Quali sono le misure di sicurezza appropriate, da dove partire?

Alessandro Vallega Clusit, Europrivacy, Oracle
June 2017

EUROPRIVACY.INFO
@EUROPRIVACY

Disclaimer: I work in Oracle but in this ppt opinions are my owns

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

GDPR

Understanding the GDPR: objectives

To understand the Regulation, implications, and specificity of some obligations it is important to know that:

- The **aim** of GDPR is to protect the rights and the freedoms of the natural persons
  - Increasing the accountability of “controllers” and “processors”
  - Giving the individuals more control over their personal data
- And that there are other key objectives such as
  - Guarantee the free movement of data across Europe
  - Harmonize and simplify the law for the companies (providing a single set of rules on data protection, valid across the EU and removing unnecessary administrative requirements)

Understanding the GDPR: good IT and good Security

The protection of natural persons in relation to the processing of personal data is a fundamental right that necessarily goes through Information Technology (IT).

In modern society IT is ubiquitous and many GDPR requirements **imply a good IT** and **a good Security**

Understanding the GDPR: GDPR and IT

- Protecting the data requires
  - Understanding where the data is
  - Which is the risk exposure
- Some obligations can / must be fulfilled
  - Through modifications of the Applications
  - Leveraging the IT Architecture

1. Records of processing

DATA INVENTORY
Personal data processing relies on the knowledge of the data managed

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility (A.30)

- A list documenting for each processing information including:
  - Purposes of processing (eg. personal appraisal)
  - Description of categories of data subjects (eg. employees)
  - Categories of personal data (eg. performance and potential)
  - Information related to transfers to a third country and international organization (eg. USA - Oracle Talent cloud service)
  - Time limits for erasure (eg. end of work relationship + 1 months)
  - Description of security measures (eg. level 3 measures in MyGroup procedure XY, + CASB)

- Records of processing should be perceived as the starting point for IT security in the framework of GDPR compliance
- Should be used as a working tool to achieve and control compliance
- Can be used to demonstrate compliance and accountability
- Can be modular extended with more information

2. Risk and Data protection impact assessment

RISK AWARENESS
Companies must understand and reduce the risks for the data subject

The word “Risk” is used 75 times in this Regulation: the controller and processor must understand and reduce the risk for data subject

- Furthermore when the processing is likely to result in a high risk to the rights and freedoms of natural persons a formal Data Protection Impact Assessement (A.35) is required, prior of the processing, to:
  - Define the security measures to apply
  - Understand if it is necessary to consult the Data Protection Authority and seek approval

- Article 29 Data Protection Working Party (WP29) published the Guidelines on Data Protection Impact Assessment (DPIA)
- The DPIA is a tool for managing risks to the rights of the data subjects, and thus takes their perspective whereas risk management in some other fields (e.g. information security) is focused on the organization.
- These guidelines make a reference to international best practices such as ISO 31000:2009, Risk management — Principles and guidelines, and ISO/IEC 29134 (project), Information technology – Security techniques – Privacy impact assessment – Guidelines

3. Articles related to the rights of the data subject

APPLICATIONS
These obligations often require application modifications

Chapter 3 “Rights of the data subject” (Section 2 and 3) provide a list of obligations for the controller

- Right of access by the data subject (A.15)
- Right to rectification (A.16)
- Right to erasure (‘right to be forgotten’) (A.17)
- Right to restriction of processing (A.18)
- Notification obligation regarding rectification or erasure of personal data or restriction of processing (A.19)
- Right to data portability (A.20)

These articles require often human intervention and/or application modification, for example:

- Erasure shall be evaluated taking into account other subjects rights and laws including for example pending invoices still to be paid (human intervention)
- Data portability requires a function to export in a machine-readable format the data requested by the data subject (application modification)

4. Articles related to security measures

ARCHITECTURE
Security measures can be often implemented in the architecture

Several articles make reference to the obligation to adopt **appropriate technical and organisational measures**

- Principles relating to processing of personal data (A.5)
- Responsibility of the controller (A.24)
- Data protection by design and by default (A.25)
- Processor (A.28)
- Security of processing (A.32)
- Communication of a personal data breach to the data subject (A.34)

The most explanatory is article 32 (Security of processing) because gives better information about this topic, including:

- Context and objectives
- An example of a security measure (encryption)
- Indications about the goals to achieve
- Elements that may be used to demonstrate compliance

Which security measures shall be implemented?

