COMPACT

CYBERSECURITY FOR LOCAL ADMINISTRATIONS

D1.2 S.E.L.P. Management Plan (v1)

Work Package: WP1

Lead partner: KUL

Author(s): Yung Shin VAN DER SYPE, Danaja FABCIC POVSE

Submission date: July 2017

Version number: 0.1 **Status:** Final

Grant Agreement N°:	740712
Project Acronym:	COMPACT
Project Title:	COmpetitive Methods to protect local Public Administration from Cyber security Threats
Call identifier:	H2020-DS-2016-2017
Instrument:	IA
Thematic Priority:	Secure societies – Protecting freedom and security of Europe and its citizens
Start date of the project:	May 1st, 2017
Duration:	30 months

Dissemination Level	
PU: Public	✓
PP: Restricted to other programme participants (including the Commission)	
RE: Restricted to a group specified by the consortium (including the Commission)	
CO: Confidential, only for members of the consortium (including the Commission)	

Horizon 2020 European Union Funding for Research & Innovation

Project co-funded by the European Commission under the Horizon 2020 Programme.

Revision History

Revision	Date	Who	Description
	20 June 2017	Ioana Cotoi	Internal review
	6 July 2017	Nelson Escravana	Internal review

Quality Control

Role	Date	Who	Approved/Comment

Disclaimer:

Table of Contents

Definitions and acronyms

COMPACT	COmpetitive Methods to protect local Public Authorities from Cyber security Threats
CyberConnector	An internal knowledge collaboration site and social network that is used to share all the information among partners.
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
S.E.L.P.	Security, Ethics, Legal and Privacy

1. The COMPACT project

Cyberattacks pose a serious threat to public authorities and its agencies are regularly targeted by hackers. The public sector as a whole collects numerous data on its citizens but often keeps it on older, more vulnerable systems. Especially for local public authorities (hereafter: LPA's), protection against cyber-attacks is an issue due to outdated technologies and budget constraints.

The COMPACT project aims to develop a framework, which delivers "COmpetitive Methods to protect local Public Authorities from Cyber security Threats". The idea behind the project is to empower LPA's to combat cyberattacks by:

1. Increasing awareness,
2. Encouraging information exchange between LPA's throughout the EU,
3. Establishing links between LPA's and major European initiatives in the field.

2. COMPACT's legal and research ethics challenges

COMPACT is an EU project, funded by the Horizon 2020 Framework. The Horizon 2020 Framework was established by Regulation no. 1291/2013/EU.[1] The rules applicable to participation and dissemination in Horizon 2020 are set out in Regulation 1290/2013/EU.[2]

Article 19 of Regulation 1291/2013 sets out the ethical principles with which all actors in Horizon 2020 projects need to comply: "All research and innovation activities carried out under Horizon 2020 need to comply with ethical principles set out in this article and with relevant legislation. Particular attention is paid to the principle of proportionality, the right to privacy, the right to protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the right to ensure high levels of human health protection. Research and innovation must be focused exclusively on civil application."

The main ethical concerns of the project relate to the involvement of human participants in the project's research, the handling of personal data and the misuse of research findings.

[1] Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC.

[2] Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)" and repealing Regulation (EC) No 1906/2006.

Regarding trials with human participation, the participants must be able to validly consent to providing their personal data. To this end, partners will comply to the Grant Agreement, Part B, Section 5, p.91-98. Moreover, partners will use the information sheet template and informed consent form template, provided by the consortium in the COMPACT Grant Agreement, Part B, p.99-100.

Regarding personal data, it will be collected through research trials and obtained from LPA's, which possess data on their employees and citizens. Throughout the project both sets of data must be protected in accordance with European legislation.

The details of the measures to prevent misuse of research findings will be provided in D8.3 'M – Requirement No. 6'.

The main legal challenges in the COMPACT project relate to privacy and data protection with regard to the research trials and eventual implementation of the resulting technologies due to monitoring, information sharing risk assessment and threat intelligence.

Processing of personal data in the EU is currently still subject to Directive 95/46/EC[3] and relevant member states' implementation legislation. However, from May 25th 2018 a new General Data Protection Regulation (hereafter: GDPR)[4] will become applicable, setting out uniform rules for the entire European Union.

