



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



---

# PUBLIC WEBSITE AND SOCIAL NETWORK PROJECT CHANNELS

---

**CLASSIFICATION:** [PUBLIC]

<b>Type:</b>	Technical documentation		
<b>Official Project Deliverable:</b>	D6.1 - Public Website and Social Networks Project Channels	<b>Submission Date:</b>	30/08/2018

<b>Author:</b>			
Camillo Del Prete	Maticmind	WP6 leader	03/08/2018
<b>Reviewed by:</b>			
Haris Mouratidis	UoB	Reviewer	15/08/2018
Andrea Praitano	BSE	Reviewer	15/08/2018
Aggeliki Tsohou	Ionian	Reviewer	16/08/2018
<b>Approved by:</b>			
Beatriz Gallego-Nicasio Crespo	ATOS	Coordinator	30/08/2018



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



## Index

1	Executive Summary .....	7
2	DEFEND Public Website.....	8
2.1	Infrastructure.....	8
2.2	Organization/structure of the menu .....	8
2.2.1	Home .....	9
2.2.2	The project.....	9
2.2.2.1	Horizon 2020 .....	10
2.2.2.2	Objectives .....	10
2.2.2.3	Work Plan .....	13
2.2.2.4	The Platform .....	15
2.2.3	The Consortium .....	16
2.2.4	Communication .....	17
2.2.4.1	Events .....	17
2.2.4.2	News .....	17
2.2.4.3	Presentations.....	17
2.2.4.4	Brochures.....	18
2.2.4.5	Articles .....	19
2.2.4.6	Newsletters.....	19
2.2.4.7	Press Releases.....	19
2.2.4.8	Contacts .....	19
3	Social Media Channels.....	20
3.1	Linkedin .....	20
3.2	Slideshare .....	21
3.3	Twitter .....	21
3.4	YouTube.....	22
4	Website and Social Media Management .....	24
4.1	Analytics.....	24
ANNEX 1	Project Start-up Presentation.....	25



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



ANNEX 2	Project Brochure.....	26
---------	-----------------------	----



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



## REVISION HISTORY

Date	Author/Reviewer	Version	Summary of Changes
2/08/2018	<b>Camillo Del Prete</b>	1.00	First version of the document
15/08/2018	<b>Haris Mouratidis</b>	1.00	Reviewed Document
15/08/2018	<b>Andrea Praitano</b>	1.00	Reviewed Document
16/08/2018	<b>Aggeliki Tsohou</b>	1.00	Reviewed Document
28/08/2018	<b>Camillo Del Prete</b>	2.00	Final version of the document
29/08/2018	<b>Beatriz Gallego-Nicasio Crespo</b>	Final	Version for submission
22/10/2018	<b>Camillo Del Prete</b>	2.1	Social Media home pages revised due to the application of the art. 38 rules



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



# DEFEND PROJECT PROFILE

<b>H2020 topic:</b>	DS-08-2017 – Cybersecurity PPP: Privacy, Data Protection, Digital Identities
<b>Acronym:</b>	DEFEND
<b>Title:</b>	<u>Data governance for supporting GDPR</u>
<b>Official Website:</b>	<a href="http://www.defendproject.eu">www.defendproject.eu</a>
<b>Start Date:</b>	01/07/2018
<b>Duration:</b>	30 months

	ATOS SPAIN SA	
 <b>University of Brighton</b>	UNIVERSITY OF BRIGHTON	
 BE Your Security	BUSINESS-E SPA	
	BIRD & BIRD LLP	
	PDM E FC PROJECTO DESENVOLVIMENTO MANUTENCAO FORMACAO E CONSULTADORIALDA	
	IONIAN UNIVERSITY	
 PERSONAL SMARTGRID SOLUTIONS	GRIDPOCKET SAS	
 Tecnologia utile	ABI LAB - CENTRO DI RICERCA E INNOVAZIONE PER LA BANCA	
 Fundación para la Investigación Biomédica Hospital Infantil Universitario Niño Jesús	FUNDACION PARA LA INVESTIGACION BIOMEDICA HOSPITAL INFANTIL UNIVERSITARIO NIÑO JESUS	
	PESHTERA MUNICIPALITY	



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



# CLASSIFICATIONS OF INFORMATION

All information, related to an organisation, not considered Secret according to the national law can be considered as information with “limited or forbidden divulgation” or “unclassified”. This classification is related to the presence of confidentiality requirements of the information.

In relation to **public information**, one classification level is defined:

- **UNCLASSIFIED:** the internal or external distribution, with reference to the Company, of this kind of information does not create damage for the Defend Consortium and for each partner.

