

Herausforderungen bei der Operationalisierung datenrechtlicher Normen in der Finanzindustrie



Agenda

1. Ausgangslage
2. Datenrechtliche Normen
3. Operationalisierung
4. Beispiel EU AI Act
5. Key Takeaways

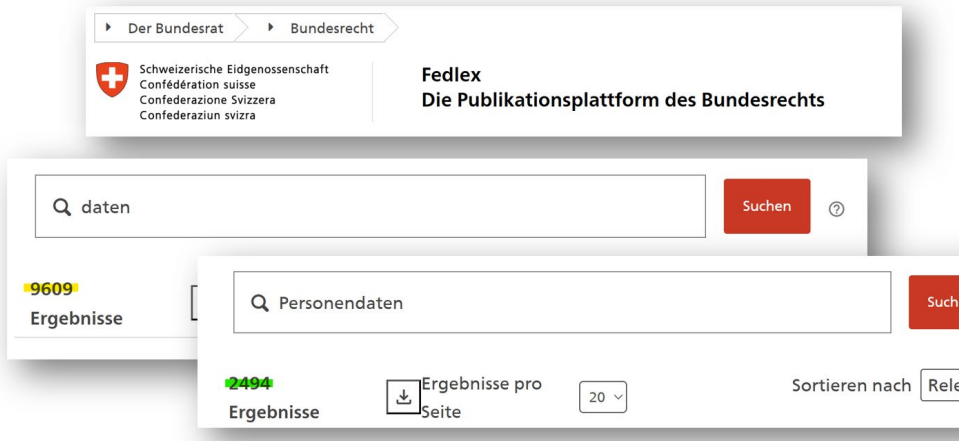


Table 1: Overview of EU Legislation in the Digital Sector

[illegible]

Datenrechtliche Normen



Operationalisierung datenrechtlicher Normen am Beispiel: Privacy by Design & Default

