Security in the General Data Protection Regulation

October 2018

Giuseppe D'Acquisto
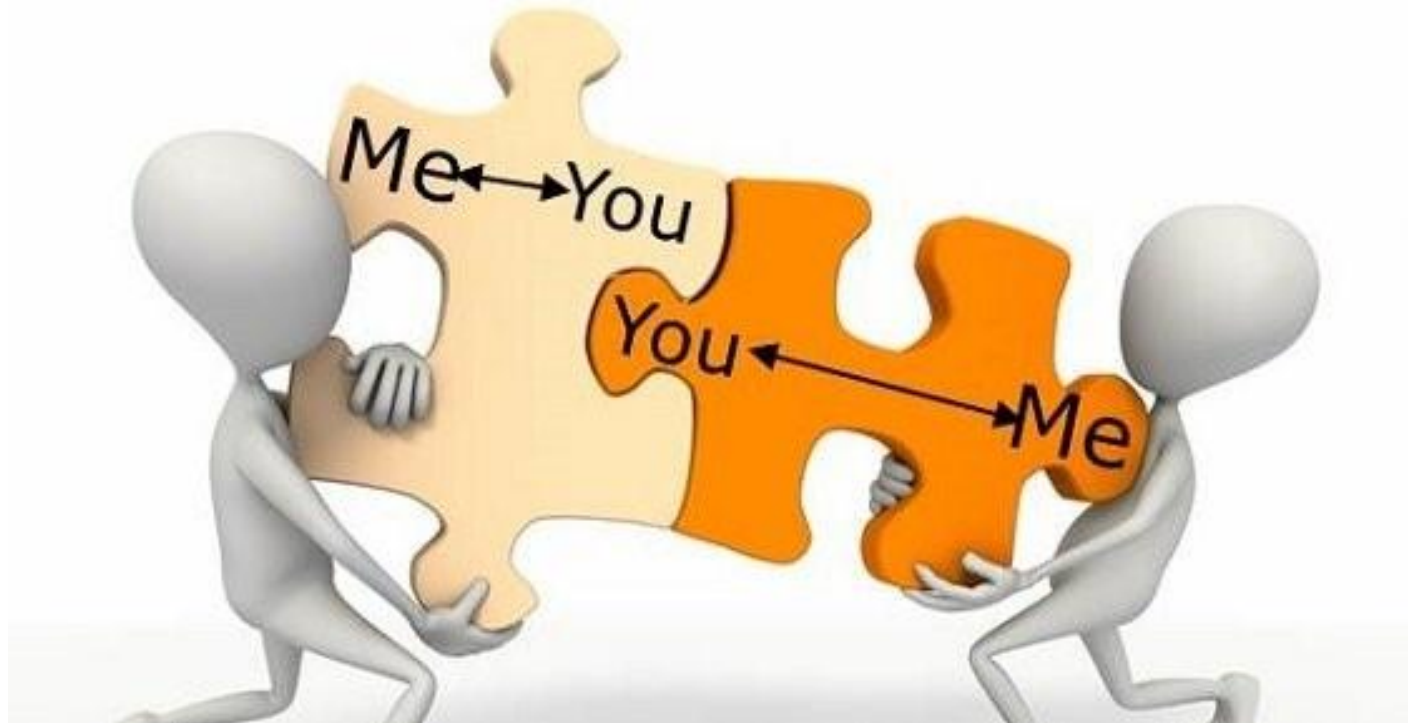
Article 32: Security of processing

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;

    (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing   systems and services;

    (c) the ability to restore the availability and access to personal data in a timely manner in the event   of a physical or technical incident;

    (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and   organisational measures for ensuring the security of the processing.