The GDPR sets out a stricter regime for data security by introducing the concept of *data protection by design and by default* (hereafter: data protection by design).[5] Data protection by design requires that data protection be included from the onset of the designing of systems, rather than as a later addition. The data controller must implement appropriate technical and organisational measures (e.g. pseudonymisation) in order to implement the data protection principles such as data minimisation (only processing data that is necessary for the purpose). Data minimisation applies to amount of data, its period of storage and its accessibility. In particular, it must be ensured that by default personal data are not made accessible to an indefinite number of people.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[4] 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).

[5] Art. 25 GDPR.

3. Scope of this report

The objective of Task 1.4 'Security, Ethical, Legal and Privacy (S.E.L.P.) Management' is to establish a single point of contact for legal and ethical questions. Management of Security, Ethical, Legal and Privacy (hereafter: S.E.L.P.) compliance is set out as a specific goal. This task will oversee the implementation of the S.E.L.P. framework and research-related legal issues. Compliance with S.E.L.P. will be monitored throughout the duration of the project.

Deliverable 1.2 'S.E.L.P. Management Plan' presents the Security, Ethical, Privacy and Legal management plan in the form of a report. It sets out criteria, with which the COMPACT research, trials and technology have to comply. These criteria are listed in the form of compliance checklists. Section 10. 'Overview deliverables' of this report lists the deliverables which require the internal ethics review. D1.2 will contribute to the WP2. 'Scenarios, Human Factors and Legal/Ethical aspects' activities and it will be updated as a second S.E.L.P. Management Plan in D1.4 in order to support the other research activities in COMPACT.

4. Internal Ethics Committee

In order to oversee the legal and research ethics compliance in the COMPACT project, an Internal Ethics Committee is established. The Internal Ethics Committee is composed of a KUL representative, Yung Shin Van Der Sype, and an ENG representative, Ioana Cotoi.

Compliance cannot be achieved with the efforts by one partner alone. Therefore, the whole consortium commits to contribute to this task. In sections 6 to 9 of this report, four checklists are set out. These checklists will be filled out by the task leaders of all legally or ethically sensitive tasks, as indicated in Section 10 of this report. The Internal Ethics Committee will oversee the self-assessment summary of the editors/task leaders. Moreover, the Internal Ethics Committee will keep a close contact with the Data Protection Officer (Salvatore D'Antonio, CINI), the Technical Coordinator (Luigi Romano, CINI) and the Trials and Ethical aspects coordinator (Andrea Minghetti, BOL). Moreover the other members of the Trials and Ethical Review Committee will be involved, as well as the users involved in the trials (BOL, CMA, CDA, DSS and BIT).

The means of communication are CyberConnector and email. Relevant threads on CyberConnector will be set up for specific questions.

5. Procedures for achieving legal and research ethics compliance in COMPACT

In order to achieve a high level of legal and research ethics compliance in COMPACT, the task leaders of ethically sensitive project tasks will perform a self-assessment and report the findings of this self-assessment to the Internal Ethics Committee.

The deliverables which are considered as legally or ethically sensitive are listed in Section 10 of this report.

Task leaders will self-assess their own input as follows:

- **First, before the beginning of the task the task leaders identify the legal and ethical challenges, based on the applicable compliance checklist (Sections 6 to 9),**
- **At the latest one month prior to the reporting deadline of the task, the task leaders report their findings to the Internal Ethics Committee,**
- **During the task the task leaders may directly contact Ioana Cotoi (ENG), as member of the Internal Ethics Committee,**
- **The final review will be conducted by Yung Shin Van Der Sype (KUL), in her role of member of the Internal Ethics Committee.**

A deliverable is internally considered as legally and ethically compliant if it meets all the criteria listed in the relevant checklist. The editor/task leader must attach a summary of the self-assessment as a separate section at the end of each deliverable. If the deliverable does not comply with the checklist, it must be updated so as to reach checklist compliance.

The checklists include preliminary legal and research ethics requirements that stem from the Horizon 2020 Ethics Self-Assessment Guidelines, in particular the provisions covering privacy and data protection.[6]

There are four different checklists in order to cover the different research areas in the COMPACT project.

