cyberwatching.eu

The European watch
on cybersecurity & privacy

Use of new technologies: Data Protection process and governance as solution?

DEFeND

DATA GOVERNANCE FOR SUPPORTING GDPR

Funded by the European Commission
Horizon 2020 – Grant # 740129

PRAITANO ANDREA

Role:

- *Senior Cyber Security Advisor*

Summary of relevant experience

- *Project Security Officer of DEFeND H2020 project*
- *Cybersecurity and privacy Advisory for major customer*

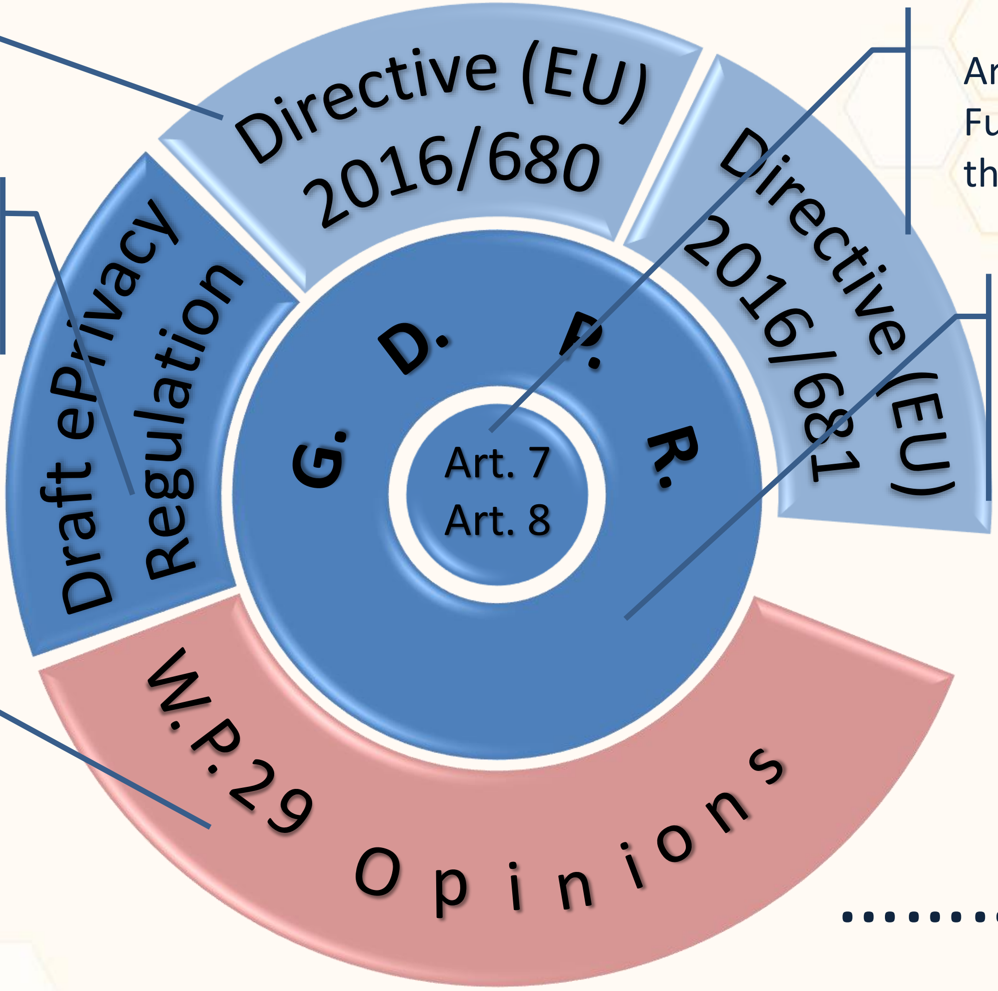
Certifications:

- *CISA, CRISC, CIPP/E, Lead Auditor ISO/IEC 27001:2013, Lead Auditor ISO 22301:2012, TOGAF 9 part 1, ITIL Expert, PRINCE2 practitioner, MSP, M_o_R, DPO based on UNI 11697:2017*

Profile summary

Andrea Praitano is an expert on cybersecurity and privacy domains. His experiences were matured in many different businesses (energy, healthcare, industry, bank, assurances, telecommunication, gaming, public administration, etc.) and in different kind of activities like audit, consulting, operational services, etc.
These experiences allow Andrea a smart and comprehensive solving-method of problems of interconnection, integration and flows among different business areas, which represent one of the most important issues in companies and governance.
His experiences includes also other domains strictly connect to cybersecurity and privacy like IT service management, IT governance, project and program management and green IT.

EUROPEAN DATA PROTECTION FRAMEWORK (1/2)



Directive (UE) 2016/680

Draft of ePrivacy Regulation
(replace the Directive 2002/58/EC)

Guidelines WP 29/EDPB and DPAs

Article 8 Charter of Fundamental Rights of the European Union

Regulation (UE) 2016/679 - GDPR
(replace the Directive 46/95/EC)

National laws

………. Personal opinion

European Data Protection framework (2/2)

The European Data protection is a framework not a single and "simple" law!

