Informationssicherheit und Compliance

Aktuelle Entwicklungen und
Brennpunkte in regulierten Sektoren

Thomas Steiner

LAUX LAWYERS AG
ZURICH | BASEL

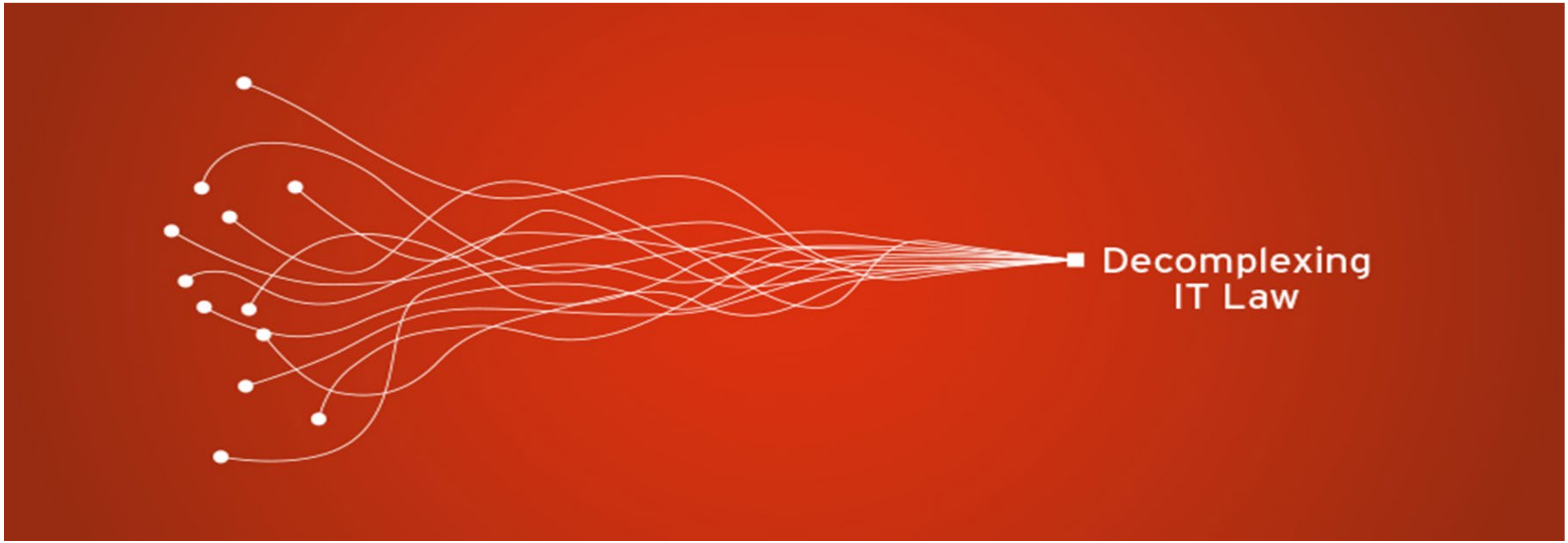
Lucerne Law & IT Summit
Universität Luzern
4. Mai 2021

Agenda

- Informationssicherheit – Datensicherheit – Datenschutz
  - Begriffsklärung und Grundsätze
  - Fragmentierter Rechtsrahmen
  - Datensicherheit gemäss neuem DSG
- Aktuelle Entwicklungen und Brennpunkte in regulierten Sektoren
  - Kritische Infrastrukturen: Meldepflicht bei Cyberangriffen
  - Banken: Informationssicherheit im Fokus der Finanzmarktaufsicht
  - Gesundheitswesen: Informationssicherheit beim Elektronischen Patientendossier (EPD)
- Informationssicherheit und Compliance
  - Informationssicherheit als Organ- und Organisationsverantwortung
  - Umsetzung im digitalisierten Unternehmen

