Algebraic Approach to Data Protection by Design for Data Subjects

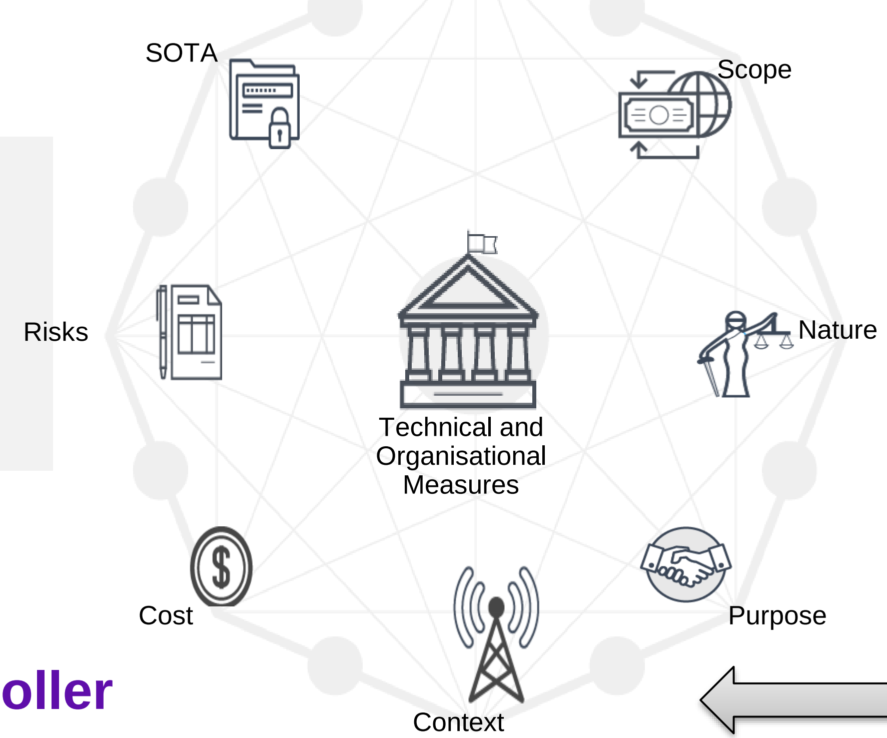
Dr. Rula Sayaf

Data Subjects

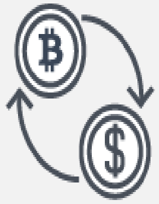
The Context:
Data Protection by Design and Default (DPbD^2)

Upon determining processing means

Data Protection by Design



During the processing

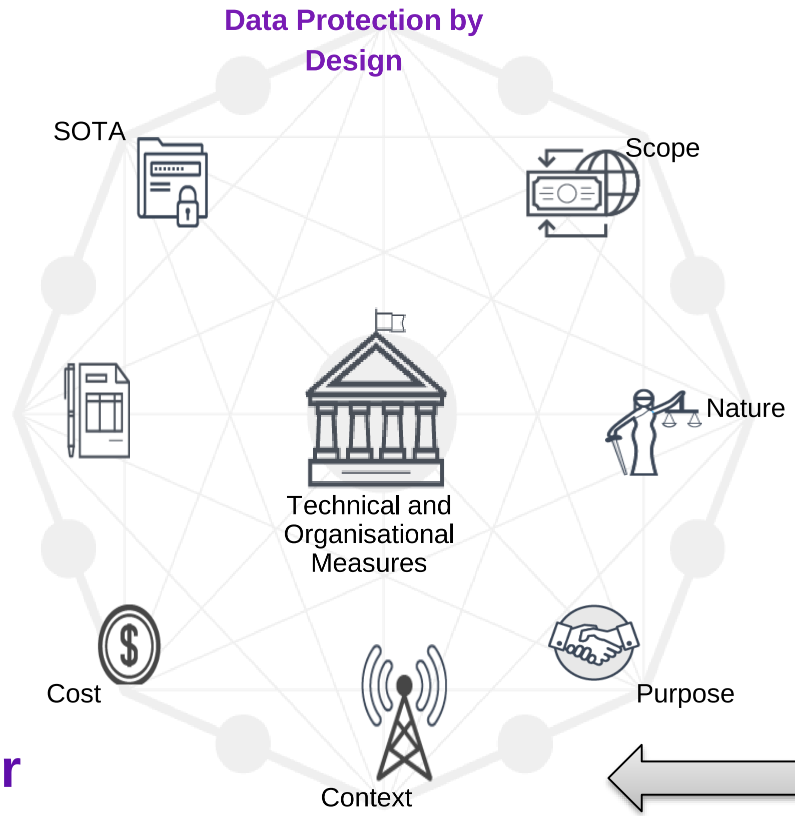


Data Controller

Data Subjects

The Context:
Data Protection by Design and Default (DPbD^2)

Upon determining processing means


Data Protection by Design
SOTA
Scope
Risks
Nature
Technical and Organisational Measures
Cost
Purpose
Context

During the processing

Data Controller

Data Subjects

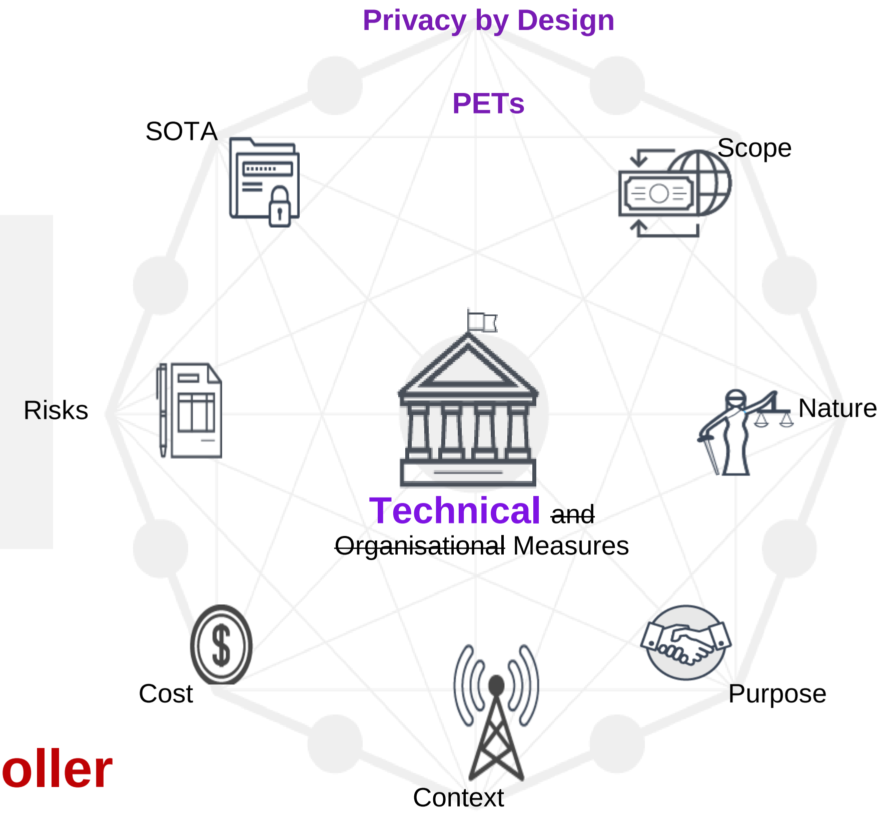
- Data minimisation
- Purpose limitation
- Accurate and update-to-date data
- Storage retention
- Transparent
- Lawful

- GDPR requirements
- Protect the rights of data subjects

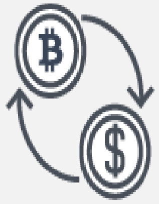
Privacy vs
Data Protection by Design and Default (DPbD^2)