Art. 7 DSGVO Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

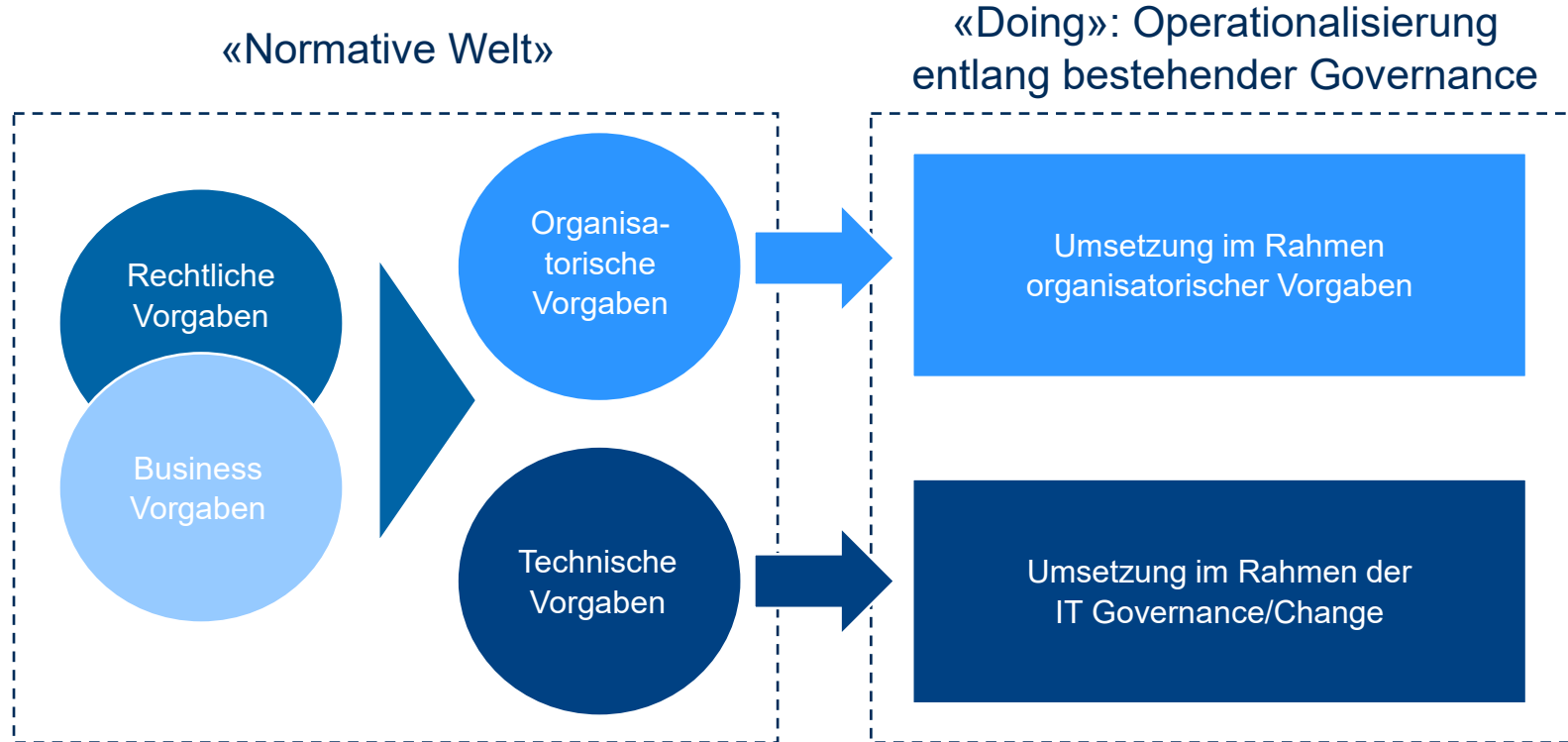


¹ Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze nach Artikel 6. Er berücksichtigt dies ab der Planung.

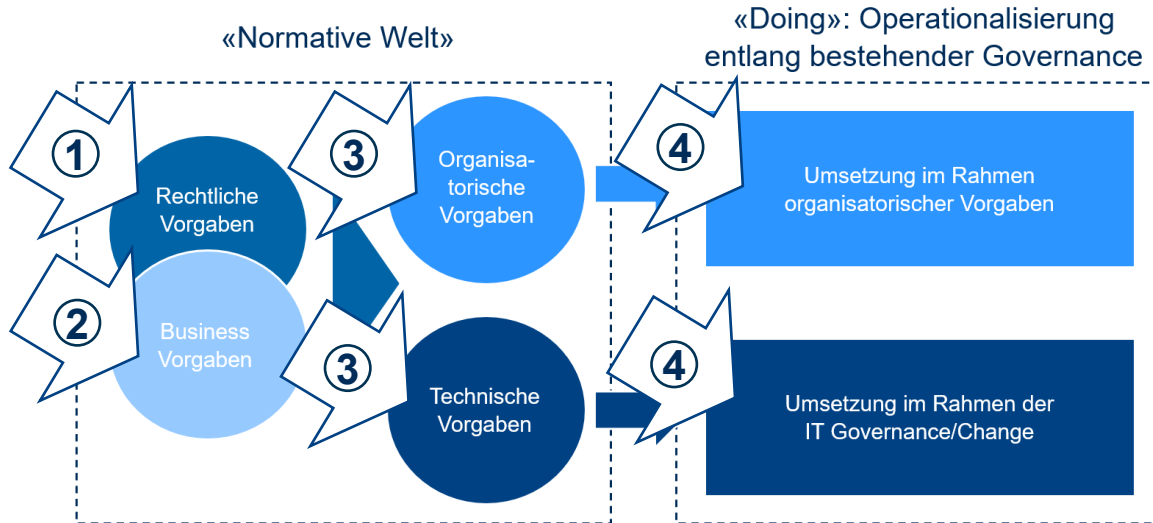
² Die technischen und organisatorischen Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, angemessen sein.

³ Der Verantwortliche ist verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt.