In relation to **private information** three levels of classification are defined, according to the confidentiality requirements:

- **INTERNAL USE ONLY:** the unauthorized distribution, the loss, the alteration, or undue use of this kind of information could create lowest level of ‘damage’ for the Defend Consortium or for one or more partners. The **personal data** shall be classified as “INTERNAL USE” and managed according to the internal consortium procedures established for this classification level, except for those data that are classified as “CONFIDENTIAL” or “TOP CONFIDENTIAL”
- **CONFIDENTIAL:** the unauthorized distribution, the loss, the alteration, or undue use of this kind of information could create significant damages for the Defend Consortium or for one or more partners. The **sensitive personal data** shall be classified as “CONFIDENTIAL” and managed according to the internal consortium procedures for this classification level, except for those data that are classified as “TOP CONFIDENTIAL”.
- **TOP CONFIDENTIAL:** the unauthorized distribution, the loss, the alteration, or undue use of this kind of information could create extreme damages, in some cases irreversible, for the Defend Consortium or for one or more partners.



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



## 1 EXECUTIVE SUMMARY

This document explains the solution that the DEFEND Consortium has identified for the DEFEND Public Website and the social network channels.

The DEFEND Public Website and the social network channels, available to all web users, represent a public deliverable.

The URL for the DEFEND website is: [www.defendproject.eu](http://www.defendproject.eu)

The choice of the “.eu” first level Internet Domain is related to the fact that DEFEND is a European Project under the Horizon2020 programme, thus the official European domain was identified as the best option.

The choice of the “defendproject” second level Internet Domain is due to the following reasons:

1. includes the acronym of the project (DEFEND);
2. includes the word “project” in order to explain the types of activities of the Consortium.

The second level Internet Domain does not include the acronym EU related to the European Union because this is included in the first level Internet Domain (.eu).

The platform selected for the implementation of the DEFEND Website is WordPress 4.9.7. Some WordPress plugins are included in order to:

- manage Cookies
- manage sharing on the social networks
- control access statistics

The social media channels are:

- Twitter
- LinkedIn
- Slideshare
- YouTube

BSE/Maticmind, as leader of the WP6, is the administrator of both the website and the social media channels.

The administrator is responsible for publishing relevant content.



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



## 2 DEFEND PUBLIC WEBSITE

### 2.1 INFRASTRUCTURE

The DEFEND Public Website is hosted by Aruba S.p.A. (<https://www.aruba.it/en/home.aspx>), which is an Italian company. Personal and administrative data is managed in Europe, in accordance with European Data Protection laws. Aruba processes the data exclusively to provide the hosting services. Data is not sold to third parties. The data stored with Aruba is completely under our control. Aruba guarantees, by standard hosting contract, that they will not access nor use the data that we store in their infrastructure. They will not access the data in our emails, hosting or Cloud. Aruba services comply with the CISPE - Cloud Infrastructure Services Provider Europe - Code of Conduct (<https://cispe.cloud/#code-of-conduct>) so they are GDPR compliant. They also provide services that help their customers to be GDPR compliant (<https://www.aruba.it/en/gdpr-european-data-privacy-regulation.aspx>)

The email and hosting services are managed exclusively within Aruba Italian data centres. These are infrastructures that Aruba owns, which are secure, reliable and certified to the highest standards (Rating 4) according to ANSI/TIA 942-A.

Aruba complies with the logical, physical and organizational standards imposed by ISO 27001 certification. They also have many other certificates, including ISO 9001, ISO 14001 and ANSI/TIA 942-A (<https://www.aruba.it/en/certifications.aspx>)

### 2.2 ORGANIZATION/STRUCTURE OF THE MENU

The menu of the website is organized on different levels:

1. Home	It is the standard menu label to come back to the home page
2. The Project	This page includes the abstract of the DEFEND project (proposal nr. 787068).
2.1 H2020	This section includes the description of the Horizon 2020 call and the topic.
2.2 Objectives	This section includes the objectives of the project
2.3 Workplan	This section describes how the work plan is organized
2.4 Platform	This section is related to the description of the platform. When ready, it will provide the link to a demo site of the DEFEND platform
3. The Consortium	This section is related to the description of the consortium
3.1 Atos Spain S.A.	Description of ATOS
3.2 University of Brighton	Description of University of Brighton
3.3 Business-e S.p.A.	Description of Business-e
3.4 Bird & Bird LLP	Description of Bird & Bird
3.5 PDM & FC	Description of PDM & FC Projecto Desenvolvimento Manutencao Formacao E Consultadorialda
3.6 Ionian University	Description of Ionian University
3.7 Gridpocket SAS	Description of Gridpocket
3.8 ABILAB	Description of ABILAB-Centro Di Ricerca E Innovazione Per La Banca





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



3.9 Hospital Universitario Niño Jesús HUNJ	Description of the Hospital Universitario Niño Jesús
3.10 Pesthera Municipality	Description of the Pesthera Municipality
4. Communication	This section is related to the dissemination documentation of the project
4.1 Events	This section is related to all the dissemination events where DEFEND partners participated
4.2 News	This section includes links that say about the DEFEND Project
4.3 Presentations	This section contains all the DEFEND public presentations made available by the project
4.4 Brochures	This section contains all the DEFEND brochures made available by the project
4.5 Articles	This section contains all the Articles and Papers related to the project and provided by the DEFEND partners
4.6 Newsletters	This section contains all the Newsletters sent by the project
4.7 Press Releases	This section contains all the Press Releases sent by the project
4.8 Contacts	This page contains the main contacts of the project

### 2.2.1 HOME

This menu entry is a link to the Website Home page.



