Regulatory and Data Privacy Aspects of FinTech / InsurTech

Workshop Netcomm Suisse, 24 October 2019

Dr. Michael Reinle, LL.M. / Dr. Reto Luthiger

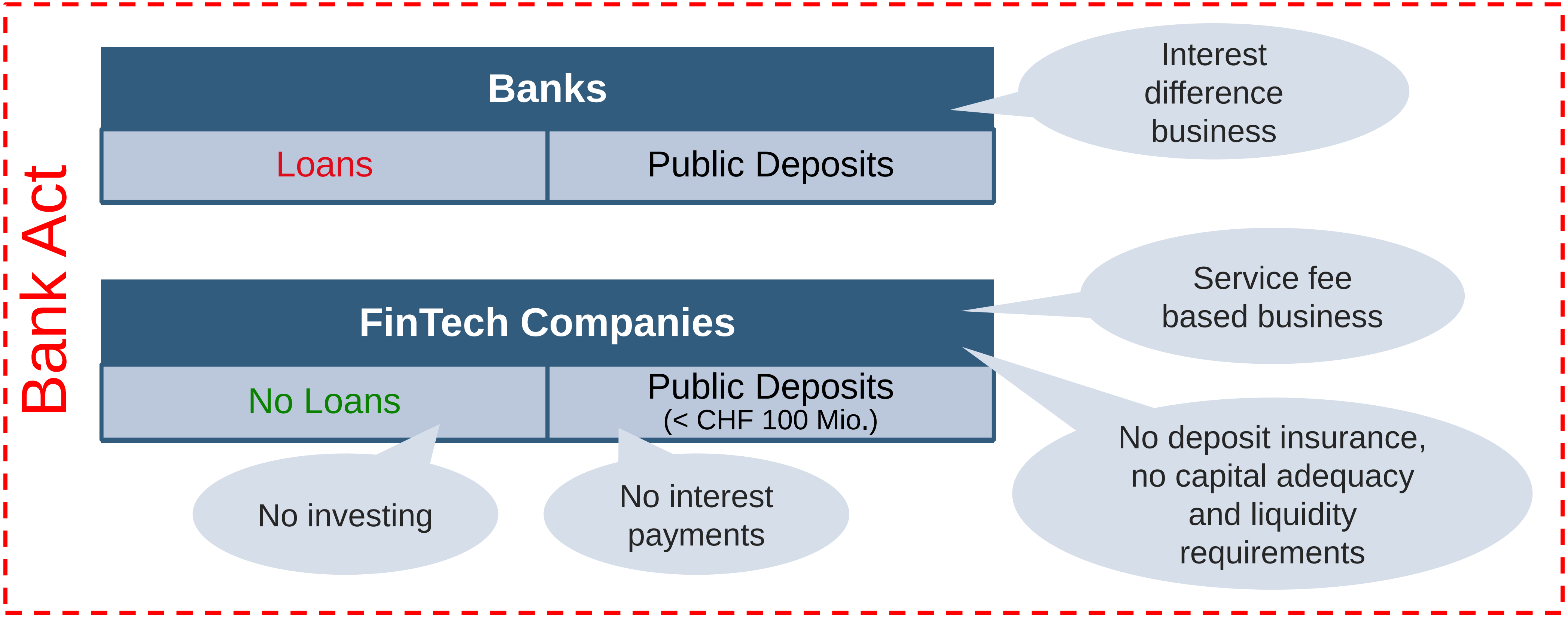
Topics

- FinTech Licence – Banking – Insurance – InsurTech
- M&A in InsurTech
- Outsourcing
- Data Processing Principles
- Cross-Border Data Transfer
- Cloud Computing
- Big Data & Data Privacy
- Internet of Things
- Blockchain, Data Privacy & Financial Market Regulations

