DEFEND - Data Governance Framework for  
Supporting GDPR

Luis Miguel Campos (PDMFC)

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

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
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
**GDPR**: Significant Changes and Implications Compared to the Previous Regulation

And of course...higher penalties!
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
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 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.
## Where we are now

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

### Timeline

- **Q1 2018**: KOM – July 2018
- **Q3 2020**: Today – July 2019

**Workshop on Privacy, Data Protection and Digital Identity**
11th July 2019, Coimbra, Portugal
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
  - Workshop on Privacy, Data Protection and Digital Identity…right now!
# Outputs produced so far (or nearly)

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

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.