

Governance & Datenschutz bei Blockchain oder anderen Emerging technologies

Webinar @Weblaw - Blockchain

RA lic. iur Carmen De la Cruz

eidg. dipl. Wirtschaftsinformatikerin, Notarin

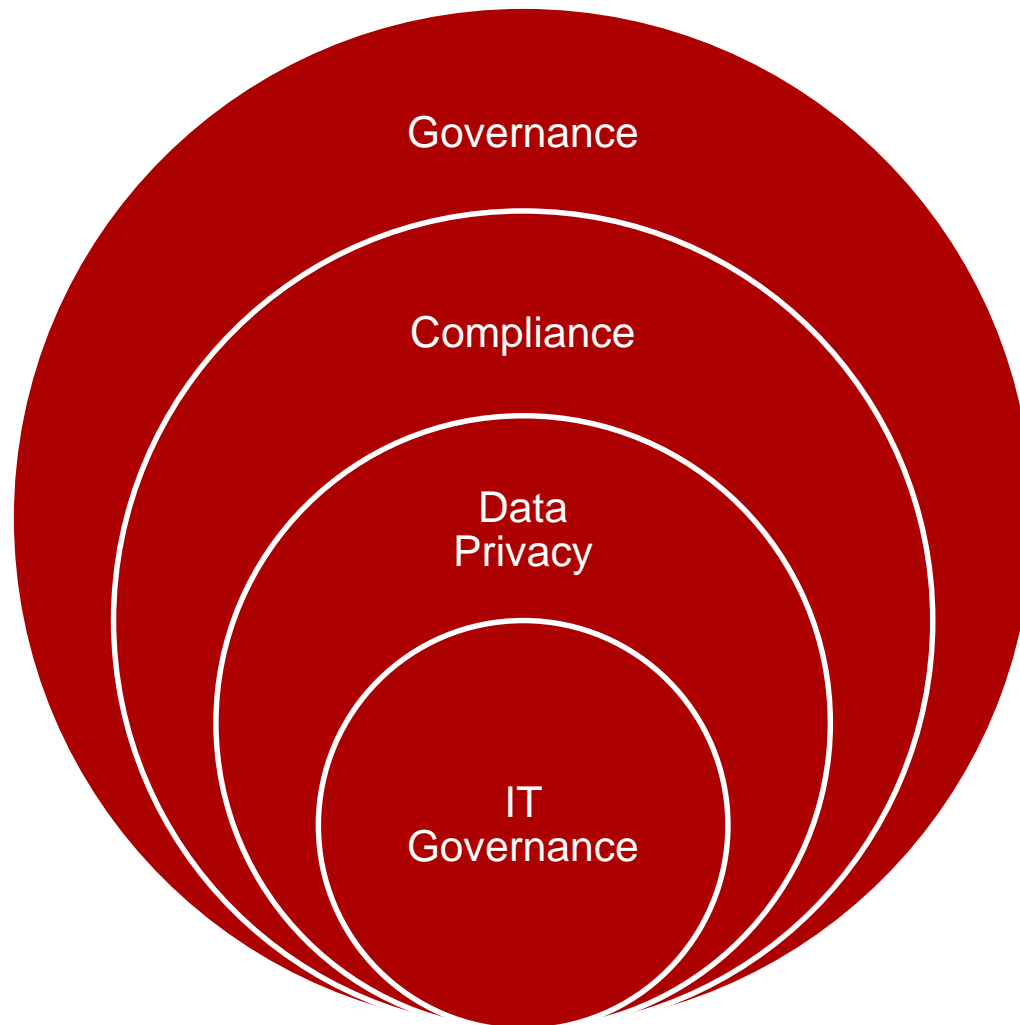
Punkte

1. Governance aus Unternehmens- und Projektsicht
2. Personenbezogene Daten – back to the roots?
3. Datenschutz und Blockchain
 - a) Datenschutz und Blockchain-Management als Teil der Governance
 - b) Datenschutz in und um die Blockchain
4. Emerging Technologies & Datenschutz
5. Summary

