GDPR – Compliance

What, why and how Utimaco could help to fulfill
the EU General Data Protection Regulation requirements.

utimaco®

What is GDPR?

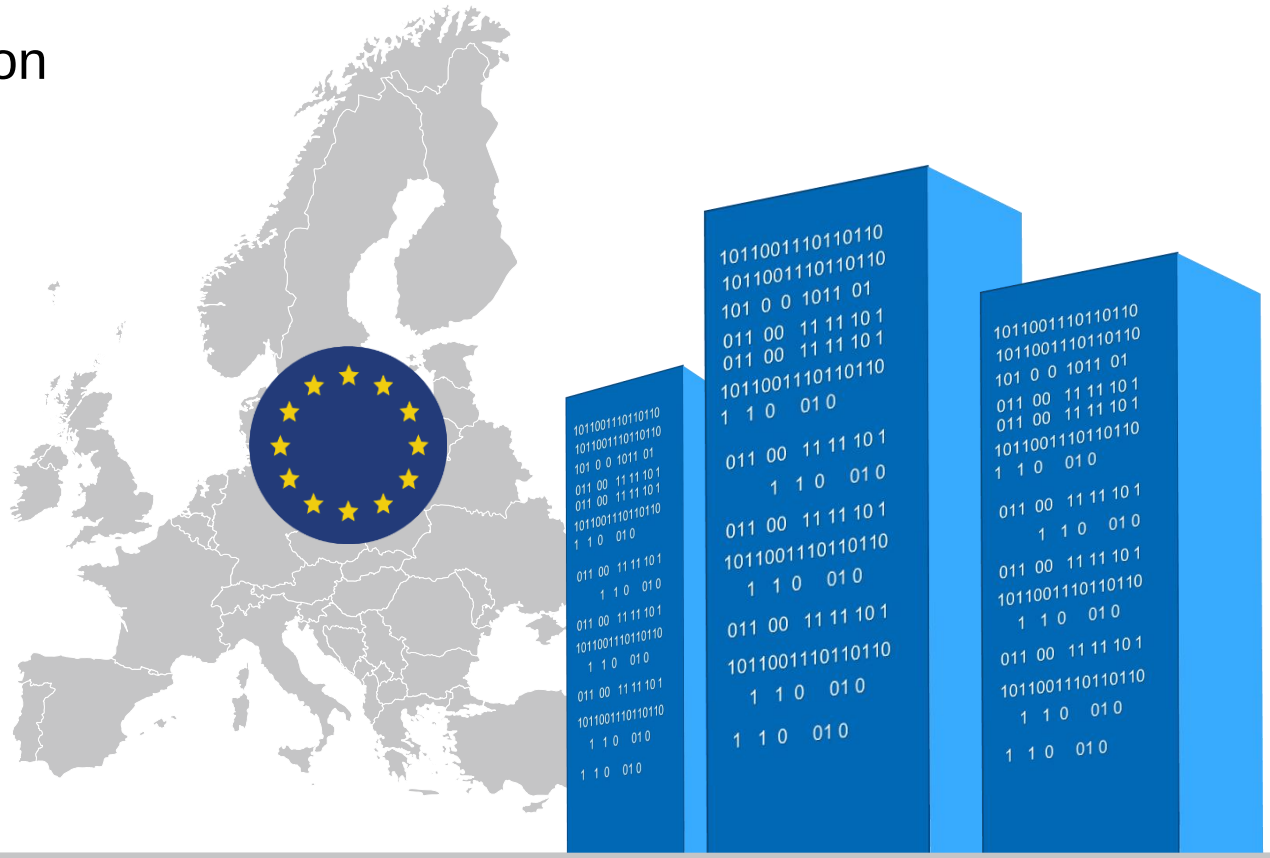
General Data Protection Regulation (Regulation (EU) 2016/679) intends to

- „**Remove the obstacles** to flows of personal data within the Union“*
- **Strengthen** and **unify** data protection for individuals within the EU

This *includes* export and processing of personal data outside the EU

Replaces the old data protection directive (Directive 95/46/EC)

It’s a regulation!
No local adaption necessary!