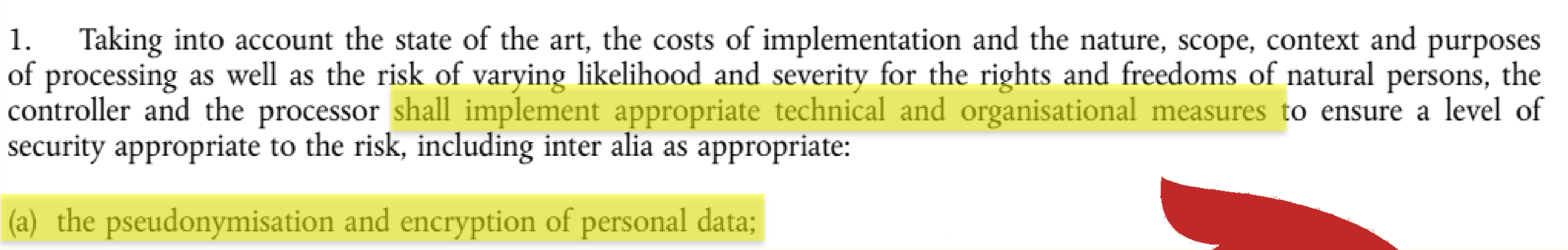
Data Protection is multidisciplinary (at minimum include law and technical expertise).

ISO
ISO/IEC 17065

In the regulation there are some indications that suggest that data protection must be seen as a process and must include governance…..

GDPR Article 32 “Security of processing”

The GDPR makes a mistake that causes confusion.



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;

It’s strange that a Regulation include:

- example of security measures (it’s not clear that these are examples);
- the examples are only on technical part.

What is the Data protection?

What is Personal Data Protection for the GDPR?

The GDPR doesn't include a definition of Persona Data Protection but through the articles could be find a definition.

Preservation of Confidentiality, Integrity, Availability and Resilience of personal data.

This definition is quite similar to the definition of information security, it's different only the scope (ISO/IEC 27000:2018 point 3.28).

Data Protection best practices

CIAR

There is many decades of experience on information security, it’s not complex transpose this experience in the Data Protection Domain!

.... but

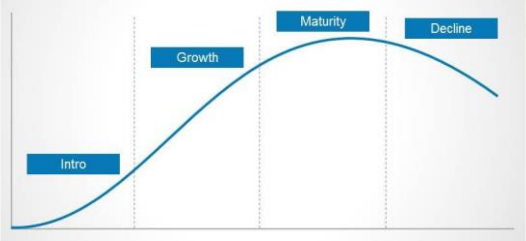
TECHNICAL VS ORGANIZATIONAL SECURITY MEASURES

The GDPR (but also the information security best practices) talk on technical and organisational security measures. **Both are important** but usually the organisations are focalised on the first one (e.g. encryption). The focalisation on the technical security measures means:

- The data protection need to follow the technology changes;
- There are no priority (or not correct priority) in the security measures;
- Technical security measures without organisational security measures don't work well;
- …….

What is the main problem of the emergency technologies?

#1 The life cycle of the products are short and some technologies don’t arrive at the level of maturity.



#2 Focalization of the data protection on the end-points is complex and expensive.

#3 There are not consolidated technologies but there are some leaders and outsiders.

THE POSSIBLE SCENARIOS (1/2)

Corporate devices:
COPE
(Corporate Owned Personally Enabled)

The organization has direct control on the:

- *Device selection;*
- *Device configuration;*
- *Device update.*

This scenario is quite good because the organization could maintain the control. Usually the organisation is not a "early adopter" and chooses consolidated devices with a defined life. Usually the "business life" of a new device is more connected to accounting (usually 3 years) and not a technical aspects.

THE POSSIBLE SCENARIOS (1/2)

Personal devices:
BYOD
(Bring Your Own Device)