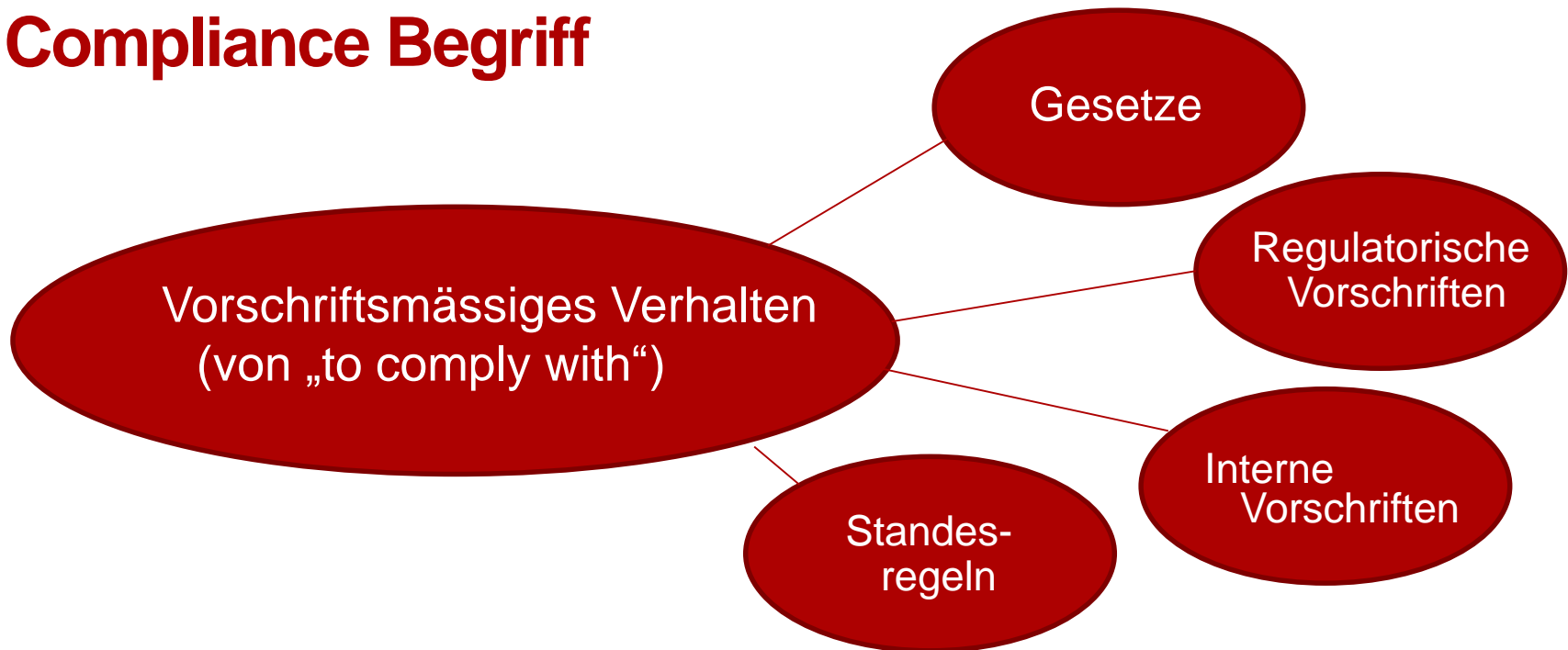
A photograph of a wooden bookshelf filled with numerous old, leather-bound books. The books are arranged in a row, showing their spines with various colors and decorative patterns. The lighting is warm, highlighting the texture of the leather and the grain of the wood.

Governance aus Unternehmens- und Projektsicht

Governance aus Unternehmenssicht



Compliance Begriff



- «Als Compliance gilt das Einhalten von gesetzlichen, regulatorischen und internen Vorschriften sowie die Beachtung von marktüblichen Standards und Standesregeln»
- (FINMA-RS 2008/24 «Interne Überwachung und Kontrolle», N 97)

→ Bedeutung von Compliance: **Regelkonformität**



Personenbezogene Daten – back to the roots?

Begriff der personenbezogenen Daten

- **Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.** Gemäss BGer(BGE 136 II 508 E.3) und EuGH (C-582/14) können auch (dynamische) IP-Adressen als personenbezogene Daten gelten, wenn der Empfänger für den Sender mit verhältnismässigem Aufwand eruierbar ist.
 - Statische IP-Adresse: wenn einem Rechner eine IP Adresse zugewiesen wird (sind fest und ändern sich nicht)
 - Dynamische IP-Adressen: der Benutzer wählt sich über einen Provider ins Internet ein, d.h. seinem PC wird bei jeder Verbindungsaufnahme neu irgendeine freie Adresse aus dem Pool des Providers zugewiesen. (sie können sich gelegentlich oder regelmässig ändern)

Fokus: Schutz der Personengezogenen Daten zur Verhinderung eines Schadens der betroffenen Person

Begriff der personenbezogenen Daten gemäss EU-Recht

Opinion 05/2014 – WP216

- **Pseudonymization**: merely reduces the linkability of a dataset with the original identity of a data subject - useful security measure.
- **Anonymization**: only useful if application / solution is properly engineered, anonymization process clearly set out, case by case solution -> based on «engineered systems»

Statement of the WP29 from April 11, 2018, on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU

Bisherige Ansätze basieren auf zentralen, veränderbaren Systemen

Personenbezogene Daten in der und um die Blockchain

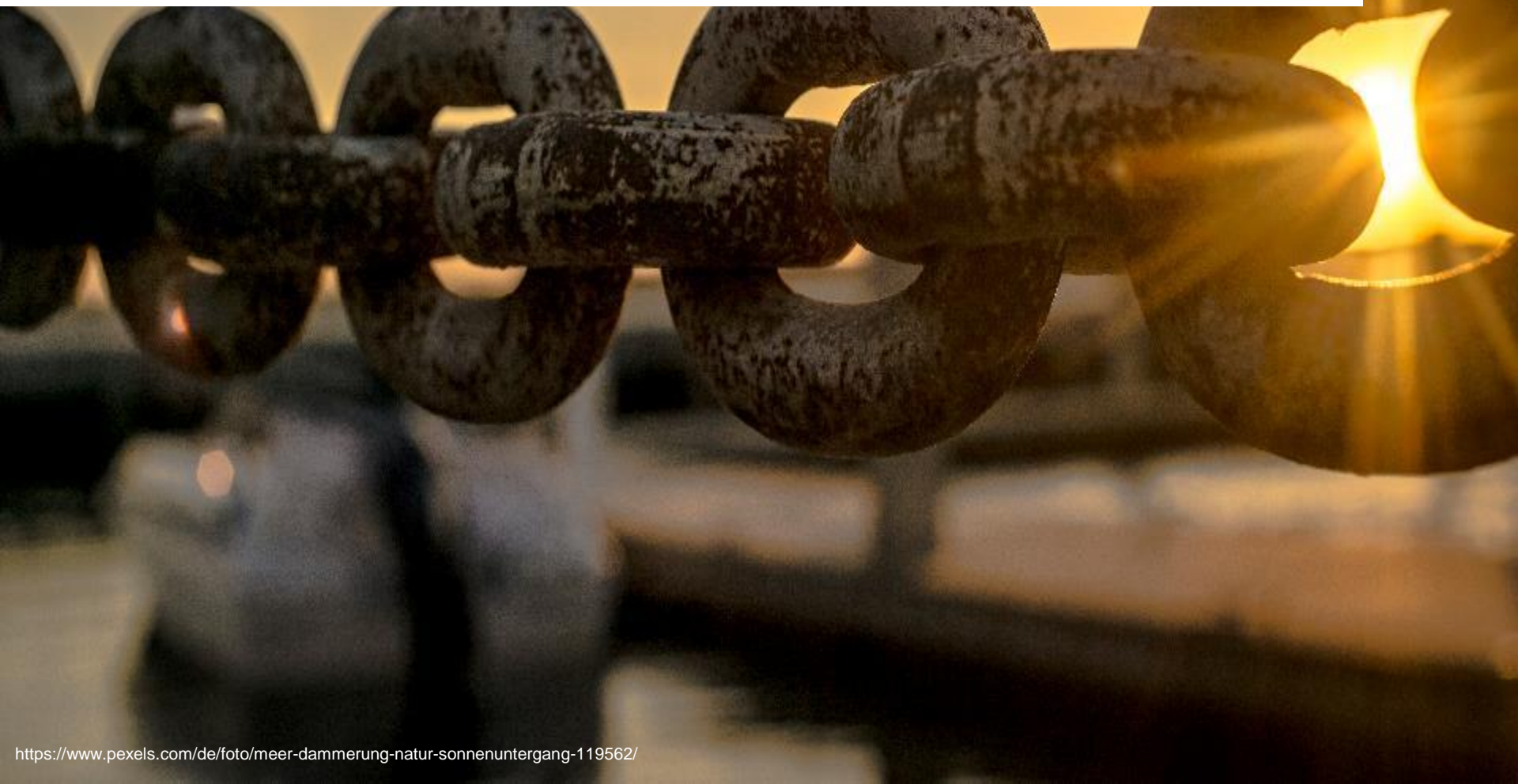
Mögliche personenbezogene Daten *im Zusammenhang mit der* Blockchain

- Public / Private Keys
- **Hashwert**
- Schlüssel des Wallets
- IP-Adresse
- Tokens
- usw.

Mögliche personenbezogene Daten *in der* Blockchain:

- Inhalt von Dokumenten, Transaktionen, etc.
- Besonders schützenswerte Perosnendaten (biometrische Daten etc.)
– je nach Leistung
- IP-Adresse(n)

Datenschutz und Blockchain



Blockchain trifft Datenschutz

Die betroffenen Personen haben die folgenden Rechte (Art. 12 ff. DSGVO):