Upon determining processing means

Data Controller



During the processing

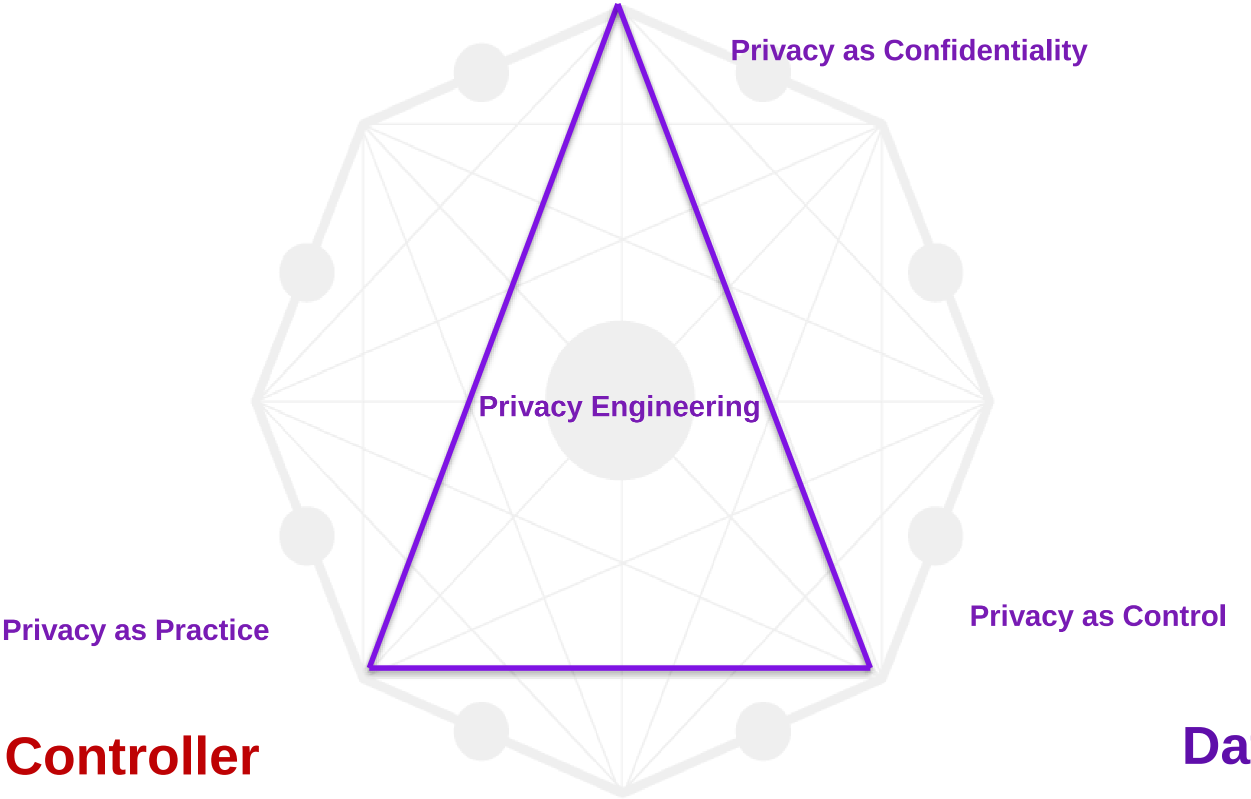


Data Subjects

- Data minimisation
- Purpose limitation
- Accurate and update-to-date data
- Storage retention
- Transparent
- Lawful

- GDPR requirements
- Protect the rights of data subjects

Privacy vs
Data Protection by Design and Default (DPbD^2)



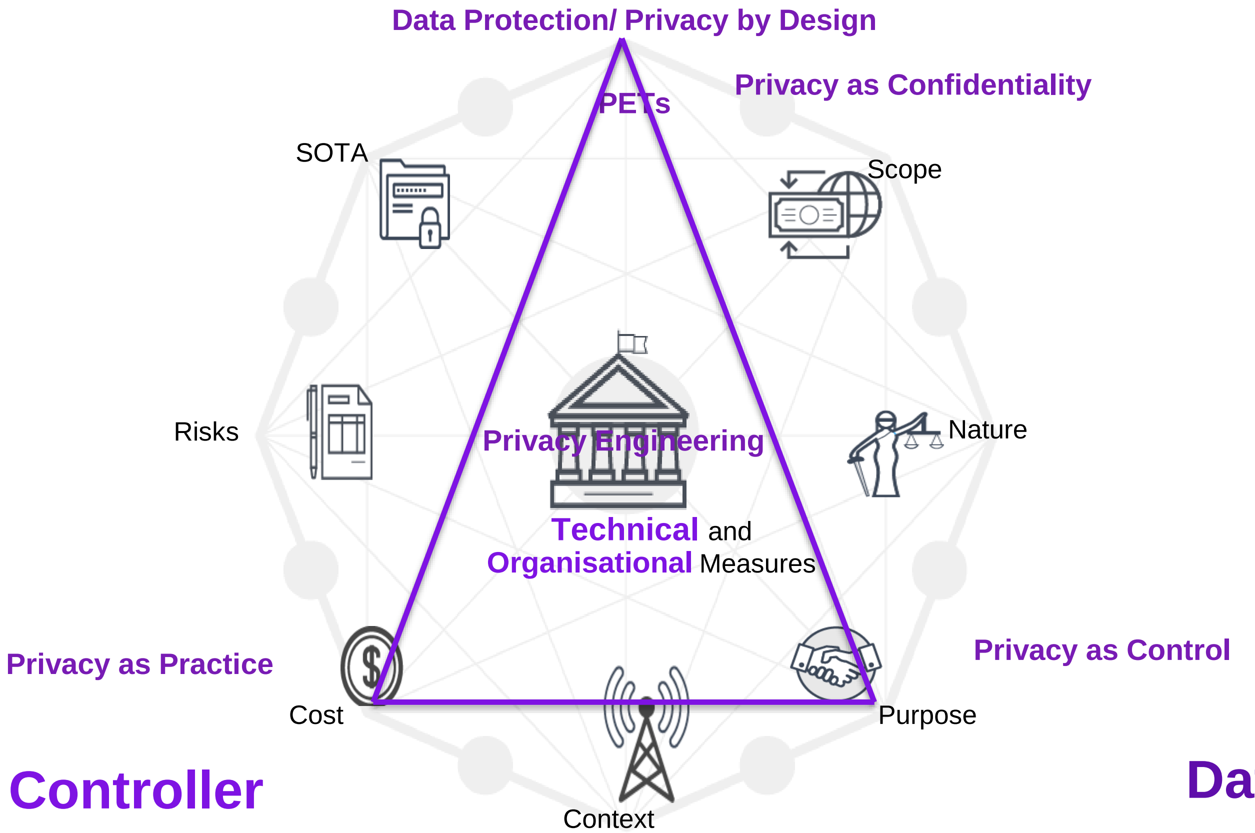
Data Controller

- Data minimisation
- Purpose limitation
- Accurate and update-to-date data
- Storage retention
- Transparent
- Lawful

Data Subjects

- GDPR requirements
- Protect the rights of data subjects

Data Protection by Design and Default (DPbD^2)



Data Controller

Data Subjects

- Data minimisation
- Purpose limitation
- Accurate and update-to-date data
- Storage retention
- Transparent
- Lawful

- GDPR requirements
- Protect the rights of data subjects

Status quo
Data Protection by Design and Default (DPbD^2)

Focus:

Data Register

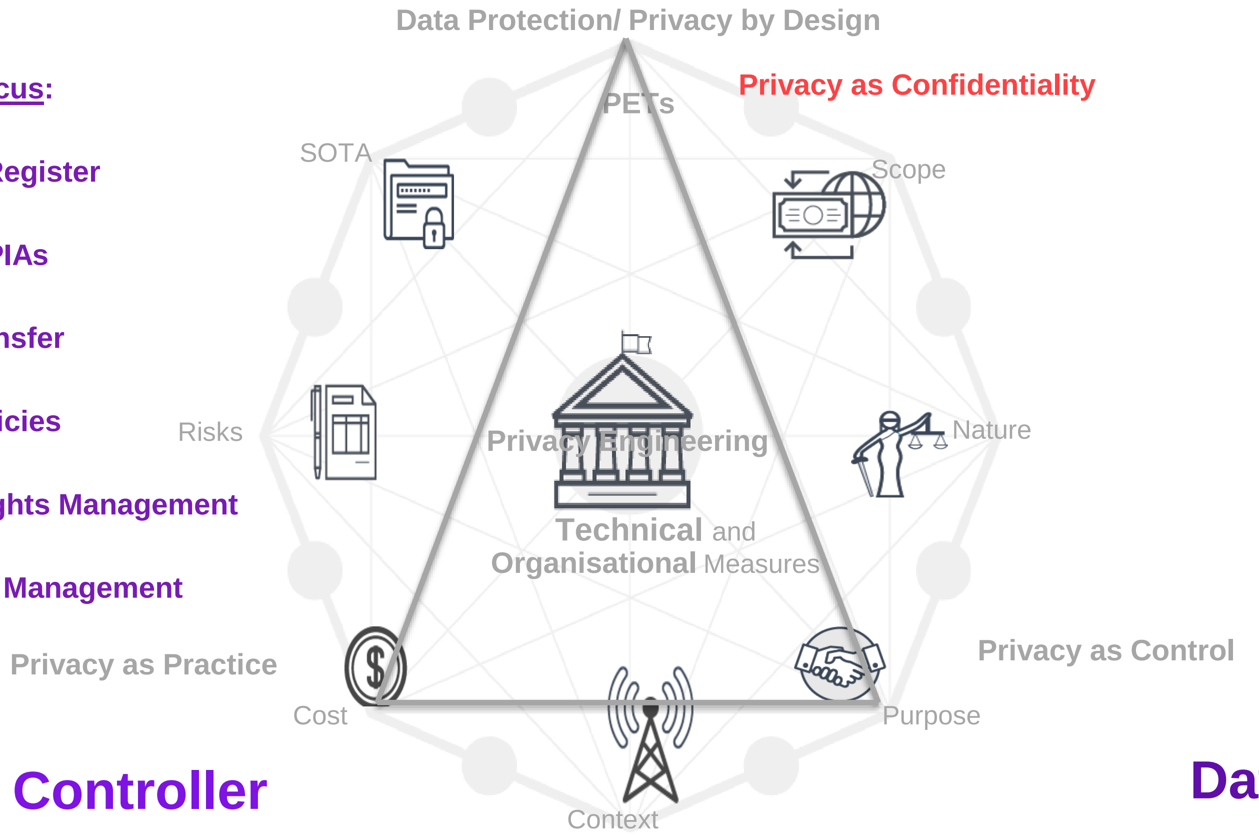
DPIAs

Transfer

Policies

Data Subject Rights Management

Compliance Management



Data Controller

Data Subjects

Data Protection by Design and Default (DPbD^2)

Data Protection/ Privacy by Design

Privacy as Confidentiality

Focus:

Data Register

DPIAs

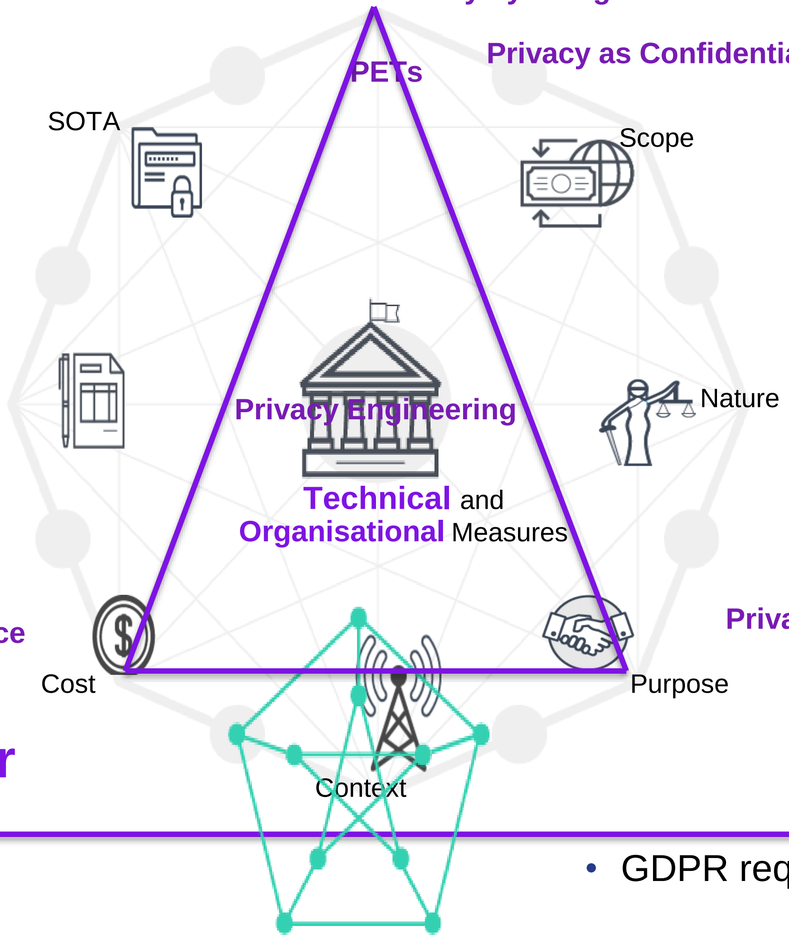
Transfer

Policies

Data Subject Rights Management

Compliance Management

Privacy as Practice



Privacy as Control

Data Controller

Data Subjects

- Data minimisation
- Purpose limitation
- Accurate and update-to-date data
- Storage retention
- Transparent
- Lawful

- GDPR requirements
- Protect the rights of data subjects

Algebraic Approach
Data Protection by Design and Default (DPbD^2)

Focus:

Data Register

DPIAs

Transfer

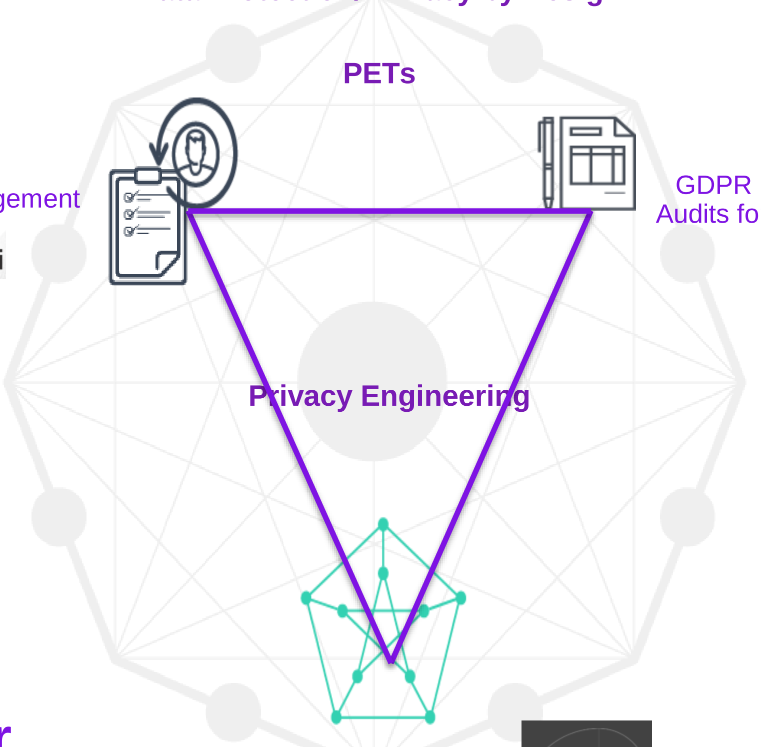
Policies

Data Subject Rights Management

Compliance Management

Sedicii

Identity Management



Data Protection/ Privacy by Design

PETs

Privacy Engineering

Privacy Algebra

Mizen Group

GDPR Compliance Management Audits for Data Controllers and Data Subjects

Data Controller

- Data minimisation
- Purpose limitation
- Accurate and update-to-date data
- Storage retention
- Transparent
- Lawful