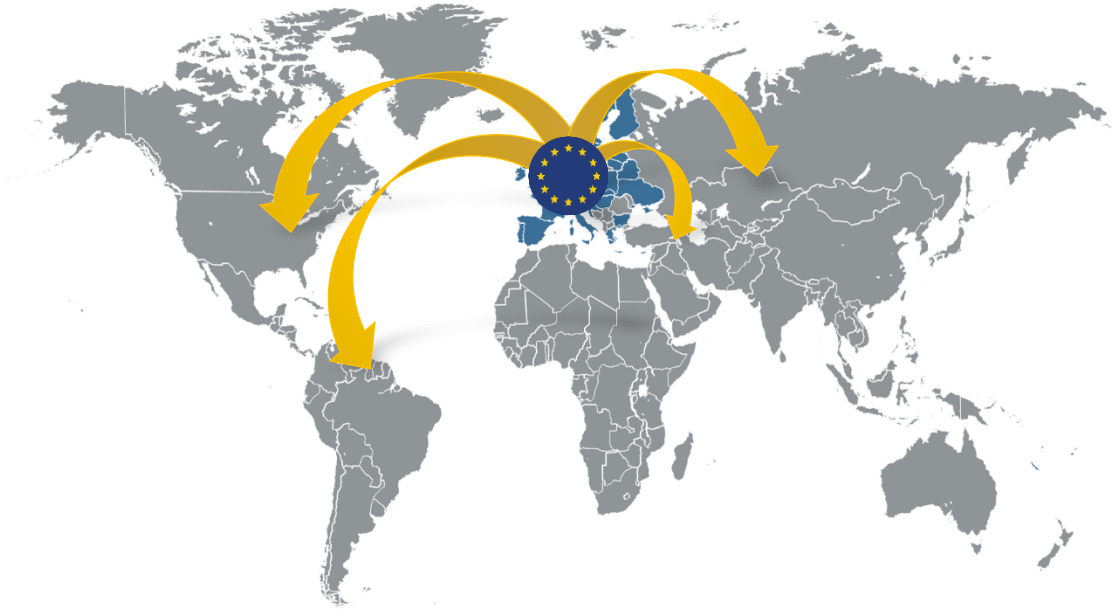
*recital (10) of (EU) regulation 2016/679

Who is affected by the GDPR

Applies to all organizations (Data Controller) based *in* the EU.

Applies to all organizations *outside* the EU (Article 3) that are

- Offering goods or services to data subjects in the EU (Article 3, § 2a)
- Monitoring behavior of data subjects in the Union (Article 3, § 2b)
- Regardless of where data processing takes place (Article 3, § 1)



"Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

What is new with GDPR

utimaco®

…and relevant to most businesses?

Supervisory Authority
Data protection regulators on national level

Need to inform of breach within 72h
(Article 33)
to Supervisory Authority;
in severe cases also to persons concerned **(Recital 75)**

Tough Penalties
Fines up to **4%** of annual global revenue

Or
20 Mio €

Cloud

Processor
Person (legal entity or individual) that processes personal data on behalf of the controller

Data subjects have **the right to be forgotten** and erased from the record**

Personal Data (PII)*
- NOT sensitive data
- Personal Data

Controller
Person (legal entity or individual) that determines the purpose and the means of the processing of personal data (collects data)

Data Protection Officer (DPO)
Advises & monitors GDPR privacy law/policy compliance; DPO contact details must be published

* Excludes “sensitive” information: on religion, sexual orientation, criminal records, „racial origin“, „electoral activity“, personal information of children
** Data subjects have the right not to be part of automatic decision making based on personal information, e.g. for credit applications or e-recruiting practices (Recital 71)

Security of processing

Section 2

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

Security of processing

- “In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as *encryption*.” (recital 83)

- The *communication* to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
  - (a) the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as *encryption*; (Article 2, § 1a)

- ‘pseudonymisation’ means the processing of personal data in such a manner that
  - the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such ***additional information*** is ***kept separately*** and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Use Cases

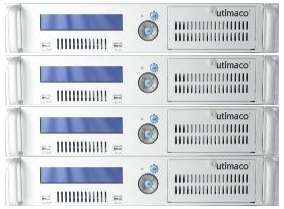
From the application perspective

- Certificate management
- Privileged account management
- Mail encryption
- Database encryption
- File/Folder encryption
- VPN encryption
- Code Signing
- Data Tokenization
- Web Servers
- …

Whenever a cryptographic key needs to be generated, used and stored, one needs to consider the implementation of an HSM

Use Case „In-house Infrastructure“

- Certificate management
- PKI Services
- Database encryption
- Mail encryption
- File/Folder encryption
- VPN encryption
- …