- Das Recht auf Information über die Erhebung und Verwendung ihrer personenbezogenen Daten
- Das Recht auf Zugang zu personenbezogenen Daten und Zusatzinformationen
- Das Recht auf Berichtigung unrichtiger personenbezogener Daten oder Ergänzung, wenn diese unvollständig sind
- **Das Recht auf Löschung (das Recht auf Vergessen)**
- Das Recht, die Verarbeitung unter bestimmten Umständen einzuschränken
- Das Recht auf Datenübertragbarkeit, das es der betroffenen Person ermöglicht, ihre personenbezogenen Daten für ihre eigenen Zwecke über verschiedene Dienste hinweg zu erhalten und wiederzuverwenden
- Das Recht, der Verarbeitung unter bestimmten Umständen zu widersprechen
- **Das Recht, die Einwilligung jederzeit zu widerrufen.**

Blockchain & DSGVO – Löschung / Erasure

Recht auf Löschung bedeutet

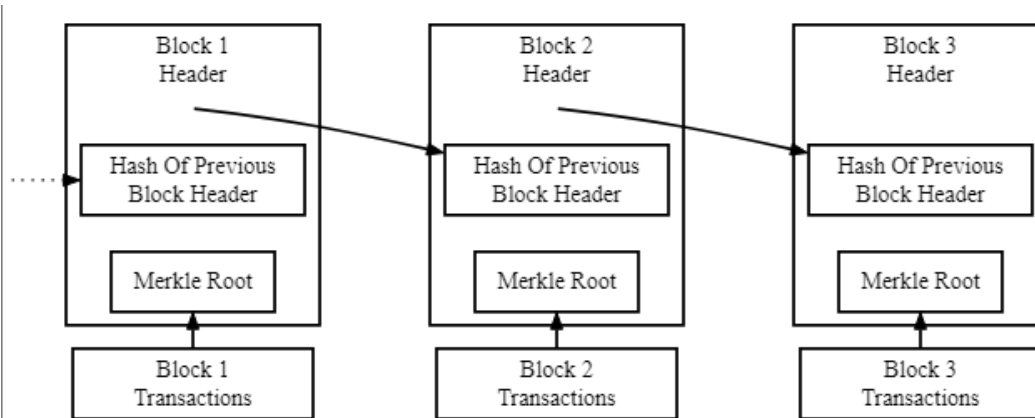
- *in extremis* sollen alle Daten der betroffenen Person gelöscht werden können
 - In der Praxis generell kaum umsetzbar,
 - In der Blockchain nicht umsetzbar
- Andere Interpretationen: Löschung des / der Links / der Verknüpfung zwischen der betroffenen Person und den personenbezogene Daten oder der Ersatz von personenbezogenen Daten (z.B. Datenkombination)
 - Auflösung der Beziehung zwischen der betroffenen Person und personenbezogenen Daten (generell umsetzbar(er))



a. Datenschutz und Blockchain-Management
als Teil der Governance

Blockchain: Begriff

- Eine Blockchain ist eine kontinuierlich erweiterbare Liste von Datensätzen (Blöcken), die mittels kryptographischer Verfahren miteinander verkettet sind.
- Jeder Block enthält dabei typischerweise einen kryptographisch sicheren Hash (Streuwert) des vorhergehenden Blocks, einen Zeitstempel und Transaktionsdaten.
- Technische Basis für Kryptowährungen