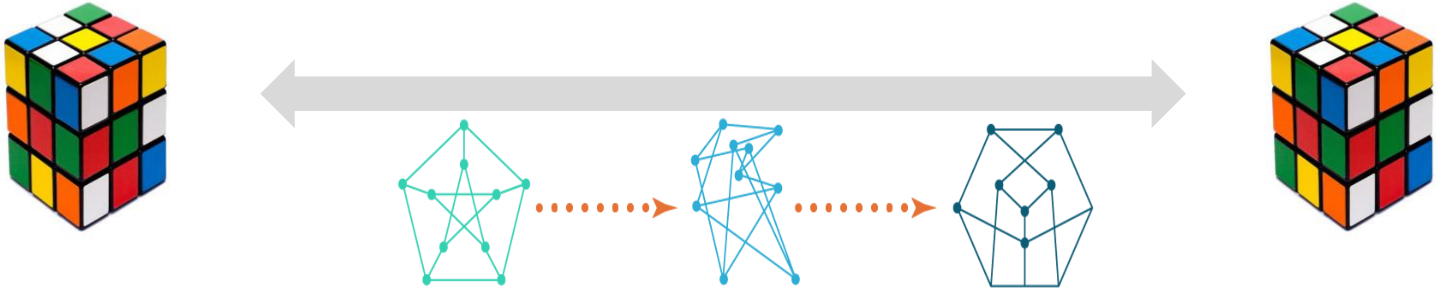
Data Subjects

- GDPR requirements
- Protect the rights of data subjects

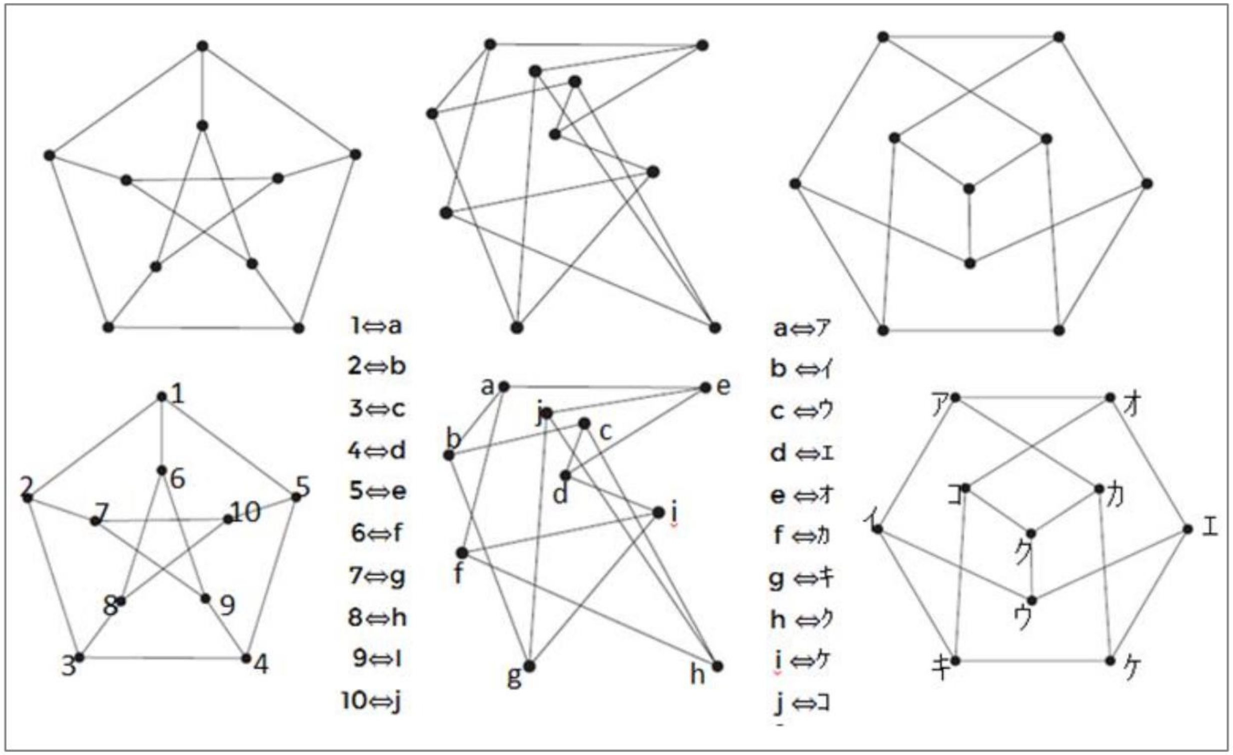
Zero Knowledge Proof (ZKP)

Interactive zero knowledge proof using graph isomorphism (US Patent: 8,411,854 B2)