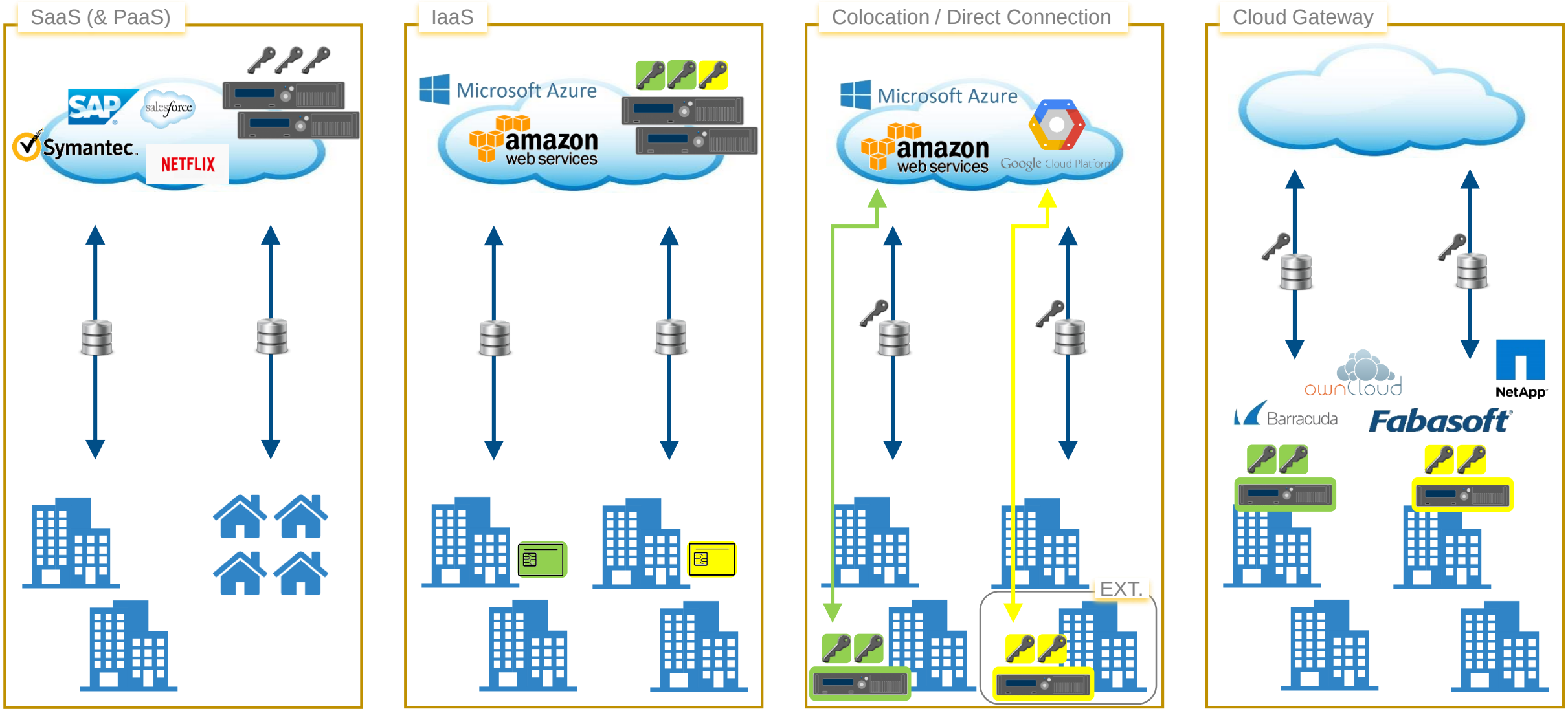
..More or less straight forward..