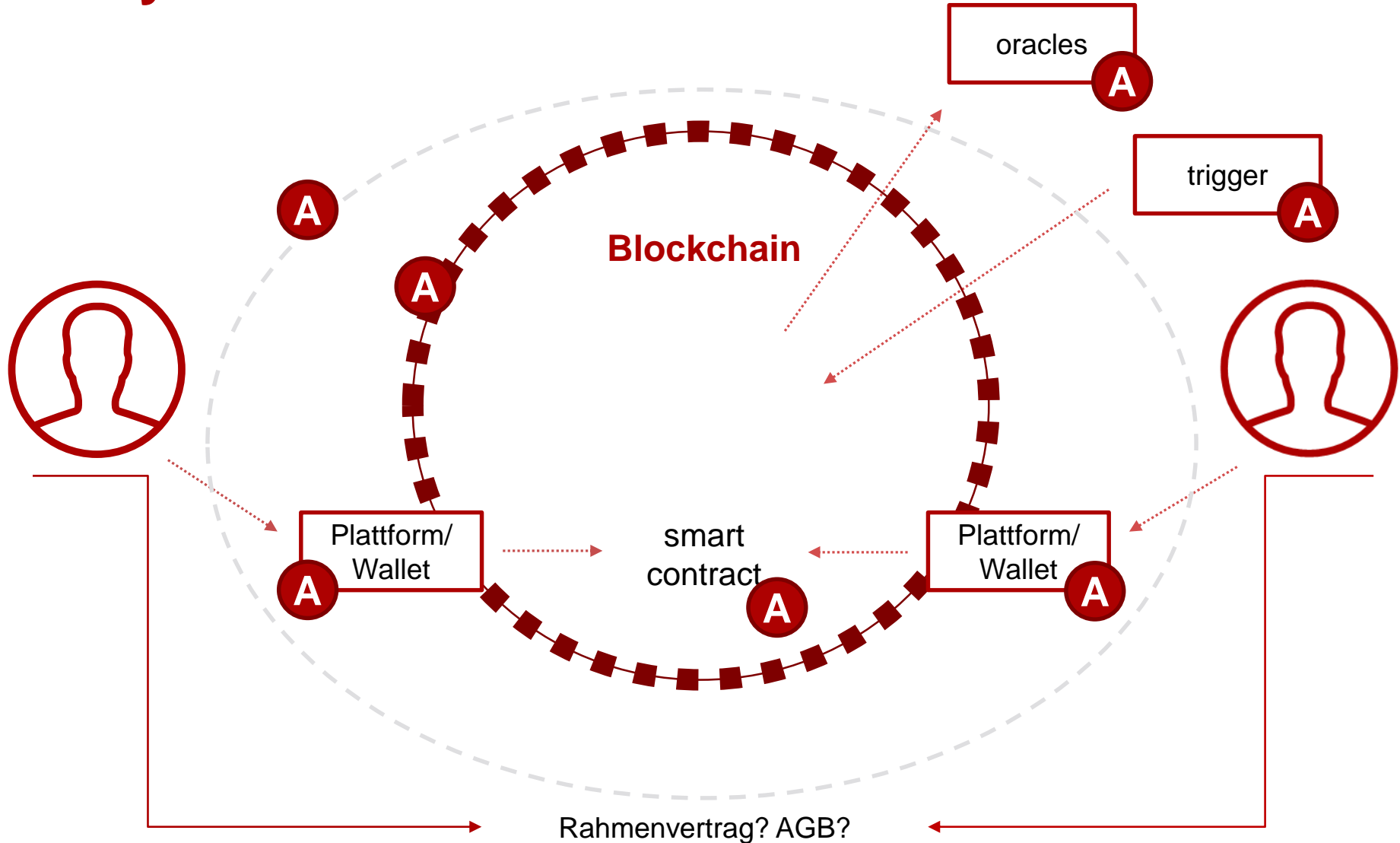
Simplified Bitcoin Block Chain

Governance aus Sicht der Blockchain

Governance bezieht sich hier auf die Prozesse, Regeln und Verfahren, die man bei der Aufrechterhaltung des Protokolls beachten muss.

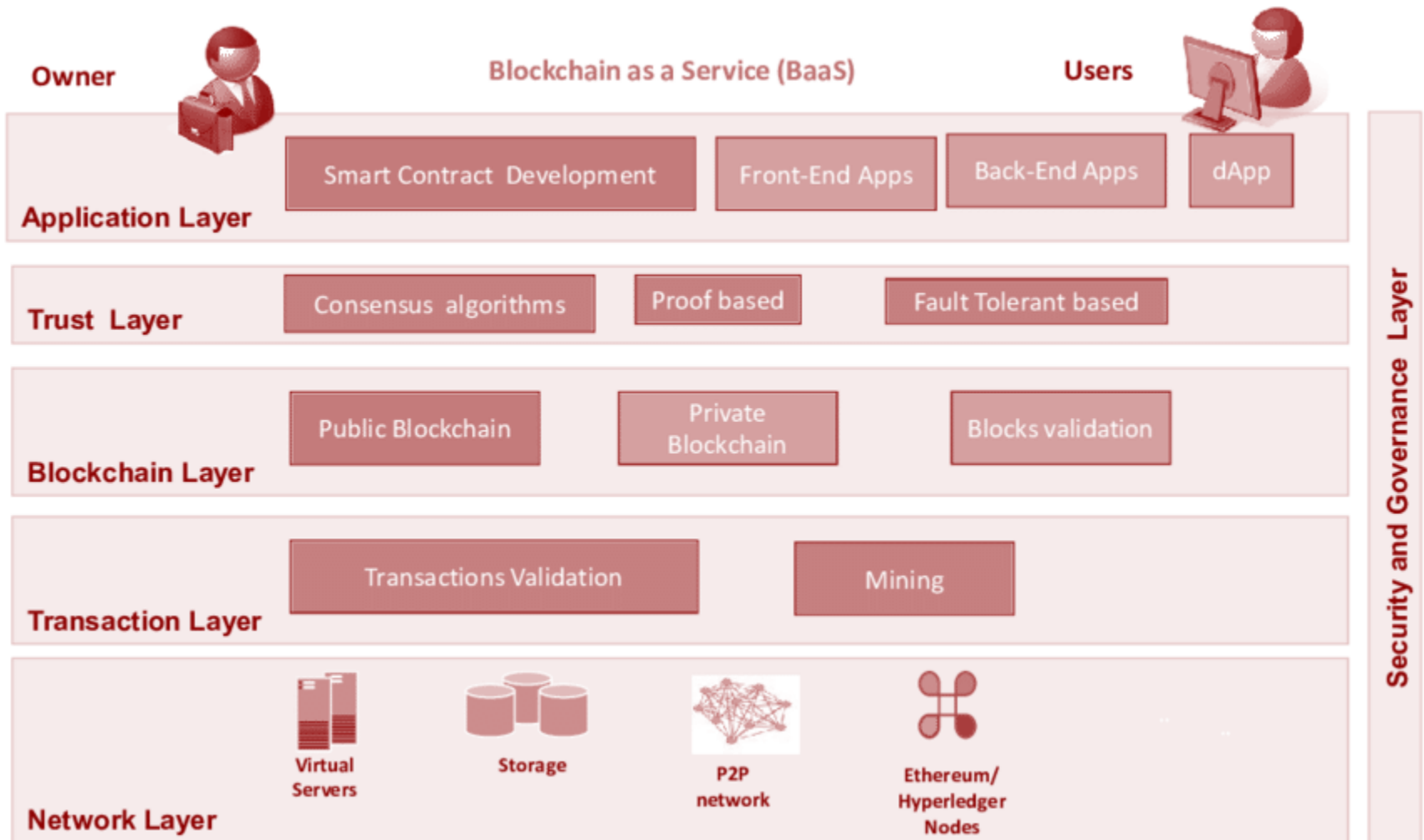
- Interne Governance
 - Gesetzgebung / Ordnungsrahmen durch die Inhaber, Nutzer oder Beteiligten eines Systems
 - Zweck ist die Wahrung der privaten Interessen
- Externe Governance
 - Regulierung zur Regelerstellung durch eine externe Behörde
 - Zweck ist die Wahrung der Interessen der Öffentlichkeit
- Governance in der Blockchain
 - Code
 - Smart Contracts
- Governance zwischen den Playern der Blockchain
 - Auswahl der Partner
 - Regelungen
 - Code