Since

- The law does not specify which specific security measures must be adopted and the controller and the processors are accountable
- Certifications and code of conducts, Data Protection Authority, judges, and court experts will refer to common sense and international best practices

You need to

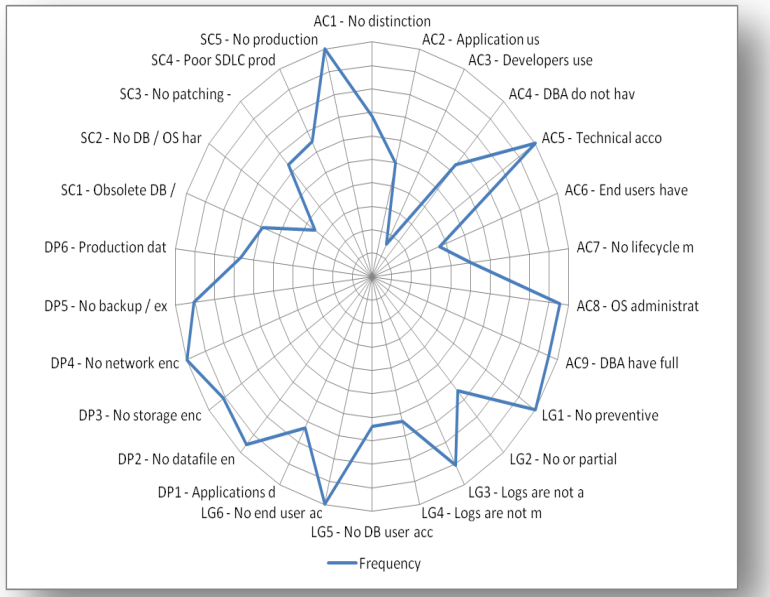
- Know which personal data are processed and where are they in the systems
- Understand the risk for the data subject
- Implement basic security measures
- Add more security and good IT

Some security concepts that are more and more important

- Strong / Multilevel / Federated Authentication
- Adaptive / Fine Grained Access Control / Authorization
- Segregation of Duties
- Need to Know / Least Privilege
- Accountability / Log Management
- Encryption
- Anonymization and Pseudinymization
- Segregation of Environment
- Secure Configuration Management / Hardening
- Backup, HA and DR

We have evidence that there is often a lack of basic security

- We are assessing our customer security posture for years with a practice called Security Assessment or Security Maturity Evaluation



- We have collected IT “Most Common Mistakes” for example:
  - Sharing passwords
  - No logging
  - Poor patching
  - No encryption
  - Eccessive privileges