Informationssicherheit – Datensicherheit – Datenschutz

LAUX LAWYERS AG
ZURICH | BASEL



Informationssicherheit – Datensicherheit – Datenschutz

LAUX LAWYERS AG
ZURICH | BASEL

Informationssicherheit

Information (mit/ohne Personenbezug), einschliesslich Kundendaten (Individuen und Unternehmen), Fabrikations-, Geschäfts- und Betriebsgeheimnissen, nicht patentierter Erfindungen und Know-how

Zuverlässigkeit **Verbindlichkeit** **Zurechenbarkeit**

Funktionssicherheit (Safety) **Authentizität**

- Informationssicherheitsgesetz (Bund)
- PrSG
- Strafrecht (StGB, DSG, BankG, KEG, EPDG)
- Gesellschaftsrecht (Sorgfaltspflicht des VR/der GL)
- Sektorspezifisch Reg. (Banken, Energie, Gesundheit)
- Leitlinien und Empfehlungen von Aufsichtsbehörden
- Standards
- Vertrag

Vertraulichkeit
Integrität
Verfügbarkeit

Resilienz

Datenschutz

Schutz der Persönlichkeit vor übermässiger und unfairer Bearbeitung von ***Personendaten***

Zweckbindung **Treu und Glauben / Transparenz**

Richtigkeit **Rechtmässigkeit**

Speicherbegrenzung **Datenminimierung**

- Persönlichkeitsrecht (Art. 28 ZGB)
- (Neues) DSG
- Strafrecht (StGB, DSG)
- Sektorsp. Reg. (Banken, Energie, Gesundheit)
- Leitlinien und Empfehlungen
- Standards
- Vertrag

Neues DSG im Überblick: Anforderungen

LAUX LAWYERS AG
ZURICH | BASEL

Bundesorgane: Rechtsgrundlage
(**Private**: Rechtfertigungsgrund, bei Persönlichkeitsverletzung!)

Grundsätze
(insbes. Zweckbindung, Transparenz, Datensparsamkeit, Speicherbegrenzung und Sicherheit)

Transparenz
(Informationspflicht)

Betroffenenrechte
(insbesondere auf Auskunft, Berichtigung und Löschung)

Dokumentationspflichten / Governance

Anforderungen an Outsourcing
(Auftragsbearbeitung)

Internat. Datenübermittlung
(über Schweizer Grenze)

Automatische Eintscheide im Einzelfall, einschliesslich Profiling

Datenschutz-Folgeabschätzung / Privacy-by-Design und Privacy-by-Default

Data-Breach-Meldepflicht

Datensicherheit

Aufsicht / Durchsetzung

Datensicherheit gemäss revDSG (1|2)