PII in the Cloud – Best practice

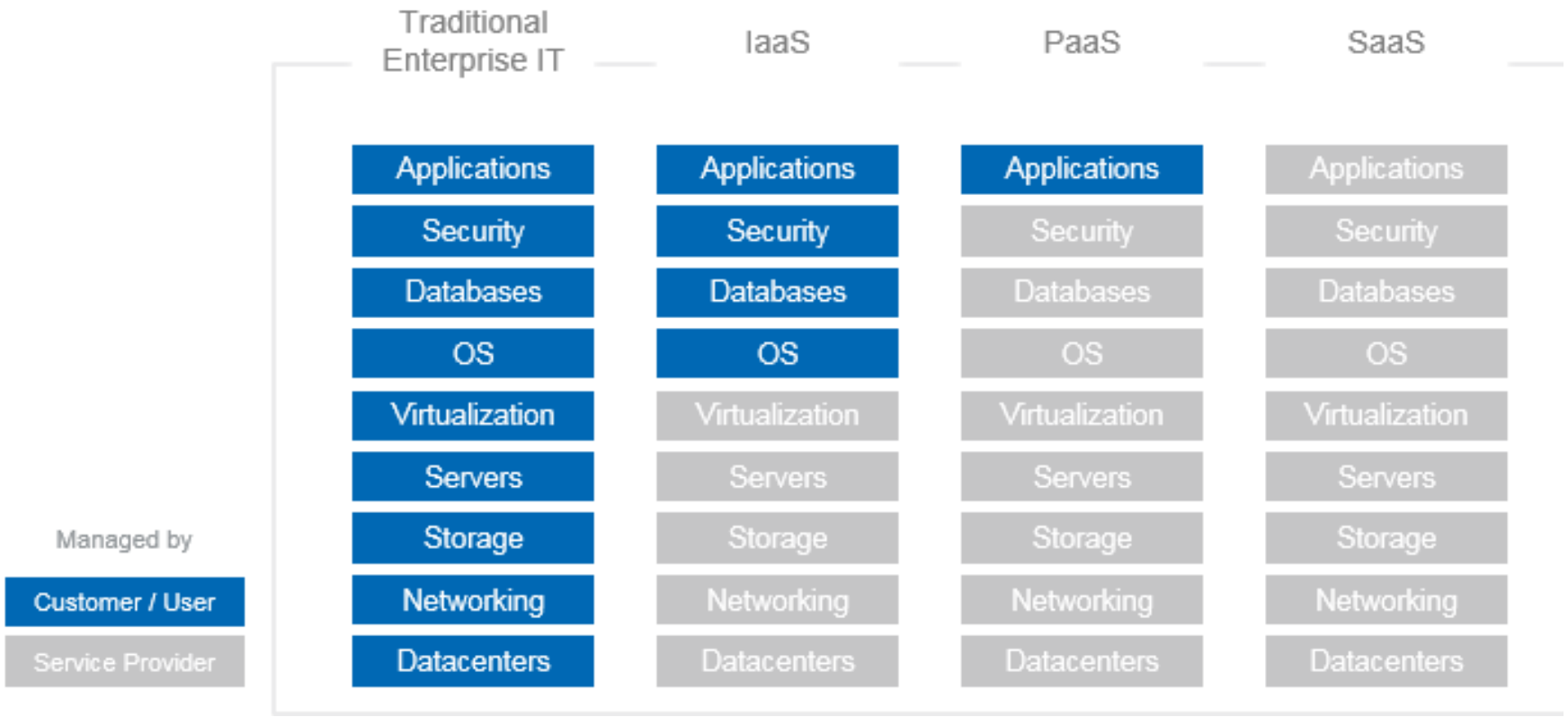
"Outsourced data storage on remote clouds is practical and relatively safe, ***as long as only the data owner, not the cloud service, holds the decryption keys"***

Report by ENISA (the European Union Agency for Network and Information Security)

Cloud Scenario– The Role of an HSM



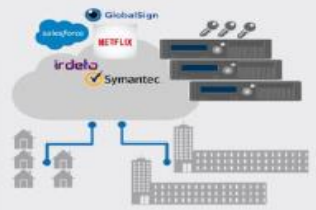
Cloud Scenario



Summary

Hardware Security in Cloud Scenarios

utimaco



SaaS (& PaaS)

HSM is part of a specific Cloud offering

Pros:
- Secure key storage
- Separation of duty
- Trust as a product USP

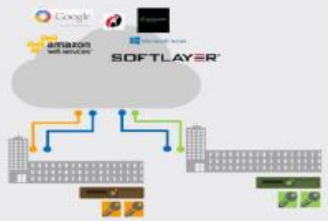
Cons:
- HSM interface needed
- Special hardware required

IaaS

HSM offered as infrastructure

Pros:
- Flexible add-on to existing onsite HSM Cluster
- Covering of load peaks
- Reuse of existing key material

Cons:
- HSMs are not interoperable
- No existing standard API, vender specific
- Custom application support



Colocation

HSM on site, with a link to the cloud application

Pros:
- Never give up key sovereignty
- Clear separation of duty

Cons:
- Security administration needed
- Business critical application hard to implement

Cloud Gateway

HSM are part of gateway appliances

Pros:
- Secure key storage
- Maximum privacy
- Integrated key management

Cons:
- Additional hardware management
- HSM integration into gateway solution
- Administration

Security is Key

Thanks for your attention!

Stephan Otten

Head of Sales EMEA
Stephan.otten@utimaco.com

Utimaco IS GmbH

Germanusstraße 4
52080 Aachen
Germany
Tel +49 241 1696 200
Fax +49 241 1696 199
Email hsm@utimaco.com

Utimaco Inc.

Suite 150
910 E Hamilton Ave
Campbell, CA 95008
United States of America
Tel +1 844 884 6226
Email hsm@utimaco.com