Figure 1: Website - Home Page

### 2.2.2 THE PROJECT

This page introduces the DEFEND project describing its main aims:

- to deliver an innovative data privacy governance platform
- to be budget-available
- to support not only organisations to comply with GDPR but consultants, (legal and/or technical) to use it as part of their consultancy services to clients seeking GDPR compliance.



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



Figure 2: Website - The Project

### 2.2.2.1 Horizon 2020

This page describes the European programme – Horizon 2020 – context:

- Call: H2020-DS-2016-2017 - Digital Security Focus Area
- Topic: DS-08-2017 - Cybersecurity PPP: Privacy, Data Protection, Digital Identities



Figure 3: Website - Horizon 2020

### 2.2.2.2 Objectives

This page describes the objectives of the DEFEND project:



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



- Developing a GDPR privacy plan
- Creating a third party management program
- Managing privacy complaints and individual rights
- Implementing privacy by design/privacy engineering
- Meeting regulatory reporting requirements
- Creating data inventory and maps
- Obtaining and managing user content
- Creating a third party management program
- Managing privacy incidents and breach notification
- Data de-identification/ anonymization
- Addressing international data transfers
- Conducting privacy risk assessments (PIAs/DPIAs)
- Selection of appropriate security technical and organisational measures



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



Figure 4: Website - Objectives



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



### **2.2.2.3 Work Plan**

This section describes the work plan of the project in terms of the work packages that the consortium will work on. Both a textual description is provided for the work plan as well as a diagrammatic illustration of the projects work packages.

The demonstration of the workplan was articulated in the website by presenting the Workpackage structure that shows how tasks are organized thematically and the Gantt diagram that shows how tasks are organized chronologically.



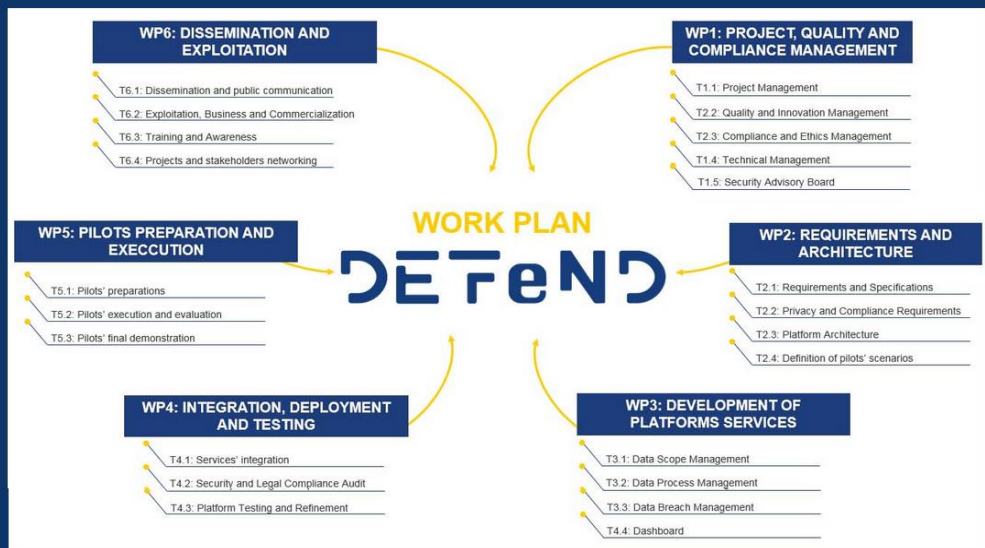


This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 787068.



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

Home The Project The Consortium Communication



Following is the Gantt of the project:

WPS	Task Name	Leader	Start	Finish	Q1		Q2		Q3		Q4		Q5		Q6		Q7		Q8		Q9		Q10										
					M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24	M25	M26	M27	M28	M29
1	DEFEND project		M01	M30																													
1.1	WP1: Project, quality and compliance management	ATOS	M01	M30																													
1.1.1	T1.1: Project Management	ATOS	M01	M30																													
1.1.2	T1.2: Quality and Innovation Management	Business-e	M01	M30																													
1.1.3	T1.3: Compliance and Ethics Management	Bird & Bird	M01	M30																													
1.1.4	T1.4: Technical Management	UoB	M01	M30																													
1.1.5	T1.5: Security Advisory Board	Business-e	M01	M30																													
1.2	WP2: Requirements and Architecture	Ionian	M01	M12																													
1.2.1	T2.1: Requirements and Specification	Ionian	M01	M09																													
1.2.2	T2.2: Privacy and Compliance Requirements	Bird & Bird	M01	M09																													
1.2.3	T2.3: Platform Architecture	ATOS	M01	M12																													
1.2.4	T2.4: Definition of pilots' scenarios	Abilab	M04	M12																													
1.3	WP3: Development of platform Services	UoB	M09	M22																													
1.3.1	T3.1: Data Scope Management	UoB	M09	M19																													
1.3.2	T3.2: Data Process Management	PDM	M10	M21																													
1.3.3	T3.3: Data Breach Management	ATOS	M11	M22																													
1.3.4	T3.4: Dashboard	Business-e	M08	M22																													
1.4	WP4: Integration, Deployment and Testing	ATOS	M18	M30																													
1.4.1	T4.1: Services' integration	ATOS	M18	M27																													
1.4.2	T4.2: Security and Legal Compliance Audit	Bird & Bird	M22	M27																													
1.4.3	T4.3: Platform Testing and Refinement	Ionian	M24	M30																													
1.5	WP5: Pilots preparation and execution	Abilab	M21	M30																													
1.5.1	T5.1: Pilots' preparation	Abilab	M21	M25																													
1.5.2	T5.2: Pilots' execution and Evaluation	Abilab	M25	M30																													
1.5.3	T5.3: Pilots' final demonstration	GridPocket	M28	M30																													
1.6	WP6: Dissemination and exploitation	Business-e	M01	M30																													
1.6.1	T6.1: Dissemination and public communication	Business-e	M01	M30																													
1.6.2	T6.2: Exploitation, Business and Commercialisation	ATOS	M17	M30																													
1.6.3	T6.3: Training and Awareness	Ionian	M17	M30																													
1.6.4	T6.4: Standardisation and Stakeholders Networking	Business-e	M01	M30																													

Privacy Policy

This website reflects only the Defend project's view. The European Commission is not responsible for any use that may be made of the information it contains.



Figure 5: Website – Work Plan



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



#### 2.2.2.4 The Platform

The DEFEND platform provides 5 main services to organisations and relevant stakeholders: Data Scope Management Service, Data Process Management Service, Data Breach Management Service, GDPR Planning Service and GDPR Reporting Service. The Figure provides a descriptive presentation of the five services of the DEFEND platform, so that interested parties can get familiar with the various functionalities that the platform will offer.

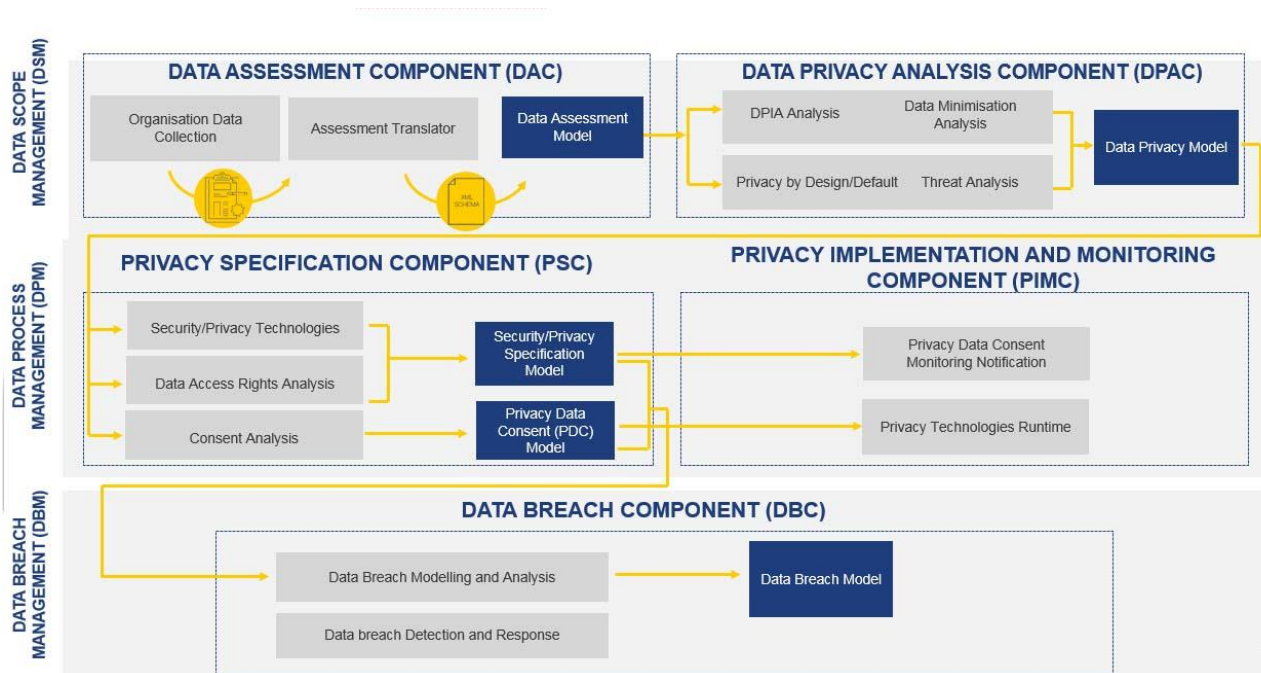


Figure 6: Website – Platform

#### Platform Dashboard

The platform dashboard acts as an interface (i.e. front-end) between the platform users (both organisations and clients/citizens, i.e. data controllers and data subjects) and the back-end components of the platform, as shown in the below figure:



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

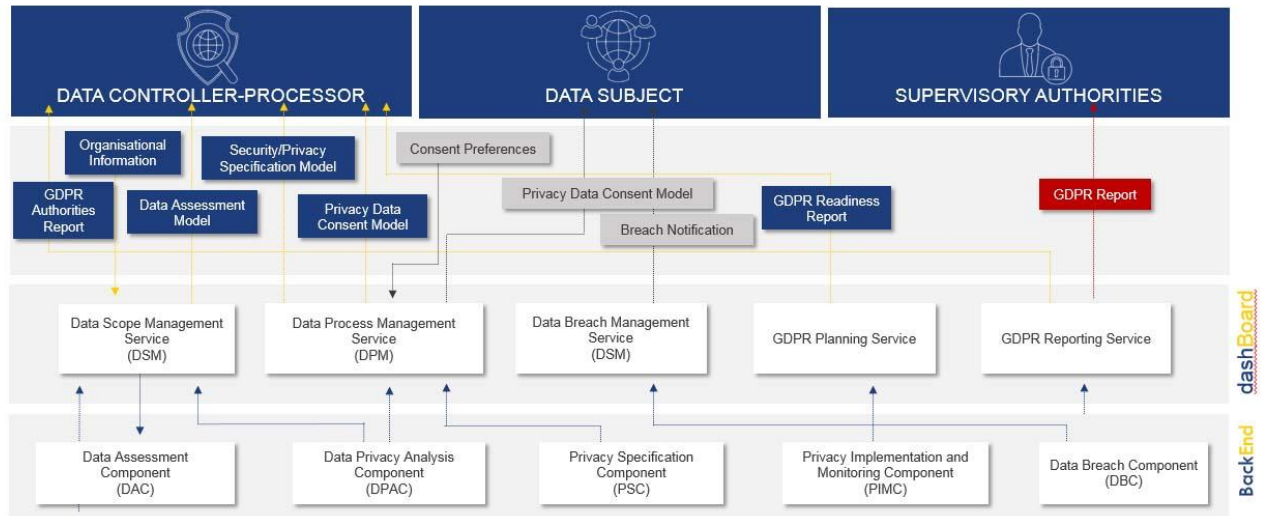


Figure 7: Website – Dashboard

### 2.2.3 THE CONSORTIUM

This page shows the list and the locations of the members of the Consortium.

Participant No	Participant organisation name	Partner short name	Country
1	Atos Spain S.A.	ATOS	Spain
2	University of Brighton	UoB	UK
3	Business-e SPA	BSE	Italy
4	Bird & Bird LLP	B&B	UK
5	PDM E FC PROJECTO DESENVOLVIMENTO MANUTENCAO FORMACAO E CONSULTADORIALDA	PDM	Portugal
6	Ionian University	Ionian	Greece
7	GridPocket SAS	GP	France
8	AbiLab-Centro di ricerca e innovazione per la banca	ABILab	Italy
9	Fundacion Para la Investigacion Biomedica Hospital Infantil Universitario Niño Jesus	FHUNJ	Spain
10	Pesthera Municipality	MoP	Bulgaria





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



Figure 8: Partners' map

There is a page for each member that contains the logo and the description of the organisation.

There is also a contact form where it is possible to communicate via email directly with each member

## 2.2.4 COMMUNICATION

This is a menu that allows to navigate through the communication items related to the project: events, news, public presentations, brochures and articles/papers.

### 2.2.4.1 Events

This page reports detailed information about the events (workshops, conferences ...) where DEFEND project members participated.

### 2.2.4.2 News

This page includes the links to on-line magazines that showed their interest in the DEFEND project. Here you can find the links to read what the web says about the DEFEND project

### 2.2.4.3 Presentations

This page collects the project presentations that can be viewed or downloaded.

