Engineering encryption for privacy in practice:

Experiences on the ground: opportunities and pitfalls

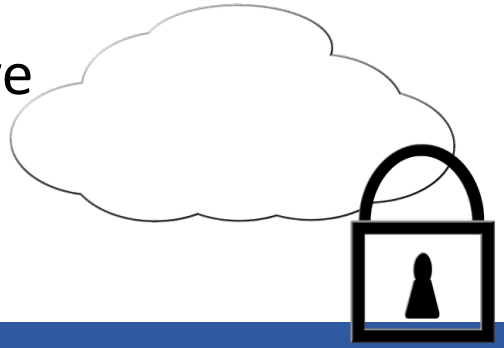
IPEN Webinar 2020

Is Encryption the solution to data protection?

“Teamwork” is the real solution!

What goes often wrong? 1/2

- Backups are forgotten
- Poor Access Control / SSO / MFA
- Unclear on/off boarding process
- Insufficient vendor assessment process
- Cloud encryption
- Lack of compliance perspective
- Insufficient awareness



What goes often wrong? 2/2

- Poor key management: back ups, restoring process
- Lack of monitoring: algorithms, key size, protocols
    - Legacy systems: may be incompatible with features surrounding access, or encryption methods. UPDATE!
    - Legacy protocols: when to stop supporting them (access logs in traffic can be important!: protocol version, cyphers, IP, user agent…)

But all these bad practices can actually also help you to achieve complete encryption of all your systems!

But all these bad practices can actually also help you to achieve complete encryption of all your systems!


Encryption deserves more attention!
(SSL/TLS is not enough!)

Ideal Situation:

Encryption program or policy part of the Enterprise Risk Management and Data Governance

Recommendations and opportunities 1/8

art.30 GDPR

Find what data you have!

Recommendations and opportunities 2/8

Data Classification

Risk-based approach

DLP*

Data discovery

*Data Loss Prevention

Recommendations and opportunities 3/8

art.30 GDPR

Where is my data?

- Asset management
- Infrastructure overview
- Third party/ SaaS

Recommendations and opportunities 4/8

art.30 GDPR

Data Lifecycle

Data must be protected throughout its lifecycle.
It is important to consider the state of the data you are trying to protect:

- **Data in motion:** being transmitted over a network
- **Data at rest:** in your storage or on devices
- **Data in use:** in the process of being generated, updated, erased, or viewed.

Recommendations and opportunities 5/8

Access Control

- How do you identify, authenticate and authorise your users / employees?
- Roles and responsibilities
- Awareness

Recommendations and opportunities 6/8

What do we need to encrypt and how?

Risk-based approach

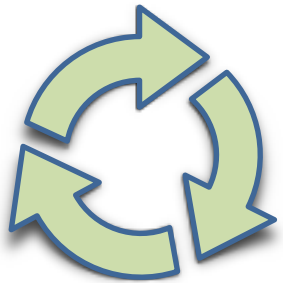
- How do we encrypt the data? check compliance!
- Select a method / tool - data life cycle
- User friendly approach / costs
- Implement key management process/tool

Recommendations and opportunities 7/8

Retention!

Data life cycle - retention

Establishing a retention period can help
when selecting the right encryption algorithm