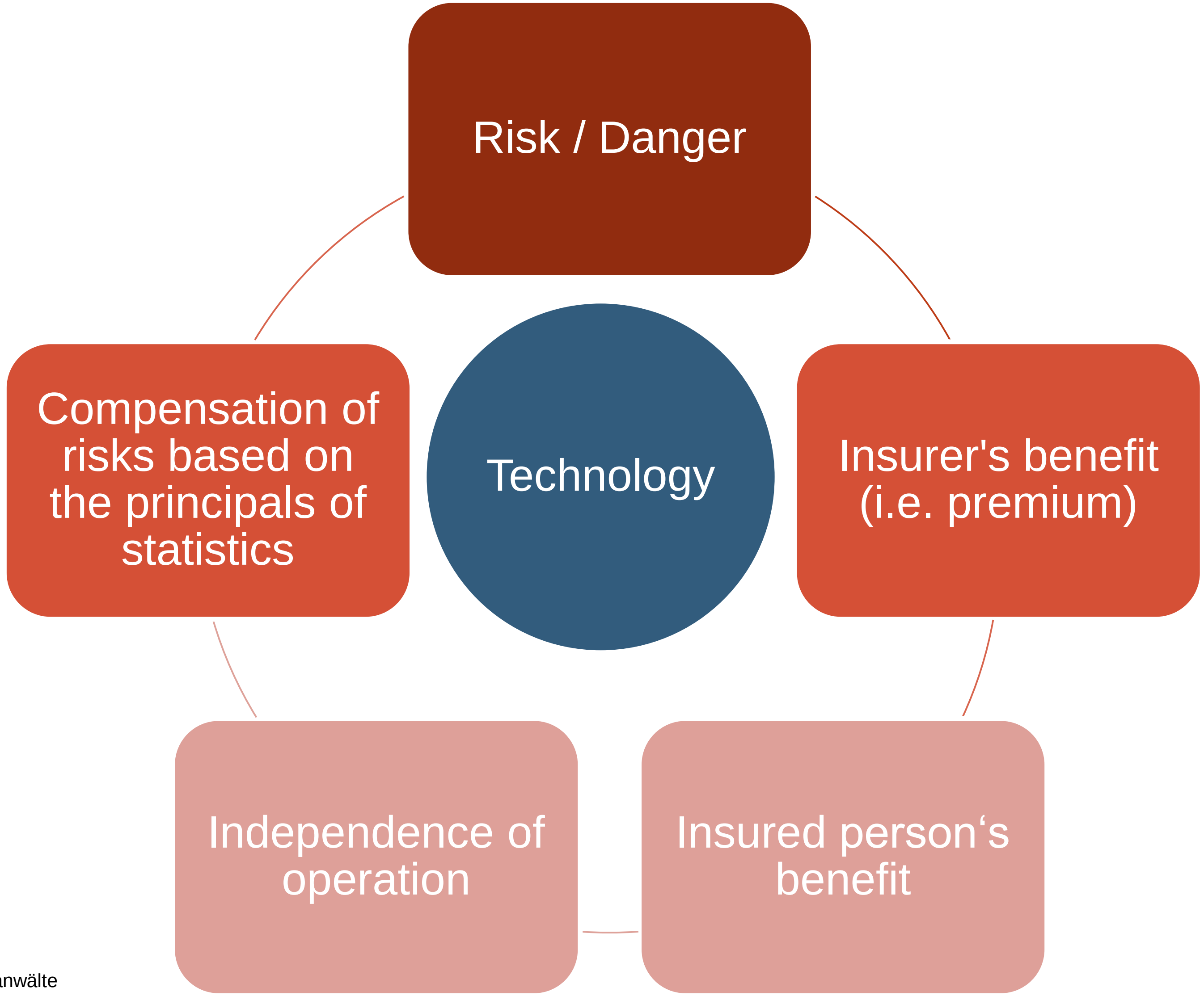
FinTech Licence – Banking – Insurance – InsurTech

FinTech Licence (Banking Licence «light») since 1.1.2019

- Aim: reducing market entry barriers for fintech companies
- Business model comparison between banks and fintech companies:



Insurance Business – 5 Elements – also Applicable to InsurTech Companies



FinTech vs. InsurTech – Example

FinTech / Banking:	InsurTech / Insurance:
• Bank guarantee business ("Garantiegeschäft"): • Securing the repayment of a loan by means of a bank guarantee to the benefit of third persons	• Credit Insurance ("Kreditversicherung"): • Covering for damage caused by non-performance of a third party

Both activities are similar from an economic perspective and both activities fulfil the 5 key elements of insurance business

➔ Not always clear differentiation between banking and insurance business possible