The first checklist in this report concerns the overall COMPACT approach regarding the processing of personal data. According to the GDPR, 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); 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*

[6] Guidelines: How to complete your ethics self-assessment, http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf.

online identifier or to one or more factors specific to the *physical, physiological, genetic, mental, economic, cultural or social identity* of that natural person (emphasis added).[7]

The 'data controller' is the entity who defines the conditions and the means of the processing operations.[8] The 'data processor' conducts the processing on behalf of another organisation following their requirements.[9]

Data controllers are responsible to ensure that a Data Protection Impact Assessment (hereafter: DPIA) is carried out when the processing operation is likely to result in a high risk to the rights and freedoms of natural persons, especially if new technologies are used. High risk is thus the deciding criterion for necessity of an DPIA. When identifying high risk, the following criteria must be considered, although this list is not definitive:

(a) Evaluation or scoring, including profiling and predicting,

(b) Automated decision-making with legal or similar significant effects,

(c) Systematic monitoring,

(d) Processing of sensitive data,[10]

(e) Data processed on a large scale, 'large scale' depending on

   a. The number of data subjects concerned, either as a specific number or as a proportion of the relevant population,

   b. The volume of data and/or the range of different data items being processed,

   c. The duration, or permanence, of the data processing activity,

   d. The geographical extent of the processing activity;

(f) Combined or matched datasets,

(g) Data concerning subjects who are vulnerable due to power imbalance between them and the data controller, e.g. children, employees, patients, asylum seekers …,

(h) Innovative use or applying technological or organisational solutions,

(i) Data transfers to non-EU countries,

[7] Art. 4(1) GDPR.

[8] Art. 4(7) GDPR.

[9] Art. 4(8) GDPR.

[10] According to Art. 9(1) GDPR, Sensitive data is personal data revealing *racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,* and the processing of *genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*.

(j) Processing that by itself prevents data subjects from exercising a right or using a service or a contract.[11]

If at least two of the above criteria are met, the processing is likely to result in a high risk and there is a need to carry out a DPIA. If fewer than two criteria are met, the processing is deemed to be low-risk and there is no need for a DPIA.[12]

DPIA takes into account the nature, scope, context and purposes of the processing. It focuses on:

- A systematic description of data processing,
- Assessment of proportionality and necessity of data processing,
- Risk management,
- Involvement of all interested parties.[13]

The second, third and fourth compliance checklist included in this report concerns more specific research areas in the COMPACT project. These checklists are grouped into three categories based on the different goals of the deliverable under review. The three identified research areas (research goals) are:

1. Providing a theoretical research assessment,
2. Reporting on studies or trials in which human participants are involved,
3. Reporting of technical progress (S.E.L.P. by design).

These checklists are divided chronologically into two or three stages. First stage refers to the period before research in the deliverable was reported (preliminary measures). Second stage refers to the time of reporting and to the reporting itself. Third stage refers to the period after the delivery of the research results.

6. Template Data Protection Impact Assessment

This template is addressed to all partners in the COMPACT consortium. It aims to facilitate compliance with EU data protection legislation.[14]

[11] Working Party 29, Guidelines on Data Protection Impact Assessment (DPIA), p. 8-9.

[12] Working Party 29, Guidelines on Data Protection Impact Assessment (DPIA), p. 9.

[13] Working Party 29, Guidelines on Data Protection Impact Assessment (DPIA), p. 21.

[14] 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).

6.1. General info

Name and role (data processor/data controller):

Names of personnel involved in the process:

Will the Data Protection Officer's[15] (DPO) counsel be sought? If yes, please identify the DPO:

Will there be opportunities for data subjects or their representatives to present their views?

If yes, please explain:

6.2. Personal data

6.2.1. Collection of personal data

	YES	NO
Does your COMPACT activity require you to collect any personal data?		

If yes, please continue.

Describe the categories of personal data that will be collected:

Explain the process of data collection (when, how, information sheets, informed consent forms, other documents, etc.):

[15] Artt. 37-39 GDPR.

Please fill in the following:

	YES	NO
Will the data be combined with other data from outside the program/change?		
Can the collected data become personal data due to links to third parties?		
Will the activity require you to collect personal data from other systems?		
Does your organisation collect only as much data as is necessary for the specific purpose(s) of data processing?		
Will data be stored for a limited period of time?		
Are you aware of the impact on data subjects' privacy?		
Are data subjects informed of their rights?		
Are data subjects able to control which data are collected?		
Are they able to control (i.e. rectify, erase, object to processing) their data after it has been collected?		
Can data subject ask for a declaration as to whether their data is being processed (right to access)?		
Can data subjects receive data concerning themselves, which has been or is being processed (right to data portability)?		