Players in und um die Blockchain



A = Anbieter

Governance & Blockchain



A blurred photograph of a crowd of people walking in a modern, brightly lit space. The walls and floor are covered in glowing white binary code (0s and 1s) projections, creating a digital atmosphere. The people are out of focus, suggesting movement and a busy environment.

b. Datenschutz in und um die Blockchain

Blockchain & DSGVO – Methoden

Anonymisierung

- Keine Rückschlussmöglichkeit zwischen einer natürlichen Person und Daten ermöglichen

Pseudonymisierung (Art. 4 Ziff. 5 DSGVO)

- Kontext zwischen natürlicher Person und Daten weitestgehend unterbinden, d.h. Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten **ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können**
 - zusätzlichen Informationen müssen **gesondert aufbewahrt** werden und
 - unterliegen **technischen und organisatorischen Massnahmen**, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden

Blockchain & DSGVO – online und offline (1)

Lösungsansatz 1

Personenbezogene Daten offline und nicht in der Blockchain speichern

Dies bedingt

- Enge Zusammenarbeit zwischen IT / Engineers & Legal
- Berücksichtigung zukünftiger Szenarien / technische Weiterentwicklungen
- Verschlüsselung

Blockchain & DSGVO – online und offline (2)

Lösungsansatz 2

Auslegung von «Löschung / Erasure» gemäss DSGVO

- Aufhebung der Relation zwischen Personendatum (z.B. Schlüssel) und dem verschlüsselten Asset
→ nachträgliche Anonymisierung

Nachteil:

- gemäss Definition der WP 29 (Guidelines 216) sind Daten nur dann anonym, wenn sie nicht mehr rückverfolgbar sind
- Da der Schlüssel theoretisch noch verfügbar sein kann, handelt es sich hier um eine Pseudonymisierung und keine Anonymisierung gemäss WP29 (Guidelines 216)

Blockchain & DSGVO – online und offline (3)

Lösungsansatz 3

Antrag auf Ausnahme / «Carve-out» von Blockchain von den Vorgaben der DSGVO

- Kaum denk- oder vertretbar
- Aber: Lösungsansatz 2 ist ein Teil von Lösungsansatz 3, in dem die DSGVO interpretiert und die Auslegung von Anonymisierung und Pseudonymisierung im Sinne der Blockchain-Technologie erfolgt

Blockchain & DSGVO – online und offline (4)

Lösungsansatz 4

Verschlüsselter Layer auf der Blockchain (peer-to-peer)

Personenbezogene Daten werden nur im verschlüsselten Layer ausgetauscht
(mit API auf die Blockchain)

Ähnlich wie Lösungsansatz 1 (hier mit peer-to-peer Verschlüsselungslayer)

Vorteil:

Nutzung der Blockchain-Technologie ohne (mit beschränktem) DSGVO-Impact

Nachteil:

Sorgfältige Strukturierung und Programmierung nötig

Mit dem Technologiewandel können u.U. später sich in der Blockchain befindliche Daten zu personenbezogenen Daten mutieren



