

A Global Workshop on
**Digital Public
Infrastructure**



Trust, DPI and data protection

Rory Macmillan, 13 September 2023



Malicious actor

Infrastructure sharing rules



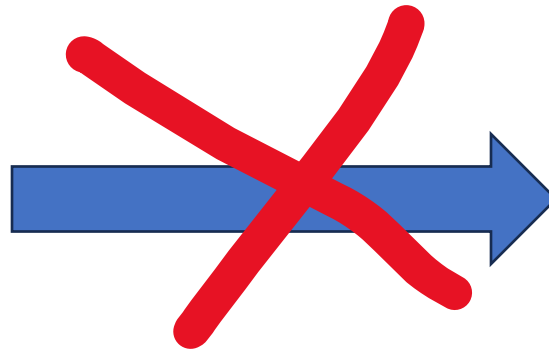


Trust system

Infrastructure architecture



FOMO



FUD

“monolithic expensive digitization vendor problem”
Pramod Varma, yesterday

DPI involves extensive processing of personal data

Digital identification systems

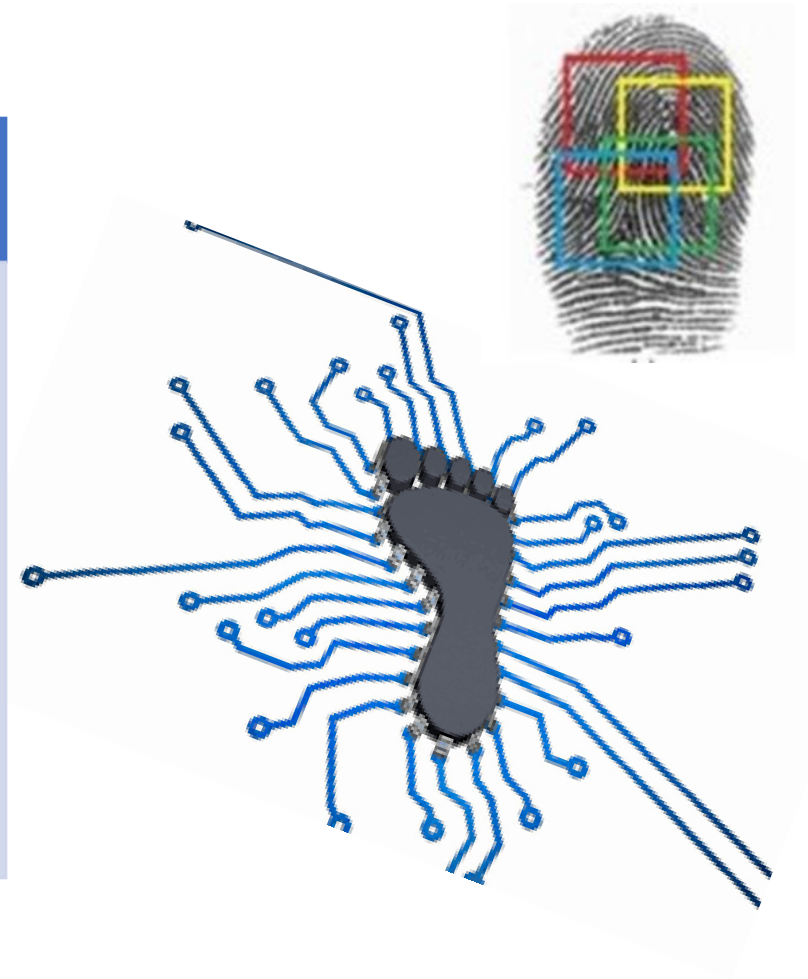
- Identification “attributes”
- Data trail from use of identification and authentication services

Digital payment systems

- Data used to identify payors, payees, accounts
- Transaction data trail of amounts, dates, regularity, location, relationships