6.2.2. Re-use of personal data

If your activity does not require you to collect any new personal data, please fill in the following:

	YES	NO
Does the activity require you to use previously collected personal data?		

If yes, please answer the following questions.

Please identify the owner of the dataset(s) (name, other important information):

Please identify the type of personal data previously collected:

Please fill in the following:

	YES	NO
Is data openly and publicly available (open source)?		
Do you have permission from the owner to use these dataset(s)?		
Do you possess informed consent forms, information sheets and other relevant documents from the previous collection?		

6.3. Data processing

What is the nature, scope, context, and purpose of the processing?

Is recording of personal data, recipients and period for which the personal data will be stored ensured?

How does the processing operation function?

How and where is personal data stored (hardware, software, networks, people, paper etc.)?

Does the processing comply with any approved code of conduct?[16]

6.4. High risk

Will you process data in ways, which are likely to result in a high risks for data subjects' rights? 'High risk' depends on whether the processing involves, among others (please note that the list is not definitive):

	YES	NO
Evaluation or scoring of data subjects, including profiling and predicting		
Automated-decision making with legal or similar significant effect		
Systematic monitoring of data subjects		
Processing of sensitive data		
Processing of data on a large scale		
Matched or combined datasets		
Data concerning vulnerable data subjects (e.g. employees or children)		
Innovative use or applying technological or organisational solutions		
Data transfer across borders outside the European Union		
Processing that by itself prevents data subjects from exercising a right or using a service or a contract		
Other similar measures		

If at least two of the above risks are met, please continue.

6.5. Impact on individuals' rights and freedoms

a. Human participation

[16] See Article 40 of the GDPR.

	YES	NO
Are you going to involve individuals in your study?		

If yes, how many subjects will be recruited to the study (by group if appropriate)?

Group	Number

b. Vulnerable groups

Will any of the subjects be from the following vulnerable groups –

	YES	NO	?
Children under 18			
Adults with learning or other disabilities			
Very elderly people			
Healthy volunteers who have a dependent			
Individuals in a subordinate relationship to investigators			
Other vulnerable groups			

If yes to any of the above, please specify and justify their inclusion:

c. Inclusion and exclusion criteria

Please indicate and argue the inclusion criteria for the project:

Please indicate and argue any exclusion criteria for the project:

d. Inducements

	YES	NO
Will any inducements be offered?		

If yes, please describe:

e. Recruitment procedure

Please describe how and where recruitment will take place:

f. Information sheet and consent form

It is assumed that as this study is being conducted on human subjects, an information sheet and associated consent form will be provided. A copy of the information sheet and form must be attached to this assessment.

If a consent form is not to be used, please provide a justification:

6.6. Ethical implications of the research

	YES	NO

Do you expect the processing to lead to discrimination?		

If yes, please explain, including any counter-measures your organisation will undertake:

	YES	NO
Do you expect the processing to lead to stigmatisation?		

If yes, please explain, including any counter-measures your organisation will undertake:

	YES	NO
Do you expect the processing to lead to stereotypization?		

If yes, please explain, including any counter-measures your organisation will undertake:

	YES	NO
Do you expect data subjects to change their behaviour due to the fact their personal data will be collected?		

If yes, please explain the possible change(s):

6.7. Risk management

Please identify the origin, nature, likelihood, particularity and severity of the following risks from the data subjects' perspective, taking into account risk sources and identifying potential impact and potential threat of a risk scenario:

Please also identify counter-measures against these risks.

Illegitimate access:

Undesired modification:

Disappearance of data:

6.8. Other

	YES	NO
Does the project activity contain any other measures that may affect privacy or other rights or freedoms of individuals?		