For example, the Project Start-up presentation (see Annex 1) includes some Microsoft Power Point slides that introduce "DEFEND". It provides general information based on the official proposal submitted by the Consortium



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

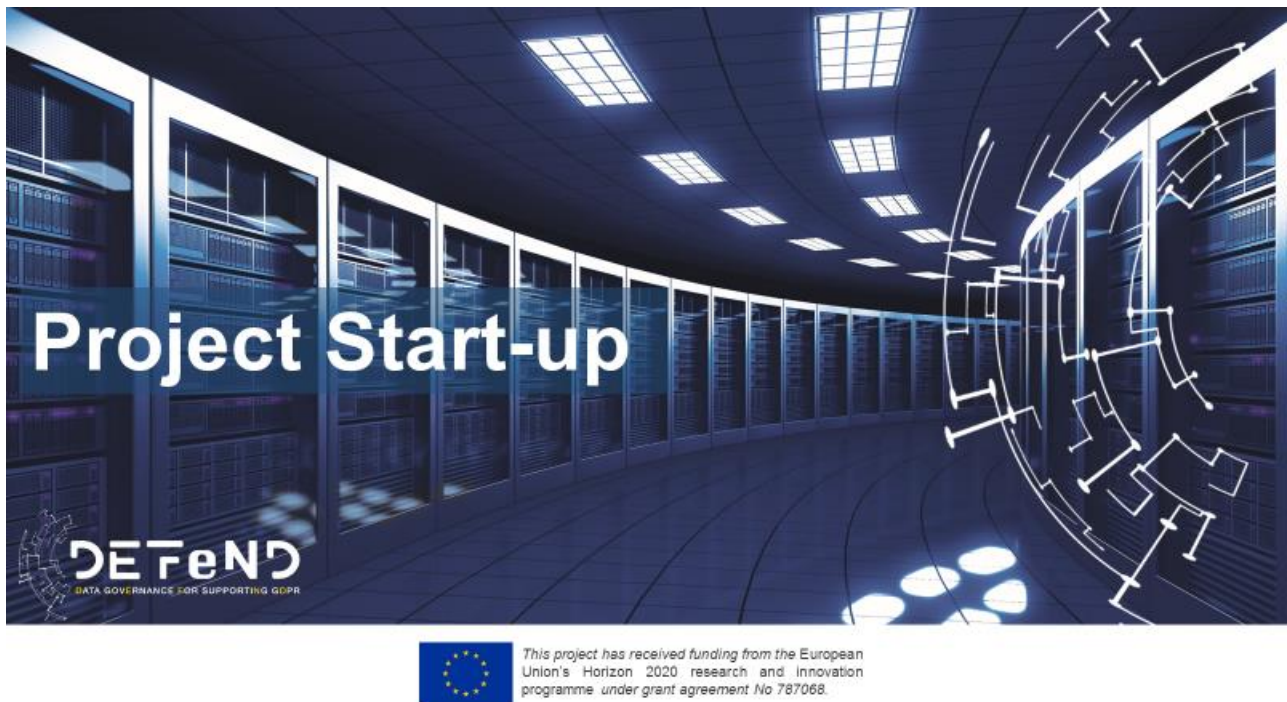


Figure 9: Presentation - Project Start-up

#### 2.2.4.4 Brochures

This page includes the brochures that can be viewed or downloaded.

For example, the Initial Project brochure (see Annex 2) includes general information about the Project



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



Figure 10: Brochure - Front Page

#### 2.2.4.5 Articles

This page includes the articles or papers related to the project and produced by the members of the Consortium. The articles/papers can be viewed or downloaded.

#### 2.2.4.6 Newsletters

This page includes the monthly newsletters sent by the project.

#### 2.2.4.7 Press Releases

This page includes the Press Releases sent by the project.

#### 2.2.4.8 Contacts

This page includes the main contacts of the project:

- Coordinator: Beatriz Gallego-Nicasio Crespo, Atos. [beatriz.gallego-nicasio@atos.net](mailto:beatriz.gallego-nicasio@atos.net)
- Technical Manager: Prof. Haralambos (Haris) Mouratidis, UoB. [H.Mouratidis@brighton.ac.uk](mailto:H.Mouratidis@brighton.ac.uk)
- Communication: [info@defendproject.eu](mailto:info@defendproject.eu)



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



### 3 SOCIAL MEDIA CHANNELS

The **social media** allow us:

- to reach an extremely wide but also **targeted audience**
- to manage our reputation
- to build networks all over the world to spread information about DEFEND Project

In addition, social media **create a community** of people interested in this argument and **engage with stakeholders**. We also expect to **increase traffic** on our website, including links to our website's content in every social media post.