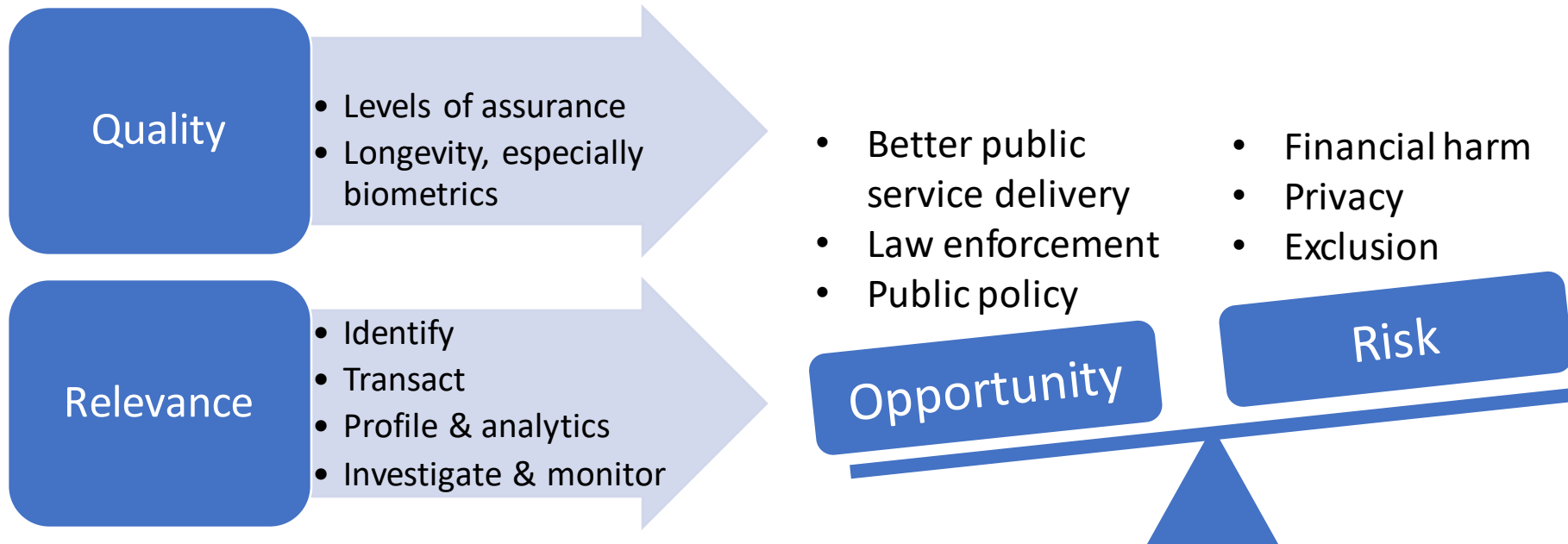
Data transfers

- Location, activity, employment, finances, health, education, relationships, appearance, biometrics, transactions, preferences, browsing, search

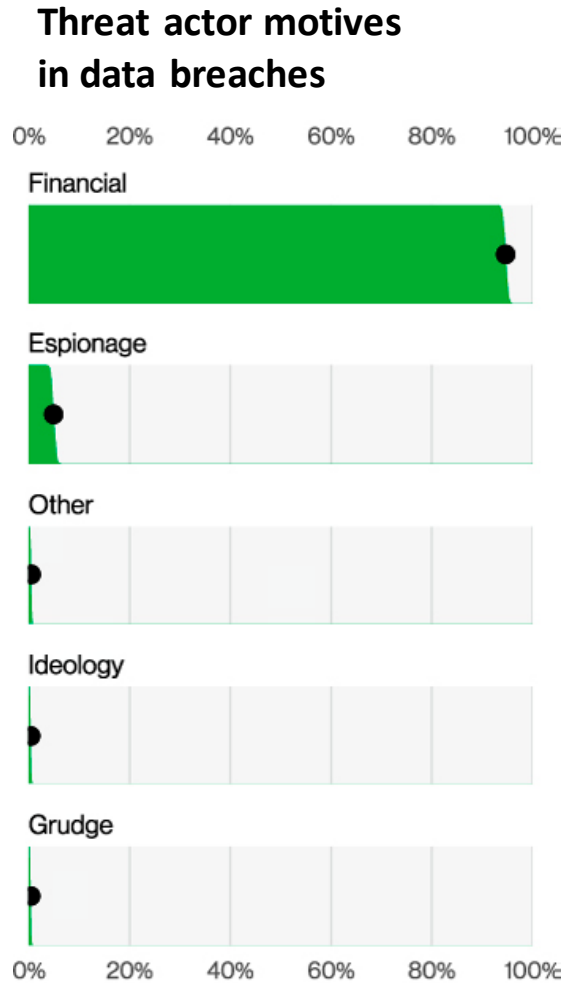


In 2022, over 2.5 quintillion bytes of data were generated each day (that’s 25 followed by 17 zeros), *Forbes*

The nature of DPI data makes it highly attractive but raises serious risk



80% of cyber attacks rely on vulnerable credentials, Verizon 2023 Data Breach Investigations Report



