GDPR Readiness - Workshop

CIMA

Zurich, 4 April 2018

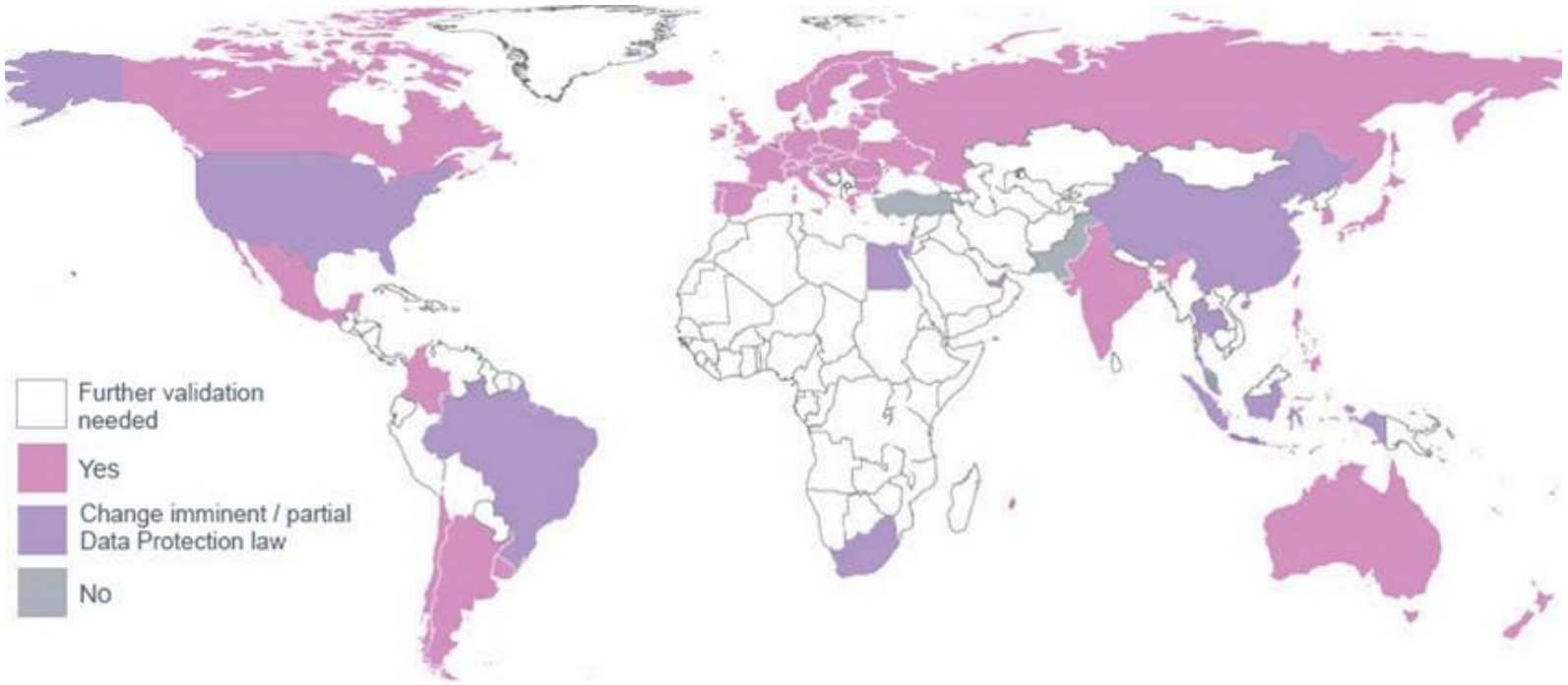
Agenda

- General Overview of Data Protection
- Aim of GDPR and Legal Framework
- Main Changes under GDPR
- New Provisions under GDPR
- Revision of Swiss Data Protection Act
- What will change?
- Specific Topics:
  - Accountability
  - Transparency
  - Processor obligations
  - New rights of data subjects
  - Data privacy impact assessments
  - Profiling
  - Data transfers

