access to insurance initiative

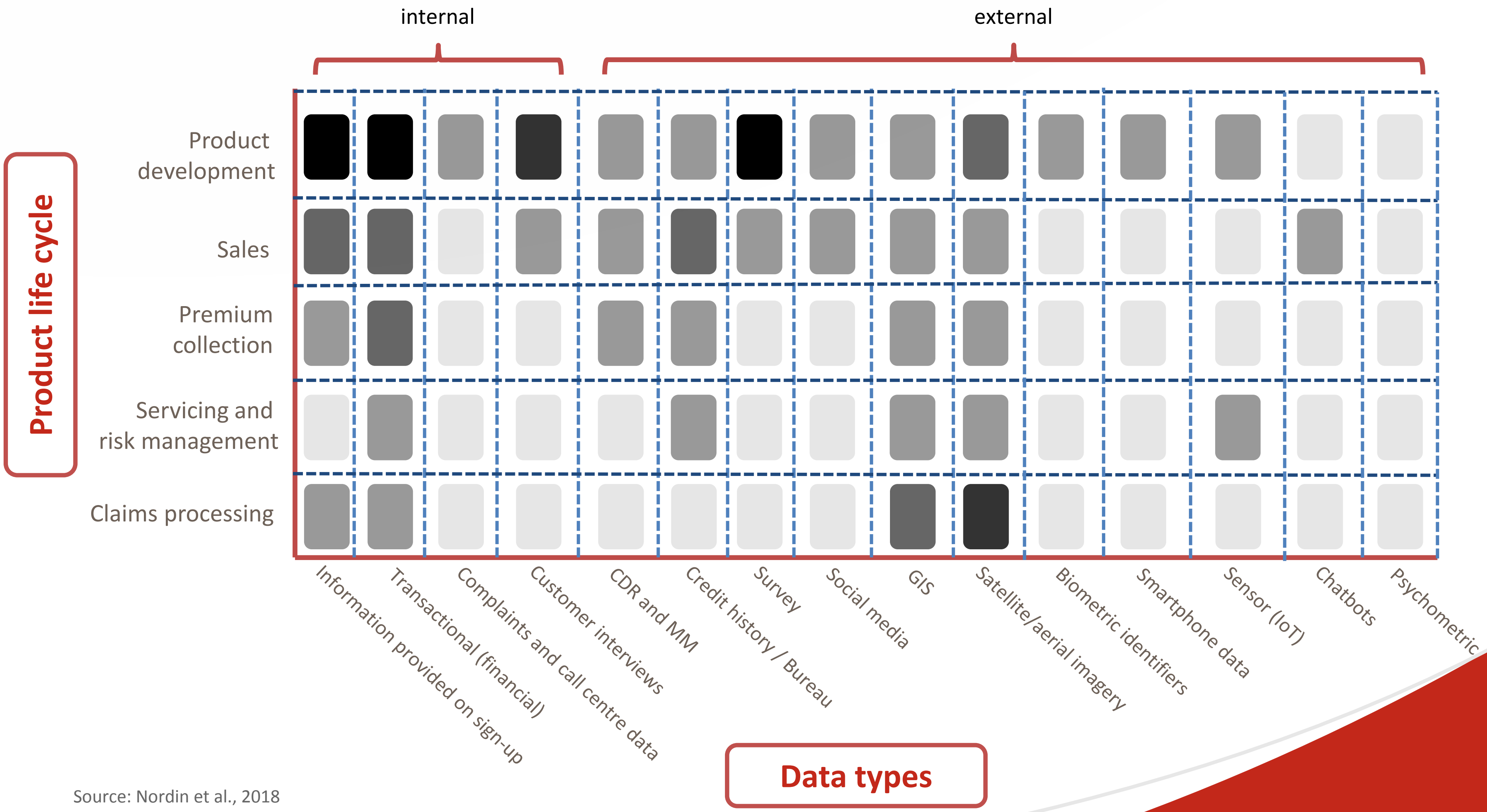
Insurance regulators' role in consumer data risk protection

Stefanie Zinsmeyer I May 2018

Supported by

Technology has allowed businesses to better understand and serve consumers through the collection and analysis of big data.