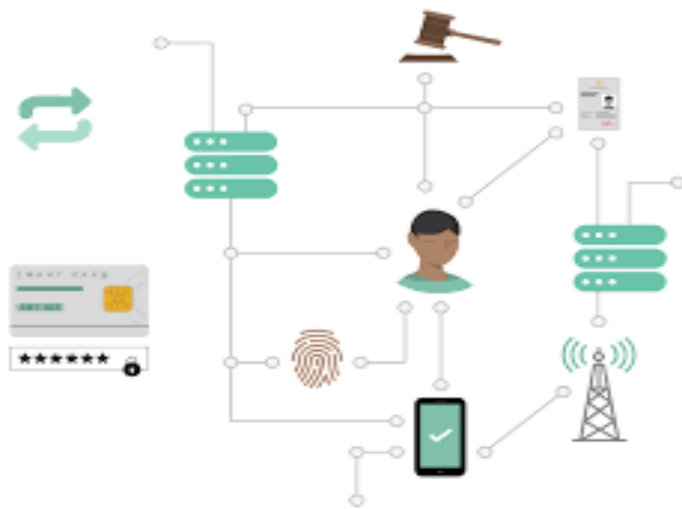
The public dimension can support trust, but not always warranted



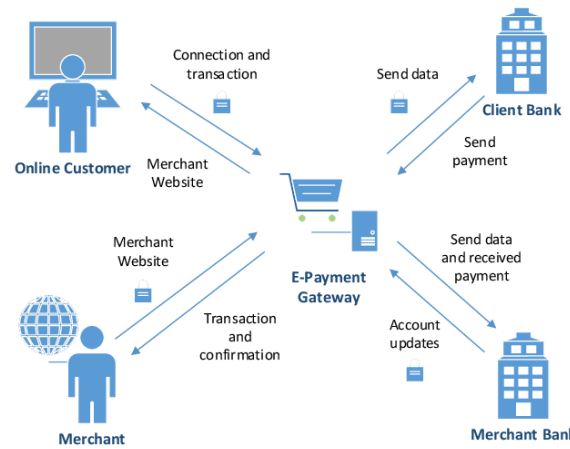
“The nine most terrifying words in the English language...”

Regulated quasi-open public-private systems involve multiple parties and weakest link exposure