Emerging Technologies & Datenschutz

Artificial Intelligence & Machine Learning

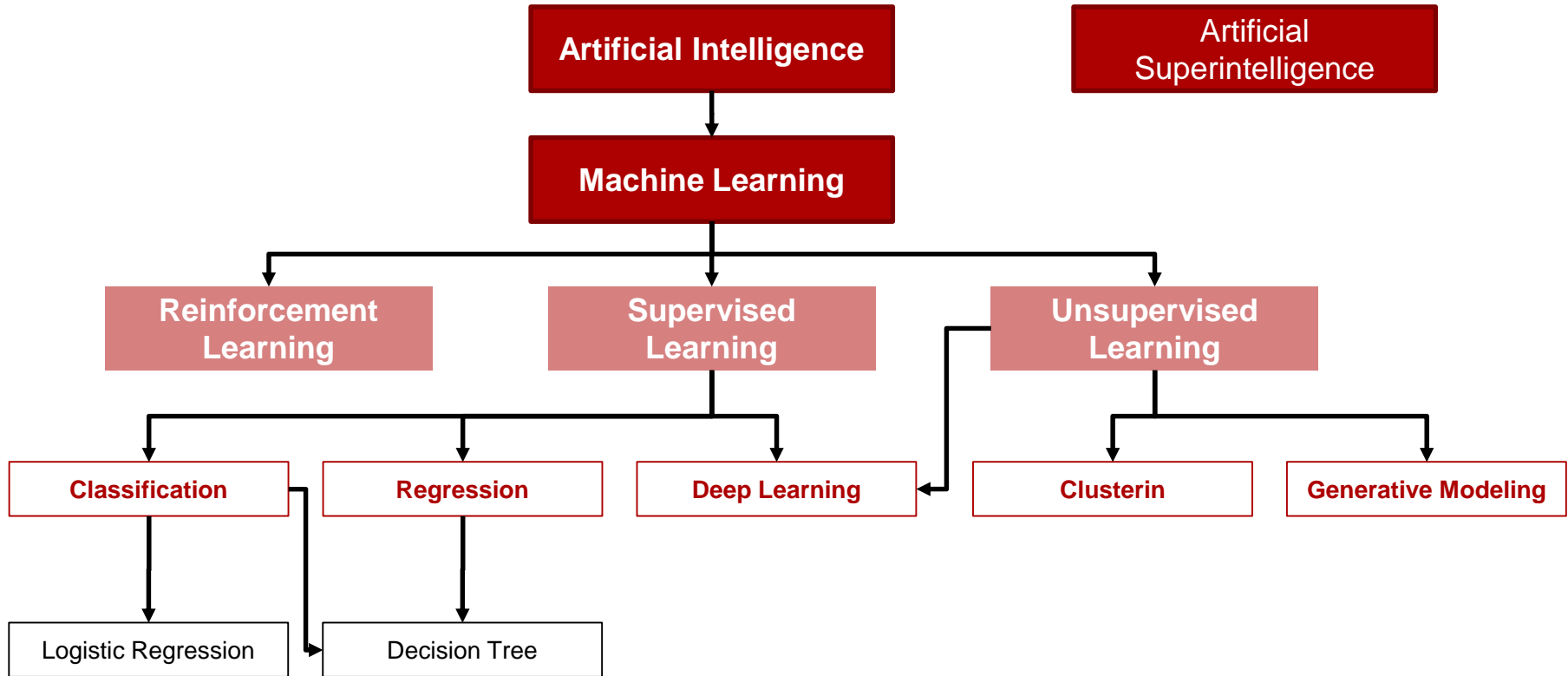
Artificial Intelligence

- Weak AI: Behandlung konkreter Anwendungsprobleme durch bloße Rechnerleistung ohne die Handlung zu verstehen.
Bspw. Spracherkennung, Navigationssysteme, Schachcomputer etc.
→ Im Anwaltsberuf insbesondere von diesem Gebrauch machen.
- Strong AI: alle Charakteristiken menschlicher Intelligenz (Bewusstsein, Empfindungsvermögen, argumentieren, komplexe Ideen verstehen und auch daraus lernen etc.)
→ nicht nur reaktiv, sondern auch aus eigenem Antrieb
bisher nicht erreicht

Machine Learning

Generierung von Wissen aus Erfahrung, beruhend auf Wahrscheinlichkeit und Statistik. Mittels Algorithmen aus enormen Daten-Inputs.

Terminologie



Artificial Intelligence und Datenschutz

Datenminimierung vs. Big Data

➤ AI benötigt viele Daten um zu lernen (auch personenbezogene Daten)

Interessante Daten für AI

- Stammdaten: Alter, Ausbildung, Wohnort, ...
- Äussere Merkmale: Rasse, Haarfarbe, Augenfarbe, Gesundheitszustand, ...
- Innere Merkmale: Herkunft, Religion, politische Gesinnung, ...