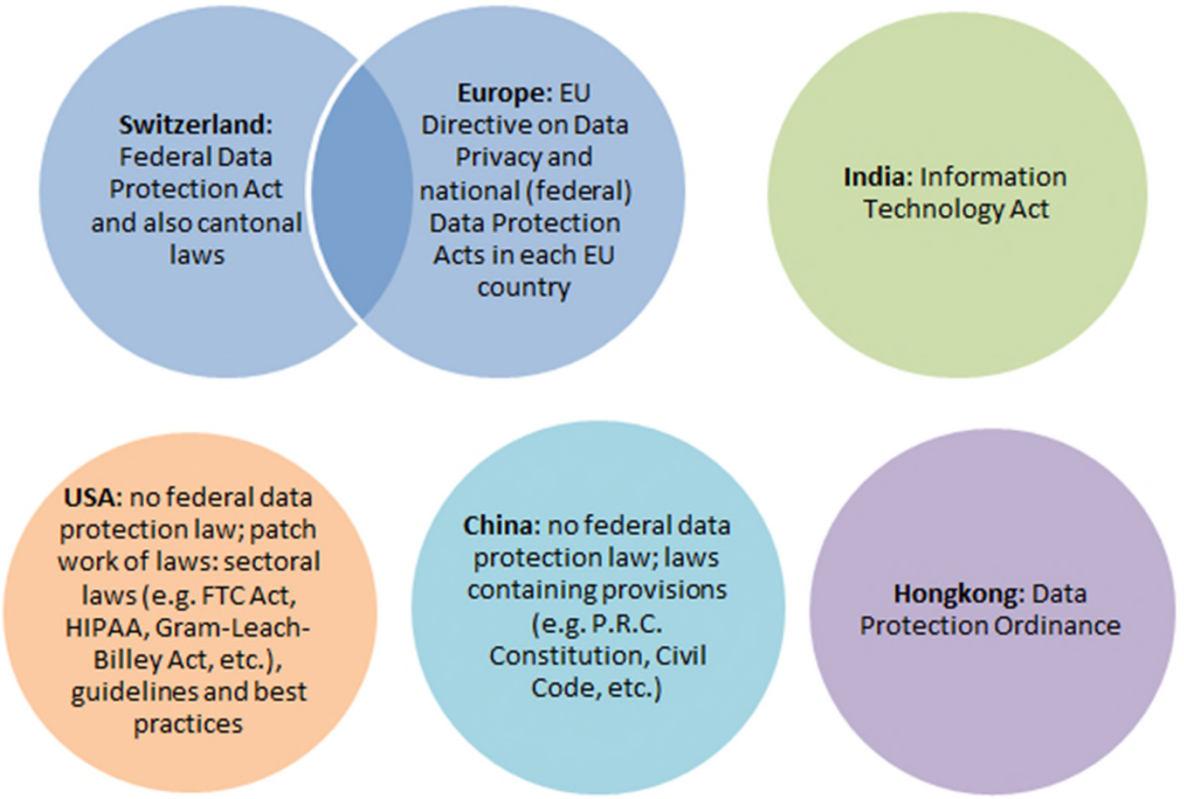
Data Protection

- 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

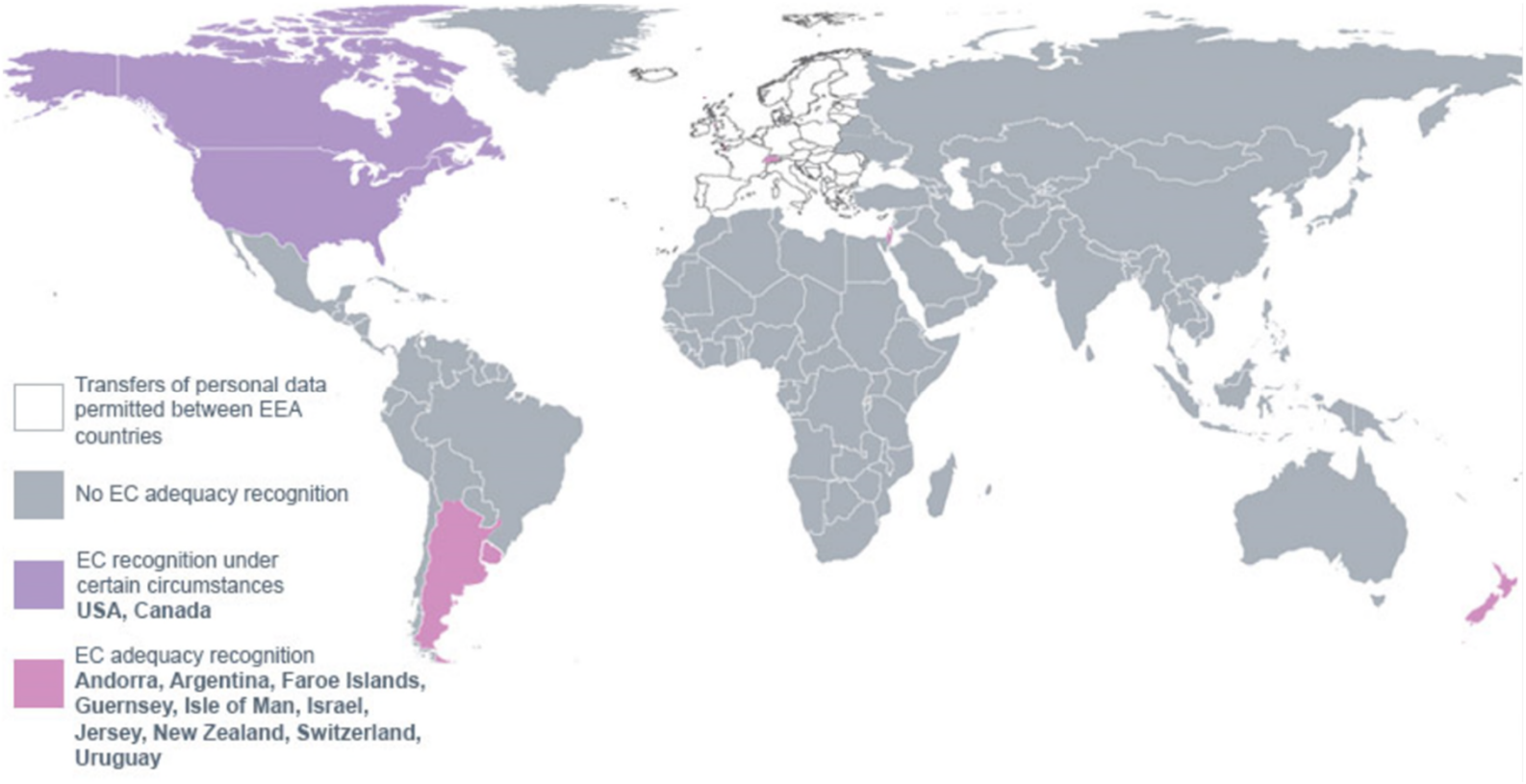
Which countries have Data Protection Laws?