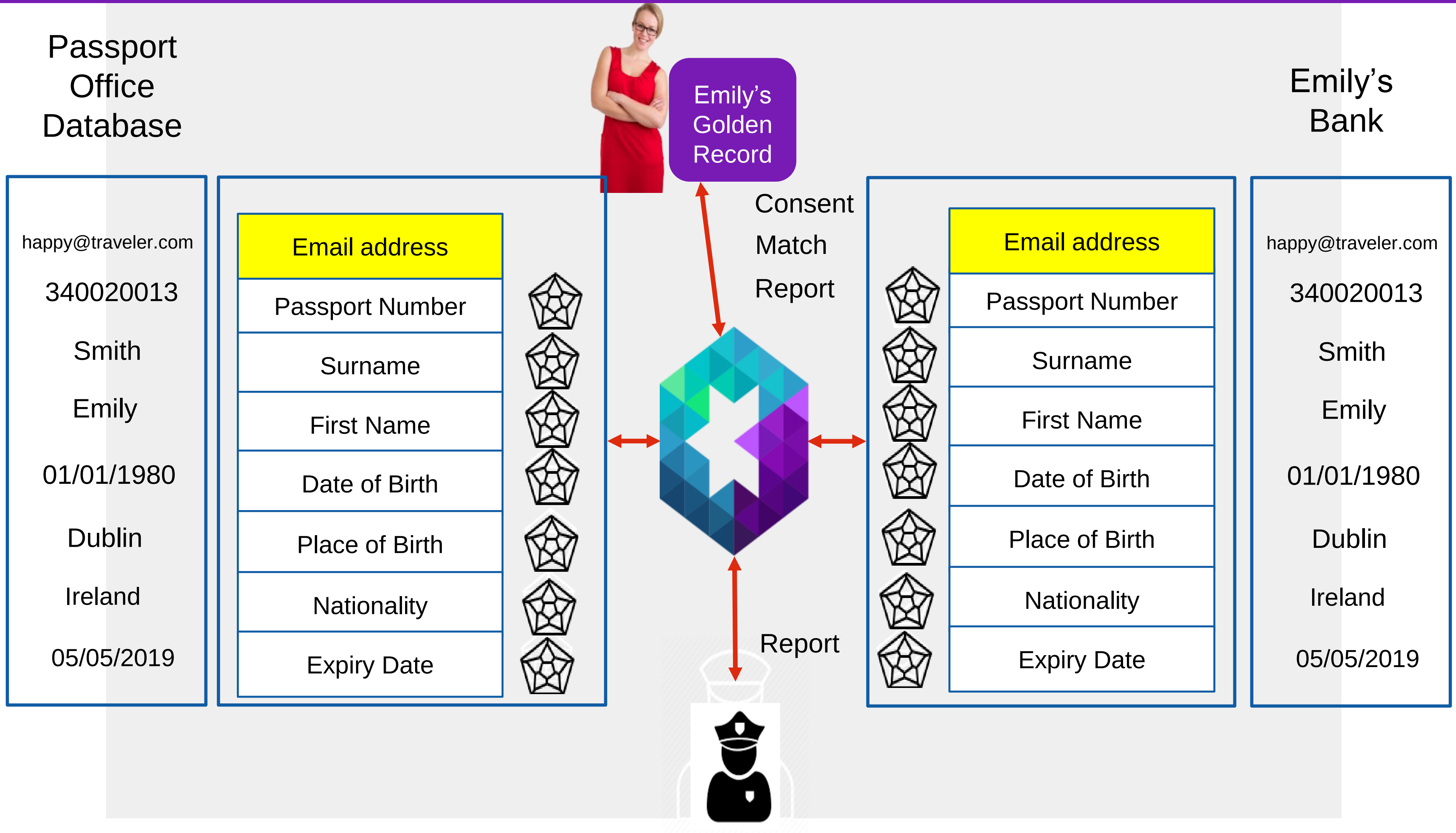
Real-Time Verifications



Zero Knowledge Proof (ZKP)
Graph Isomorphism



Zero Knowledge Proof (ZKP)
How it Works - Passports



Passport Office Database

happy@traveler.com

340020013

Smith

Emily

01/01/1980

Dublin

Ireland

05/05/2019

Email address

Passport Number

Surname

First Name

Date of Birth

Place of Birth

Nationality

Expiry Date

Emily's Golden Record

Consent

Match

Report

Report

Email address

Passport Number

Surname

First Name

Date of Birth

Place of Birth

Nationality

Expiry Date

Emily's Bank

happy@traveler.com

340020013

Smith

Emily

01/01/1980

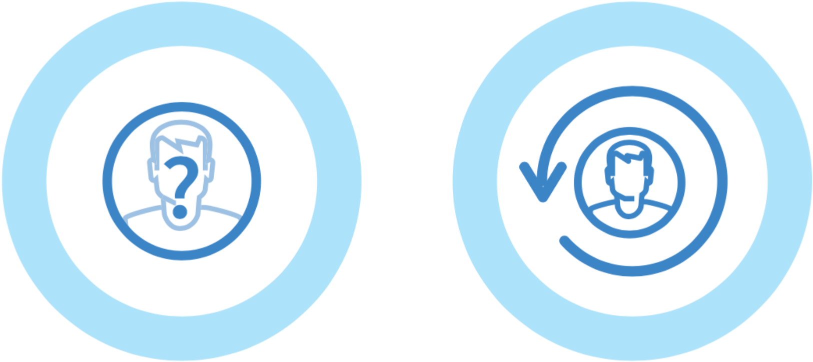
Dublin

Ireland

05/05/2019

Passport Matching in Real-Time against Authoritative Source for ID Proofing

Zero Knowledge Proof (ZKP) Scenarios

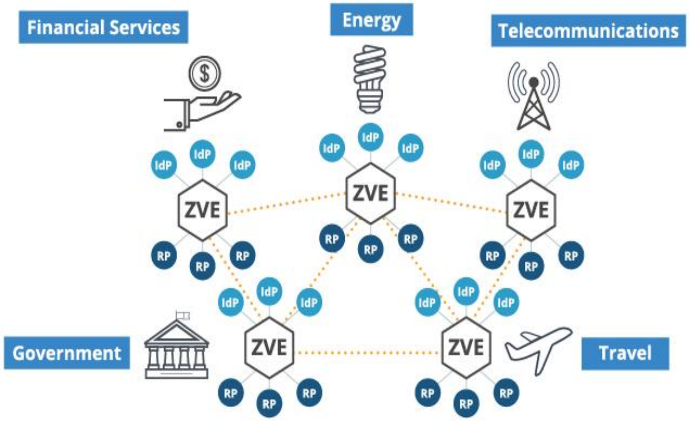


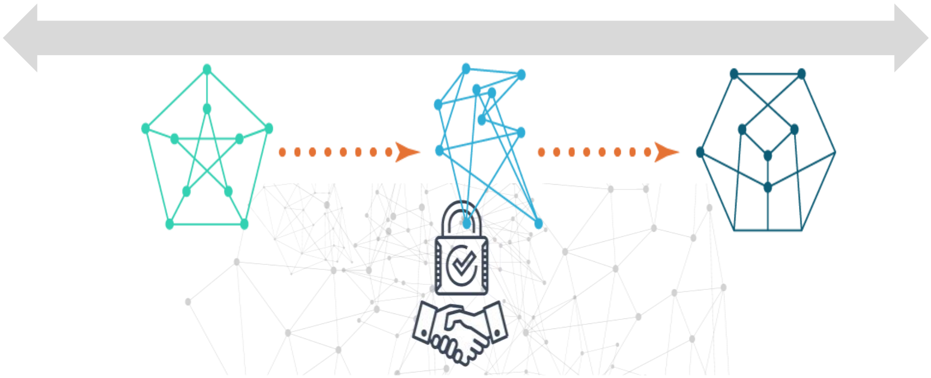
ANONYMOUS

REAL-TIME KYC

Zero Knowledge Proof (ZKP)
Network of Identity Providers

KRIPTAN

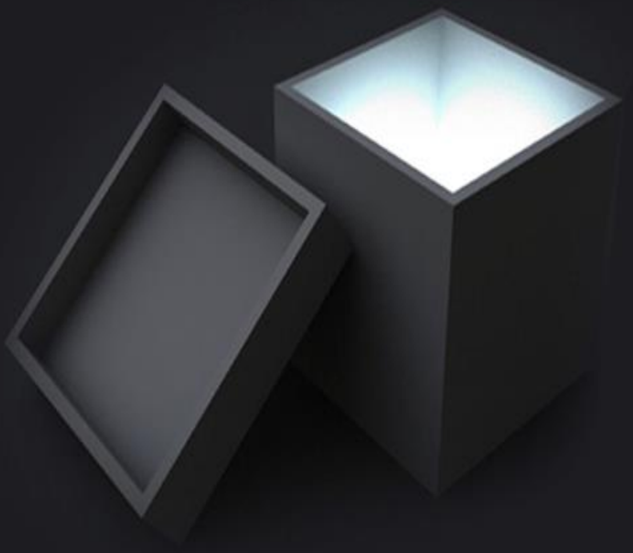


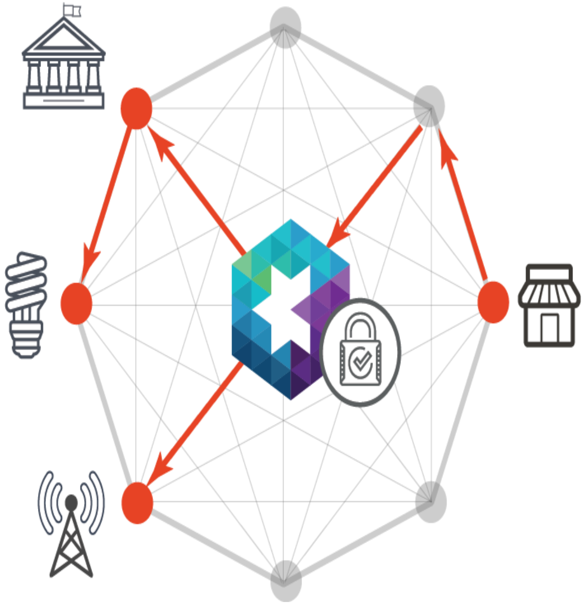


Zero Knowledge Proofs (ZKP)
+
DPbD²

"I know something you know.

I can prove it without telling you what I know."





Privacy-preserving, minimised personal data collection, unless the subject consents.

The subject **controls data,** and is involved by running a mobile app

Data collection is **transparent** to subjects

Data is **abstracted, not encrypted** in the traditional sense.

