

NIEDERER KRAFT & FREY

Niederer Kraft & Frey Ltd
Bahnhofstrasse 13 · CH-8001 Zurich
Telephone +41 58 800 8000 · Telefax +41 58 800 8080
nkf@nkf.ch · www.nkf.ch



Disruptive Technologies – Legal and Regulatory Aspects

16 May 2017 – Investment Summit - Swiss Global Enterprise

NKF

Legal and Regulatory Framework in Switzerland

■ Legal and regulatory Framework:

- no laws or provisions relating specifically to disruptive technologies
- statutory provisions in general formulated in a technology-neutral manner
- some Circulars from some supervisory authorities: e.g. Swiss DPA, FINMA, etc. relating to topics such as digitalization and cloud

■ But a lot in the pipeline:

- Federal Council Strategy for a digital Switzerland
- Smart Switzerland Initiative
- Consultation on new Fintech Regulations

Data and Technologies

- (raw) data
- devices (sensors, gateways, ...)
- software
- telecommunications
- encryption / security services
- data warehouse / analytics platform services (cloud)
- ...

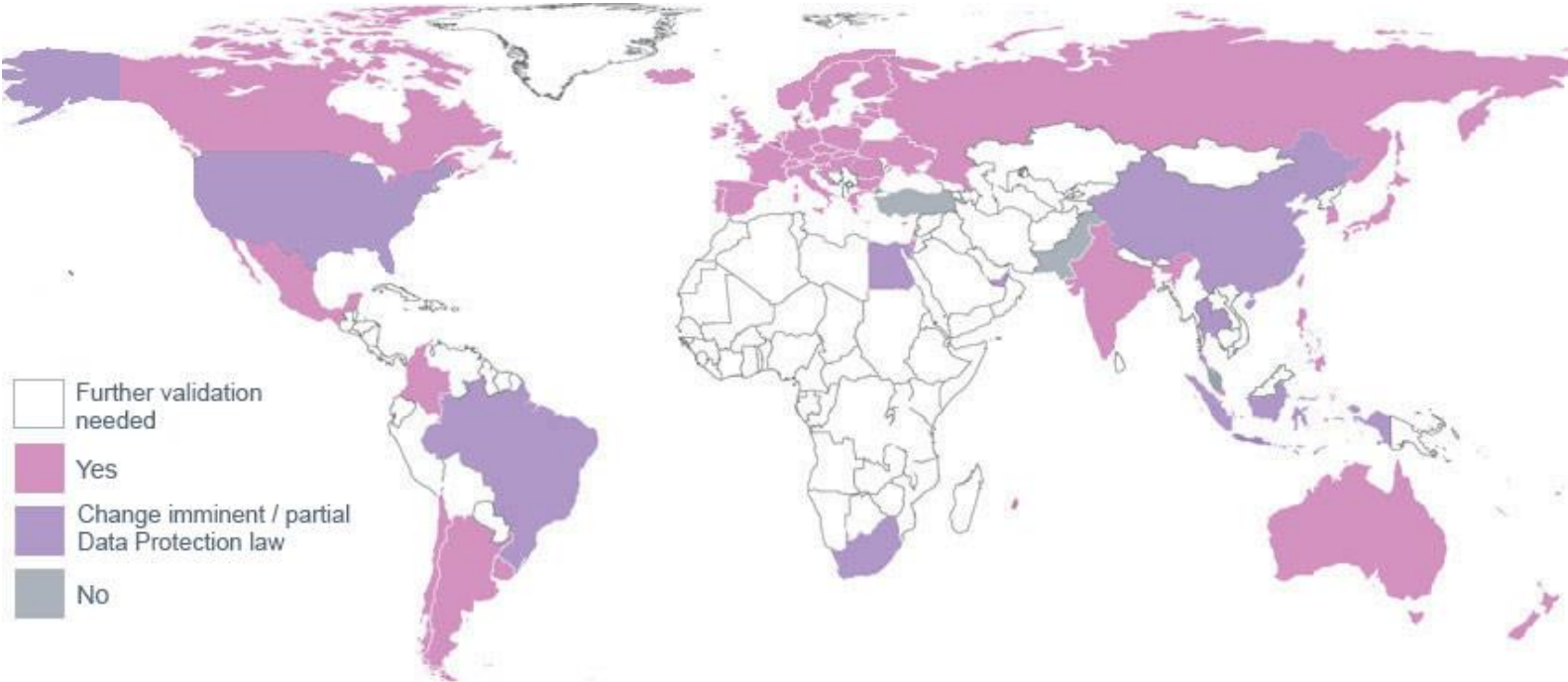
Common Legal and Regulatory Risks

- **data breach**
- **data privacy laws**
- data quality / errors
- **liability**
- device malfunctions / product liability
- IP / proprietary rights (data as an asset?)
- **regulatory hurdles**
- processing errors
- service quality
- software errors...

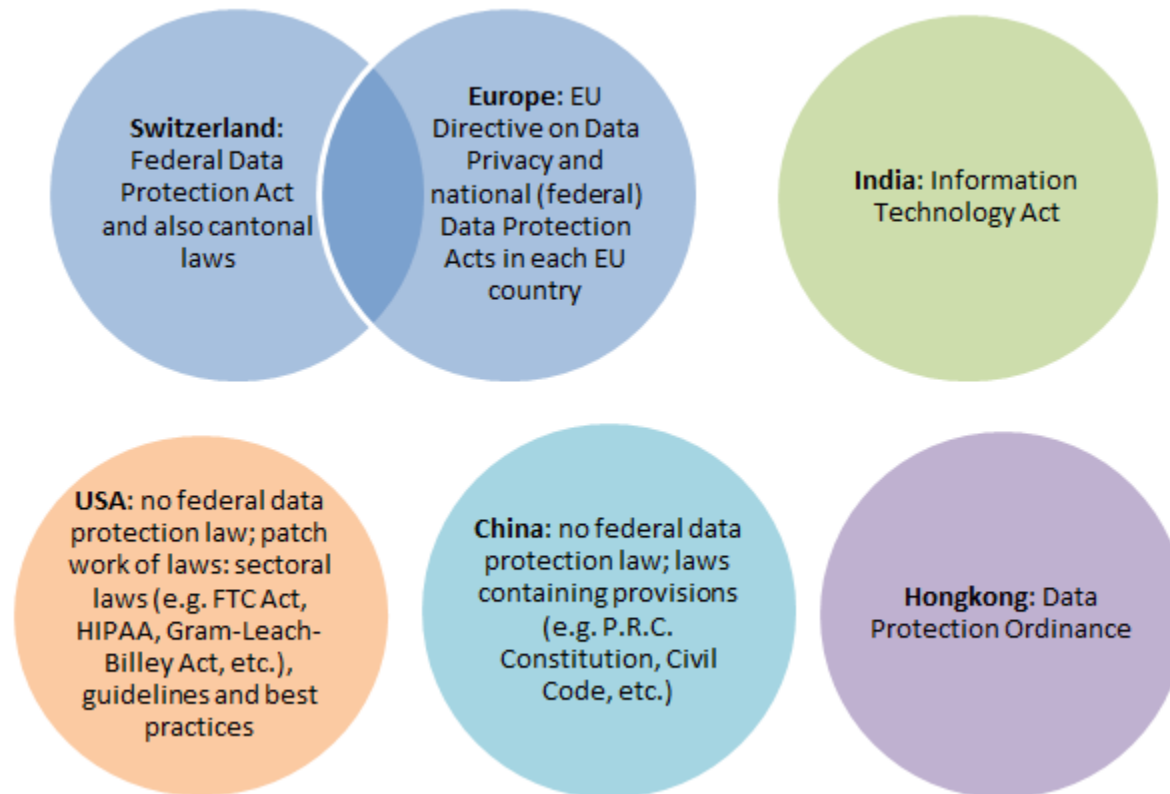
Data Protection I

- What is data?
 - any kind of information
 - created by human or machine
 - no statutory protection per se for only data
- What is personal data?
 - Personal data is any data relating to an **identified** or **identifiable** person
 - Protection of personality rights and not of the data itself
 - Accordingly anonymous data is not considered personal data
 - Federal Act on Data Protection dated 19 June 1992 (DPA)
- Questions:
 - personal data or just any kind of other data (e.g. machine data)?
 - how can data be protected?
 - strict requirements relating to personal data