Data types currently being used through the insurance product life cycle in emerging markets



Product life cycle	internal				external										
	Information provided on sign-up	Transactional (financial)	Complaints and call centre data	Customer interviews	CDR and MM	Credit history / Bureau	Survey	Social media	GIS	Satellite/aerial imagery	Biometric identifiers	Smartphone data	Sensor (IoT)	Chatbots	Psychometric
Product development	█	█	░	▓	░	░	█	░	░	▒	░	░	░	□	□
Sales	▒	▒	□	░	░	▒	░	░	░	░	□	□	□	░	□
Premium collection	░	▒	□	□	░	░	□	□	░	░	□	□	□	□	□
Servicing and risk management	□	░	□	□	□	░	□	□	░	░	□	□	░	□	□
Claims processing	░	░	□	□	□	□	□	□	▒	▓	□	□	□	□	□

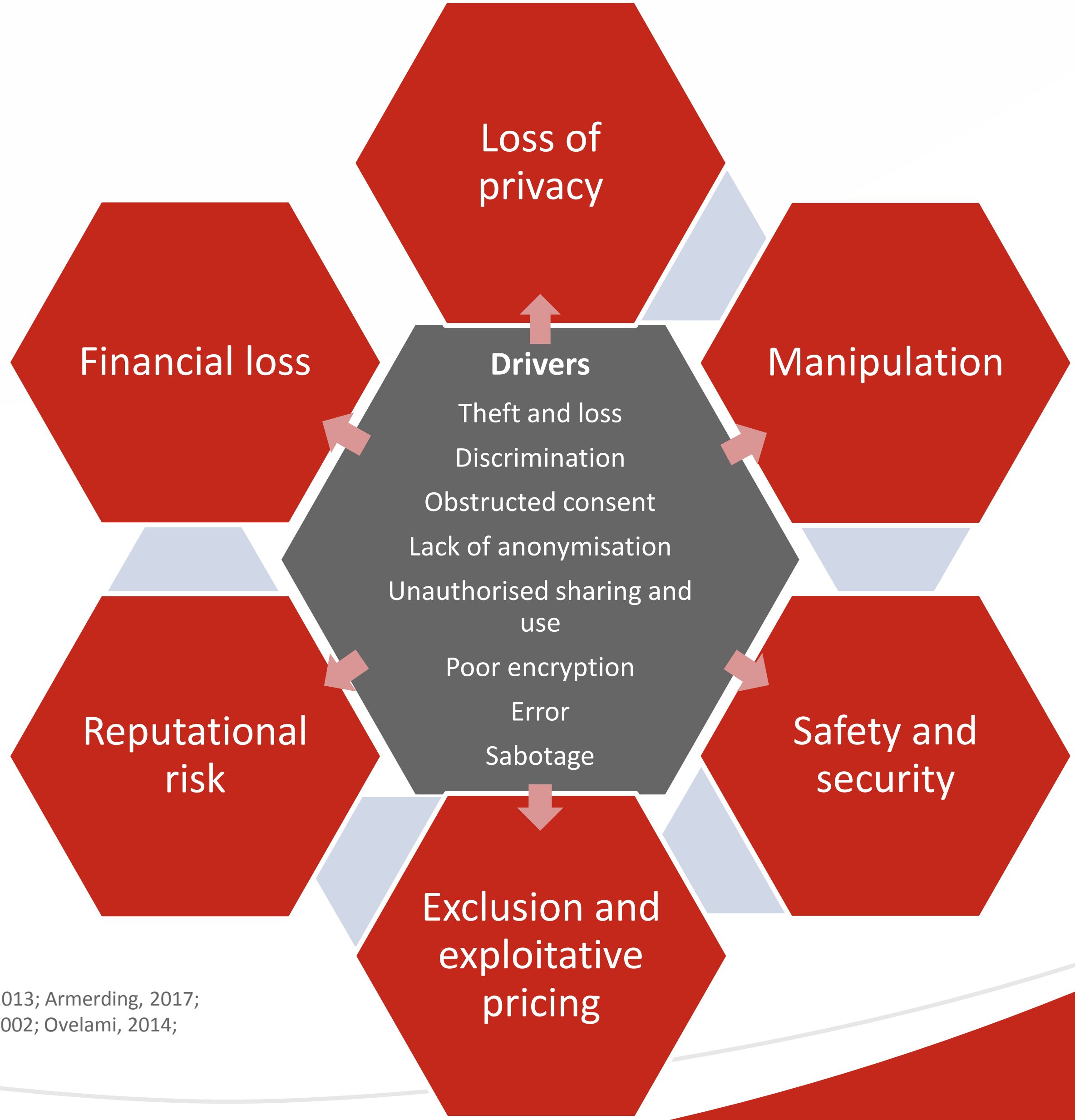
Data types