Recommendations and opportunities 8/8

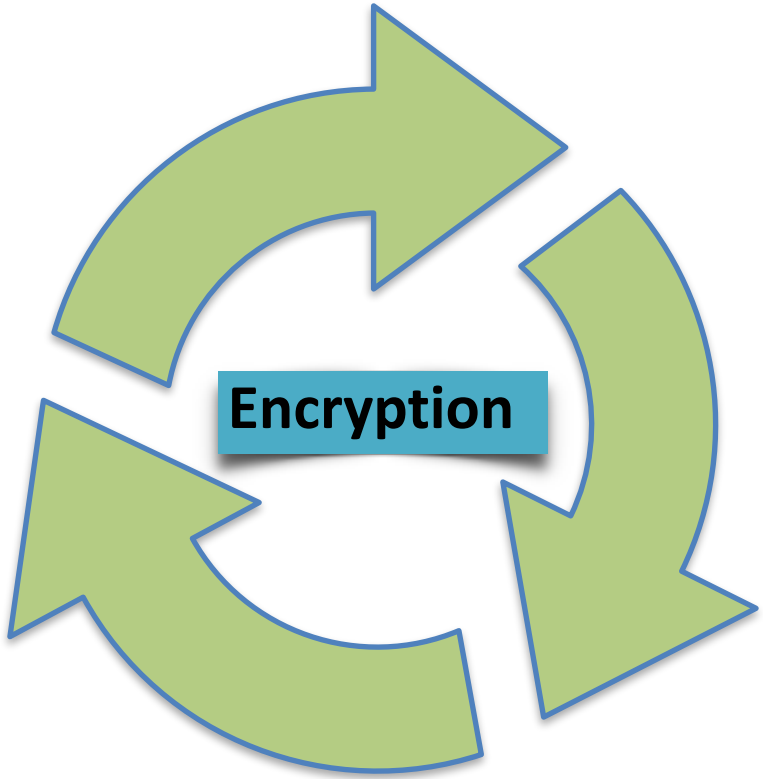
Awareness

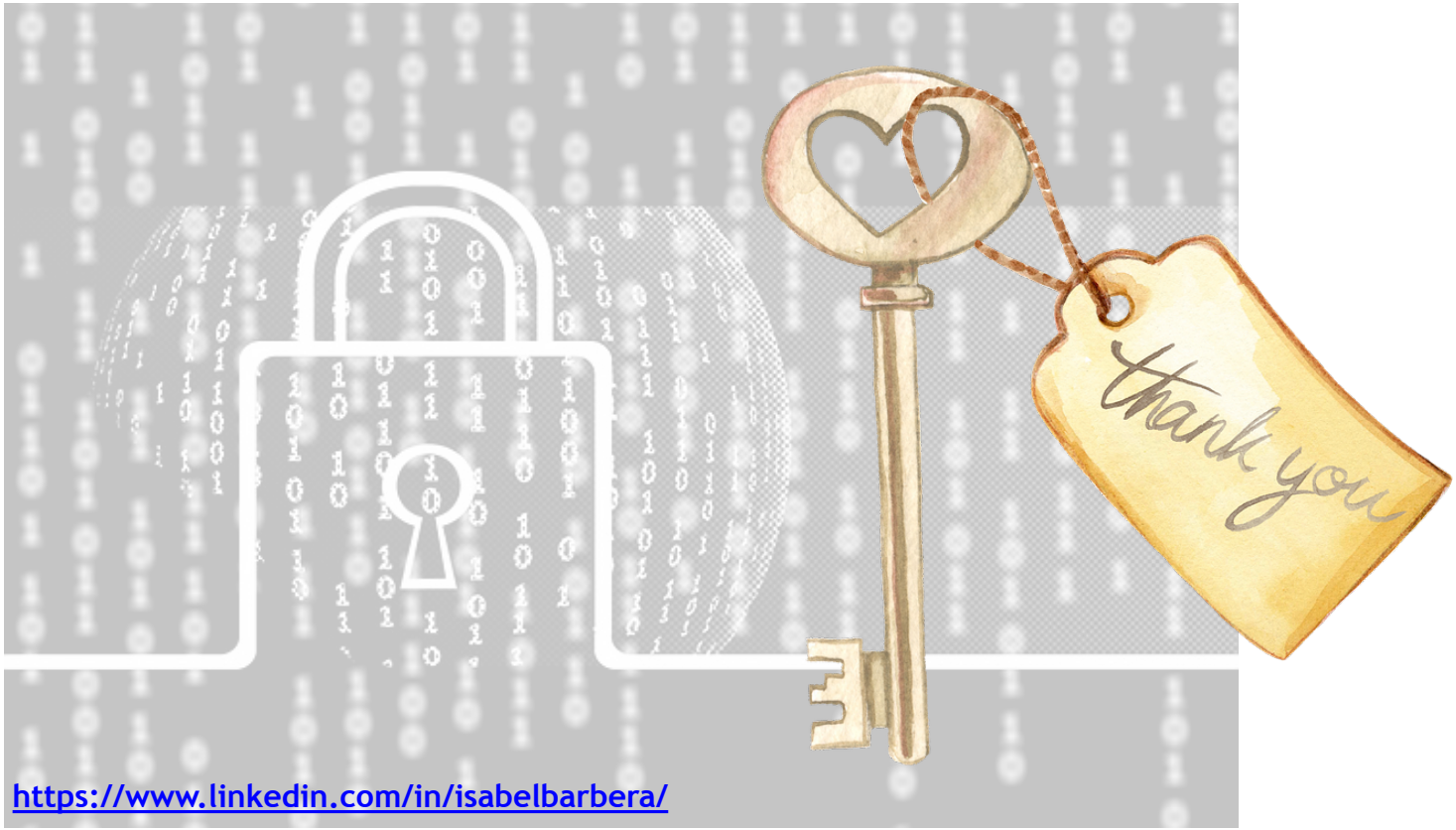
Awareness Policy

Establish clear rules/processes and
train your employees in data protection!

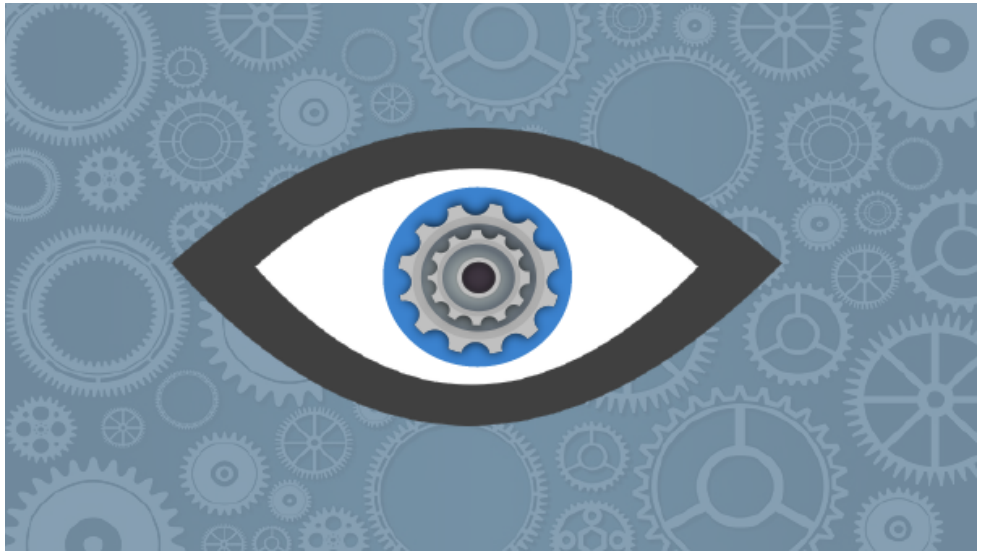
- How to protect and share data and keys
- Acces Control rules & responsibilities

Conclusion





https://www.linkedin.com/in/isabelbarbera/



Privacy Engineering Netherlands

Meetup Group