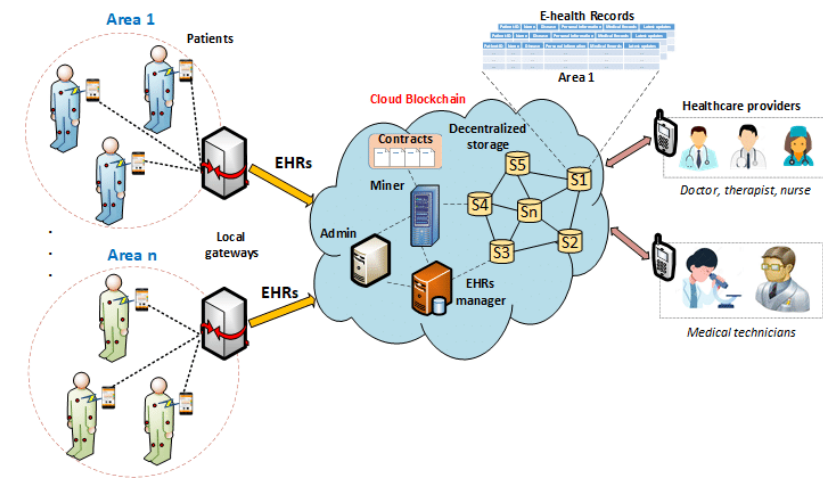
Digital identification



Digital payments

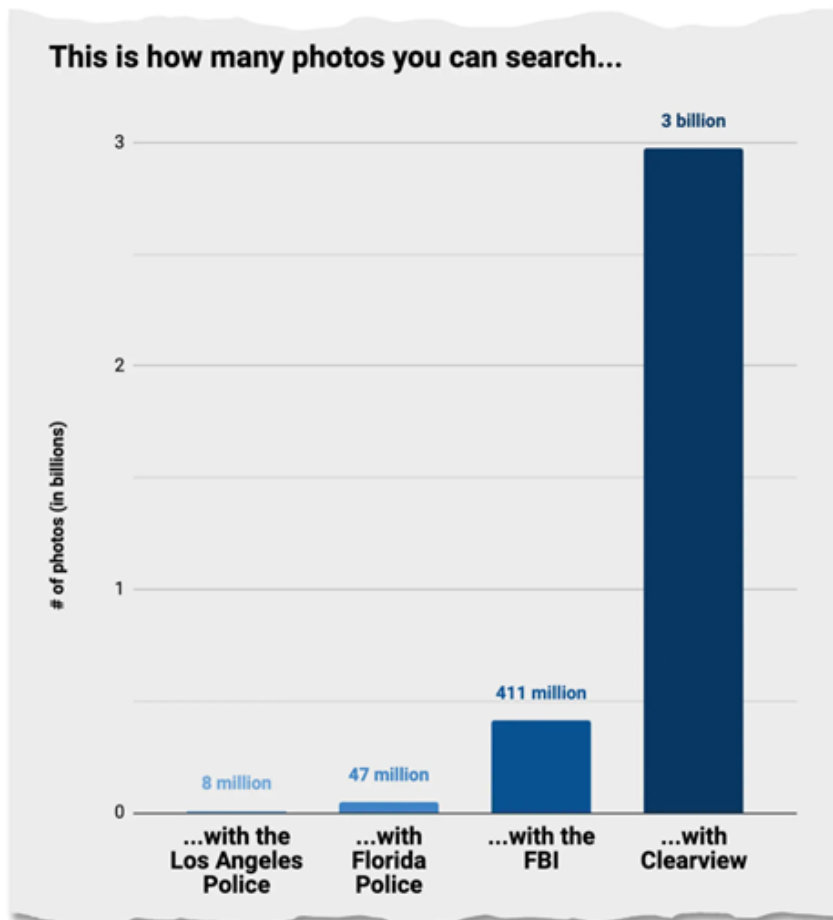


Data sharing



The opportunities and risks are stark in some systems, e.g., facial recognition

Clearview AI



- UKRAINE**
How Clearview AI Helped Shape the War in Ukraine
- CAPITOL RIOTS**
Helping Track Down Those Who Attacked the Capitol
- CHILD EXPLOITATION**
Finding Child Predators & Rescuing Children Victims
- EXONERATION**
Locating a Witness in a Vehicular Homicide Case

Other countries also have systems (e.g., Tiandyi) that are exported to governments internationally

30+ Billion Images in our law enforcement database – **the largest** in the world by far

99+% accuracy for all demographics¹

Trained on the **largest and most diverse** dataset

#1 in US for most difficult category "Wild Photos"²

The trust issue can impede DPI development



In a 2021 referendum, 64% rejected the Swiss eID, mistrusting reliance on licensing private companies to operate it



Conseil Constitutionnel de France, *Décision n° 2012-652 DC du 22 mars 2012*, rejected ID scheme for collecting data **disproportionate to the purpose**



Supreme Court in *Madhewoo v Mauritius* found the ID card scheme's **indefinite period of retention** of biometrics unconstitutional



Supreme Court in *Justice Puttaswamy v Union of India* ordered that, **without data protection** legislation, Aadhaar could not be used to verify individual identity to secure loans, file tax returns, open bank accounts, make large purchases or sell property



Mexico's Supreme Court suspended law requiring collection of **biometrics** by telcos for SIM registration



High Court in *Nubian Rights v Attorney General of Kenya* found the National Integrated Identity Management System unconstitutional violation of **privacy**, and prohibited the government from collecting GPS and DNA information, and also prohibited the government from conditioning access to public services on national identity registration



Supreme Court in *Robinson v Attorney General of Jamaica* declared the country's National Identification and Registration Act system that collected demographic, biometric and biographic information unconstitutional and void ("impact the **trust** level between citizen and state")

Insert poll here:

**Has your country faced any objections
to a digital identification system?
Yes/No**

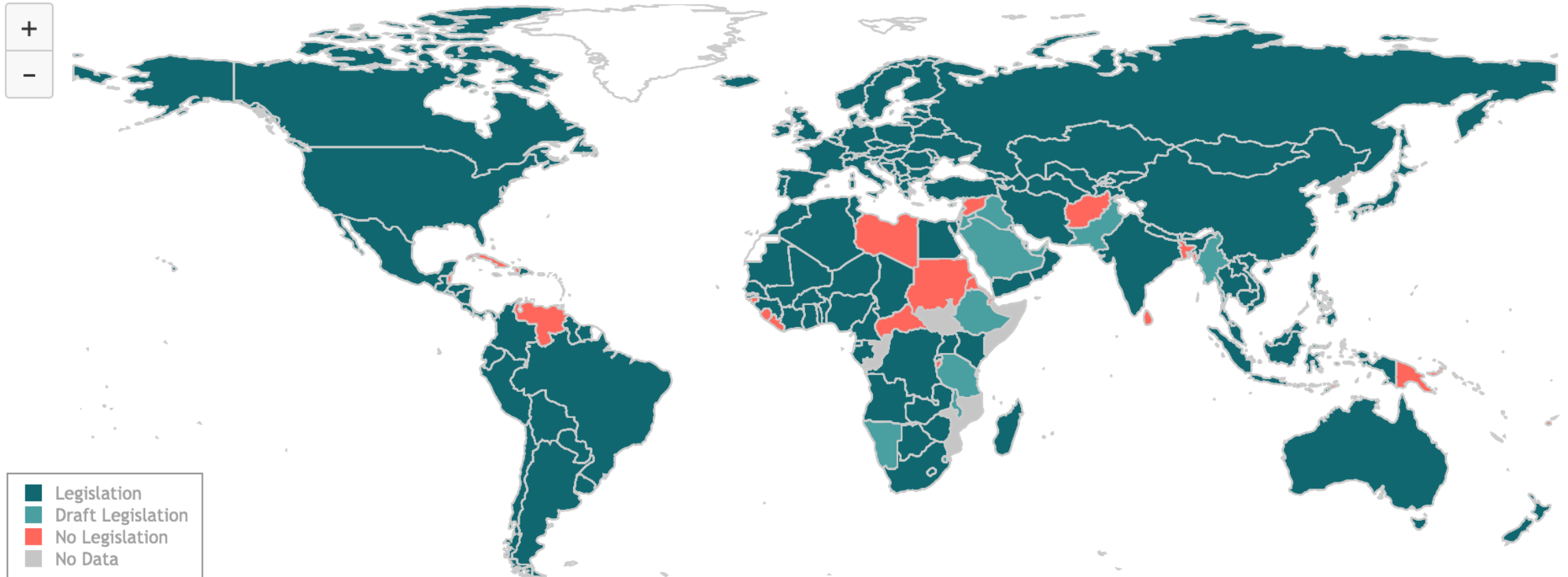
Insert poll here:

Does your country have:

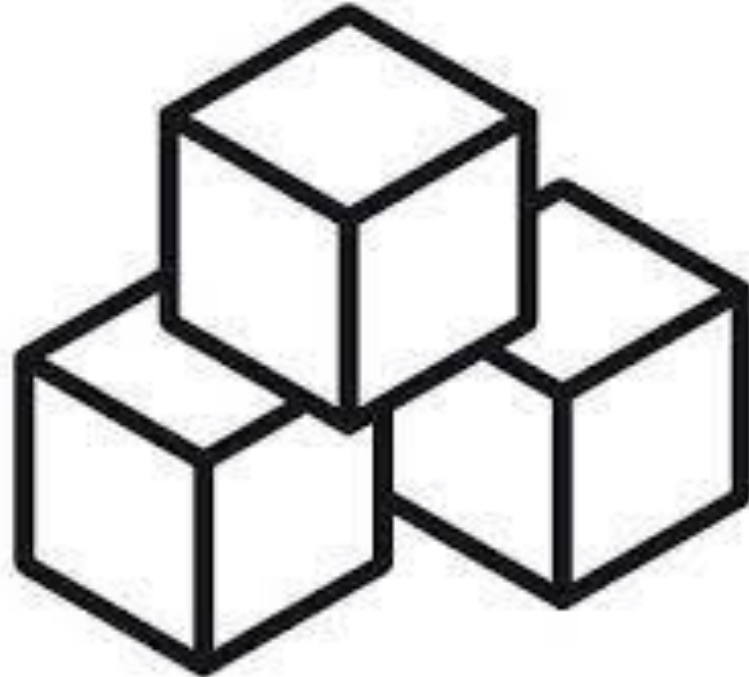
- (1) a data protection law in place,**
- (2) a bill before the legislature,**
- (3) a draft bill under preparation, or**
- (4) nothing as yet?**

The importance of trust is leading to the roll out of data protection legislation globally

