Privacy Challenges in Fintech

Virginia Cram-Martos

TriΔngulΔrity

What is Fintech?

Computer programs and other technology used to support or enable banking and financial services

Oxford English Dictionary*

* https://www.lexico.com/en/definition/fintech Underlining added by the presenter

With Shared and Separate Privacy and Policy Issues

Computer Programs & Technology

- Privacy legislation such as GDPR
- ICT Security
- Data collection and bias (in big data and AI)
- Access to technology and access to privacy

Banking and Financial Services

- Privacy legislation such as GDPR
- Know Your Customer (KYC) and Anti-Money Laundering (AML) Rules
- Access to financial services

Privacy Legislation
Example GDPR – 6 Principles
for processing personal data

1. Processed lawfully, fairly and in a transparent manner in relation to individuals
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed
4. Accurate and, where necessary, kept up-to-date
5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
6. Processed in a manner that ensures appropriate security of the personal data

Underlined text may require interpretation and interpretations may evolve over time (for example “appropriate security” in 5 years will not be the same as it is today).

GDPR is Not the Only Data Privacy Legislation

CHINA – Increasing data-privacy rules for companies

- March 2018 a national standard on personal information protection issued: *GB/T 35273-2017 Information Technology – Personal Information Security Specification*
- 5 May 2019: Cyberspace Administration of China (CAC) issued a new set of draft privacy guidelines for app operators
- *Comprehensive national legislation is under development*

*https://technode.com/2019/06/19/china-data-protections-law/ and
https://slate.com/technology/2019/02/china-consumer-data-protection-privacy-surveillance.html

GDPR is Not the Only Data Privacy Legislation

JAPAN – Updated its Legislation after GDPR

The 2017 Act on the Protection of Personal Information (APPI), like the GDPR, applies to companies processing data about Japanese individuals even if they are not based in Japan

https://www.endpointprotector.com/blog/data-protection-in-japan-appi/

https://izanau.com/article/view/data-privacy-in-japan

SOUTH KOREA – In some areas stricter than GDPR and rules also apply to the government

For a point by point comparison with GDPR, see https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/

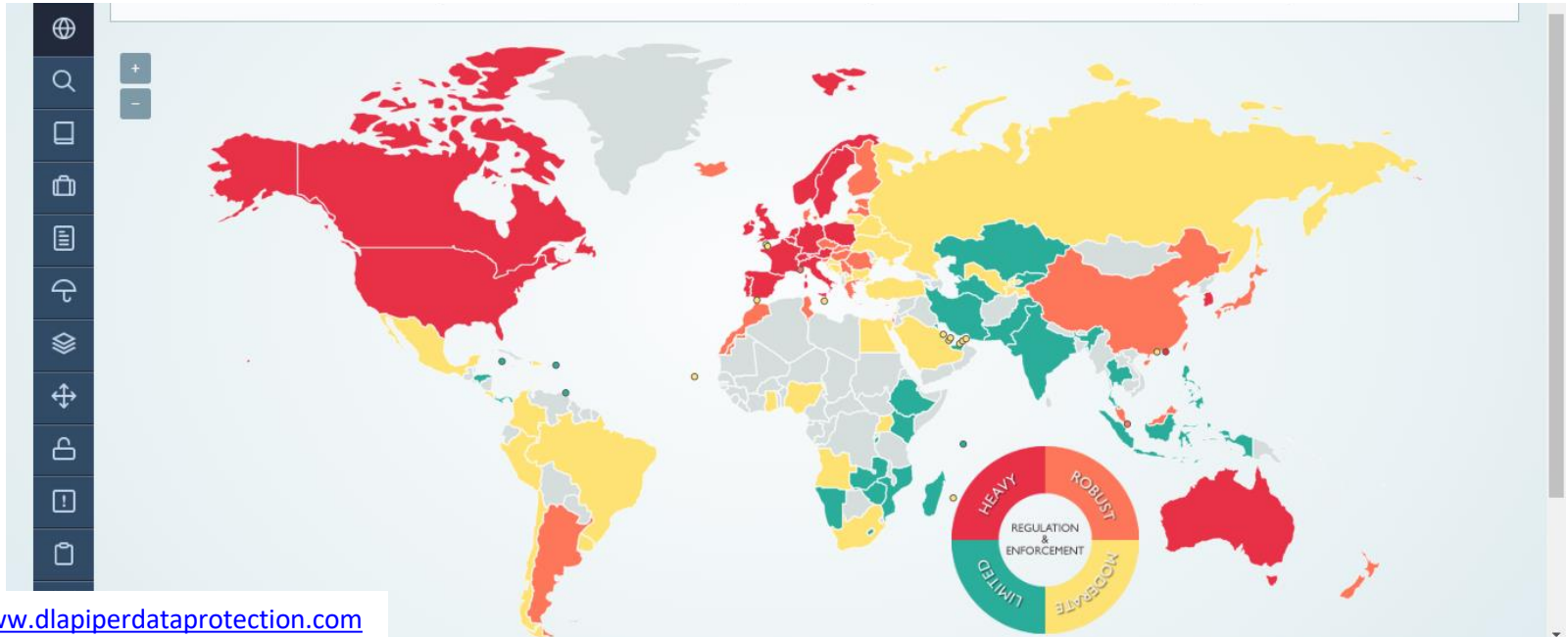
UNITED STATES – Has Legislation that is Highly Fragmented by Sector and State