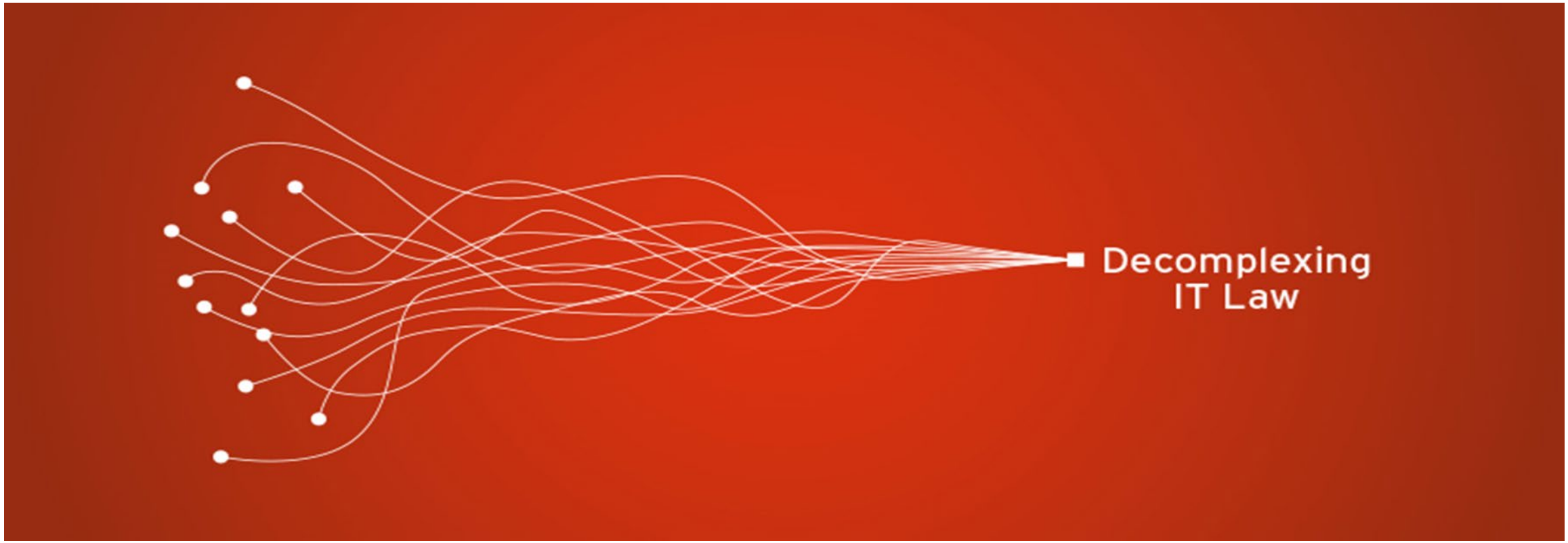
- Schutzziel: Vertraulichkeit, Integrität und Verfügbarkeit der Personendaten
  - **Risikobasierter Ansatz**: «dem Risiko angemessene Datensicherheit» *(Art. 8 Abs. 1 revDSG)*
  - **Technische Massnahmen**: Pseudonymisierung, Verschlüsselung, Authentifizierungsverfahren, Zugangs- und Zugriffsbeschränkungen, Zugriffs- und Änderungslogs
  - **Organisatorische Massnahmen**: Schulungen, Zugriffskonzepte, Backup-Konzepte, Weisungen, Verfahren zur regelmässigen Überprüfung der Wirksamkeit und Geeignetheit der Massnahmen
  - **Mindestanforderungen an Datensicherheit**: gemäss revVDSG *(aktuell Art. 8–9 VDSG)*
  - **Neu strafbar:** Vorsätzliche Nichteinhaltung der Mindestanforderungen an die Datensicherheit gemäss revVDSG *(Art. 61 lit. c revDSG)*

Datensicherheit gemäss revDSG (2|2)

- Meldung von Datensicherheits-Verletzungen (Personal Data Breaches)
  - **Verletzungen der Datensicherheit**: eine Verletzung der Sicherheit, die dazu führt, dass *Personendaten* unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden *(Art. 5 lit. h revDSG)*
  - **Meldepflicht des Verantwortlichen**
    - an *EDÖB* («so rasch als möglich») bei voraussichtlich hohem Risiko *(Art. 24 Abs. 1 revDSG)*
    - Meldung an *betroffene Personen*, wenn es deren Schutz erfordert oder der EDÖB dies verlangt *(Art. 24 Abs. 4–5 revDSG)*; Ausnahmen *(Art. 24 Abs. 5 i.V.m. Art. 26 Abs. 1 lit. b und 2 lit. b revDSG)*
  - **Meldepflicht des Auftragsbearbeiters**: an *Verantwortlichen* «so rasch als möglich» *(Art. 24 Abs. 3 revDSG)*

Aktuelle Entwicklungen und Brennpunkte in regulierten Sektoren

LAUX LAWYERS AG
ZURICH | BASEL



Kritische Infrastrukturen: Meldepflicht bei Cyberangriffen und Sicherheitsvorfällen