If yes, please explain:

7. Checklist for theoretical research

Risk	Requirement
Potentially severe impact of research results on human rights of individuals or groups (e.g. privacy issues, discrimination, stigmatisation)	• Risk assessment (fill in the DPIA) • Indicate the methods used for correct interpretation of research results, to avoid/reduce the negative impact on human rights • Indicate the methods used regarding the dissemination and publication of results, to reduce the negative impact on human rights • State that no data other than the results of the project (software and documentation) will be exported to non-EU Member States
Please justify your measure(s):	

Risk	Requirement
Potential misuse or abuse of research	• Indicate the measures used to reduce/avoid the potential misuse or abuse of the research
Please justify your measure(s):	

Risk	Requirement
Potentially negative impact of research on	• Use appropriate methods for

human rights	correct interpretation of research results
Please justify your measure(s):	

Risk	**Requirement**
Disclosure of confidential information	• Indicate the methods used regarding the dissemination and publication of results, to avoid the disclosure of confidential information of partners • State that partners complied with non-disclosure agreements and internal contracts in relation to research data
Please justify your measure(s):	

Risk	**Requirement**
Data loss	• Detail the measures on storage assessment (including access control), to avoid or reduce the data loss
Please justify your measure(s):	

8. Checklist for research involving human participants

Risk	Requirement
Potentially severe impact of research results on human rights of individuals or groups (e.g. privacy issues, discrimination, stigmatisation)	• Risk assessment (fill in the DPIA) • Indicate the methods used for correct interpretation of research results, to avoid/reduce the negative impact on human rights • Indicate the methods used regarding the dissemination and publication of results, to reduce the negative impact on human rights • State that no data other than the results of the project (software and documentation) will be exported to non-EU Member States
Please justify your measure(s):	

Risk	Requirement
Potential misuse or abuse of research	• Indicate the measures used to reduce/avoid the potential misuse or abuse of the research
Please justify your measure(s):	

Risk	**Requirement**
Non-compliance with data protection legislation	• Risk assessment (fill in the DPIA)
Please justify your measure(s):	

Risk	**Requirement**
Potentially negative impact of research on human rights	• Use appropriate methods for correct interpretation of research results
Please justify your measure(s):	

Risk	**Requirement**
Non-compliance with data protection legislation regarding human volunteers	• Risk assessment (fill in the DPIA)
Please justify your measure(s):	

Risk	**Requirement**
Disclosure of confidential information	• Indicate the methods used regarding the dissemination and publication of results, to avoid the disclosure of confidential

	information of partners • State that partners complied with non-disclosure agreements and internal contracts in relation to research data
Please justify your measure(s):	

Risk	**Requirement**
Data breach (loss) during execution of tests	• Indicate the methods used regarding the protection of the stored data and transfer of data
Please justify your measure(s):	

Risk	**Requirement**
Loss of personal data	• Indicate detailed measures on storage assessment, including access control • Provide details on the access control, e.g. safety measures
Please justify your measure(s):	

Risk	**Requirement**

Storage of vast quantities of data for long time periods	• Indicate the procedures and methods for erasure and anonymization of data
Please justify your measure(s):	

9. Checklist for S.E.L.P. by design

Risk	Requirement
Potentially severe impact of research results on human rights of individuals or groups (e.g. privacy issues, discrimination, stigmatisation)	• Risk assessment (fill in the DPIA) • Indicate the methods used for correct interpretation of research results, to avoid/reduce the negative impact on human rights • Indicate the methods used regarding the dissemination and publication of results, to reduce the negative impact on human rights • State that no data other than the results of the project (software and documentation) will be exported to non-EU Member States
Please justify your measure(s):	

Risk	Requirement
Potential misuse or abuse of research	• Indicate the measures used to reduce/avoid the potential misuse or abuse of the research • Indicate details on the storage and destination of research data • If applicable, store copies of personnel security clearances
Please justify your measure(s):	

Risk	**Requirement**
Non-compliance with data protection by design and by default principles	• Risk assessment (fill in the DPIA)
Please justify your measure(s):	

Risk	**Requirement**
Disclosure of confidential information	• Indicate the methods used regarding the dissemination and publication of results, to avoid the disclosure of confidential information of partners • State that partners complied with non-disclosure agreements and internal contracts in relation to research data
Please justify your measure(s):	

10. Overview of reviewed tasks and deliverables

This section lists deliverables, which require verification by Internal Ethics Committee before submission.