M&A in InsurTech

mll

Buying InsurTech Competence – M&A Transactions in InsurTech

Buying InsurTech by **Share Deal**:

Share Interest > 10, 20, 33, 50%

➔ *Intervention possibility of FINMA*

➔ *Notification or approval requirement*

(indirect) business plan amendment

Group Supervision (insurance group/cong-lomerate)

➔ *Partial supervision of all group companies*

Asset Deal – Transfer of Technology:

Various mandatory legal provisions

➔ *e.g. joint and several liability, employee consultation or information duties, FusG provisions*

➔ *Notification or approval requirement*

business plan amendment

No non-insurance business

➔ *Direct link to insurance business necessary, exemption approvals by FINMA possible, but rare*

Outsourcing

Outsourcing to FinTech/InsurTech Companies

Code of Obligations

- Art. 716a CO: non-transferable and irrevocable duties of the Board of Directors

Data Protection Act

- Principle regarding the protection of personal data

Anti-Money Laundering Act

- Delegation of AML duties of care
- Outsourcing of internal AML commission

Banking Act

- FINMA-Circ. 18/3 Outsourcing – Banks and Insurance Companies
- Bank client secrecy

Insurance Supervision Act

- FINMA-Circ. 18/3 Outsourcing – Banks and Insurance Companies
- Filing and approval of amended business plan with/by FINMA

Data Processing Principles

Data Processing Principles

- Principle of Transparency
- Principle of Data Minimization
- Purpose Limitation
- Justification for Data Processing (Consent, Legitimate Interests)
- Anonymized Data
- Prohibition of Automated Individual Decision-Making without Legal Justification

Cross-Border Data Transfer

Cross-Border Data Transfer

Switzerland

- Transfer to countries with adequate data protection laws: No specific safeguards
- Countries without adequate data protection laws – contractual safeguards or consent of the person concerned
- Sample outsourcing agreement of Swiss Federal Data Protection and Information Commissioner or EU Standard Contractual Clauses
- Since April 2017: U.S.-Swiss Privacy Shield Framework certification

EU

- Similar legal framework
- EU-U.S. Privacy Shield Framework

Cloud Computing

Cloud Computing & Data Privacy

- Main Issues:

Where is the data stored

Who has access to the data?

Standard contracts of cloud service providers

Statutory or contractual confidentiality duties

Cloud Computing in Banking: Guidelines of SwissBanking

- SwissBanking, "Cloud Guidelines: A guide to secure cloud banking", 26 March 2019
- Four main areas covered by the Guidelines:

Governance

- Choosing the cloud provider and its subcontractors, consent to a change of subcontractor

Data Processing

- Processing data on bank clients and bank-client confidentiality

Authorities and Proceedings

- Transparency and collaboration between institutions and cloud providers with regard to measures ordered by the authorities and the courts

Audit

- Auditing the cloud services and the cloud infrastructure used to deliver them

Big Data & Data Privacy

Big Data & Data Privacy

Big Data (Gartner IT):

High-volume, high-velocity and high variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making

Artificial Intelligence:

The analysis of data to model some aspect of the world. Inferences from these models are then used to predict and anticipate possible future events

Machine Learning:

The set of techniques and tools that allow computers to think by creating mathematical algorithms based on accumulated data

Big Data & Data Privacy

Distinctive Aspects of Big Data

- Use of algorithms
- Opacity of the processing («black box»)
- Tendency to collect all the data
- Repurposing of data
- Use of new types of data

New Types of Data

- Provided Data: Given by individuals
- Observed Data: Collected by tracking tools, IoT
- Derived Data: Produced from other data
- Inferred Data: Produced by more complex analysis

Big Data & Data Privacy

Data Processing Principles affected by Big Data

- Transparency Principle
- Limitation of Purpose
- Principle of Data Minimization
- Information Duties
- Consent Conditions