- You hardly comply if you do not have a basic security

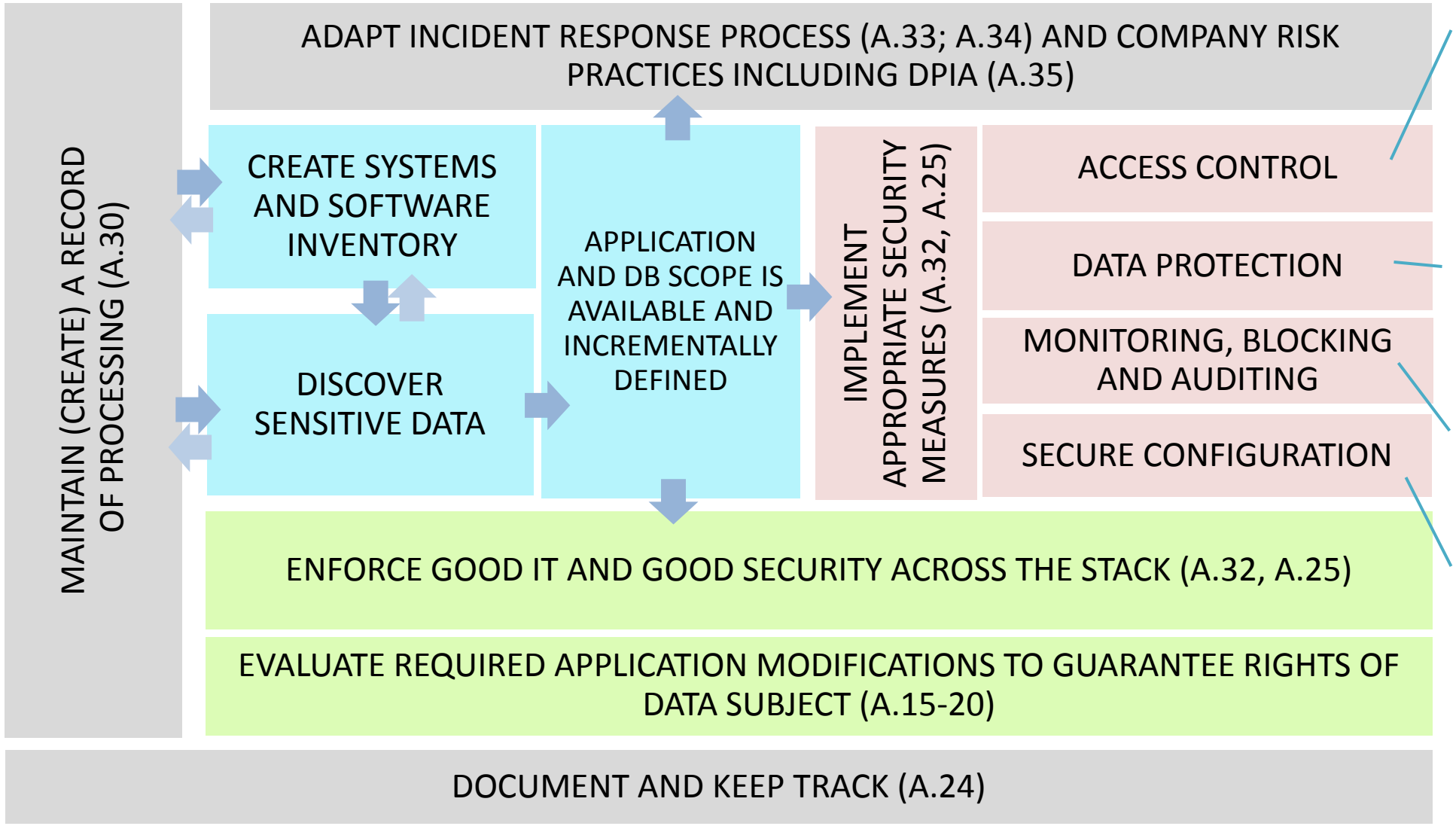
Ask a Security Assessment
Check this video for the DBSecurity http://bit.ly/29GIYF3
Ask the Most Common Mistake white paper

GDPR & Technology

- GDPR compliance requires a set of coordinated actions by different departments in every company. In fact it requires to cover many aspects including:
  - Organization
  - Legal and Contracts
  - Information Technology

