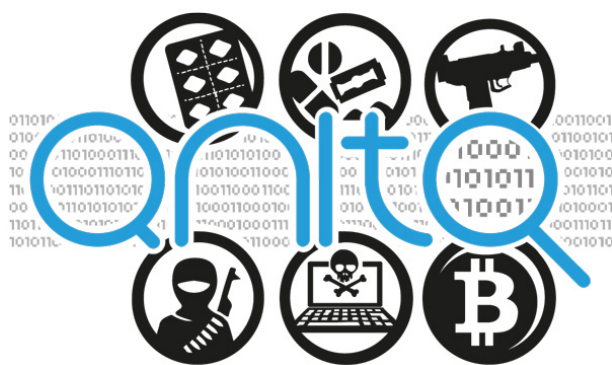




This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n° 787061



Advanced Tools for fighting Online illegal trafficking

D12.2 – POPD – Requirement No. 3

WP number and title	WP12 – Ethics Requirements
Lead Beneficiary	ENG
Contributor(s)	IIP
Deliverable type	Ethics
Planned delivery date	31/05/2018
Last Update	02/07/2018
Dissemination level	CO





Disclaimer

This document contains material, which is the copyright of certain ANITA contractors, and may not be reproduced or copied without permission. All ANITA consortium partners have agreed to the full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

The ANITA Consortium consists of the following partners:

Participant No	Participant organisation name	Short Name	Type	Country
1	Engineering Ingegneria Informatica	ENG	IND	IT
2	Centre for Research and Technology Hellas CERTH - ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	RTO	GR
3	Centro Ricerche e Studi su Sicurezza e Criminalità	RISSC	RTO	IT
4	Expert System S.p.A.	EXPSYS	SME	IT
5	AIT Austrian Institute of Technology GMBH	AIT	RTO	AT
6	Fundacio Institut de BioEnginyeria de Catalunya	IBEC	RTO	ES
7	Istituto Italiano per la Privacy	IIP	NPO	IT
8	SYSTRAN SA	SYSTRAN	SME	FR
9	Stichting Katholieke Universiteit Brabant	TIU-JADS	RTO	NL
10	Dutch Institute for Technology, Safety & Security	DITSS	NPO	NL
11	Belgian Road Safety Institute	ISBR	RTO	BE
Law Enforcement Agencies (LEAs)				
12	Provincial Police Headquarters in Gdansk	KWPG	USER	PL
13	Academy of Criminalistic and Police Studies – Kriminalisticko-Policijska Akademija	AoC	USER	RS
14	Home Office CAST	CAST	USER	UK
15	National Police of the Netherlands	NPN	USER	NL
16	General Directorate Combating Organized Crime, Ministry of Interior	GDCOC	USER	BG
17	Local Police Voorkempen	LPV	USER	BE

To the knowledge of the authors, no classified information is included in this deliverable



Document History

VERSION	DATE	STATUS	AUTHORS, REVIEWER	DESCRIPTION
V0.1	25/05/2018	Draft	ENG	First draft
V0.2	30/05/2018	Draft	ENG	Second draft
V0.3	14/06/2018	Completed version	ENG	Version ready for peer review
V0.4	20/06/2018	Final	IIP	Final
V0.5	02/07/2018	Final	ENG	Minor changes



Definitions, Acronyms and Abbreviations

ACRONYMS / ABBREVIATIONS	DESCRIPTION
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
LEA	Law Enforcement Authority



Table of Contents

Executive Summary6

1 Complying with the Requirement No. 37

2 Annex.....9

List of Tables

Table 1: DPOs of the partners processing personal data in ANITA.....9



Executive Summary

The goal of Work Package 12 is to ensure compliance with the “ethics requirements” described in the Grant Agreement. In this frame this specific deliverable aims to answer to the following requirement “Each Beneficiary involved in collecting and/or processing of personal data must nominate a Data Protection Officer.

Therefore, the following 2 sections describe, firstly, the new legal framework applicable with regards to the obligation of designating a Data Protection Office and secondly, the deliverable describes the way the consortium answered to this legal obligation, listing the DPOs nominated by the partners.



1 Complying with the Requirement No. 3

The data protection reform is a legislative package including:

- a general data protection regulation ('GDPR')¹
- a directive on protecting personal data processed for the purpose of criminal law enforcement ('LEAs Directive')²

On 24 May 2016, the GDPR entered into force and become applicable from 25 May 2018. The directive on protecting personal data processed for the purpose of criminal law enforcement entered into force on 5 May 2016. Member states had until 6 May 2018 to translate the directive into national law.

Due to the purpose of ANITA and the type of organisations the consortium is made of, it is necessary to consider that GDPR is applicable when LEAs Directive is not. So, both legal frameworks were considered in understanding the legal obligation of appointing a Data Protection Officer ('DPO').

The General Data Protection Regulation provides a modernised, accountability-based compliance framework for data protection in Europe. DPOs are at the heart of this new legal framework for many organisations, facilitating compliance with the provisions of the GDPR. Under the GDPR, it is mandatory for certain controllers and processors to designate a DPO. This is the case for all public authorities and bodies (irrespective of what data they process), and for other organisations that - as a core activity - monitor individuals systematically and on a large scale, or that process special categories of personal data on a large scale. Even when the GDPR does not specifically require the appointment of a DPO, organisations may sometimes find it useful to designate a DPO on a voluntary basis³.

Specifically, article 37(1) of the GDPR requires the designation of a DPO in three specific cases:

- a) where the processing is carried out by a public authority or body;
- b) where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or
- c) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Therefore, as the LEAs are "public authorities" in charge of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties they fall under art. 37(1)(a) of the GDPR that applies to processing "*carried out by a public authority or body*". In this sense, the appointment of a DPO is also mandatory for the LEAs.

For the purpose of this deliverable, it is necessary to take into account also the fact that article 37 of the GDPR applies to both controller and processors with respect to the designation of a DPO. Depending on

¹ 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,

² Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

³ ARTICLE 29 DATA PROTECTION WORKING PARTY, 16/EN WP 243 rev.01, *Guidelines on Data Protection Officers ('DPOs')*



who fulfils the criteria on mandatory designation, in some cases only the controller or only the processor, in other cases both the controller and its processor are required to appoint a DPO (who should then cooperate with each other)⁴.

Based on the above description, it is obvious that the legal requirement regarding the designation of a DPO is not related to the ANITA purposes and to the collection and/or processing activities that partners will do during the project, but rather to the profile of the partners (in the case of LEAs or other public authorities/bodies) or to their core activity.

Therefore, in order to correctly address Requirement No. 3, the consortium partners were debriefed about this legal obligation and were requested to assess their core activities in order to understand if appointing a DPO is mandatory or not.

In Annex, the list of the partners who appointed a DPO (as a legal obligation or on a voluntary basis) together with the name of the DPO can be found.

As a conclusion, ANITA consortium considers that Requirement No. 3 was addressed correctly and in an exhaustive manner, going beyond the legal obligations required under art. 37 GDPR and art. 32 LEA Directive.

⁴ ARTICLE 29 DATA PROTECTION WORKING PARTY, 16/EN WP 243 rev.01, Guidelines on Data Protection Officers ('DPOs')



2 Annex

Partner	DPO name
ENG	
CERTH	
EXPSYS	
AIT	
IBEC	
SYSTRAN	
TIU-JADS	
DITSS	
ISBR	
KWPG	
AoC	
CAST	
NPN	
GDCOC	
LPV	

Table 1: DPOs of the partners processing personal data in ANITA