Deliverable	**Deliverable information**	**Checklist according to the work described in the GA**
D2.1 'Technological review and update'	Lead beneficiary: CINI Due date: M3	Theoretical
D2.2 'Psychological factors'	Lead beneficiary: AIT Due date: M6	Research with human participation
D2.3 'User requirements and use cases'	Lead beneficiary: S21SEC Due date: M6	Research with human participation
D2.4 'LPAs community model'	Lead beneficiary: ENG Due date: M6	Theoretical / S.E.L.P.
D2.7 'Awareness methods'	Lead beneficiary: AIT Due date: M12	Research with human participation
D3.1 'Services and Contents Specification'	Lead beneficiary: SIL Due date: M9	S.E.L.P.
D3.2 'Overall COMPACT architecture v1'	Lead beneficiary: CINI Due date: M9	S.E.L.P.
D3.3 'Components Evolution Plan'	Lead beneficiary: ENG Due date: M12	S.E.L.P.
D3.5 'Overall COMPACT architecture v2'	Lead beneficiary: CINI Due date: M24	S.E.L.P.
D4.1 'COMPACT Awareness and Education Adaptation v1'	Lead beneficiary: ENG Due date: M18	S.E.L.P.

D4.2 'COMPACT Risk Assessment Adaptation v1'	Lead beneficiary: ENG Due date: M18	S.E.L.P.
D4.3 'COMPACT Threat intelligence and monitoring Adaptation v1'	Lead beneficiary: CINI Due date: M18	S.E.L.P.
D4.4 'COMPACT Community Tool Adaptation and User Profile Development v1'	Lead beneficiary: ENG Due date: M18	S.E.L.P.
D4.5 'COMPACT Integration v1'	Lead beneficiary: S21SEC Due date: M18	S.E.L.P.
D4.6 'COMPACT Awareness and Education Adaptation v2'	Lead beneficiary: ENG Due date: M24	S.E.L.P.
D4.7 'COMPACT Risk Assessment Adaptation'	Lead beneficiary: ENG Due date: M24	S.E.L.P.
D4.8 'COMPACT Threat intelligence and monitoring Adaptation v2'	Lead beneficiary: CINI Due date: M24	S.E.L.P.
D4.9 'COMPACT Community Tool Adaptation and User Profile Development v2'	Lead beneficiary: ENG Due date: M24	S.E.L.P.
D4.10 'COMPACT Integration v2'	Lead beneficiary: S21SEC Due date: M24	S.E.L.P.
D4.11 COMPACT Gamified Educational Contents'	Lead beneficiary: KSP Due date: M24	S.E.L.P.
D5.1 'Validation and Demonstration scenarios'	Lead beneficiary: BOL Due date: M15	S.E.L.P./ Research with human participation
D5.2 'Trials Setup'	Lead beneficiary: BOL	Research with human participation

	Due date: M18	
D5.3 'Pilot execution and demonstration report v1'	Lead beneficiary: CINI Due date: M22	Research with human participation
D5.4 'Pilot execution and demonstration report v1'	Lead beneficiary: CINI Due date: M27	Research with human participation
D5.5 'Validation & Feedback Provision'	Lead beneficiary: BOL Due date: M27	S.E.L.P./ Research with human participation
D6.5 'Best practices and guidelines for immediate adoption by local PA v1'	Lead beneficiary: BIT Due date: M20	Theoretical
D6.8 'Best practices and guidelines for immediate adoption by local PA v2'	Lead beneficiary: BIT Due date: M30	Theoretical
D7.3 'Public Administration Information Security Sharing Best Practice'	Lead beneficiary: CINI Due date: M18	Theoretical
D7.6 'Public Administration Information Security Sharing Best Practice''	Lead beneficiary: CINI Due date: M30	Theoretical

11. Conclusion

The DPIA template must be filled in by all partners.

The checklists are task-specific and must be filled in by the task leaders of the tasks identified in the previous section. Before the beginning of these identified tasks, the task leader prepares a legal and ethical compliance strategy, using the relevant checklist provided at the end of this document.

During the task, the task leader reports on legal and ethical compliance via the CyberConnector platform or by email. This progress will be monitored by the Internal Ethics Committee.

Before completing the task, the editor of the deliverable attaches the relevant checklist at the end of the deliverable, so as to report the required self-assessment.

In the filled-in checklist, the editor describes which requirements are applicable to the deliverable.

In order to know whether a requirement is applicable, the editor consults the above analysis.

For all applicable requirements, the editor describes how the requirements from the checklists are met, and if any additional measures were taken, the editor describes those as well. In case the editor decides that the requirements are not applicable, this decision must be justified.

Unless specifically required, the checklists are not to be answered in a yes/no manner. Justification of measures taken is essential in order to raise overall ethics awareness.

The Internal Ethics Committee will oversee the correct implementation of the compliance checklists in each of the identified deliverables.