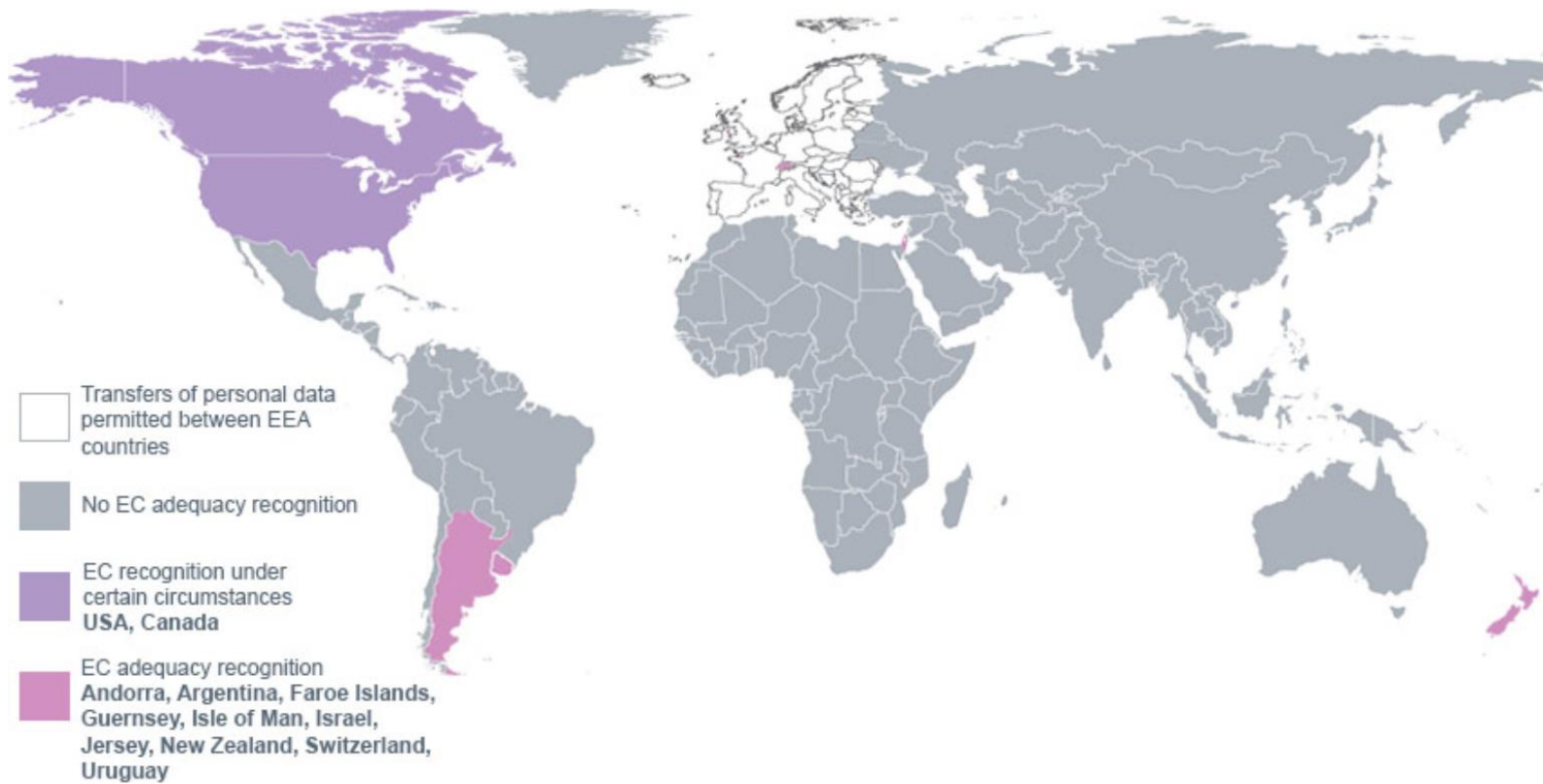
Which Countries have Data Protection Laws?



