Token

Transformative impact of disruptive technologies
in public services

www.token-project.eu

D8.4: PODP Req. N.4
Appointment of Data Protection Officer (DPO)

Project full title
Transformative impact of disruptive technologies in public services

Contract No.
870603

Strategic Objective
SC6-TRANSFORMATIONS-2019

Project Document Number
SC6-TRANSFORMATIONS-2019-870603-WP8-D8.4

Project Document Date
30.03.2020

Deliverable Type and Security
ETHICS - CO (Confidential, only for members of the consortium (including the Commission Services))

Author
Karen Vega. FIWARE Foundation

Contributors

Sofia Terzi CERTH, Jorge Munoz FBA, Johnny Choque & Laura Rodríguez de Lope UC, Juan Echevarria Cuenca AYTOSAN, Joris Finck IMEC,Kris Neyens VIL, MUKA

Revision

Stefano de Panfilis FIWARE Foundation

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

1 Introduction

Executive Summary

Institutions responsible for the hosting of personal data within the four user cases of TOKEN have listed in section 4 their Data Protection Officer. The contact details of the DPO will be made available to all data subjects involved in the research. For host institutions not required to appoint a DPO under the GDPR a detailed data protection policy for the project will be submitted as a deliverable.

About this document

This document contains the list of DPOs for the TOKEN project. Each DPO name was provided by the corresponding institution. The document will be updated if necessary as the user cases advance on the project.

Intended audience

Confidential, only for members of the consortium (including the Commission Services)

Reading recommendations

This document is divided into 5 sections:

Section 1: Introduction contains executive summary ,Section 2: Objective and Scope ,Section 3: Definitions, Section 4: List of DPOs & Section 5: List of User cases

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

The reader can go directly to section 4 where the list of DPO's is provided in an excel sheet. For convenience of the institutions in charge of the user cases we have provided definitions in section 3. On Section 5 there is a list of the institutions in charge of the user cases. A description of the user cases is provided on the next deliverable D8.5.

We would like to thank the host institutions that collaborated in providing the needed information for this deliverable.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

2 Objective & Scope

2.1 Objective

The objective of this WP is to ensure compliance with the 'ethics requirements' set out in this work package from Month 1 to 36. This WP has 8 deliverables.

2.2 Scope

D8.4 The requirement set by the European Commission for this deliverable set forth that the host institution appoints a Data Protection Officer (DPO).

In this case we defined host institution as : each institution in the TOKEN consortium hosting personal data used in the use cases of WP3. The contact details of the DPO will be made available to all data subjects involved in the research. For host institutions not required to appoint a DPO under the GDPR a detailed data protection policy for the project will be submitted as a deliverable.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

3 Definitions

The host institution.- Beneficiary of the TOKEN project that is hosting personal data in the user case of TOKEN. The 4 user cases and institutions listed in section 4.

Data Protection Officer (DPO).- The General Data Protection Regulation (GDPR) has established the concept of a Data Protection Officer (DPO) in Europe. Contrary to popular belief, decisive for the legal obligation to appoint a Data Protection Officer is not the size of the company but the core processing activities which are defined as those essential to achieving the company's goals. If these core activities consist of processing sensitive personal data on a large scale or a form of data processing which is particularly far reaching for the rights of the data subjects, the company has to appoint a DPO. Public bodies on the other hand always have to appoint a DPO, with the exception of courts who are acting in their judicial capacity. In addition, the legal norm to appoint a Data Protection Officer has a flexibility clause for Member States. These are free to decide whether a company has to appoint a Data Protection Officer under stricter requirements (e.g. Section 38 German Federal Data Protection Act). If such an obligation exists under the General Data Protection Regulation or a more specific national law, a group of undertakings can also appoint a single Data Protection Officer. If the group decides to do so, he must be easily accessible for the supervisory authorities, employees and external data subjects. If no legal obligation exists, companies can appoint a DPO on a voluntary basis to help with data protection compliance (which is for example recommended by the French data protection authority CNIL).[1]

Groups and companies have two possibilities to meet their obligation to appoint a Data Protection Officer. Either they name an employee as an internal Data Protection Officer, or they appoint an external Data Protection Officer. In selecting such a person, they must ensure that an internal Data Protection Officer is not subject to a conflict of interest due to his work in the IT Department, HR Department or senior management, where he would have to supervise himself. Regardless of which option is chosen, a Data Protection Officer must

[1] https://gdpr-info.eu/issues/data-protection-officer/

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

provide expert professional knowledge in data protection law and IT security, the scope depending on the complexity of data processing and the size of the company.

The duties of a Data Protection Officer include: Working towards compliance with all relevant data protection laws, monitoring specific processes, such as data protection impact assessments, increasing employee awareness for data protection and training them accordingly, as well as collaborating with the supervisory authorities. Therefore, the employee acting as Data Protection Officer must not be dismissed or penalised due to his fulfilment of his tasks. Despite his monitoring function, the company itself remains responsible for complying with data protection laws. Therefore it has to involve the Data Protection Officer in all issues which relate to the protection of personal data "properly and in a timely manner". When a Data Protection Officer is appointed, his superior must publish his contact data, and communicate his appointment and contact data to the data protection supervisory authorities. If a company voluntarily appointed a DPO they also must adhere to the criteria and provisions laid out above. Also note that the willful or negligent failure to appoint a Data Protection Officer despite a legal obligation is an infringement subject to fines[2].