- Good technology can help to achieve compliance

A path towards GDPR – tasks and activities



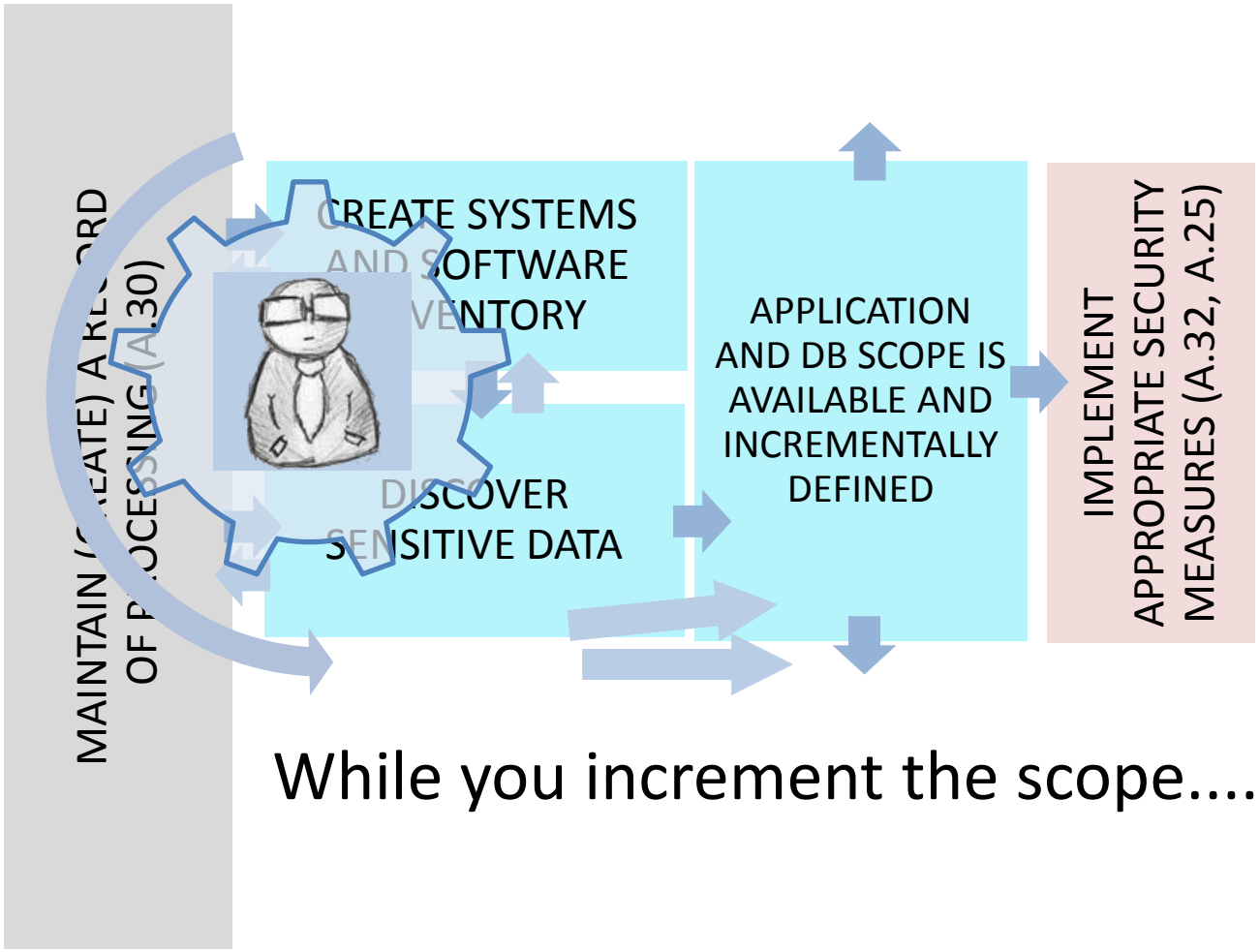
Modernize identity management to guarantee authentication and authorization both for business user and IT personnel

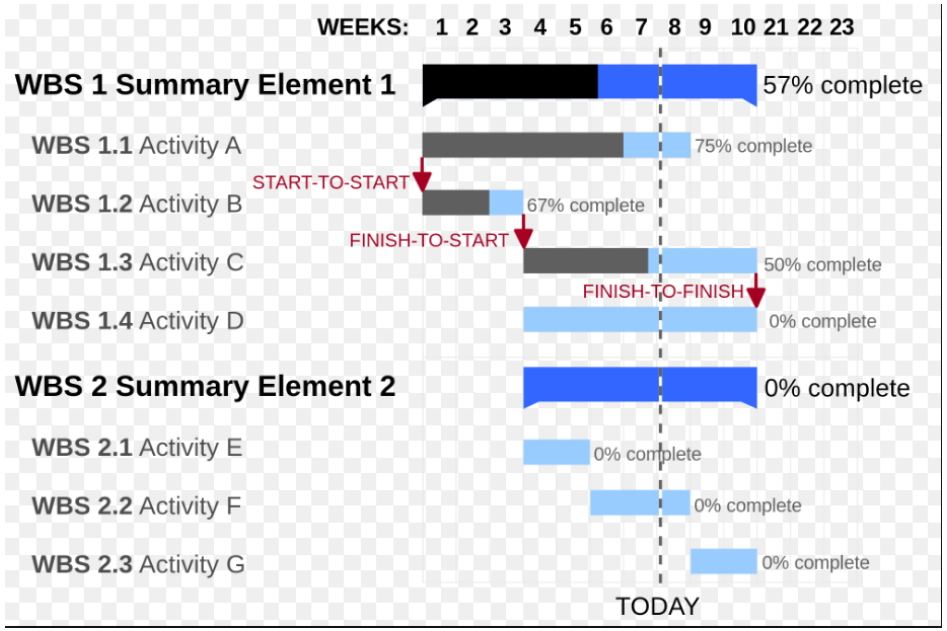
Protect the data wherever it is (encryption A.32) and avoid using real data where non necessary (A.5 and W.26)

