REDALERT

Data Privacy Checklist

Report: D5.1.1. Data Privacy Check-list (PU)

Project acronym:	**RED-Alert**
Project full title:	**Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing**
Grant agreement no.:	**740688**
Responsible:	**MITLA**
Contributors:	**CITY, SO15, SPP, MOPS, GUCI, SPPS**
Document Reference:	**D5.1.1.**
Dissemination Level:	**Public**
Version:	**V1.0**
Date:	**10.10.2017**

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740688

History of Changes

Version	*Date*	*Modification reason*	*Modified by*
0.1	29.09.2017	Beta Version #1	Sarah Cannataci; Michael Zammit Maempel (MITLA)
0.2	29.09.2017	Quality check	Cristina Popescu; Daniela Chiricioaia (SIVECO)
0.3	05.10.2017	Review Beta Version #1	Adriana Prodan(SIVECO)
1.0	10.10.2017	Final reviewed deliverable	Daniela Chiricioaia (SIVECO)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740688

List of abbreviations

Acronym	Explanation
DPA	Data Protection Authority
EEA	European Economic Area
GDPR	General Data Protection Regulation
MITLA	Malta IT Law Association
CITY	CITY UNIVERSITY OF LONDON
EC	European Commission
GUCI	MINISTERIO DEL INTERIOR
LEA	Law Enforcement Agency
MOPS(INP)	MINISTRY OF PUBLIC SECURITY (ISRAEL NATIONAL POLICE)
SO15	MAYOR'S OFFICE FOR POLICING AND CRIME
SPP	SERVICIUL DE PROTECTIE SI PAZA
SPPS	SERVICIUL DE PROTECTIE SI PAZA DE STAT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740688

Introduction & General Notes

This document is intended to provide users, and particularly the law enforcement agencies within the consortium, with an easy-to-use checklist of all personal data considerations they may have to consider or flag when processing personal data in connection with the RED-Alert project. It is a privacy checklist against which all processing operations are to be measured and assessed.

The list does not purport to be a fully comprehensive solution to all privacy legal issues that may arise throughout the term of the project – and beyond – but is simply a tool that enables issues that may cause concern and require escalation to be flagged at initial stages.

This privacy list is likely to be updated one or more times during the course of the project. The current list is based on the framework set out in EU Regulation 679/2016 – General Data Protection Regulation ('GDPR'), and the obligations that are set out therein. There are, however, two important disclaimers that need to be set out at this stage:

(i) The GDPR will be brought into force in May, 2018, and although there is a body of experience and practice that has built up to date from the current laws in place in the various EU member states and beyond, the fact remains that it is an untested law, and that once put into effect it may give rise to practices that are different to those currently in place. In this event, this list may need to be amended to some extent or another, in order to apply to that future reality.

(ii) This list uses the GDPR as an objective benchmark, especially given that this is also the 'gold standard' by which other privacy laws across the world are typically measured. Different jurisdictions, including those jurisdictions in which the various consortium partners are based, and especially those that are not EU member states, have different (and at times, conflicting) laws and regulations concerning the subject. At the time of writing, a full and detailed analysis into the various jurisdictions in question remains ongoing. Once this review is finalised we expect new and different obligations to come to light and consequently this list may again need to be revised in order to incorporate these additional obligations.

In summary, therefore, this privacy checklist is designed to be a starting point on the basis of which the work of the consortium members may effectively take off. As always in the field of law, in the event of any concerns that may arise along the way, it remains necessary to seek advice on the specific query in hand, and not to plough ahead regardless.

A final word about using the checklist: the list does not (for practical purposes) make any distinction between obligations that arise in the capacity of a controller, and those arising as a processor of personal data [*Note*: a controller is broadly defined as that person/entity that decides how, why and when personal data is processed, and for which purposes; whilst a processor is a person/entity engaged, directly or indirectly, by the controller to carry out those processing operations, without having any decision-making power in the data process itself]. If, when using the checklist, you determine that a particular obligation may apply to you, regardless of whether you are a controller or a processor, you are advised to flag this either with your own internal legal advisors, or with MITLA.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740688

PRIVACY CHECKLIST

Question	✓/✗
General	
Are you processing personal data?	
Are you processing sensitive personal data (such as data reveling racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life and relating to criminal convictions)?	
Are you collecting and processing personal data of children?	
Are you a data controller (do you decide what should be the purpose of the data, which categories of personal data should be stored and which operations should be applied to them)?	
Are you a data processor (do you process personal data on behalf of the controller)?	
Are there any joint data controller relationships?	
Data Protection Principles	
Is there a lawful ground for processing the personal data for **each** processing operation?	
Is there a lawful ground for processing sensitive personal data for each processing operation?	
How is consent obtained?	
How is consent demonstrated?	
Can data subjects withdraw their consent?	
Do you have a data subject consent withdrawal procedure in place?	
Is the data subject notified of commencement of processing?	
If the data is collected from the data subject, is the required information (purpose of processing, identity of controller, information of rights) given to them?	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740688

If the data is not collected from the data subject, is the required information (purpose of processing, identity of controller, information of rights) given to them?	
Is personal data only used for the purposes for which it was originally collected?	
Is personal data collected adequate, relevant and not excessive in relation to the purposes for which it was collected or processed?	
Is the personal data limited to what is necessary for the purposes for which it is processed?	
Do you have a data review procedure in place to ensure that personal data is accurate and up to date?	
Do you have data retention policies in place which regulate archiving and destruction of data?	
Do you have appropriate security measures in place to protect the data?	
Can you demonstrate compliance with the data protection principles?	
Data Subject Rights	
Do you have a data subject access request procedure in place?	
Are you able to respond to a data subject access request within one month?	
Do you have data portability measures in place allowing the data subject to get their personal data in a structured, commonly used and machine readable format?	
Do you have a data subject erasure/rectification request procedure in place?	
Are data subjects informed of their right to demand erasure or rectification of the data held about them?	
Do you have a data subject objection procedure in place?	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740688

Are data subjects informed of their right to object to certain types of processing?	
Do you carry out profiling of data subjects?	
Is profiling based on consent?	
Data Security	
Is personal data systematically destroyed, erased or anonymized when it is no longer required to be retained or to fulfill the purpose(s) for which it was collected?	
Do you have a data pseudonymization procedure in place?	
Do you have a data breach notification procedure in place with respect to DPAs?	
Do you have a data breach notification procedure in place with respect to data subjects?	
Data Transfers	
Is personal data transferred outside of the EEA?	
Is sensitive personal data transferred outside of the EEA?	
Is personal data only transferred for the purposes for which it was originally collected?	
Are data subjects notified of transfers of their personal data?	
Do you have a data transfer request procedure in place?	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740688

References

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, and repealing Directive 95/46/EC (General Data Protection Regulation): http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740688