Our social media strategy was based on the recommendations of the "Social media guide for EU funded R&I projects". So, we analyzed the following points:

- **Platforms.** Based on the analysis of the channels that are more suitable to achieve our goals and where we can find the right target audience, we decided to use **LinkedIn, SlideShare, Twitter and YouTube**. We decided to exclude other social media because they are mostly B2C (**Facebook or Instagram** for instance). The choice of the four platforms was based on the evaluation of several criteria: popularity, number of users, target audience.
- **Responsibility.** Since BSE/Maticmind is in charge of Work Package 6, the administration of the social media channels and the contents publishing is also in charge of BSE/Maticmind. The "Marketing specialist" Team member of BSE/Maticmind will be responsible for implementing the strategy and for the operations.
- **Target Audience.** The "Impact" paragraph 2 of the Annex 1 Description of Action (part B) and in particular the "DEFEND project dissemination strategy", was used as input to identify the target audience of the social media channels. The Consortium partners have individual dissemination plans to reach a broad range of industry sectors related to security, privacy, cloud computing and public administration authorities, in order to disseminate and promote the project and its results. Based on that we split the target audience in the following categories:
  - Industry
  - Scientific and research communities
  - Public administration
  - Citizens
- **Metrics.** How to evaluate the impact of the DEFEND social media channels? The KPI will be the number of followers and posts in Twitter and LinkedIn. As per the official proposal (Proposal-SEP-210452738.pdf), the success indicators are:
  - 150 followers per channel
  - 200 posts per channel
- **Language.** English is the language of the DEFEND social media channels.

#### 3.1 LINKEDIN

We created a LinkedIn **Company Profile** to get connected with experts. With DEFEND Project profile we will connect with **existing groups** that talk about the specific topics related to the DEFEND project.

We decided to open a company page to share **press releases, industry news**, links to **blog posts** and to celebrate **project achievements**.

We didn't open a group since we thought it is more efficient the LinkedIn page. It is a one-way communication channel and everybody could share a post. <https://www.linkedin.com/company/defendproject/>



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

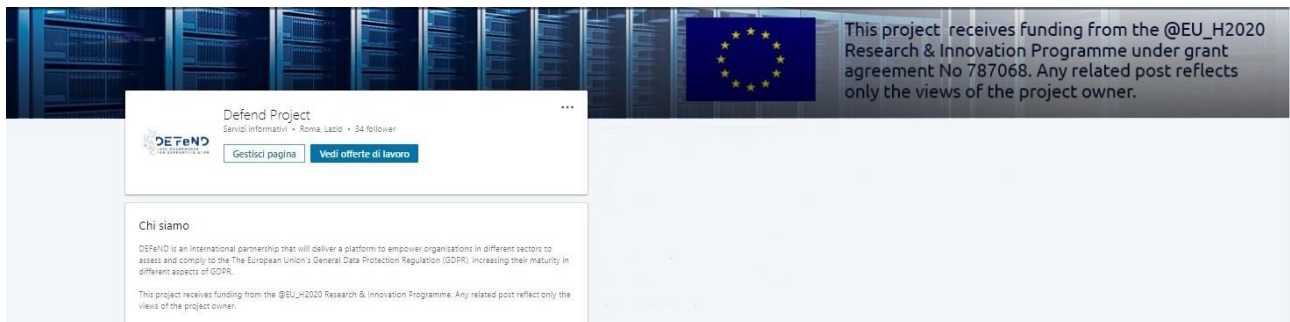


Figure 11: LinkedIn Page

## 3.2 SLIDESHARE

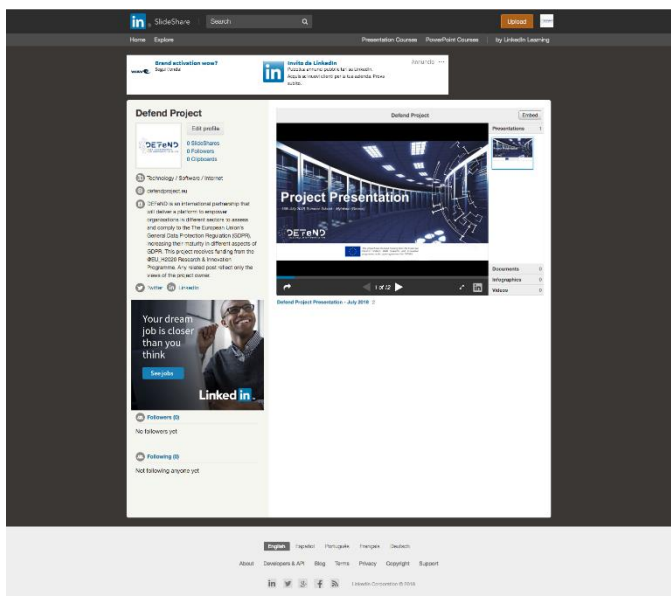


Figure 12: SlideShare Page

We created a Slideshare Profile, a platform to **share presentations, slides and documents**. By sharing high-quality content we will give the customers the possibility to find us and recognize the **authority of the DEFEND Project**.

<https://www.slideshare.net/DefendProject>

## 3.3 TWITTER





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



Figure 13: Twitter Page

We created a @DefendProject Profile on Twitter to **share comments** and **retweet** about **relevant content**. Inside the profile description we inserted a **summary** of **DEFEND Project's goals**.

We will also publish many posts that contain text about fund's origins as suggested by the guidance (Social Media Guide for EU funded R&I projects).