Collect, secure and analyze audit logs and implement SQL boundary defenses

Secure configurations, remediate vulnerabilities, and control production baselines

A path towards GDPR –parallelizable tasks





While you increment the scope....

... You can start security projects as you go

A path towards GDPR – security assessment

APPLICATION AND DB SCOPE IS AVAILABLE AND INCREMENTALLY DEFINED

IMPLEMENT APPROPRIATE SECURITY MEASURES (A.32, A.25)

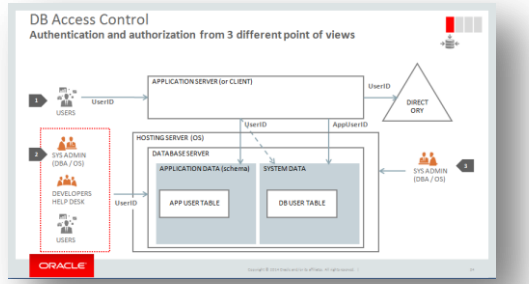
- ACCESS CONTROL
- DATA PROTECTION
- MONITORING, BLOCKING AND AUDITING
- SECURE CONFIGURATION

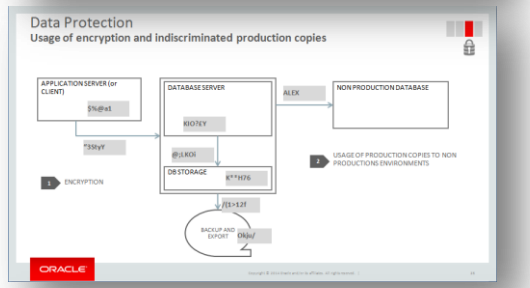
Modernize identity management to guarantee authentication and authorization both for business user and IT personnel

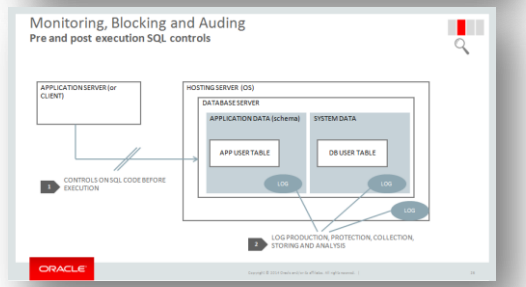
Protect the data wherever it is (encryption A.32) and avoid using real data where non necessary (A.5 and W.26)

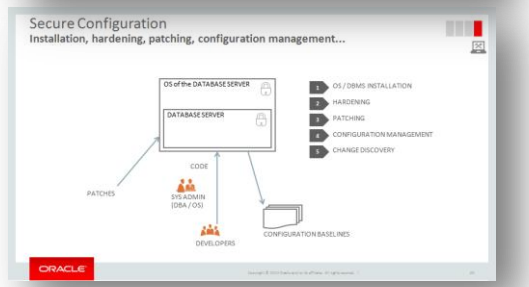
Collect, secure and analyze audit logs and implement SQL boundary defenses

Secure configurations, remediate vulnerabilities, and control production baselines









To start you need to assess your security and prioritize remediation projects

@EUROPRIVACY

Associazione Utilizzatori Sistemi E tecnologie Dell'Informazione

Clusit

Oracle Community For Security

Domande e Risposte

EUROPRIVACY.INFO
@EUROPRIVACY