- Einführung einer Meldepflicht bei Cyberangriffen
  - 13.12.2019: Prüfauftrag des Bundesrats *(BR, Bericht, Postulat 17.3475 Graf-Litscher)*
  - 11.12.2020: Beschluss des Bundesrats: EFD erarbeitet Vernehmlassungsvorlage bis Ende 2021
- Eckwerte der Meldepflicht gemäss Bundesrat
  - Meldepflicht für Betreiber kritischer Infrastrukturen (insb. Energieversorgung, Telekommunikation, Finanz- und Versicherungswesen) bei Cyberangriffen und Entdeckung von Sicherheitslücken
  - Zentrale Meldestelle und Frühwarnsystem
  - Modalitäten: sektorspezifische Besonderheiten berücksichtigen, Abstimmung auf bestehende sektorielle und datenschutzrechtliche Meldepflichten

Banken (1|4) – Informationssicherheit im Fokus der Finanzmarktaufsicht

- Cyberrisiko als Toprisiko für Finanzplatz Schweiz
  - Risiko von Cyber-Attacken erhöht – namentlich «in besonderen Stress-Situationen, wie die aktuelle COVID 19-Pandemie» *(FINMA-Aufsichtsmitteilung 05/2020, S. 2)*
  - Risiko von Cyber-Attacken «höher als im Jahr davor» *(FINMA-Jahresbericht 2020, S. 35–36)* – «eines der sieben Toprisiken für den Finanzplatz Schweiz» *(FINMA-Risikomonitor 2020, S. 11–12)*
- FINMA verstärkt Aufsichtstätigkeit zu Informationssicherheit und Cyber-Attacken
  - Vor-Ort-Kontrollen der FINMA
  - Aufsichtsprüfung durch Prüfgesellschaften
  - Sensibilisierung der Institute auf Umgang mit Cyberrisiken

Banken (2|4) – Meldepflicht bei Cyber-Attacken

- FINMA-Aufsichtsmitteilung 05/2020 **Meldepflicht bei Cyber-Attacken**
  - **Meldepflicht** für Vorkommnisse – beispielsweise Cyber-Attacken, die für die Aufsicht von wesentlicher Bedeutung sind *(Art. 29 Abs. 2 FINMAG)*
  - Wesentlich: Cyber-Attacken auf **kritische Funktionen** beaufsichtigter Institute, einschliesslich Zahlungsverkehr, Bargeldversorgung und Börsenhandel *(vgl. Art. 14 FinfraG)*
- Unverzügliche Meldung an FINMA bei Cyber-Attacken auf kritische Funktionen
  - Vororientierung der FINMA innerhalb von **24 Stunden** durch *Key-Account Manager*
  - Eigentliche Meldung innert 72 Stunden über webbasierte Plattform der FINMA
  - Abschliessender Ursachenbericht wenn Schweregrad “Hoch” oder “Schwerwiegend”

Banken (3|4) – Risikomanagement (CID-Vertraulichkeitsvorfälle)

- Prozess für die Identifikation von und Reaktion auf Verletzungen der Vertraulichkeit von identifizierenden Bankkundendaten (CID-Vertraulichkeitsvorfälle)
- interne Berichterstattung zu Risiken von CID-Vertraulichkeitsvorfällen
- klare Strategie für die interne Meldung von CID-Vertraulichkeitsvorfällen
- Klare Kommunikationsstrategie betreffend schwerwiegender CID-Vertraulichkeitsvorfälle
- Laufende Verfeinerung des Rahmenkonzepts zur Sicherstellung der CID-Vertraulichkeit

(Art. 47 BankG; Art. 12 Abs. 2 BankV / 2019 revidiertes FINMA-Rundschreiben 2008/21 Operationelle Risiken – Banken)

Banken (4|4) – Risikomanagement (Cyber-Attacken)