Rechtliche- & TOM-Vorgaben: 2 Stufiger Ansatz



Risikobasierter Ansatz & Kontrollen

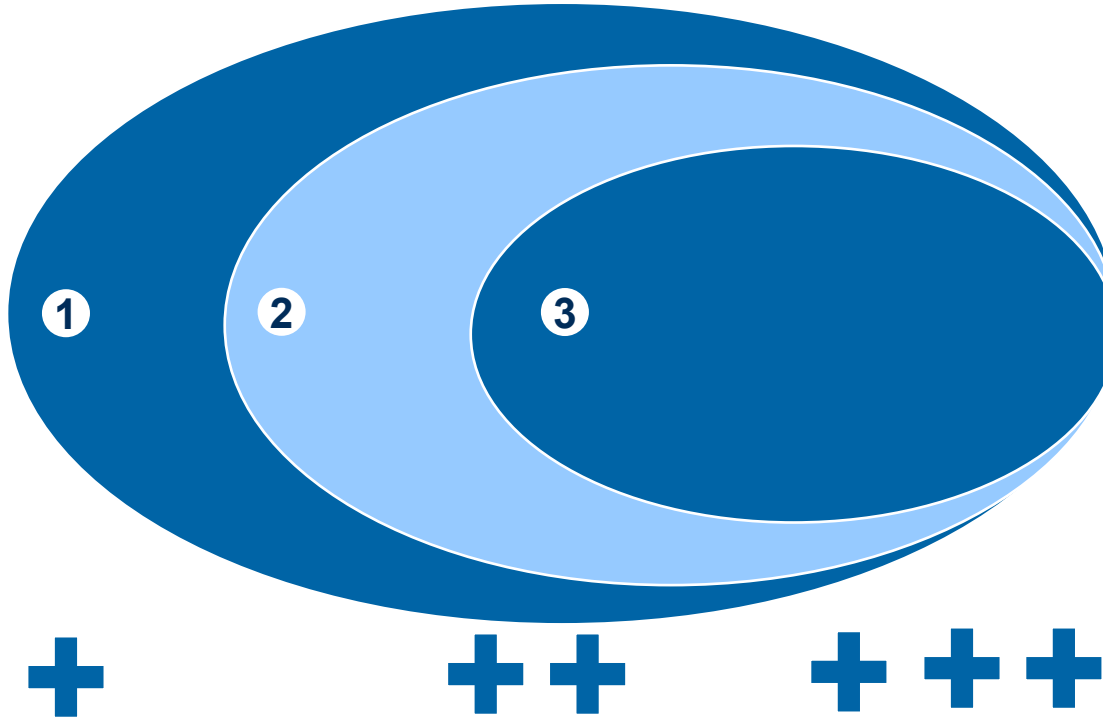


TOM = Technische / organisatorische Massnahmen

- ① Auslegungsrisiken
- ② Strategie & Rep Risk
- ③ Operationelle Risiken bei der Definition von TOM-Vorgaben
- ④ Operationelle Risiken bei der Operationalisierung von TOM im Change & Run

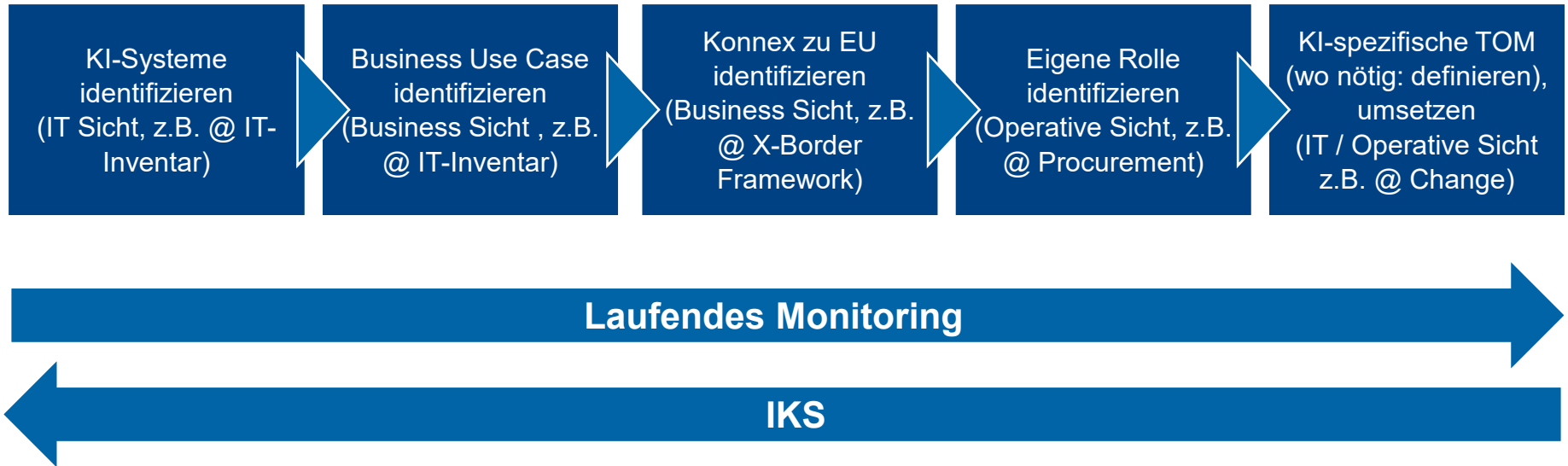
Governance!

