DEFEND - Data Governance Framework for Supporting GDPR

Luis Miguel Campos (PDMFC)

Workshop on Privacy, Data Protection and Digital Identity
2019, July 11th, Coimbra, Portugal

DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787068.

Outline

- The General Data Protection Regulation (GDPR): milestones and challenges
- The DEFeND project at a glance
  - Objectives
  - Architecture and Components
  - Management and Organization of work
- Current status of the DEFeND project and roadmap of planned work

DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

The drivers of the GDPR regulation

- Need for *modernization*: new or advanced online services and technologies compared to the era that previous regulation rules were introduced (e.g., social networks, location-based services, cloud computing, data processing and storage capabilities)
- Need to give to individuals back *control* over of their personal data
- Need to *simplify* the regulatory environment for business
  - Unnecessary administrative requirements for businesses (e.g. notification to several data protection authorities) causing significant costs

Some Milestones for the GDPR

- In January 2012 EU proposes a reform of data protection rules to increase users' control of their data and to cut costs for businesses
- In March 2014 the European Parliament approves the proposal for the new regulation (first reading)
- In April 2016 the GDPR is announced
- In May 2016 the GDPR enters into force
- In May 2018 the GDPR applies

GDPR: Significant Changes and Implications Compared to the Previous Regulation

- Extension of data that fall under the categories of personal data and special categories of personal data
- Heavier responsibility and role for the data controllers and processors
- Appointment of Data Protection Officer
- Wider territorial scope
- Additional rights to the data subjects
- Differentiations on the role for the data protection authorities
- Privacy by default and personal data impact assessment as core principle for the design of information systems

DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

GDPR: Significant Changes and Implications Compared to the Previous Regulation

And of course…higher penalties!

GDPR: CHALLENGES

7 KEY PRINCIPLES

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Integrity and confidentiality
- Storage limitation
- Accuracy
- Accountability

ACCOUNTABILITY

- Contractual organization
- Privacy-by-design & Privacy-by-default
- Records of data processing activities
- Privacy Impact Assessments
- Data Protection Officer

RIGHTS OF INDIVIDUALS

- Information
- Access
- Rectification
- Erasure
- Restriction
- Portability
- Objection
- Automated decision-making / profiling

The DEFeND Project at glance

START DATE

1 July 2018

DURATION

30 months

GRANT AMOUNT

EUR 2,737,300.00

CALL TOPIC

H2020-DS08-2017 Cybersecurity PPP: Privacy, Data Protection, Digital Identities

DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

OBJECTIVES

1

Design and development of a successful, **MARKET-ORIENTED, PLATFORM** to support organizations towards GDPR compliance

2

Develop a **MODULAR SOLUTION** that covers different aspects of the GDPR

3

AUTOMATED methods and techniques to elicit, map and **ANALYZE DATA** that organizations hold for individuals

4

Advanced modelling languages and methodologies for privacy-by-design and **DATA PROTECTION** management

5

Specification, management and enforcement of **PERSONAL DATA CONSENT**

6

Integrated **ENCRYPTION AND ANONYMIZATION** solutions for GDPR

7

DEPLOYMENT and **VALIDATION** of the DEFeND platform in real operational environments

DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

DEFeND PILOTS

DEFeND platform will be tested in operational environment (**TRL 7**) for two different types of scenarios across **four sectors**, focusing on the **GDPR compliance** process for end-users and on the GDPR implications for external stakeholders.

ENERGY SECTOR (PRIVATE)
GP (France)

BANKING SECTOR (PRIVATE)
ABILab (Italy)

HEALTH CARE (PUBLIC)
Fundacion Para la Investigacion Biomedica Hospital Infantil Universitario Niño Jesus (Spain)

PUBLIC ADMINISTRATION (PUBLIC)
PESHTERA MUNICIPALITY (Bulgaria)

WORK PLAN

DEFeND

WP6: DISSEMINATION AND EXPLOITATION

- T6.1: Dissemination and public communication
- T6.2: Exploitation, Business and Commercialization
- T6.3: Training and Awareness
- T6.4: Projects and stakeholders networking

WP1: PROJECT, QUALITY AND COMPLIANCE MANAGEMENT

- T1.1: Project Management
- T2.2: Quality and Innovation Management
- T2.3: Compliance and Ethics Management
- T1.4: Technical Management
- T1.5: Security Advisory Board

WP5: PILOTS PREPARATION AND EXECCUTION

- T5.1: Pilots' preparations
- T5.2: Pilots' execution and evaluation
- T5.3: Pilots' final demonstration