Privacy Paradox

Big Data with Data Privacy

Use of Privacy Enhancing Technologies

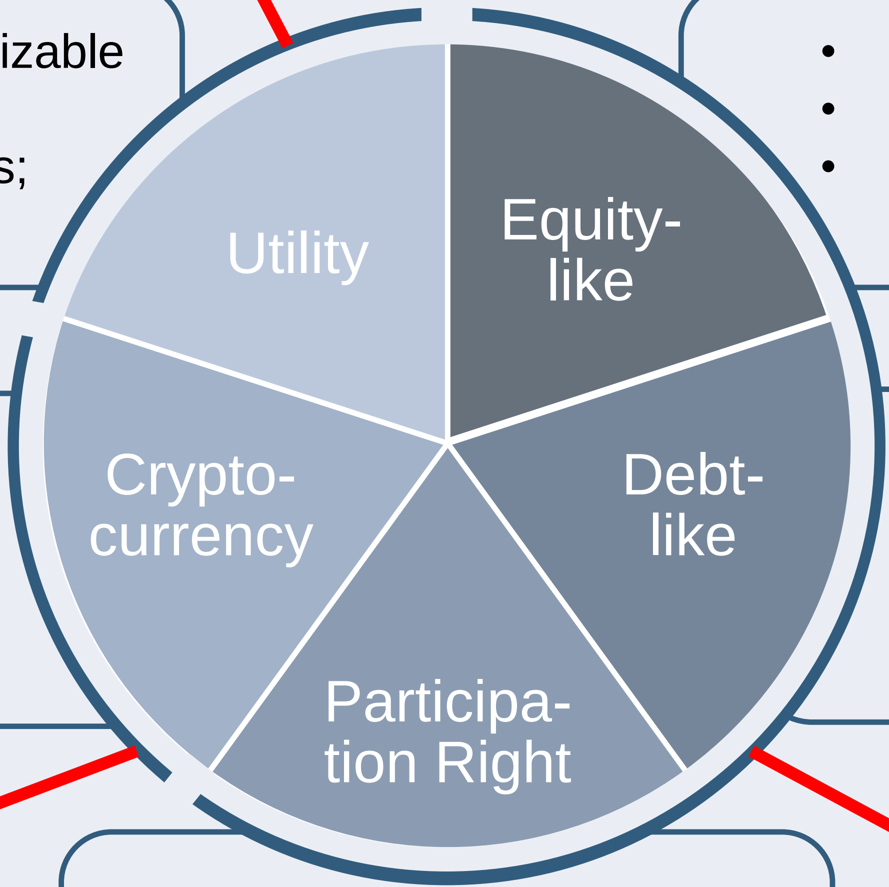
Blockchain, Data Privacy & Financial Market Regulations

Blockchain – Tokens & Financial Market Regulations

Utility Token

- Very versatile / customizable
- Digital access rights to applications or services;
- “fuel” of platform

- Equity of issuer
- Profit based (dividends)
- Shares / participation certificates



- No claims / rights against issuer
- Means of payment
- Exchange into other currencies

- Liability of issuer
- Repayment obligation
- Loans / derivatives / structured products

Payment Token

Asset Token

- Revenue based (turnover of issuer, not dividends)
- No equity of issuer

Blockchain & Data Privacy

Two-Sided Medal

- Blockchains enhance data privacy
- Blockchains raise data privacy concerns

Challenges and Benefits of Blockchains

- Blockchains are decentralized and distributed: Who is the data controller?
- Blockchains are public and transparent
- Blockchains are non-editable: Right to rectify and right to be forgotten?

Blockchains Enhance Data Privacy

- Enhanced data security: Blockchains are decentralized and distributed – no single points of failure; use of encryption
- Better data control because blockchains are public and transparent
- Pseudonymity and data minimization (public key of sender and recipient, cryptographic hash of transaction content, time stamp)

Blockchain & Data Privacy

Data Privacy Issues Raised by Blockchains

- Who is the controller of personal data on the blockchain?
- Which laws should be applied to blockchain technology?
- What constitutes personal data in the blockchain context? Are public keys personal data? Anonymization or just pseudonymization?
- Purpose Limitation and Data Minimization? Data is maintained on every node of the network and publicly accessible to anyone, regardless of the original purpose
- How can right to rectify or right to be forgotten be implemented?

Dr. Michael Reinle, LL.M.
michael.reinle@mll-legal.com
www.mll-legal.com | www.mll-news.com

Dr. Reto Luthiger
Reto.luthiger@mll-legal.com
www.mll-legal.com | www.mll-news.com

Thank you!

Thank you for your time and interest in Meyerlustenberger Lachenal