Different Data Protection Regimes Worldwide



Countries with Appropriate Data Protection Level



NKF

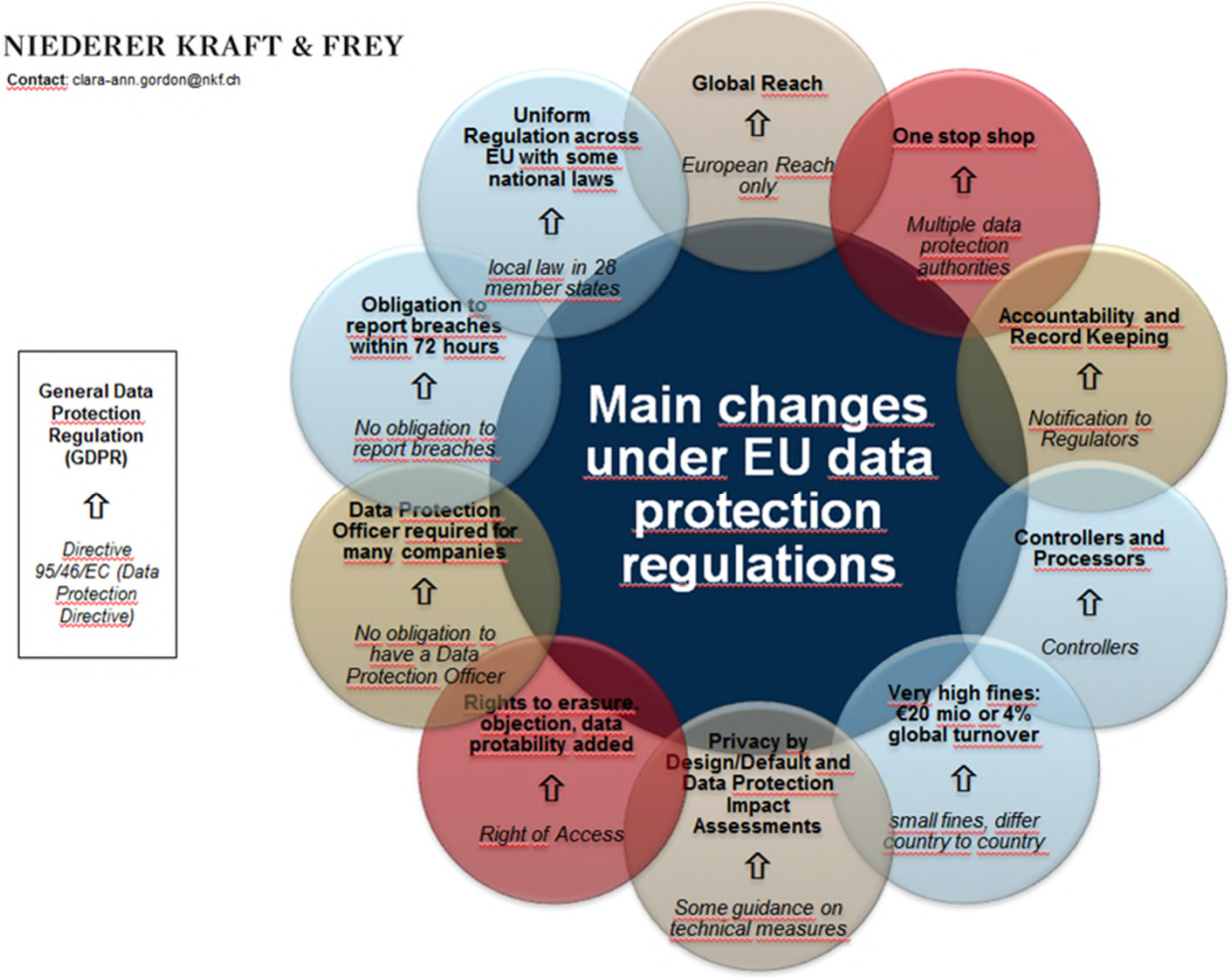
Aim of GDPR and Legal Framework

- The Aim:
  - Extraterritorial reach
  - Putting people in control of their data
  - Focus on practical compliance
  - Stronger enforcement powers

- The Legal Framework:
  - EU General Data Protection Regulation
    - Directly applicable
    - 25 May 2016: Entry into force
    - 25 May 2018: Applicability
  - National laws
    - Opening clauses in GDPR
    - Germany, Ireland, Netherlands etc.

Main Changes under the GDPR

NIEDERER KRAFT & FREY
Contact: clara-ann.gordon@nkf.ch



GDPR – New Provisions

- 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
  - Massive fines: up to 20 million Euro or up to 4% of worldwide annual turnover
  - In general importance of data protection compliance has massively increased

GDPR and Data Breaches/Data Security

- 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

Revision of the Swiss Data Protection Act

- Reasons for the revision of the Swiss Data Protection Act
  - Ratification of convention 108 (ETS No. 108) by Switzerland
  - Adaptions to the provisions of the GDPR – to achieve recognition from European Union as country with adequate data protection level

- Time Table for revised Swiss Data Protection Act
  - 21 December 2016: publication of preliminary draft
  - 4 April 2017: expiry deadline of consultation process
  - September 2017: White Paper (*Botschaft*) to the Parliament and draft DPA
  - January 2018: decision to deliberate on the draft DPA in two stages
  - January 2019? Entry into force of revised act

- GDPR
  - 25 May 2018: Entry into force

- Other Developments:
  - EU-US Privacy Shield: in place since 11 January 2017
  - Swiss-US Privacy Shield: starting 12 April 2017

NKF

What was not adopted from the GDPR?

- Not adopted from the GDPR:
  - Regulations concerning internal data protection officer (DPO)
  - Processing of data relating to children
  - Right to be forgotten
  - Right of data portability
  - Obligation to consult with data protection authorities
  - etc.

What will change?