Source: Nordin et al., 2018

But how to balance the potential value against emerging risks?

Question for regulators: How to act and when to act?

Emerging risks to consumers from data use



Source: Based on AIG, 2013; Armerding, 2017; Isaca, 2012; Newman, 2002; Ovelami, 2014; Uydess et al., 2018

How is this relevant for insurance regulators?

- Substantial number of consumers are unserved, new data can open new markets.
- New data approaches allows more targeted risk pricing – risk pooling breaks down and risks excluding customers.
- Data abuses increasingly prevalent – data privacy, financial loss, reputational loss and manipulation of choice.

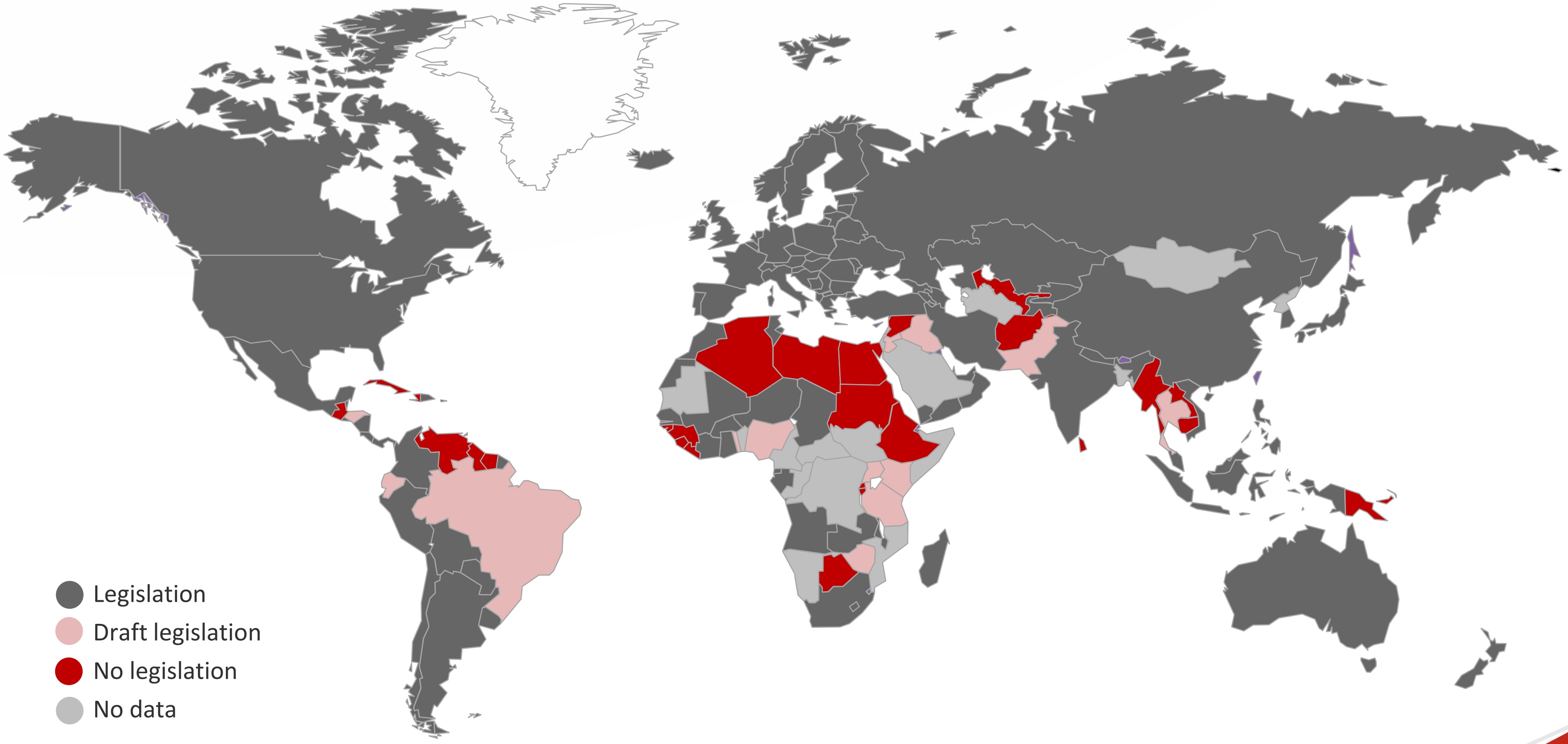
How urgent?