The "state of the art"

The "costs"

$$\text{Security goal} \subset \bigcup m_i$$

$$\sum \text{Cost}(m_i) \leq \text{Budget}$$

The "risks"

Prescriptive approach

Risk based approach
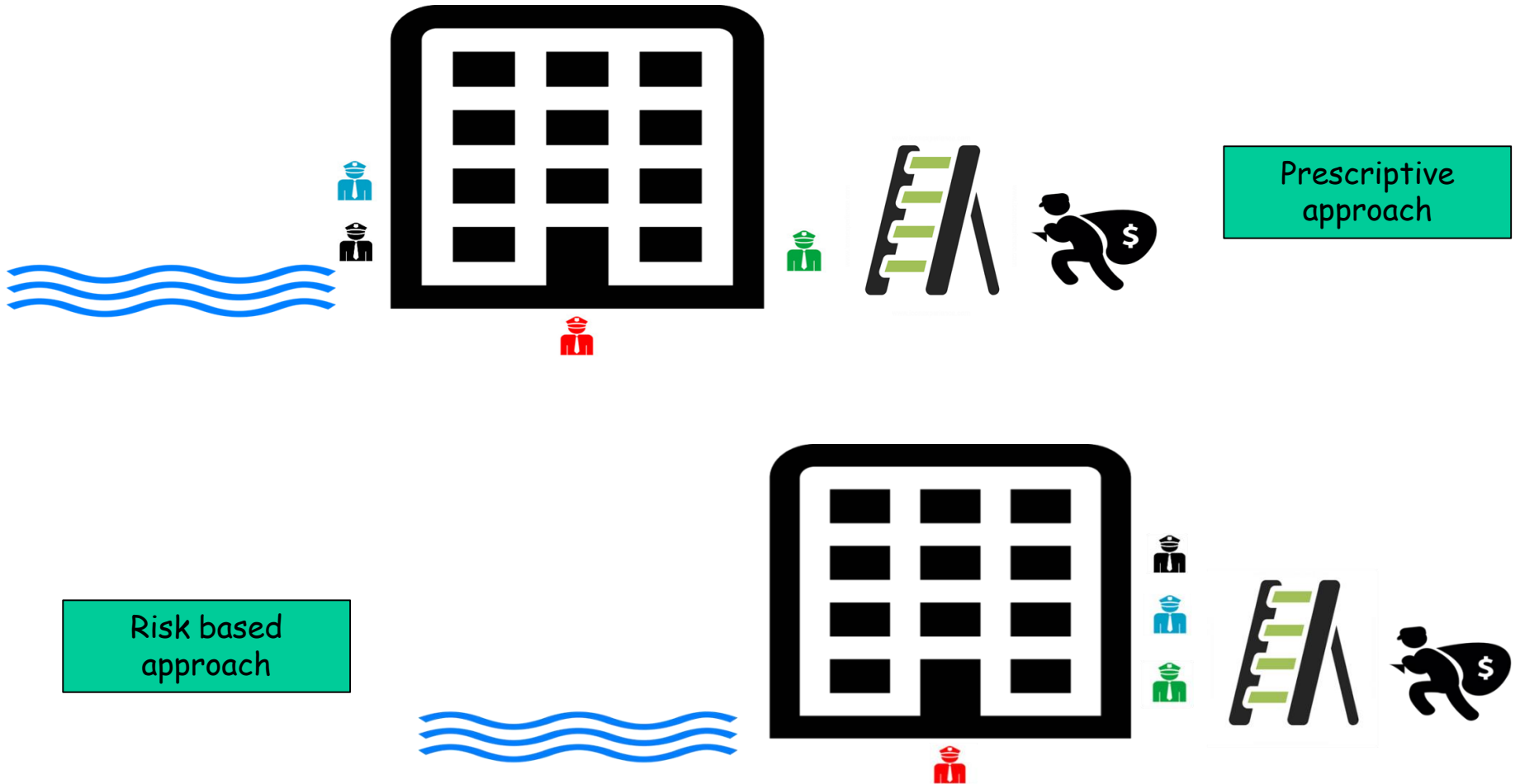
Article 5: Principles relating to processing of personal data

1) Personal data shall be:

…

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

New security paradigm

Deefensive
security

Security as a
principle

New security paradigm
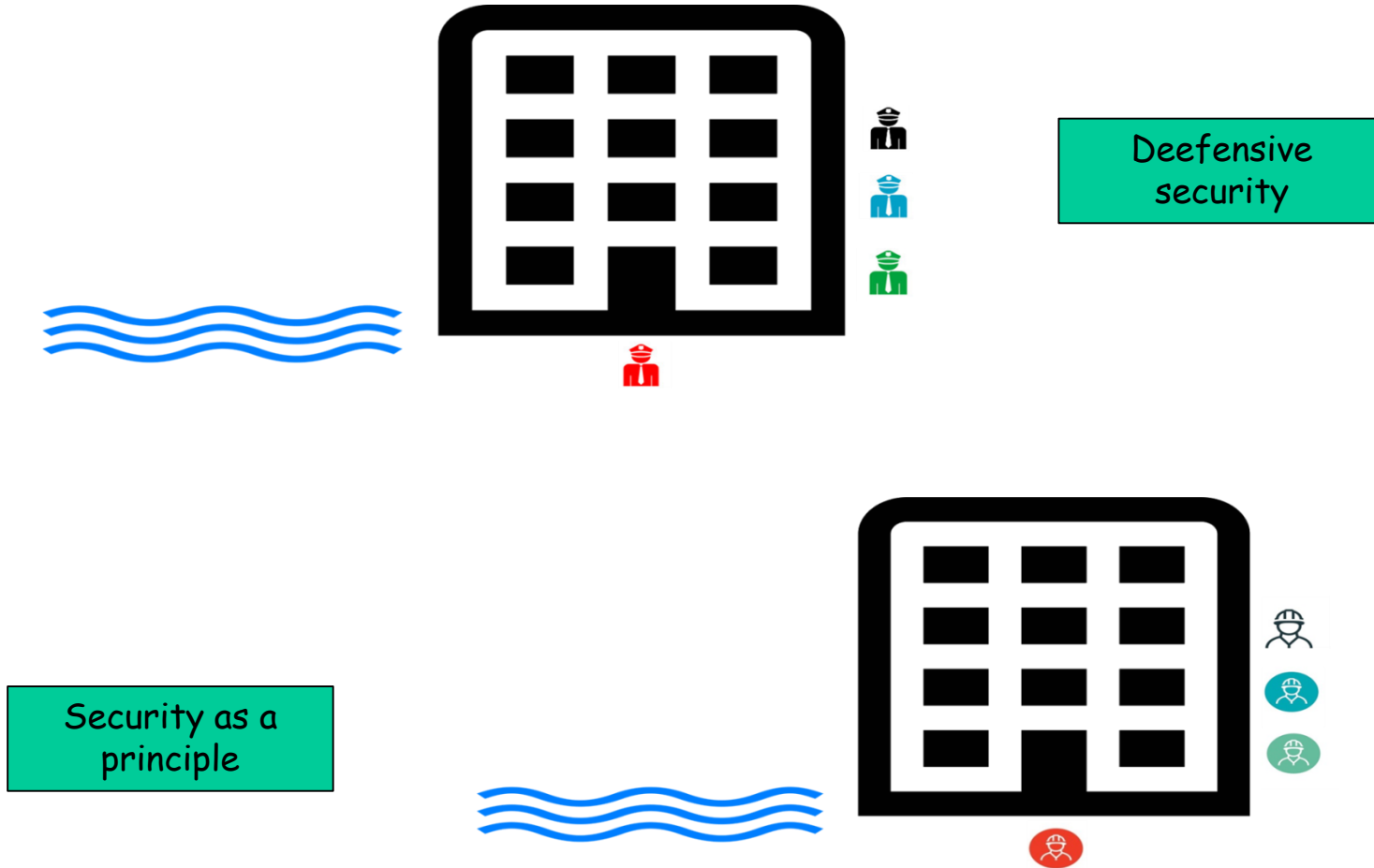
- Security for trust
- Security for data quality
- Security for interoperability
- Security for reliability/resiliency
- Security for the safety of objects
- Security for the safety the environment
- Security for health
- Security for wellbeing
- …..

Thanks

g.dacquisto@gpdp.it