ZKP
Data Protection by Design and Default (DPbD^2)

Focus:

Data Register

DPIAs

Transfer

Policies

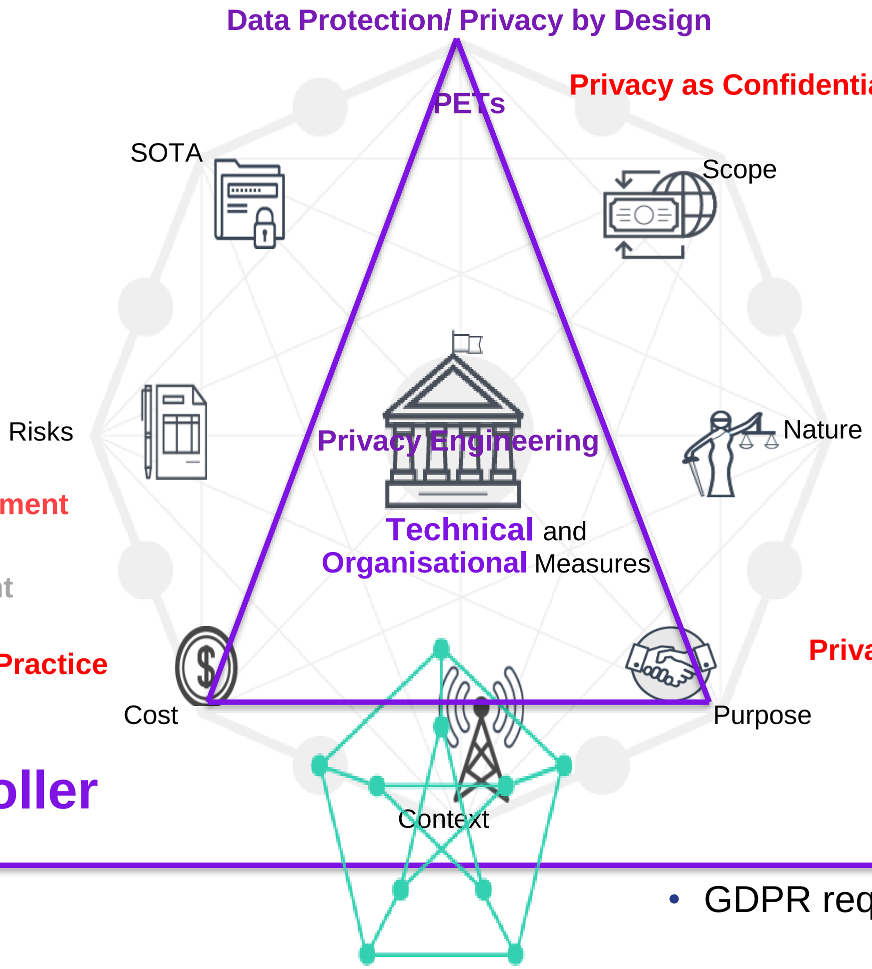
Data Subject Rights Management

Compliance Management

Privacy as Confidentiality

Privacy as Practice

Privacy as Control



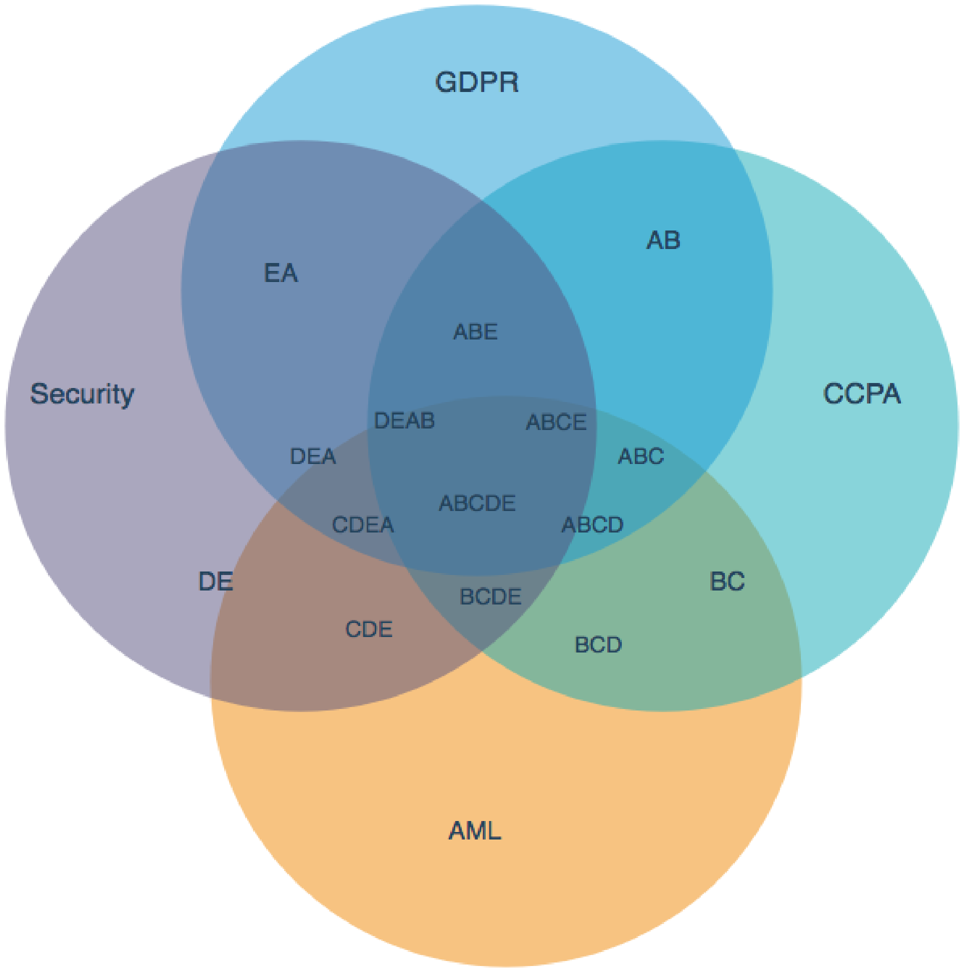
Data Controller

Data Subjects

- Data minimisation
- Purpose limitation
- Accurate and update-to-date data
- Storage retention
- Transparent
- Lawful

- GDPR requirements
- Protect the rights of data subjects

Algebraic Approach
Compliance Management



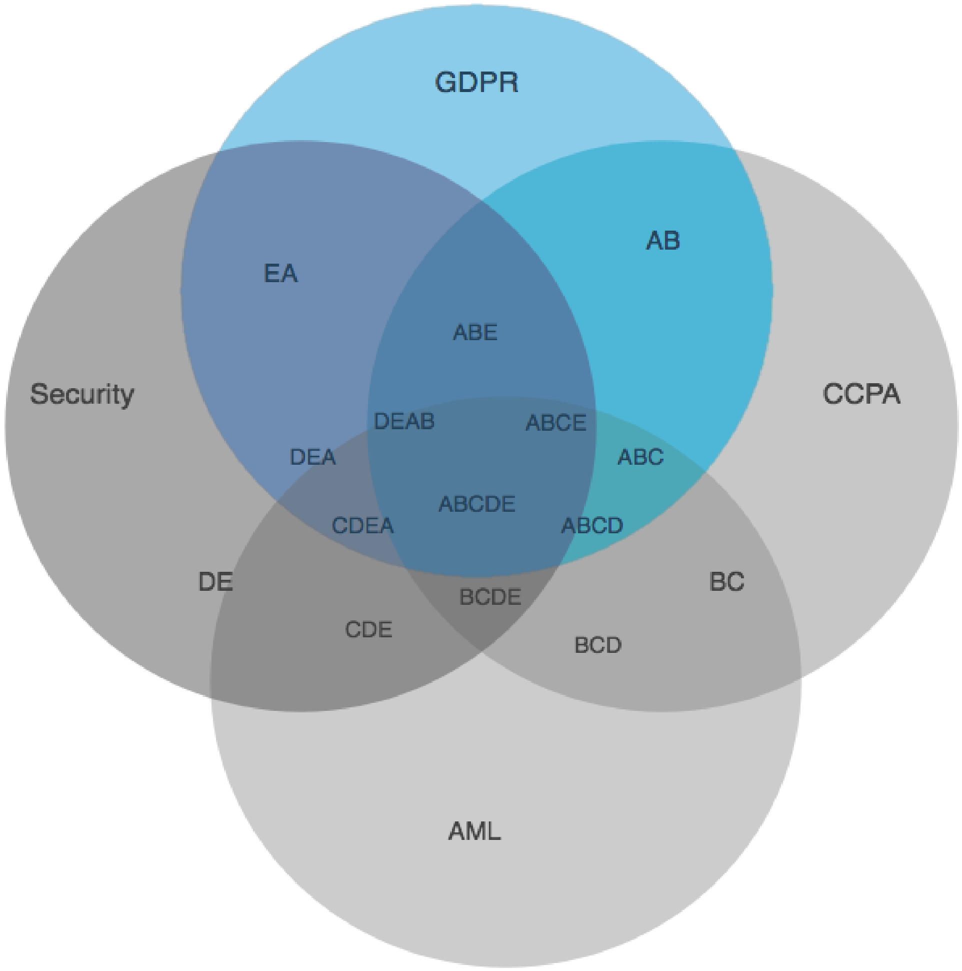
Data Controller

Mizen Group

GDPR Compliance Mangement Audits:

- Focus on PETs
- Evidence-based compliance
- Cross-regulatory compliance management

Algebraic Approach
Compliance Management



Data Subjects

Mizen Group

GDPR Feedback Assessments for Data Subjects:

- What PETs
- Data controller response
- Amount of personal data
- Degree of transparency
- …

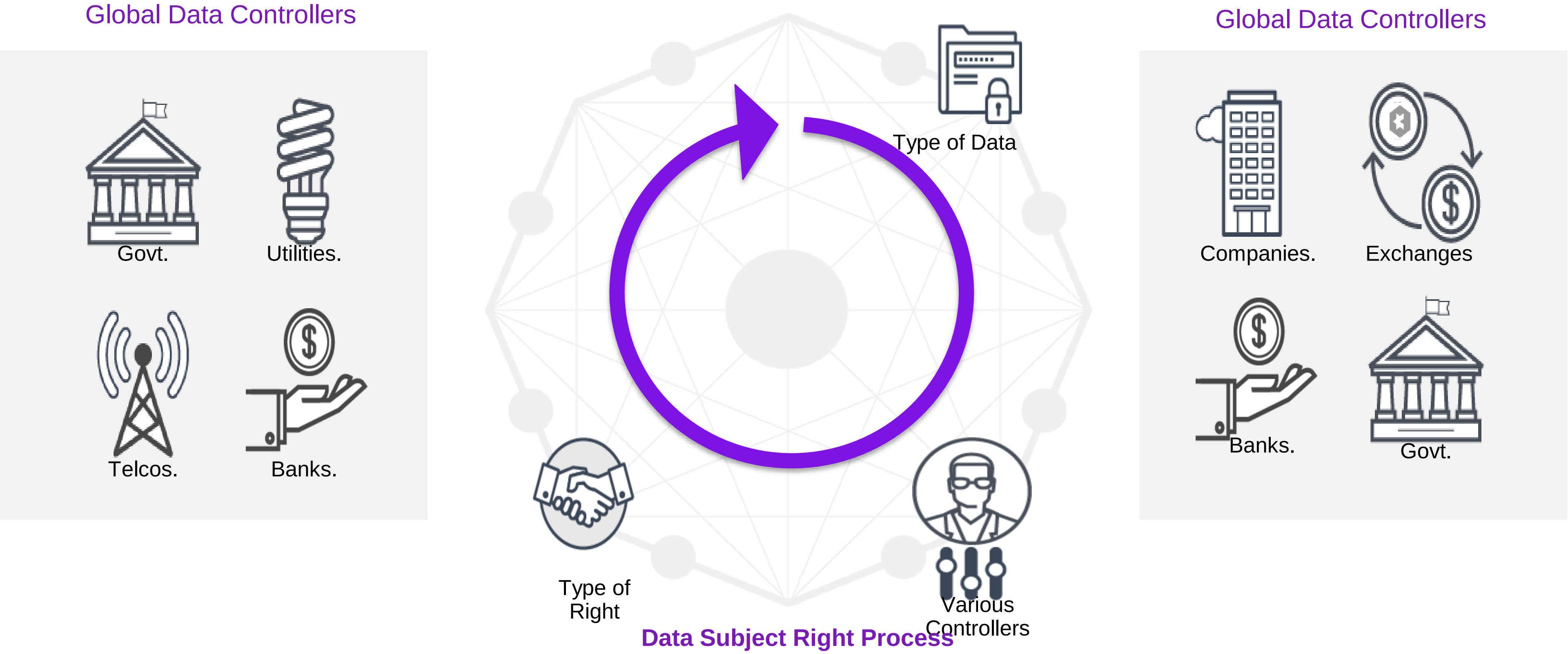
The | Mizen | Group

Data Subject Rights Automation

PersonalData.io (adversarial position)

- Data Controller
- Collected personal data
- The type of processing

- Access to data
- Information about processing
- Algorithmic accountability



Global Data Controllers

Govt.

Utilities.

Telcos.

Banks.

Type of Data

Type of Right

Various Controllers

Data Subject Right Process

Global Data Controllers

Companies.

Exchanges

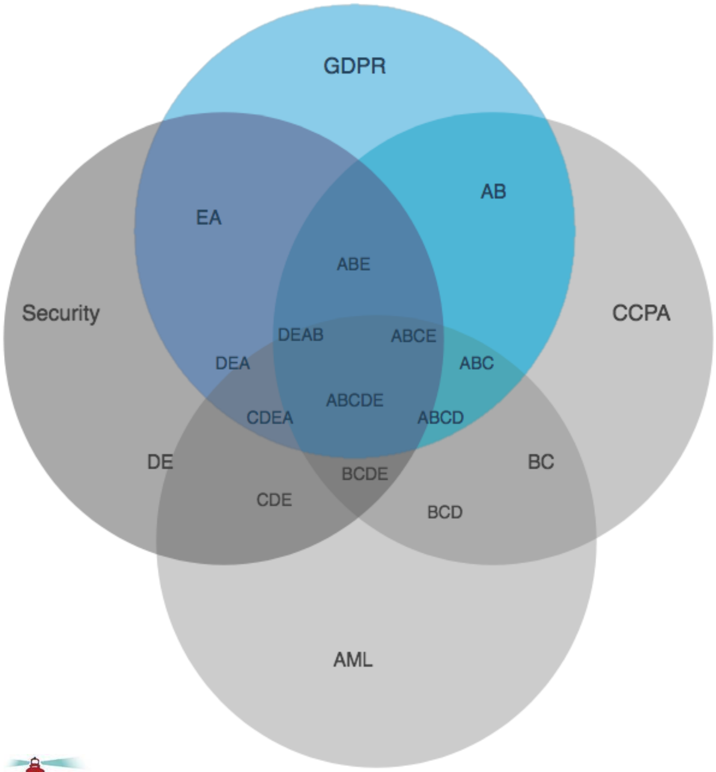
Banks.

Govt.

Data Subject Rights Automation

Mizen Group

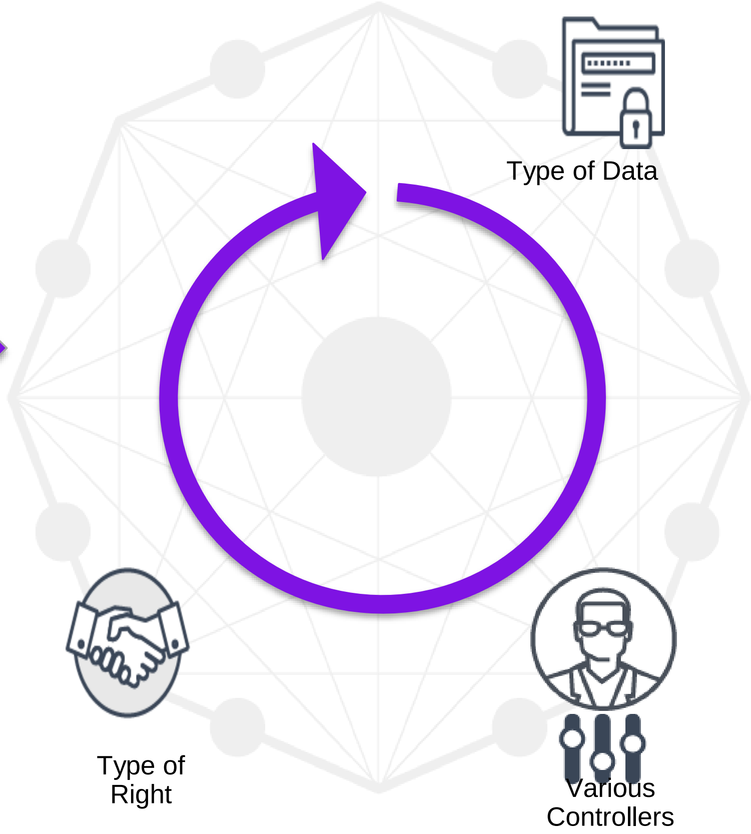
PersonalData.io



Data Subjects

+ Insights about Data Controllers and the collected data

Data Subject Right Process



Data Protection by Design and Default (DPbD^2)