Beispiele:

- E-Commerce Plattform möchte mit AI bessere Kaufempfehlungen vorschlagen
- Bank will Risiko bei Vergabe von Krediten beurteilen
- Spital will automatisierte Erkennung von Krankheitsbildern

Artificial Intelligence – Risiken

Die AI wird heute in gewissen Sektoren u.a. folgendermassen genutzt:

- Mittels Algorithmen und Machine Learning wird benutzerspezifisch Werbung aufgeschaltet
- Bei Anstellungsprozessen wird die AI zur Auswertung der CV's und somit zur Auswahl von möglichen Kandidaten verwendet

Art. 22 Abs. 1 DSGVO: «Die betroffene Person hat das Recht, **nicht einer ausschließlich auf einer automatisierten Verarbeitung** – einschließlich Profiling – beruhenden Entscheidung **unterworfen zu werden**, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.»

- Ausnahmen
 - Recht zu wissen, wie die Informationen verarbeitet wurden
 - Recht zu wissen, wie Entscheidungen gefällt wurden

Artificial Intelligence und Datenschutz

Lösungsansätze

- Anonymisierte Daten
- Synthetische Daten
 - Google Car = 3 Millionen simulierte Meilen pro Tag
- dumb-in / clever-out
- 2-Phasen-Verarbeitung

Artificial Intelligence und Datenschutz

Offene Fragen, die es zu klären gilt:

- Wie kann der Datenschutz bei AI gewährleistet werden?
- Was passiert, wenn der Bezug zur Datenbearbeitung aufgrund fortgeschrittener AI-Technologie verloren geht?
- Was soll überhaupt noch als personenbezogene Daten definiert werden?
- Ist eine Begriffsanpassung für die «Anonymisierung» notwendig?
- Wie sieht es mit der Haftung von AI aus?

Zurückhaltung ist geboten

Sorgfalt mit neuen Technologien vs. rasanter Fortschritt & Entwicklung

Lösungsansätze der Blockchain – Analogie?

Lösungsansatz 1

Personenbezogene Daten offline und durch nicht die AI speichern lassen

- Starke Einschränkung der AI mit Gefahr, dass der Nutzen & Sinn dahinter verloren geht

Lösungsansatz 2

Auslegung von «Löschung / Erasure» gemäss DSGVO

- riskant, da sich Löschung bei AI schwierig darstellt (andauernder und aufbauender Lernprozess)

Lösungsansatz 3

Antrag auf Ausnahme / «Carve-out» der AI von den Vorgaben der DSGVO

- Nicht empfehlenswert, da nicht haltbar

Lösungsansätze der Blockchain – Analogie?

Lösungsansatz 4

Verschlüsselter Layer in der AI (peer-to-peer)

Personenbezogene Daten werden nur im verschlüsselten Layer ausgetauscht

Ähnlich wie Lösungsansatz 1 (hier mit peer-to-peer Verschlüsselungslayer)

Nachteil:

Sorgfältige Strukturierung und Programmierung nötig

Mit dem Technologiewandel könnte u.U. später die Kontrolle über die lernende AI verloren gehen

Resumée

Zusammenfassung Note Away

Schlussfolgerung

Take Bottom End

Fazit

Summary

- Compliance als Weg zur Regelkonformität
- Personenbezogene Daten im Wandel?
- Blockchain und Löschung – ein Ding der Unmöglichkeit?
- Governance in der Blockchain
- Datenschutz in und um die Blockchain – Methoden und Lösungsansätze
- AI & Machine Learning
 - Problematik der Leitidee Datenminimierung vs. Big Data
 - Lösungsansätze der Blockchain als Analogie?
 - Risiken der automatisierten Entscheidungen im Einzelfall

de la cruz beranek

RECHTSANWÄLTE ■ ATTORNEYS AT LAW



de la cruz beranek Rechtsanwälte AG
Industriestrasse 7
6300 Zug
Tel. 041 710 28 50
delacruz@delacruzberanek.com
www.delacruzberanek.com

Alle Rechte an dieser Präsentation bleiben vorbehalten.
Jede Verwertung dieser Präsentation ist ohne Einwilligung der de la cruz beranek Rechtsanwälte AG unzulässig. Dies gilt insbesondere für Vervielfältigungen (grafisch, technisch, elektronisch und/oder digital, einschliesslich Fotokopie, down- und uploading), Übersetzungen und das Speichern und Bearbeiten in und mit elektronischen Systemen. Jede Verwertung in den genannten oder in anderen als den gesetzlich zugelassenen Fällen bedarf der vorherigen schriftlichen Einwilligung der de la cruz beranek Rechtsanwälte AG.