Different Data Protection Regimes Worldwide



Countries with Appropriate Data Protection Level



GDPR and Revision of Swiss Data Protection Act

- Stricter Rules and massively higher fines as from 25 May 2018:
 - Extraterritorial reach of the GDPR
 - Stronger enforcement powers
 - Transparency rules extended
 - New accountability obligations
 - Data protection by design and default
 - Stricter consent rules
 - Right of access, right to data portability, right on automated processing
 - Right to be forgotten
 - Data security measures
 - Massive fines: up to 20 million Euro or up to 4% of worldwide annual turnover
 - Swiss Data Protection Act in revision in order to achieve adequacy level of GDPR
 - In general importance of data protection compliance has massively increased

Data Security – Data Breaches

- DDos Attacks and the like
- Predicted market growth will accentuate the issue
- Financial liability for lack of security
- What is appropriate level of data security?
 - no specific act
 - state of the art / appropriateness of data security systems
 - ISO / IEC 27k family of standards
 - other useful guidelines
- Data Breaches
 - new and stricter rules under the GDPR and Swiss law
 - ongoing confidentiality, integrity, availability and resilience
 - ability to restore
 - process for regular testing
 - data breach notification (72 hours)
 - also under new Swiss Data Protection duty to inform
 - massive fines if no notification

Special Regulatory Questions

■ Hurdles for regulated sectors

- Finance (banks, insurances), Telecom, Pharma
- Audit Right
- Location of storage of data

■ Banking Sector

- Protection of Banking Secrecy
- FINMA Circular 2008/7 «Outsourcing Banks»
- FINMA Circular 2008/21 «Operational Risks – Banks»

■ Telecom Sector

- Ban for foreign providers to provide telco services in Switzerland
 - > Duty to comply with employment legislation and related standards/customs
 - > Duty to comply with lawful intercept and surveillance legislation

Liability I

- Issues:
 - delegation of task from operators to technology
 - humans as controllers and supervisors
 - machine intelligence and autonomy
 - challenge of complexity
 - how to maintain control, prevent and mitigate failures
- Who is responsible in case something goes wrong?
 - Providers (software, hardware, services)?
 - Users?
 - Organisations (companies, agencies)?
- Who is liable to compensate for damages to persons and goods?
 - Who is liable to compensate for damages to persons and goods?
 - Providers (software, hardware, services)?
 - Organisations (companies, agencies)?

Liability II

- Legal framework:
 - Statutory provisions:
 - Product Safety Act and Product Liability Act
 - Code of Obligations – tort
 - Act on Technical Barriers on Trade
 - Standards and State of the Art
 - Criminal liability
 - Contractual liability:
 - Exclusion of liability?
 - Back-to-back liability provisions
 - Expand force majeure provisions: for hacking incidents etc.

Conclusions

- No specific law relating to disruptive technologies as such – but a lot of initiatives in the pipeline
- Swiss authorities are open minded
- Increase of investment in disruptive technologies by Swiss companies – e.g. Switzerland ranked no. 1 by EPO in filing for computer technology patents
- Data protection compliance – massively increased importance
- Decisive to remain competitive – implementation of cyber security response plan
- Regulatory compliance – close cooperation with Swiss supervisory authorities
- Implementation of contracts dealing with back to back liability
- The future is bright for Disruptive Technologies in Switzerland!