Focus:

Data Register

DPIAs

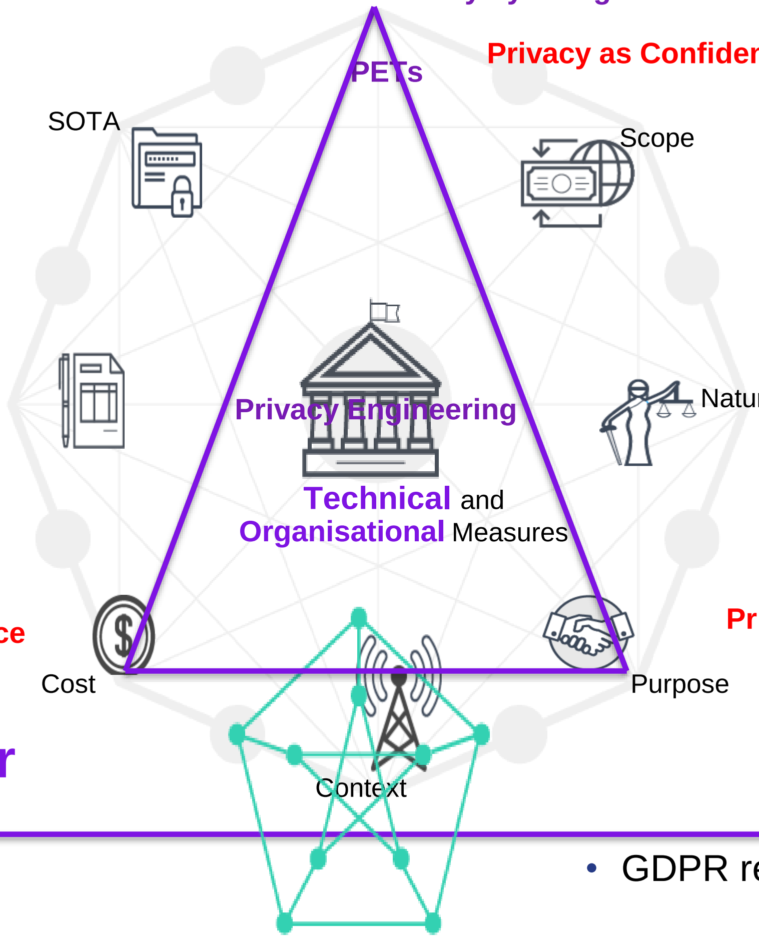
Transfer

Policies

Data Subject Rights Management

Compliance Management

Privacy as Practice



Data Protection/ Privacy by Design

Privacy as Confidentiality

PETs

SOTA

Scope

Risks

Nature

Privacy Engineering

Technical and **Organisational** Measures

Cost

Purpose

Context

Privacy as Control

Data Controller

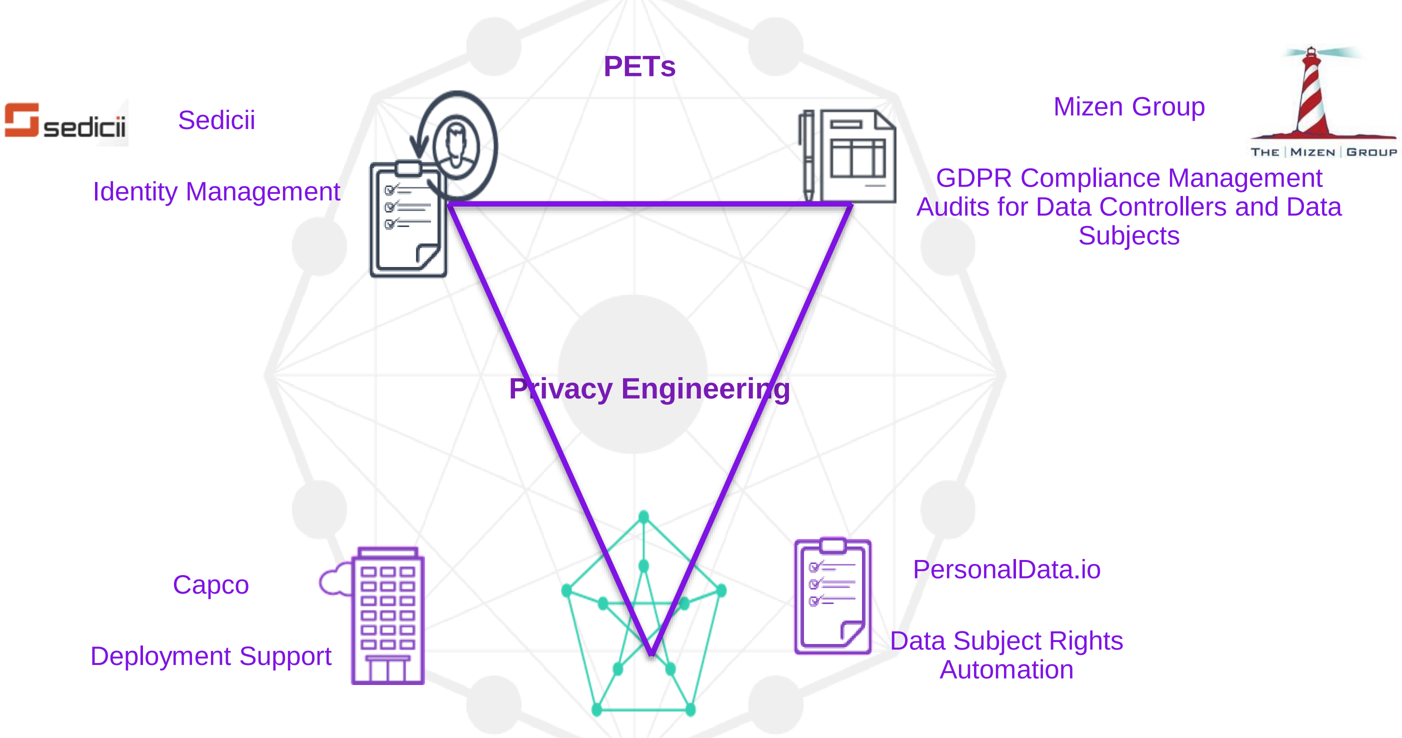
Data Subjects

- Data minimisation
- Purpose limitation
- Accurate and update-to-date data
- Storage retention
- Transparent
- Lawful

- GDPR requirements
- Protect the rights of data subjects

Algebraic Approach
Data Protection by Design and Default (DPbD^2)

Data Protection/ Privacy by Design



PETs

Sedicii

Identity Management

Mizen Group

GDPR Compliance Management
Audits for Data Controllers and Data
Subjects

Privacy Engineering

Capco

Deployment Support

PersonalData.io

Data Subject Rights
Automation

Privacy Algebra

References

Berendt, Bettina, Sören Preibusch, and Maximilian Teltzrow. "A privacy-protecting business-analytics service for on-line transactions." International Journal of Electronic Commerce 12.3 (2008): 115-150.

GÜRSES, S. Multilateral privacy requirements analysis in online social network services. PhD thesis, KU Leuven,

2010. pages 3, 17, 86

GÜRSES, S., AND BERENDT, B. PETS in the surveillance society: A critical review of the potentials and

limitations of the privacy as confidentiality paradigm. In Data Protection in a Profiled World. Springer, 2010, pp.

301–321. pages 7, 8, 18, 121

Veale, Michael, Reuben Binns, and Jef Ausloos. "When data protection by design and data subject rights clash." International Data Privacy Law 8.2 (2018): 105-123.

Morton, Anthony, et al. "" Tool Clinics"–Embracing multiple perspectives in privacy research and privacy-sensitive design." Dagstuhl Reports 3.7 (2013): 96-104.

Hoepman, Jaap-Henk. "Privacy design strategies." IFIP International Information Security Conference. Springer, Berlin, Heidelberg, 2014.

THE | MIZEN | GROUP

Thank You!

rula@privacyalgebra.com