungsbedarf und Lösungsansätze: «Cry and pray ... and document»

iapp News Connect Train Certify

"A way to protect your company is to at least gather information and try to find solutions, document in order to be able to demonstrate your accountability to the regulator," he said.

From there, companies can assess their level of risk, evaluate whether there are measures to be taken that can mitigate that risk, and determine what might be the best option for them.

The final option, Kagan said, "is of the cry and pray genre."

"Be vocal about how difficult this is."

Author

Jennifer Bryant
IAPP Staff Contributor

Q & A

Anselm Filliger und Vinzenz Ernst, SBB AG
24. August 2022