Data Subject.- Identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[3]

Designation of the data protection officer[4].- The controller[5] and the processor [6]shall designate a data protection officer in any case where:

1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
2. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

[2] https://gdpr-info.eu/issues/data-protection-officer/
[3] https://gdpr-info.eu/art-4-gdpr/
[4] https://gdpr-info.eu/art-37-gdpr/
[5] means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (art. 4 GDPR)
[6] means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (art.4 GDPR)

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

3. the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

GDPR.-The European General Data Protection Regulation (GDPR) is applicable as of May 25th, 2018 in all member states to harmonize data privacy laws across Europe. https://gdpr.eu

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

4 List of DPOs

Each institution in the consortium hosting personal data used in the user cases has filled the information below. According to our understanding and internally discussed with the TOKEN Coordinator from FIWARE Foundation and WP3 Leader only the use cases which are hosting personal information have listed their DPO'.s. Hence this table has been filled by the responsible user case and is not applicable to the other institutions in the consortium. In case it is requested , we can update this document on a new version of this deliverable.

Table 4.1: DPO list TOKEN project

Each institution has filled the below table concerning the appointment of their DPO. We have considered this applicable to the institutions in charge of user cases.

Institutions	Location	Will you host data within the project? Y/N	If Y, have you appointed a DPO ?	If Y. Name of DPO	Email of DPO (*)	How will you make available the contact details of the DPO to all the data subjects involved in the research?	If you are NOT required to appoint a DPO under the GDPR, please answer N. A detailed data protection policy for the project will need to be submitted by your institution as part of the deliverable.	Please provide a link to a document where we can find your data protection policy
AYTOSAN	Spain	Y	Y	Rosendo Ruíz	innovacion@ayto-santander.es	Through the usual channel of the entity for personal data issues.	This was defined by the project to be applicable to user cases that host data	http://santander.es/ayuntamiento/proteccion-datos/derechos
CERTH	Greece	Y	Y	Ioannis Chalinidis	ivchal@certh.gr	By sharing the DPO email	This was defined by the project to be applicable to user cases that	https://www.certh.gr/01BF01A8.el.aspx

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

							host data	
Demos	Finland	N.A					This was defined by the project to be applicable to user cases that host data	N.A
FBA	Poland	Y	**Y**	Jorge Fernández	jorge@fundingbox.com	Via a contact form in the "Contact us" section of the FundingBox Platform	This was defined by the project to be applicable to user cases that host data	https://fundingbox.com/legal/privacy
FBR	Denmark	N.A					This was defined by the project to be applicable to user cases that host data	N.A
FIWARE	Germany	N.A					This was defined by the project to be applicable to user cases that host data	N.A
IMEC	Belgium	Y	Y	Klaas Ghesquiere	privacy@imec.be		This was defined by the project to be applicable to user cases that host data	https://www.imec-int.com/en/privacy-statement
INF	Luxembourg	N.A					This was defined by the project to be applicable to user cases that host data	N.A
MUKA	Greece	N.A					This was defined by the project to be applicable to user cases that host data	https://katerini.gr/πολιτική-απορρήτου/
UC	Spain	Y	Y	Gema Bilbao	dpd@unican.es		This was defined by the project to be applicable to	https://web.unican.es/consejo-direccion/gerencia/rgpd/politica-gener

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

							user cases that host data	al-de-proteccion-de-datos-en-la-universidad-de-cantabria
VIL	Belgium	N.A					This was defined by the project to be applicable to user cases that host data	N.A

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

5 List of institutions in charge of use cases

5.1 User Case 1: Public Funding Distribution (FBA)

5.1.1 Funding Box Accelerator sp.z o.o.(FBA).

Data protection appointed, see above for contact details.

5.2 User Case 2: Transparent Management of Public Accounts (CERTH, MUKA)

5.2.1 The Center for Research & Technology Hellas (CERT)

Data protection appointed, see above for contact details.

5.2.2 Municipality of Katerini (MUKA)

Their general policy is mentioned here https://katerini.gr/πολιτική-απορρήτου/

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

5.3 User Case 3: Last Mile City Logistic Services (IMEC, VIL)

5.3.1 Interuniversitair Micro-Electronica Centrum vzw (IMEC)

Data protection appointed, see above for contact details.

5.3.2 Flanders Institute for Logistics (VIL)

VIL will play a supporting role in the user case. Hence they will be under the policies and rules of IMEC.

5.4 User Case 4: Data Valorisation Services (UC, AYTOSAN)

5.4.1 Santander Municipality (AYTOSAN)

Data protection appointed, see above for contact details.

5.4.2 University of Cantabria (UC)

Data protection appointed, see above for contact details.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603