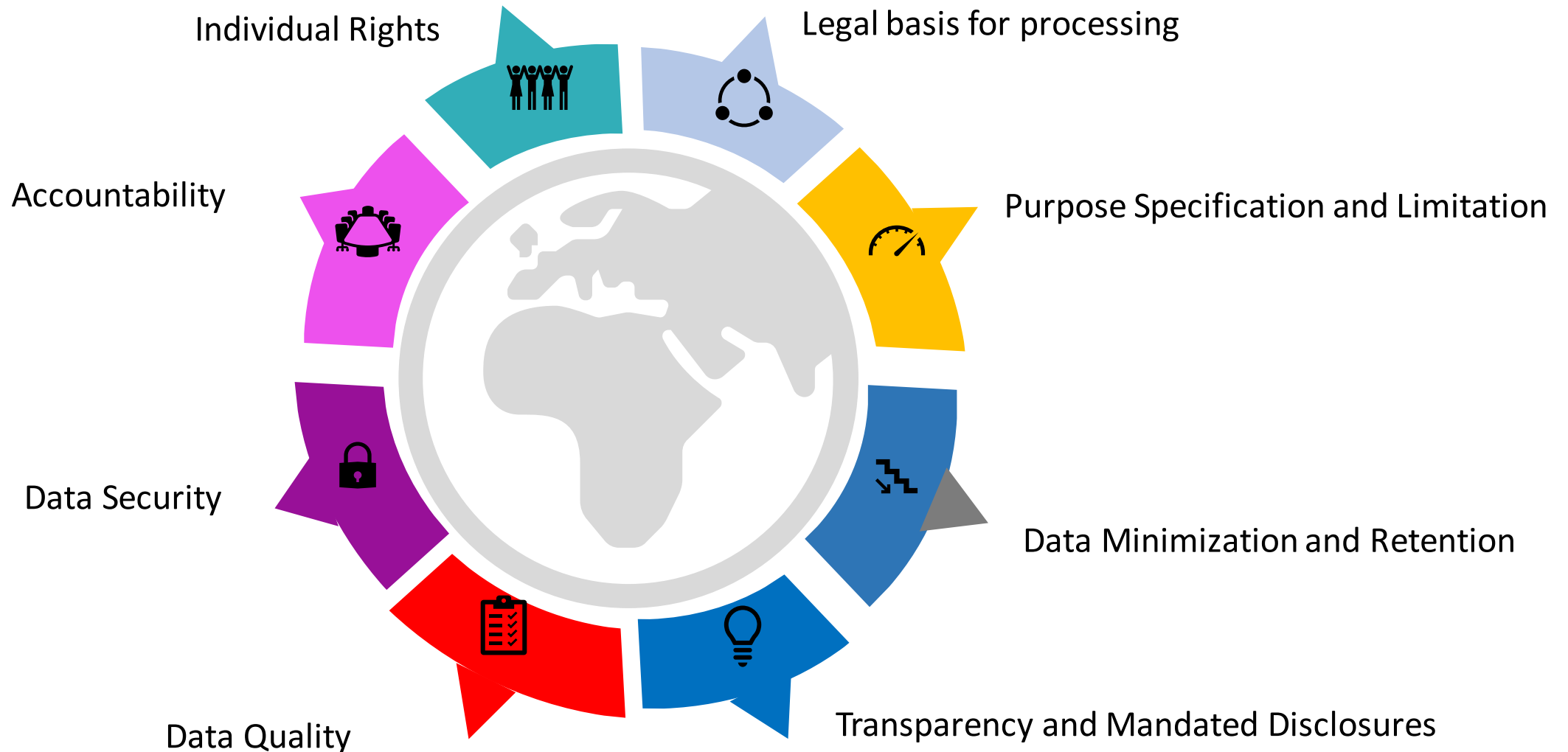
Data Protection and Privacy Legislation Worldwide



Let's call it **legal** digital public infrastructure



These laws are (more or less) addressing a variety of data protection themes



Many laws aim to build trust by empowering individuals



Informed about purpose of processing, who is processing, data breaches and rights



Consent (?)