- Law will become stricter
- New obligations to comply with
- Focus on policies and procedures
- Increased exposure of weak practices and security
- Emphasis on safe data flows
- Heavy EU-wide fines

Specific Topics

- Accountability
- Transparency
- New rights of data subjects
- Data privacy impact assessments
- Profiling
- Data transfers

Accountability

- Under GDPR accountability has become more important

- The three main accountability principles:
  - Responsibility: the appropriate technical and organisational measures have been implemented and are maintained proactively, systematically, and on an ongoing basis.
  - Ownership: the technical and organisational measures are embedded at each level in the organisation, within each department or function that processes the personal data.
  - Evidence: the relevant documentation can be produced and used as evidence to demonstrate compliance at any time.

- What measures will be appropriate in each case, will depend on the nature, scope, context and purposes of the relevant processing as well as the risks for rights and freedoms of individuals

- GDPR provides very little guidance - further guidance expected from the Art. 29 WP

Transparency

- Principle of transparency not defined in GDPR. Articles 12-14 GDPR codify the transparency obligations

- Art. 29 WP has published a Guideline:
  - present information about data processing efficiently and succinctly in order to avoid “information fatigue” on the part of individuals
  - make the information intelligible, in that it should be "understood by an average member of the intended audience"
  - when processing the data of children or vulnerable persons, ensure that the "vocabulary, tone and style of the language used" is appropriate to that audience
  - spell out not just the scope, but also the consequences of processing, in unambiguous language
  - make information "easily accessible", in that it should be immediately apparent where the information can be obtained; and
  - provide information in "clear and plain language", meaning in as simple a manner as possible, avoiding complex sentence and language structure.