A relatively new example is the California Consumer Privacy Act of 2018 (CCPA), effective January 1, 2020

https://www.cfr.org/report/reforming-us-approach-data-protection

Enterprises and Governments Need a Global Picture

One high-level view of data privacy laws across the world is provided by the DLA Piper Law Firm : https://www.dlapiperdataprotection.com/ Another good information source is the International Association of Privacy Professionals : https://iapp.org/

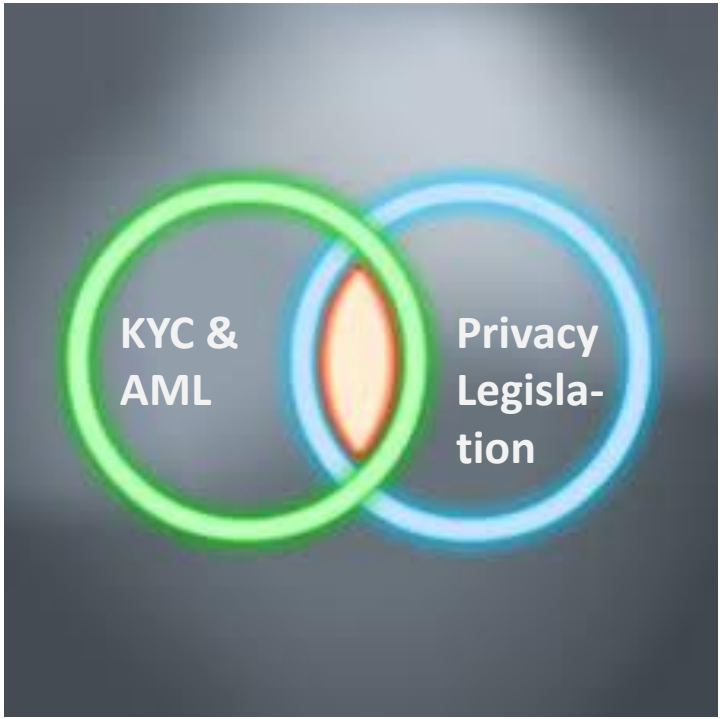


From https://www.dlapiperdataprotection.com

Enterprises are Left With Complicated Dilemmas

- How to evaluate adherence to rules in the countries of all clients?
- How to interpret legislation where little or no jurisprudence exists?
- How to reconcile conflicting or “similar but not the same” requirements?

Overlap and Tension Between Data Privacy and KYC/AML



- KYC and AML laws require the collection and storage of personal information and its use in risk analysis
- Privacy legislation puts strict constraints on what personal information can be collected, processed and stored

KYC and AML

Most frequently, legal requirements take precedence over privacy requirements

GDPR example

- Article 6(c) – allows for the processing of personal data “for compliance with a legal obligation to which the controller is subject”
- Article 6(f) – allows for data processing for “legitimate interests”, justifiable on a case-by-case basis

But what is “required for compliance” or a “legitimate interest” may be interpreted differently in different jurisdications

Enterprises are Left With More Dilemmas

- Again, how to interpret legislation where little or no jurisprudence exists?
- How to manage different interpretations of the same legislation or the same concepts in different jurisdictions?
- How to reconcile conflicting requirements without guidance?

ICT Security is a Key Element in Privacy

Privacy rules protect data from abuse by those who collect the data

However, it is equally important to protect data from theft which negates all of the data protection put in place legislation as well as by data collectors and processors

BUT News of Large Data Thefts is Common Place

The “latest” in August 2019

Almost 28 million records including "fingerprint data, facial recognition data, face photos of users, unencrypted usernames and passwords, logs of facility access, security levels and clearance, and personal details of staff“ was stolen from Suprema, a company that supplies biometric data used by 5700 organizations in 83 countries for access control systems

https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#579951246c60

AND Many ICT Security Standards Already Exist

The majority are referenced in the existing ITU ICT Security Standards Roadmap which SG17 is updating*

Currently, 4982 ICT Security Standards are listed of which only 445 are labelled as sector specific

Perhaps, this is part of the problem…

* https://www.itu.int/net4/ITU-T/landscape#?topic=0.1&workgroup=1&searchValue=&page=1&sort=Revelance
And https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/default.aspx

Data Collection & Bias
A “Personal” Perspective

When AI is used to process personal data, how will the decision-making process be documented?

When AI “learns” using biased or incomplete data, and then is used to process personal data, how will these errors be identified and consequences measured?

Now that permission must be asked in order to use personal data for machine learning, how will this impact the data sets used and will this aggravate problems of bias?

Access to

Technology
Financial Services
Privacy

How are we ensuring that

- Privacy protection does not become a barrier to trade in services from developing countries?
- Developing country populations also have privacy protection?
- The cost of privacy does not price financial services out of the reach of the poor and “almost poor”?

There are many questions,

Skilled individuals are needed

to look for answers

I would encourage you to be one of them!

Un Grand Merci!

Many Thanks!

Muchas Gracias!

Virginia Cram-Martos

crammartos@triangularity.net