The hashtag **#DefendProject** is unused on Twitter and also in other chosen social media. By using it we will give the users the possibility to find all contents related to the project under the same hashtag.

<https://twitter.com/DefendProject>

Moreover, we have also analysed other **Top Hashtags** or **Growing Hashtags** to give more visibility to our posts. An example below:

Hashtag	Post	Users	Engagement	Reach	Impressions
#Privacy	711	680	204.237	6.375.436	6.453.893
#Cybersecurity	688	575	25.614	16.366.868	17.477.697
#GDPR	601	555	1.991	2.567.710	3.024.144
#Security	194	188	192.227	54.025.402	160.842.316
#Data Protection	149	142	587	4.373.299	4.550.264
#InformationSecurity	48	158	155	3.325.781	3.329.958
#DefendSecurity	0	0	0	0	0

We will also add #H2020, #InvestEUresearch, #HorizonEU, #EUBudget to our tweets whenever we think it is convenient.

### 3.4 YOUTUBE



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

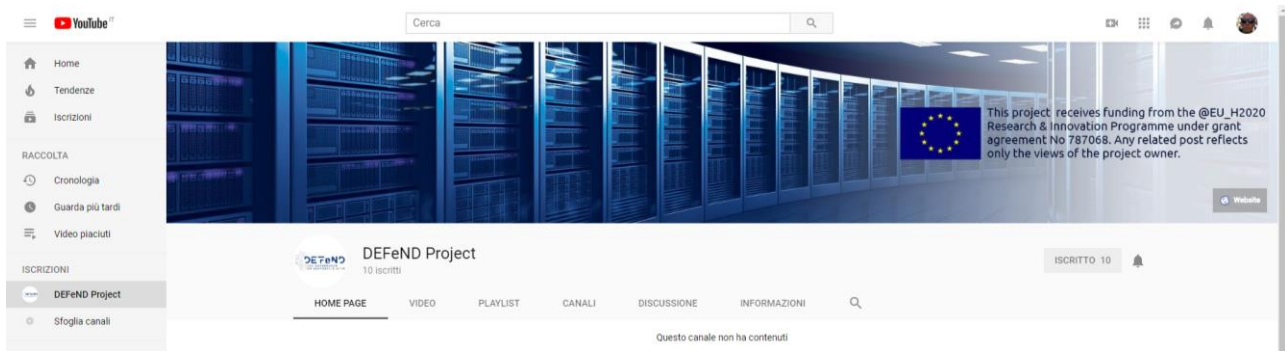


Figure 14: YouTube Page

We created a YouTube Profile to collect all the video contents and **share them on other social media**. Today, that information is increasingly coming from digital video, we decided to open a YouTube account to accommodate the growing trend of those users who prefer to gather information through videos rather than reading articles.

<https://www.youtube.com/channel/UC-EIn6YMV36meRSIO0XLFJw>



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



## 4 WEBSITE AND SOCIAL MEDIA MANAGEMENT

The public website and the social media content will be managed by BSE/Maticmind.

About the Website, there are two different roles in charge of updating it.

One role is technical. The person is responsible for maintaining the web pages. In case of changes or fixes to the website structure, the BSE/Maticmind webmaster will take care of them.

Another role is operational and it is related to content updates of the “communication” section of the website. The BSE/Maticmind marketing specialist will take care of them.

All the partners are required to send presentations, articles, papers and to report press releases, events and news to the following email address: [info@defendproject.eu](mailto:info@defendproject.eu). The Marketing Specialist will revise the format and will upload them onto the website.

About the Social Media, the “Marketing Specialist”, as responsible of the strategy and the operations, will take care of uploading files and sending. If a partner wants to suggest to include something in a Social Media channel, it could be done through the official email address “[info@defendproject.eu](mailto:info@defendproject.eu)”.

In order to facilitate the internal communications, a monthly call will be arranged by the WP6 leader so to involve all the partners on the Social Media and Website updates.

### 4.1 ANALYTICS

Analytics are very important for an effective digital marketing strategy: with analytics we can see if our digital strategy is working, if our target audiences are engaged with our content and last but not least monitor project's goals through KPIs.

We decided to use Google Analytics for the website to collect information like:

- Who visits your website
- How they got there
- What they did once they landed there
- Where they went afterward
- Demographic data such as what country they are visiting from

Every social media channel we choose (LinkedIn, SlideShare, Twitter and YouTube) offer a built-in social analytics tool to monitor reach and engagement of every single post. So we can measure also our social media strategy effectiveness and adjust strategy based on the insight we see in the social dashboards.





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



# ANNEX

## ANNEX 1 PROJECT START-UP PRESENTATION



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



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



## ANNEX 2 PROJECT BROCHURE



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



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



.....

**LAST PAGE OF THE DOCUMENT**

**INTENTIONALLY LEFT BLANK**

.....