- Insurers already collect and store a lot of sensitive personal information on their customers.
- Partnership and data sharing common and set to further increase, e.g. health wearables, social scoring, social media, location tracking and genome mapping

It is important for regulators to understand and prepare accordingly

Data protection and privacy legislation worldwide

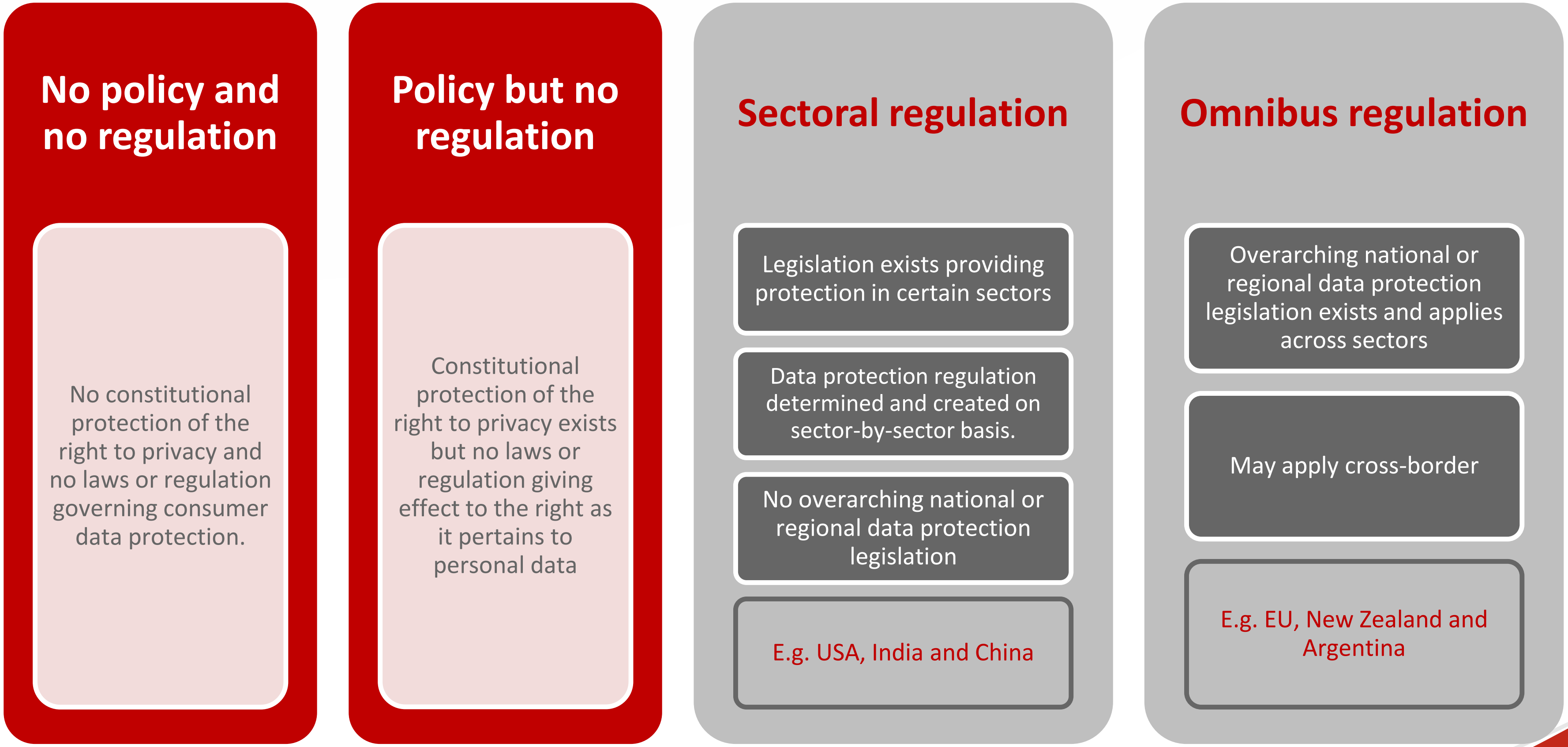
Percentage of UN countries with or without current or pending privacy legislation