WP2: REQUIREMENTS AND ARCHITECTURE

- T2.1: Requirements and Specifications
- T2.2: Privacy and Compliance Requirements
- T2.3: Platform Architecture
- T2.4: Definition of pilots' scenarios

WP4: INTEGRATION, DEPLOYMENT AND TESTING

- T4.1: Services' integration
- T4.2: Security and Legal Compliance Audit
- T4.3: Platform Testing and Refinement

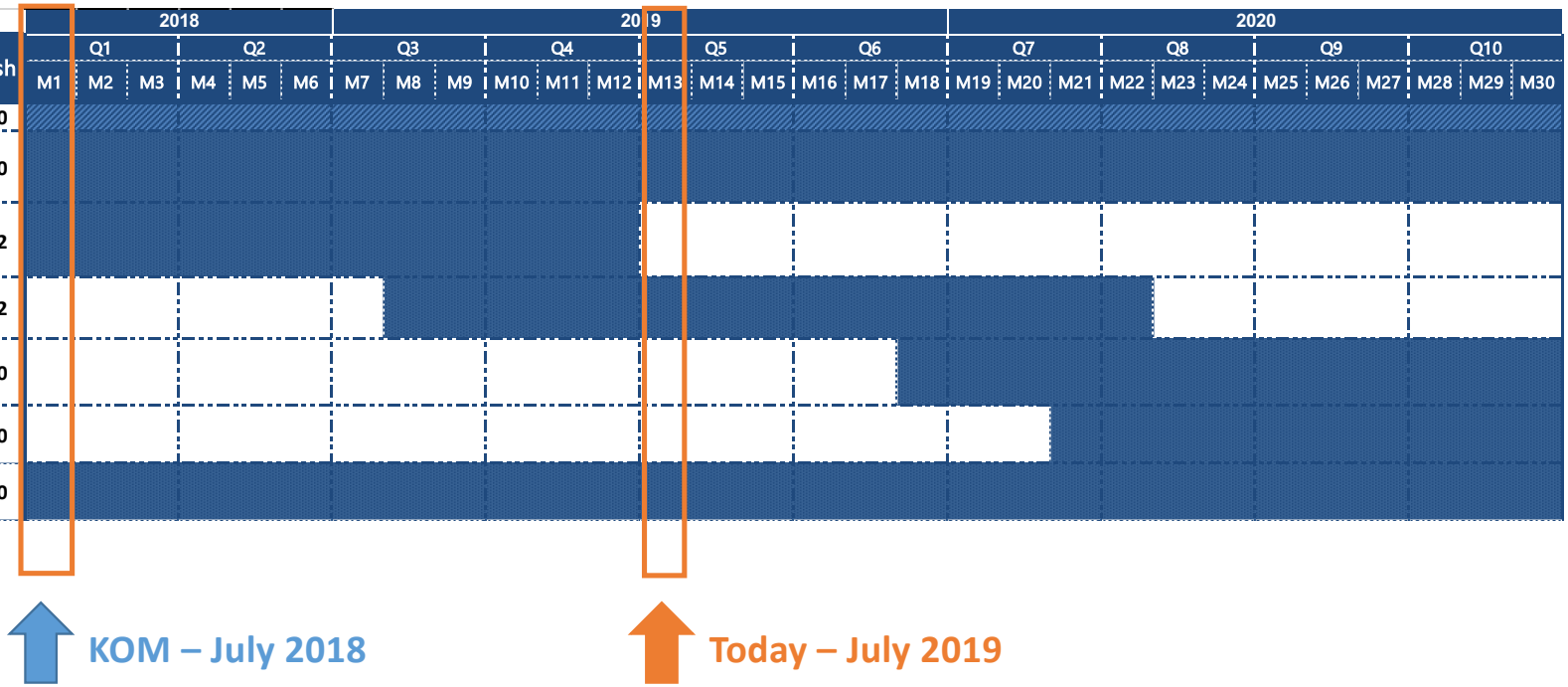
WP3: DEVELOPMENT OF PLATFORMS SERVICES

- T3.1: Data Scope Management
- T3.2: Data Process Management
- T3.3: Data Breach Management
- T4.4: Dashboard

DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

Where we are now

Task Name	Leader	Start	Finish
DEFeND project	ATOS	M01	M30
WP1: Project, quality and compliance management	ATOS	M01	M30
WP2: Requirements and Architecture	Ionian	M01	M12
WP3: Development of platform Services	UoB	M08	M22
WP4: Integration, Deployment and Testing	ATOS	M18	M30
WP5: Pilots preparation and execution	AbiLab	M21	M30
WP6: Dissemination and exploitation	MM	M01	M30



DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

Progress achieved so far

- All **management activities** were defined and now are up & running (administrative and financial, communication, quality procedures, risk management, etc).
- The **project advisory boards** Security Advisory Board and Ethical Committee were set up and various briefing meetings held. The External Ethical Advisor was selected and started work upon signature of NDA.
- **Technical activities** concentrated in WP2, active months 1-12. Specifically:
  - To define and formalize the requirements of the platform
  - To define and formalize the security and compliance requirements for the platform
  - To define the architecture of the platform
  - To thoroughly define the scenarios for the pilots
- The project created initial **dissemination** materials and was active in social media and conferences to create awareness of DEFeND.
  - www.defenproject.eu – Twitter, LinkedIn, YouTube, SlideShare
  - EU-promoted Cluster of H2020 GDPR projects
  - ERA 2018, IPICS 2018, RAID 2018, European Banking Federation F2F Meeting 2019, European Utility Week 2018, Forum ABI Lab 2019, 1st Public Project Dissemination Event, 8th May2019, Brighton, UK
  - Workshop on Privacy, Data Protection and Digital Identity…**right now!**

Outputs produced so far (or nearly)

Del. No	Deliverable title	Due by	Status
D6.1	Public Website and social network channels	M2	Submitted
D7.3	GEN - Requirement No. 6	M4	Submitted
D1.7	GDPR guidelines and requirements	M4	Submitted
D1.1	Project Handbook	M4	Submitted
D6.3	Public Project Presentation	M6	Submitted
D6.2	Dissemination and public communication strategy	M6	Submitted
D1.2	Semester Management Report 1	M7	Submitted
D2.2	Security and privacy requirements for platform	M9	Submitted
D1.8	Security Strategy and Guidelines	M9	Submitted
D2.1	Citizens and End-Users' Privacy Requirements	M9	Submitted
D2.4	Scenarios for the Pilots	M12	Submitted
D1.3	Intermediate Report	M12	Work in Progress
D2.3	Specifications and Architecture of the Platform	M12	Submitted
D7.4	GEN - Requirement No. 7	M12	Work in Progress

Interesting Findings!

- Tools for data inventory and mapping were considered by the end-users are the most critical and less difficult to achieve
- End users believed that the most important features of a platform would be to guarantee the separation of duties to prevent fraud and error when processing personal data, and to allow them to review compliance activities and keep records for internal/external reporting to demonstrate compliance
- End users believed it is challenging to incorporate tools for incident response plans in compliance with the GDPR and their obligations for reporting a breach

Interesting Findings!

- Both end users and citizens stated that the assessment of organization's readiness for the GDPR is the most important feature of such platform.
- Other important tools include functionalities that allow measurement of the privacy level that the organization achieves.
- Also tools for implementing security and privacy controls (e.g., anonymisation, encryption and authorisation) were considered important.
- The end users also pointed out the criticality of notification of the data subjects about privacy violations.

Roadmap for the future – technical activities

- **Development** of the DEFeND **services and components**
  - Implement the necessary enhancements of the existing tools
  - Develop the following platform components:
    - Data Scope Management – **D3.1 due by end of January 2020**.
    - Data Process Management – **D3.2 due by end of March 2020**.
    - Data Breach Management – **D3.3 due by end of April 2020.**
    - Dashboard – **D3.3 due by end of April 2020**.

Roadmap for the future – legal, compliance, ethical activities

- **Ethics strategy of the project, data and IPR management**
  - Define the strategy for the project related to the ethics issues and represent a general guideline on this topic
  - Provide a policy document on ethics and data management protocols and procedures to be used by the project team.
  - Deliverable **D1.6 due by end of September 2019**
- Ethics Pre-Grant Requirements
  - Humans - **D7.1 H - Requirement No. 2 due by end of February 2020**
  - Protection of Personal Data - **D7.2 POPD - Requirement No. 3 due by end of February 2020**

THANK YOU

DEFeND

DATA GOVERNANCE FOR SUPPORTING GDPR

Contacts

Coordinator: Beatriz Gallego-Nicasio Crespo, Atos,

beatriz.gallego-nicasio@atos.net

Technical Manager: Prof. Haralambos (Haris) Mouratidis, UoB,

H.Mouratidis@brighton.ac.uk

Communication: info@defend.eu | Project website: www.defendproject.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787068.