*The organization has **not** directed control on the:*

- *Device selection;*
- *Device configuration;*
- *Device update.*

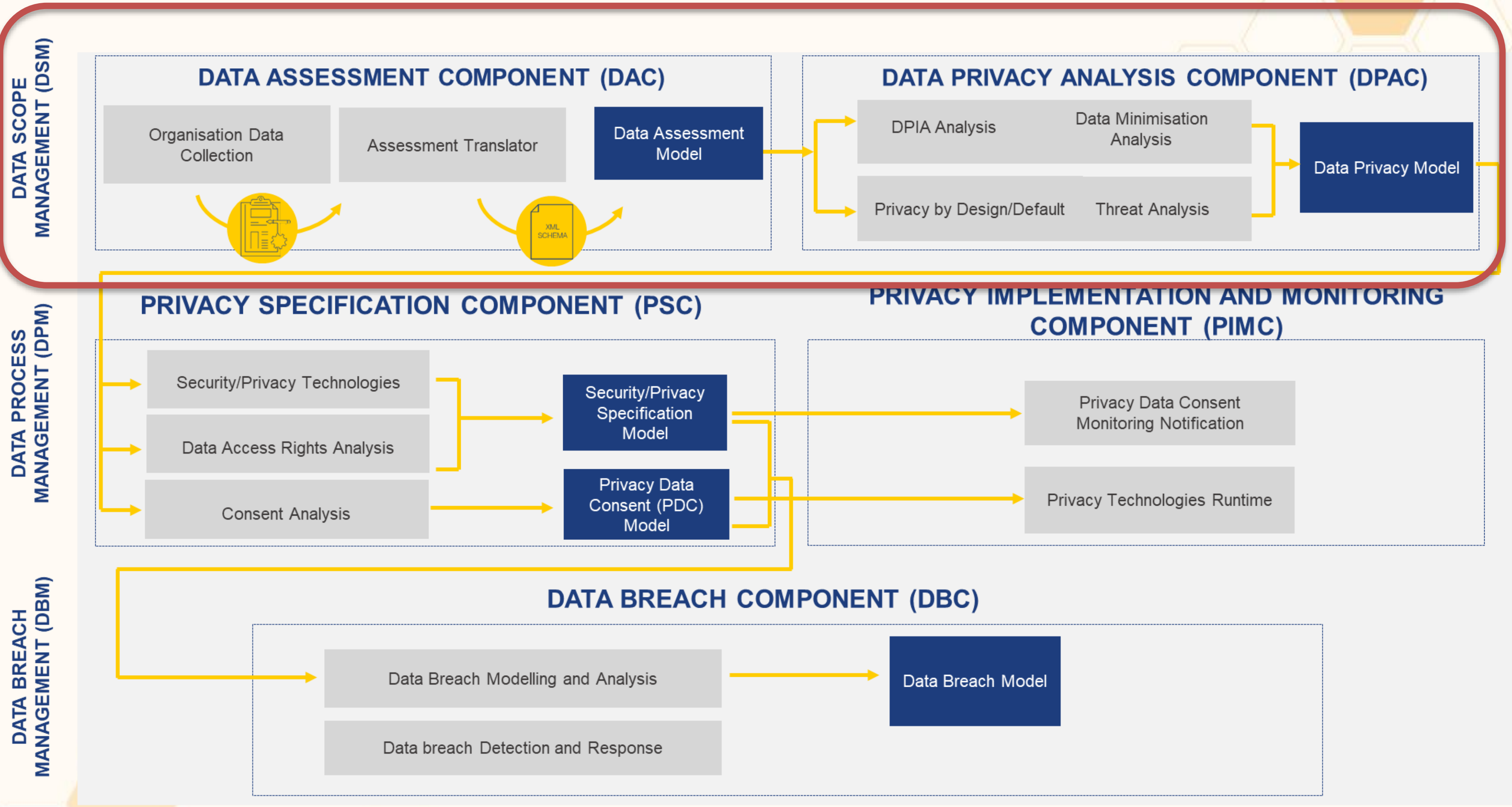
In this scenario the device is out of control. The employee could be a “early adopter” but also the opposite (he/she could use a old device).

How can we approach the data protection?

- The organisation (data controller or data processor) has the ownership of the personal data protection.
- The data protection must be under control

  ….this mean that the organisation could authorise or deny the personal data processing based on roles but also devices
- <u>The organisation has to implement personal data process and governance!</u>

The DEFeND Platform



DATA SCOPE MANAGEMENT (DSM)

DATA ASSESSMENT COMPONENT (DAC)

- Organisation Data Collection
- Assessment Translator
- Data Assessment Model

DATA PRIVACY ANALYSIS COMPONENT (DPAC)

- DPIA Analysis
- Data Minimisation Analysis
- Privacy by Design/Default
- Threat Analysis
- Data Privacy Model

DATA PROCESS MANAGEMENT (DPM)

PRIVACY SPECIFICATION COMPONENT (PSC)

- Security/Privacy Technologies
- Data Access Rights Analysis
- Consent Analysis
- Security/Privacy Specification Model
- Privacy Data Consent (PDC) Model

PRIVACY IMPLEMENTATION AND MONITORING COMPONENT (PIMC)

- Privacy Data Consent Monitoring Notification
- Privacy Technologies Runtime

DATA BREACH MANAGEMENT (DBM)

DATA BREACH COMPONENT (DBC)

- Data Breach Modelling and Analysis
- Data breach Detection and Response
- Data Breach Model

DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

Andrea Praitano, eMBA, CIPP/E, CISA, CRISC

Security Project Officer of DEFeND Project

andrea.praitano@maticmind.it

www.defendproject.eu

@apraitano

+39 348 4054673

it.linkedin.com/in/andreapraitano/

DEFeND

DATA GOVERNANCE FOR SUPPORTING GDPR