Right to object to processing



Rights of access, correction and erasure



Redress systems



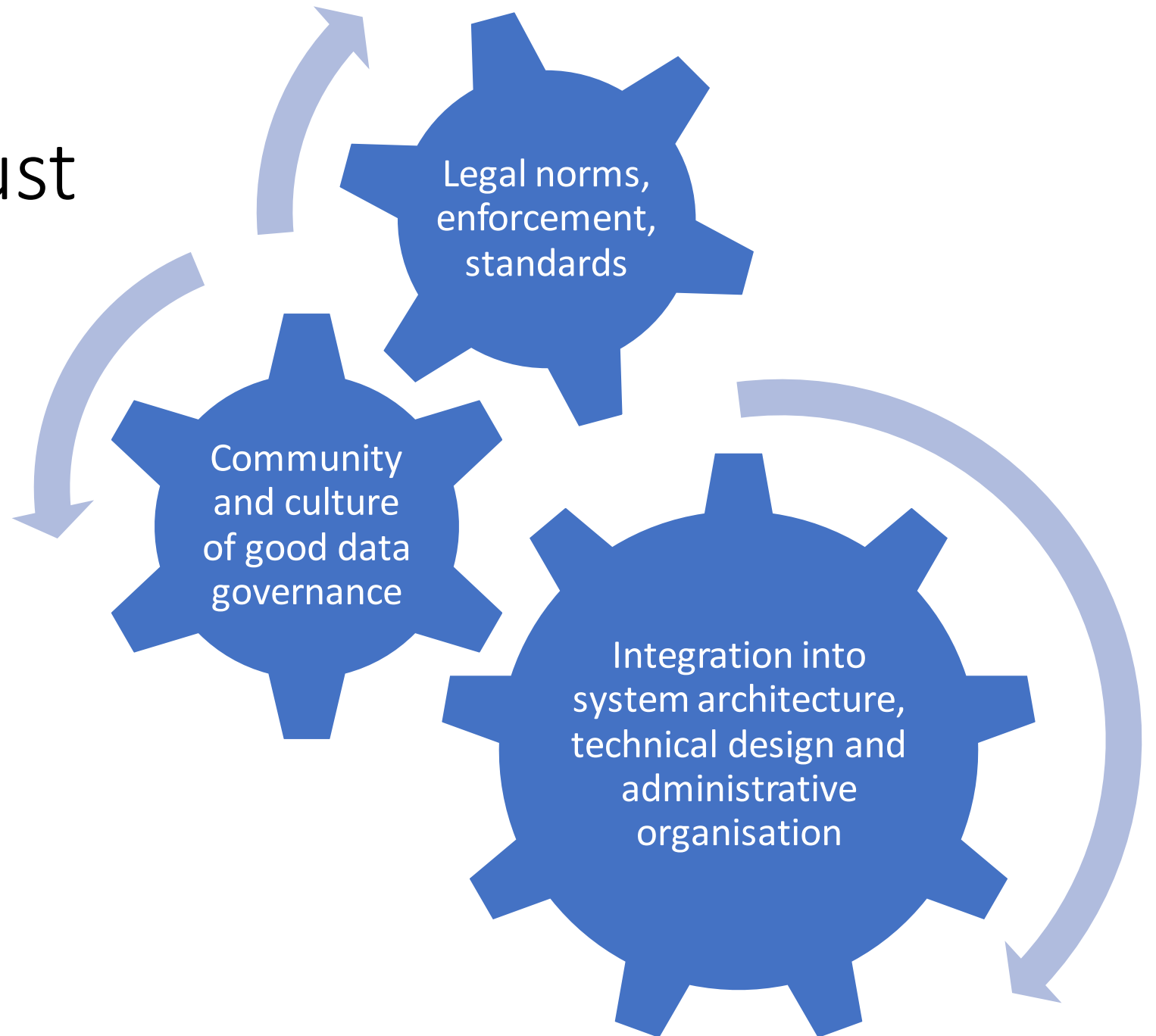
Too good to be true?

Yeah...

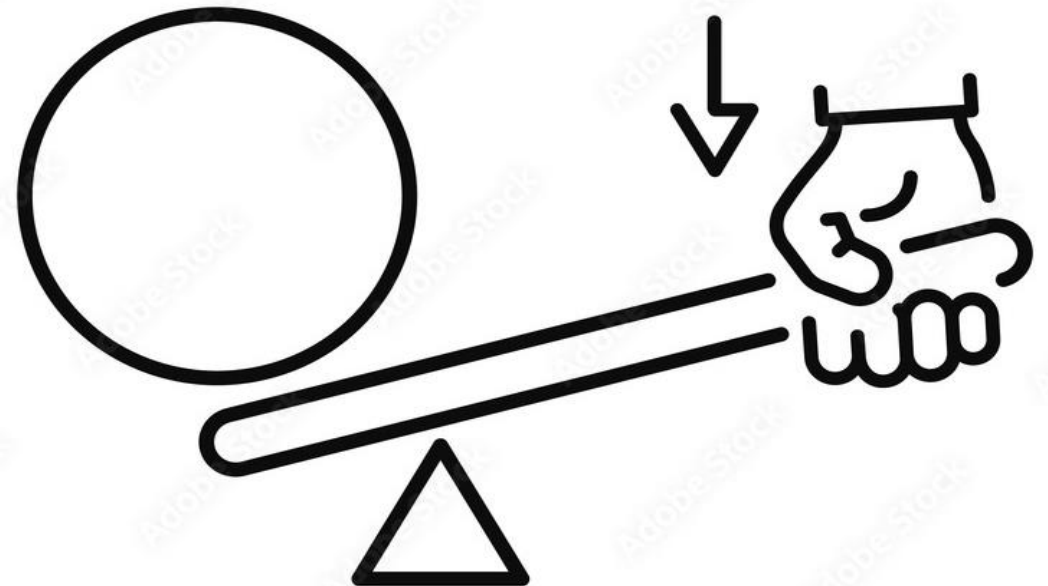
But...