New Processor Obligations

- GDPR imposes privacy compliance obligations directly on data processors and hold them directly liable for non-compliance with those obligations.

- For instance, data processors will be required by law to:
  - implement appropriate technical and organisational measures to ensure a certain level of data security
  - keep detailed records of their processing activities
  - appoint a data protection officer ("DPO") in certain instances and a representative located within the EU if the processor is located outside of the EU
  - comply with the same cross-border transfer requirements as data controllers; and
  - notify data controllers of data breaches

- In the event of non-compliance with their obligations under the GDPR, processors may be subject to direct enforcement action by supervisory authorities ("SAs")

New Rights of Data Subjects

- GDPR provides the following rights for individuals:
  - right to be informed
  - right of access
  - right to rectification
  - right to erasure
  - right to restrict processing
  - right to data portability
  - right to object
  - rights in relation to automated decision making and profiling.

Data Privacy Impact Assessments I

- Where a type of data processing is likely to result in a high risk for the rights and freedoms of individuals, controllers shall carry out a DPIA prior to the processing to assess the impact of the envisaged processing operations on the protection of personal data

- GDPR provides the following non-exhaustive list of cases in which DPIAs must be carried out:
  - automated processing for purposes of profiling and similar activities intended to evaluate personal aspects of data subjects
  - processing on a large scale of special categories of data or of data relating to criminal convictions and offences
  - systematic monitoring of a publicly accessible area on a large scale
  - in case of large-scale processing operations which aim at processing considerable amounts of data and could affect a large number of individuals

Data Privacy Impact Assessments II

- Scope of DIA – information to be included:
  - a systematic description of the envisaged processing operations and the purposes of the processing
  - an assessment of the necessity and proportionality of the processing operations in relation to the purposes
  - an assessment of the risks to the rights and freedoms of data subjects that are likely to result from the processing
  - the measures envisaged to address the risks, including safeguards, security measures and mechanisms

- Further noteworthy points:
  - Where a set of similar processing operations present similar high risks, a single DPIA may be undertaken to address all of those processing operations
  - Controllers must seek the advice of their DPO (if any) when carrying out DPIAs
  - Without prejudice to the protection of commercial or public interests or the security of processing obligations, where appropriate, controllers shall seek the views of data subjects on any intended processing

Profiling

- “Profiling" is any automated data processing that involves the use of personal data to evaluate certain personal aspects of an individua (including aspects relating to the individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements)
- The activity of profiling as such is not prohibited. But as a form of data processing profiling is subject to the general rules governing the processing of personal data. As such, profiling requires a legal ground (e.g., the data subject's consent) and must comply with data protection principles.
- Individuals have certain rights to object to profiling which must be honored by controllers, unless
  - based on the data subject's explicit consent
  - necessary for the entering into, or performance of, a contract between the data subject and the controller; or
  - authorised by EU or Member State law to which the controller is subject

Data Transfers I

- In principle, GDPR will retain the cross-border data transfer rules of the Directive

- Noteworthy changes to the cross-border data transfer rules include the following:
  - Transfers will no longer be subject to country-specific authorisation processes except that transfers based on contractual clauses which have not been adopted or approved by the Commission will require specific supervisory authority approval
  - Adequacy decisions will be subject to clearer and more prescriptive standards as well as regular review and may be made in relation to territories and industry-sectors within a country.
  - GDPR offers certification mechanisms and codes of conduct as additional options for adducing appropriate safeguards
  - BCRs will be formally recognised as measures adducing appropriate safeguards and will be subject to uniform rules when it comes to their adoption

Data Transfers II

- Approved standard contractual clauses may be supplemented with additional clauses or safeguards subject to certain conditions.
- Transferors wanting to rely on consent as a derogation will need to inform the data subject about the risks resulting from the transfer before obtaining his/her explicit consent.
- GDPR will introduce one new but very limited derogation which may help legitimise occasional transfers which are small in scope and would otherwise be prohibited.

Thank you for your attention!

Your contact

Clara-Ann Gordon
Partner
clara-ann.gordon@nkf.ch

Niederer Kraft Frey Ltd
Bahnhofstrasse 53
CH-8001 Zurich
Switzerland

Phone +41 58 800 8000
Fax +41 58 800 8080
Web http://www.nkf.ch

Niederer Kraft Frey AG Bahnhofstrasse 53 CH-8001 Zürich T +41 58 800 80 00 F +41 58 800 80 80 nkf.ch