Datenkategorien (stark vereinfacht)



- ① Daten ohne Personenbezug
(z.B. Statistische Daten → Geschäftsgeheimnisse)
- ② Daten mit Personenbezug
(z.B. Namen und Adressen → Datenschutzgesetze)
- ③ Berufsgeheimnisse
(z.B. Kundendaten → Bankkundengeheimnis)

Zusammenspiel Daten, Technologie, Business Use Cases & Governance am Beispiel EU AI Act



Key Takeaways

1. Datenrecht ist interdisziplinär und stark arbeitsteilig
2. Keine one-size-fits-all Lösungen
3. Eigene Organisation, Strategie, Governance, Target Operating Model, Business Model kennen
4. Abhängigkeiten kennen: Daten, Business Use Cases, Technologie & betroffene Population

SZW/RSDA 6/2024

685

Operationalisierung datenrechtlicher Normen in der Finanzindustrie

Michał Cichocki*

Data and technology are highly valued in the financial industry. With AI technology, their importance is also likely to grow significantly in the future. This is also increasingly preoccupying legislators and regulators, meaning that the already high level of regulation will continue

to increase. Despite a high degree of material variation, however, data law standards have similarities in their operationalization. This article takes a closer look at these facts from the perspective of a legal practitioner and presents possible solutions.

Inhaltsübersicht

- I. Ausgangslage
- II. Datenrechtliche Normen
 1. Definition
 2. Daten mit Personenbezug
 3. Daten ohne Personenbezug
 4. Zwischenfazit
- III. Kodifikation datenrechtlicher Normen
 1. Im Allgemeinen
 2. In der Finanzindustrie
 3. Zwischenfazit
- IV. Operationalisierung datenrechtlicher Normen im Allgemeinen
 1. Datenrechtliche Normen sowie Vorgaben für technische und organisatorische Massnahmen (TOM-Vorgaben)
 2. Datenschutz durch Technik
 3. Der risikobasierte Ansatz
 4. Zwischenfazit
- V. Operationalisierung datenrechtlicher Normen in der Finanzindustrie
 1. Branchenspezifische Eigenheiten
 2. Vorgehen am Beispiel der angemessenen Datensicherheit (Art. 8 Abs. 1 DSGVO)
 3. Zwischenfazit
- VI. Konklusion

I. Ausgangslage

In der Finanzindustrie haben Daten und Technologie traditionellerweise einen hohen Stellenwert. Durch die fortschreitende digitale Transformation¹, zum Beispiel bei der Automatisierung von Prozessen², der Personalisierung von Kundenerlebnissen und Dienstleistungen³, dem Einsatz von Blockchain, Kryptowährungen⁴, Open Banking und API-Ökosystemen⁵ sowie Cloud Computing⁶, hat der Umgang mit Daten nochmals stark zugenommen. Der Siegeszug von KI-Technologien wird dieser Entwicklung voraussichtlich einen weiteren Schub verleihen⁷.

Der zunehmende Umgang mit Daten beschäftigt nicht nur die Finanzindustrie an sich, sondern auch

¹ Vgl. z.B. <<https://www.swissbanking.ch/de/themen/digitalisierung-innovation-cyber-security>> oder <<https://www.digital.swiss/de/>>.

² Z.B. Robotic Process Automation (RPA) und künstliche Intelligenz (KI) werden zunehmend eingesetzt, um manuelle und repetitive Aufgaben z.B. in den Bereichen Transaktionsüberwachung zu automatisieren.

³ Z.B. durch personalisierte Ansprache auf elektronischen Kanälen oder durch noch stärker individualisierte Anlageempfehlungen.

Herzlichen Dank!

The opinions expressed in this presentation and on the slides are solely those of the presenter and not necessarily those of his employer or other any associated stakeholders. The presentation is informational only. It does not constitute legal or professional advice. You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation.

Vielen Dank.