- **Cyber-Risikomanagement** mit klar definierten Aufgaben, Rollen und Verantwortlichkeiten:
  - Identifikation möglicher institutionsspezifischer Bedrohungen durch Cyber-Attacken
  - Schutz der Geschäftsprozesse und der Technologieinfrastruktur vor Cyber-Attacken
  - Zeitnahe Erkennung und Aufzeichnung von Cyber-Attacken auf Basis eines Prozesses
  - Reaktion auf Cyber-Attacken durch zeitnahe und gezielte Massnahmen
  - Sicherstellung einer zeitnahen Wiederherstellung des normalen Geschäftsbetriebs nach Cyber-Attacken
- Erfordert regelmässige Verwundbarkeitsanalyse und Durchdringungstests

(Art. 47 BankG; Art. 12 Abs. 2 BankV / 2019 revidiertes FINMA-Rundschreiben 2008/21 Operationelle Risiken – Banken)

Gesundheitswesen (1|2) – EPD

- Verspätete Einführung
  - Spitäler und Pflegeheime arbeiten an Umsetzung
  - Erste Stammgemeinschaften haben technische Plattform erstellt (warten auf Zertifizierung)
  - Einführungstermin (15.04.2020) aufgrund komplexer Zertifizierungsverfahren verpasst
  - eine von zwei Zertifizierungsstellen wartet auf Akkreditierung durch Akkreditierungsstelle
- Komplexe Anforderungen an Informationssicherheit
  - Detaillierte technische und organisatorische Zertifizierungsvoraussetzungen für (Stamm-) Gemeinschaften («TOZ»; Anhang 2 der EPDV-EDI) seit Inkrafttreten 2017 mehrfach revidiert
  - (Gescheiterter?) Versuch, «Stand der Technik» mit mehr als 100 Anforderungen zu definieren