Source: UNCTAD 2018

How are countries currently dealing with this?

Data protection regulatory approaches



No policy and no regulation

No constitutional protection of the right to privacy and no laws or regulation governing consumer data protection.

Policy but no regulation

Constitutional protection of the right to privacy exists but no laws or regulation giving effect to the right as it pertains to personal data

Sectoral regulation

Legislation exists providing protection in certain sectors

Data protection regulation determined and created on sector-by-sector basis.

No overarching national or regional data protection legislation

E.g. USA, India and China

Omnibus regulation

Overarching national or regional data protection legislation exists and applies across sectors

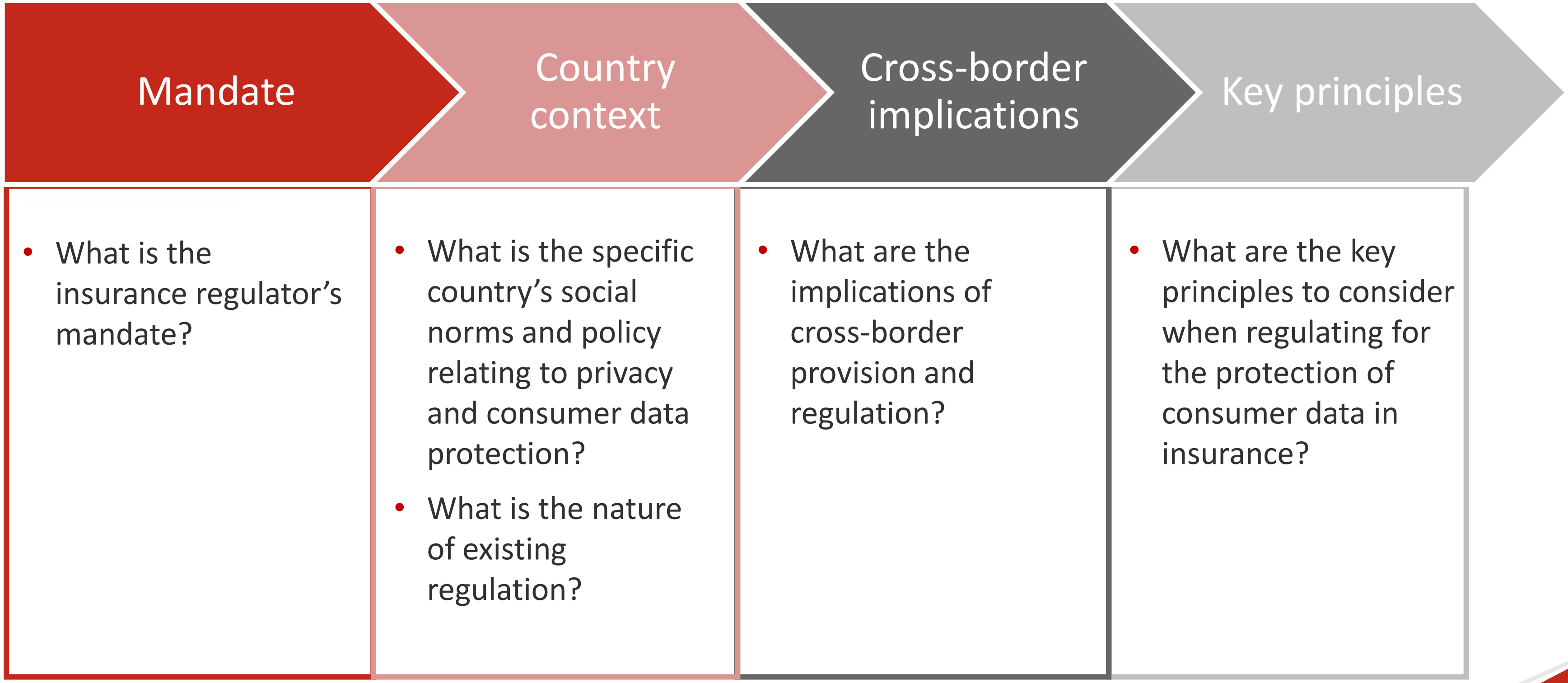
May apply cross-border

E.g. EU, New Zealand and Argentina

Countries falling into a particular category may have draft or pending legislation, which once in operation, may change the applicable framework category.

Source: Based on DLA Piper, 2018
and Deloitte, 2017

What are the key factors for the insurance regulator to consider?



Mandate	Country context	Cross-border implications	Key principles
• What is the insurance regulator's mandate?	• What is the specific country's social norms and policy relating to privacy and consumer data protection? • What is the nature of existing regulation?	• What are the implications of cross-border provision and regulation?	• What are the key principles to consider when regulating for the protection of consumer data in insurance?

Key principles

What are the key principles to consider when regulating for the protection of consumer data in insurance?

- *Data-handling requirements* relate to requirements in respect of inter alia the collection, processing and storage of consumer data. Such requirements may include restricting the collection of only certain specific data, only using it for a specific purpose and only storing it for a certain (specified) period.