Consider Schrems (and all the other cases)

Scale + VVV means data protection must go further than compliance and enforcement of legal rights and obligations

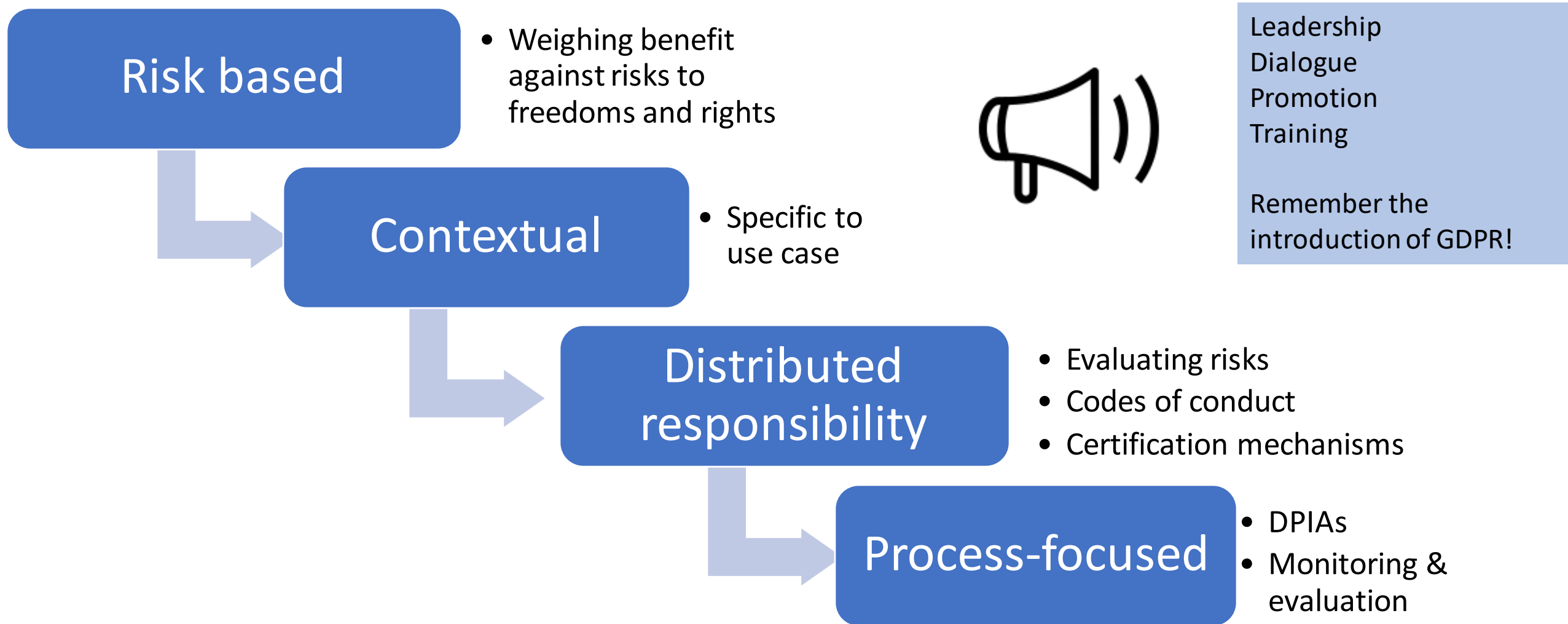


Authorities need a paradigm shift as to what a regulator does



E.g., cross border data

Data protection depends on an amplification effect together with some high-profile enforcement cases



As with DPI itself, some major use cases will boost wider adoption and require deep DPA engagement

System architecture

- Data collected
- Randomised UINs
- Services provided
 - Y/N inquiry, authentication
- Interoperability with other systems (e.g., population register, CRVS)
- Data segregation
- Retention & deletion

Administrative organisation

- Access control
 - Separation of duties
 - Least privilege
- Relying party eligibility, certification and conditions
- Outsourcing & procurement
- Access by law enforcement and security

Privacy enhancing technologies

- Encryption
- Tokenisation
- eWallet
- Sovereign/distributed identities
- Anonymisation when allowing access for research & public policy

In summary

- Take trust seriously
- Use law and regulation
- But push further into architecture, design and organisation
- Leverage and amplify
- Engage deeply with the big DPIs