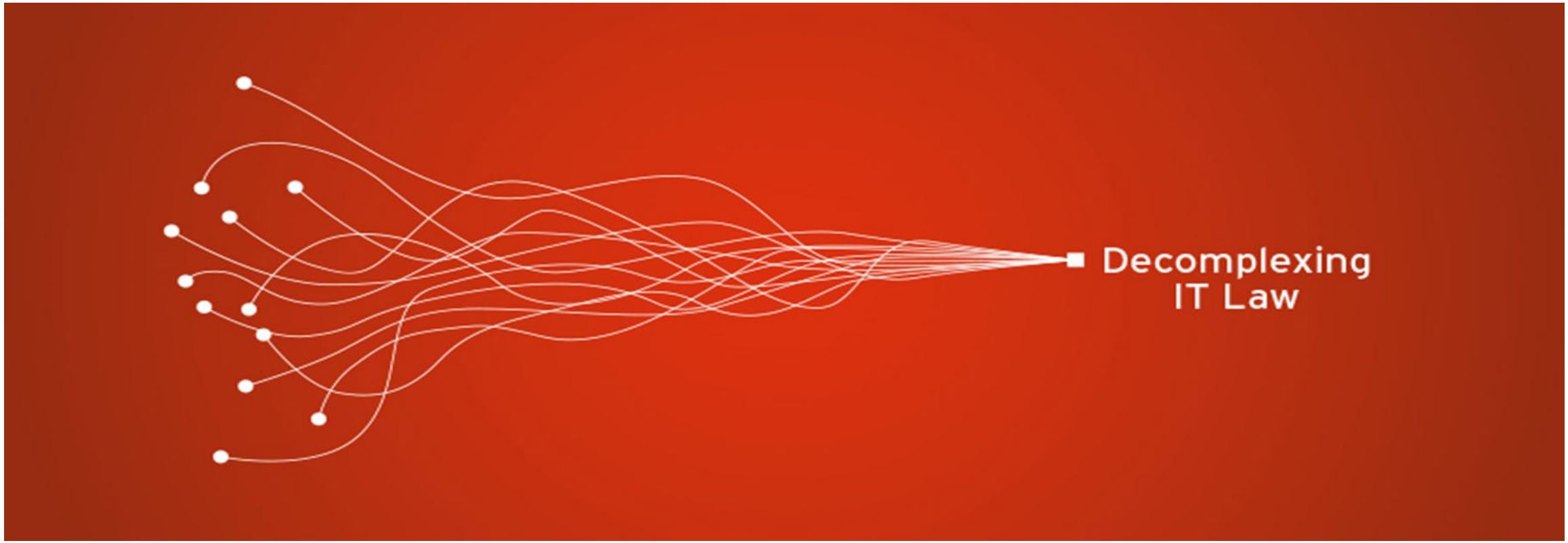
Gesundheitswesen (2|2) – EPD

- Anwendungsebene (Auswahl)
  - Sichere Authentifizierung aller Benutzer
  - Protokollierung von Zugriffen
- Technischen Systeme und Netzwerke (Auswahl)
  - Anomalie-Erkennung und automatische Alarmierung
  - Verschlüsselte Datenaufbewahrung, sichere Kommunikationsverbindungen
- Organisation (Auswahl)
  - Kontinuierliches Sicherheitsmanagement, Meldepflicht bei Sicherheitsvorfällen
  - Anforderungen an Auswahl und Instruktion von Benutzern und administrativem Personal

(GDK, Factsheet: Top 10 Sicherheitsmassnahmen im EPD, e-health-suisse.ch; Anhang 2 der EPDV-EDI, www.ehealth.admin.ch)

Informationssicherheit und Compliance

LAUX LAWYERS AG
ZURICH | BASEL



Informationssicherheit als Organ- und Organisationsverantwortung (1|2)

- Oberleitung und Festlegung der Organisation sind unübertragbare Aufgaben des Verwaltungsrats
- Angemessenes Risikomanagement ist wesentlicher Bestandteil der Organ- und Organisationsverantwortung
  - Bedrohung informationstechnischer Systeme identifizieren, begrenzen und überwachen
  - Sicherheitsmassnahmen fachgerecht auswählen, implementieren und kontrollieren
  - Zeitnahe Wiederherstellung des normalen Geschäftsbetriebs sicherstellen

Informationssicherheit als Organ- und Organisationsverantwortung (2|2)

- Klare Aufgaben, Verantwortlichkeiten und Kompetenzen definieren
- Vordefinierte Prozesse; interne Weisungen, Berichterstattung, Überprüfung, Schulung
- Notwendige finanzielle und fachliche Ressourcen (technisches und juristisches Know-how)
- Standards als Benchmark:
  - FINMA-Rundschreiben 2008/21
  - ISO/IEC 27001 (Information Management System – ISMS)
  - ISO/IEC 27701:2019-08 (Privacy & Information Management System – PIMS)
  - IKT-Minimalstandard des Bundesamts für wirtschaftliche Landesversorgung (BWL)

Umsetzung im digitalisierten Unternehmen (1|2)

- Klare Aufgaben, Verantwortlichkeiten und Kompetenzen definieren
  - *Incident Response*-Leiter und Datenschutzberater benennen
- Datenflüsse verstehen
  - wie die Organisation Daten erhebt, speichert, weitergibt, schützt und löscht
- Datenbearbeitungstätigkeiten hinsichtlich geltender Gesetze und Richtlinien überprüfen
  - (national, regional, international) anwendbare Gesetze, Verordnungen; Aufsichtsbehörden

Umsetzung im digitalisierten Unternehmen (2|2)

- Erforderliche Dokumentation erstellen und implementieren
  - jährlich überprüfen, auditieren und überwachen; Schulungen durchführen
- Angemessene Überprüfungen durchführen (Informationssicherheit, Datenschutz, Cyber-Risiken)
  - in Übereinstimmung mit anwendbarem Recht und branchenüblicher Praxis

Kontakt

Thomas Steiner
Dr. iur., LL.M., Rechtsanwalt, Senior Advisor

@ thomas.steiner@lauxlawyers.ch
w http://www.lauxlawyers.ch

LAUX LAWYERS AG
Seegartenstrasse 2
Postfach
8024 Zürich
+41 44 880 24 24