- *Informed consent requirements* consider the freedom of the consumer (data subject) to give consent and to understand the consequences thereof, and for such consent to be requested in clear and plain language.
- *Defining personal and sensitive data.* Many jurisdictions distinguish between personal and sensitive data, often having more onerous requirements or putting in place greater restrictions on the use of sensitive data in order to protect consumers. A common distinction made between the two includes the consideration of personal data as data with which a person can be identified, whereas data is considered sensitive where the distribution thereof may lead to harm or, more specifically, discrimination.
- *Reasonable use* refers to the use of consumer data only in the context of the use of the data for which consent was specifically provided, for the purpose of which the consent specified, and to the extent to which consent was given.
- *Security mechanisms* include the protection of consumer data by means of, for example, deanonymisation and encryption. In this way, consumers should not be able to be identified by their data in the event of a breach.

Thank you.

Follow us on Twitter @a2ii_org, Youtube and LinkedIn

Supported by

cenfri fsdafrica UKaid from the British people

The Initiative is a partnership between:

IAIS INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

CGAP

BMZ Federal Ministry for Economic Cooperation and Development

FINMARK TRUST Making financial markets work for the poor

ILO International Labour Office

UNCDF Microfinance • Capital Development

ADB

FIRST Initiative

OMIN Fondo Multilateral de Inversiones Miembro del Grupo BID

Making Finance Work for Africa

Ministry of Foreign Affairs of the Netherlands

Hosted by:

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH