COMPACT

CYBERSECURITY FOR LOCAL ADMINISTRATIONS

D1.4 S.E.L.P. Management Plan v. 2

Work Package:	WP1
Lead partner:	KUL
Author(s):	Danaja Fabčič Povše (KUL), Erik Kamenjašević (KUL), Anton Vedder (KUL)
Submission date:	February 2018
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
0.1	4/01/2018	Danaja Fabčič Povše	Initial table of contents, initial content in all sections
0.2	29/01/2018	Danaja Fabčič Povše, Erik Kamenjašević	Input in all sections
0.3	30/01/2018	Danaja Fabčič Povše, Erik Kamenjašević, Anton Vedder	Adapted according to comments + final editorial review
0.4	12/02/2018	Danaja Fabčič Povše, Erik Kamenjašević, Anton Vedder	Final edit

Quality Control

Role	Date	Who	Approved/Comment
Internal reviewer	30/01/2018	Ioana Cotoi	Approved with minor comments
Internal reviewer	08/02/2018	Ion Larrañaga	Approved with minor comments

Disclaimer:

Table of Contents

List of Tables

List of Figures

Definitions and acronyms

CC	CyberConnector
CyberConnector	An internal knowledge collaboration site and social network that is used to share all the information among partners. Referred to also as CC.
DPIA	Data protection impact assessment
DPO	Data protection officer
ENG	Engineering Ingegneria Informatica
GDPR	General Data Protection Regulation
KUL	KU Leuven
PET	Privacy-enhancing technique
S.E.L.P.	Security, ethics, legal and privacy
WP2	Work package 2 – Scenarios, Human factors and Legal and Ethical aspects
WP3	Work package 3 – COMPACT Architecture
WP29	Article 29 Working Party, advisory body to the European Commission on personal data

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 in older, more vulnerable systems. Especially for local public authorities (hereafter: LPAs), 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 LPAs to combat cyberattacks by:

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

2. The scope of the deliverable

The purpose of this deliverable is to set out the procedures, according to which the COMPACT project aims to comply with legal and ethical requirements applicable to it. This is done via checklists/checkpoints and a data protection impact assessment (DPIA). The latter is filled in by all COMPACT partners, whereas there are three different checklists, on theoretical research, human participation and S.E.L.P. by design.

Monitoring compliance is an ongoing task in the COMPACT project: in D1.2, S.E.L.P. Management Plan v1, an early version of checklists and DPIA was circulated, and the Internal Ethics Committee was set up. Further, it listed all the deliverables, which need to be monitored for compliance, and which checklists they should fill out, as well as the procedures, necessary for compliance. However, as D1.2 was due early in the project, it has been updated in this deliverable. Specifically, in order to support WP3 activities, which will define (inter alia) the COMPACT architecture and S.E.L.P. by design from a technical point of view. The deliverables envisaged are D3.1 (Services and contents specifications), D3.2 (Overall COMPACT architecture v1), D3.3 (Components evolution plan) and D3.5 (Overall COMPACT architecture v2).
D3.4 (S.E.L.P. by Design in COMPACT) is a deliverable focussing on legal and ethical aspects, outlining the implementation of privacy and data protection requirements into the COMPACT architecture.

However, since compliance management is an on-going task, and architecture will be updated in M24, the S.E.L.P. management plan outline in this deliverable will apply to architecture, defined before the submission of this deliverable. If necessary to support further architecture specifications, management plan will be adapted in the upcoming deliverable D3.4.

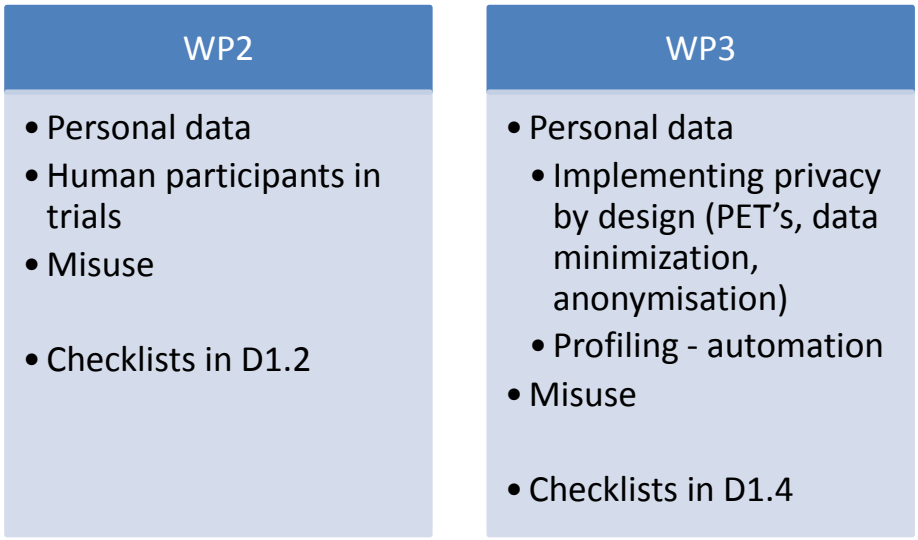

Figure 1: Non-compliance risks in COMPACT WP2 and WP3

Accordingly, the updated checklists for S.E.L.P. by design and the Data Protection Impact Assessment (DPIA) of this deliverable will apply to **the following deliverables: D3.1, D3.2, D3.3 and D3.5.**

3. The work of the ethics committee

With the deliverable D1.2, an internal Ethics Committee was set up, composed of a KUL and a ENG representative. The committee oversees the implementation of compliance checklists in the ethically sensitive deliverables. So far, the following deliverables have been submitted, which contain compliance checklists:

Deliverable	Date of submission	Checklist
D2.2 'Psychological factors'	M6	Research with human participation
D2.3 'User requirements and use cases'	M6	Research with human participation
D2.4 'LPAs community model'	M6	Theoretical / S.E.L.P.

Table 1: Submitted deliverables with compliance checklists

Deliverable D2.1 'Technology review update' did not contain the theoretical research checklist. Nonetheless, legal and ethical concerns were adequately addressed in its Chapter 2.5.2.[1] The chapter is replicated here in 9.1.1.

[1] Mariacarla Staffa et al., D2.1 'Technology Review Update', p 70.

The Internal Ethics Committee has found that relevant risks were adequately addressed and answered in COMPACT so far.

Further, it has also received a DPIA from AIT (see Annex I).

The procedure for legal and ethical management remains unchanged. The lead partner fills out the applicable checklist(s), with the committee overseeing the self-assessment summary of the editors/task leaders.
The means of communication remain CC and email.

4. Legal and ethics requirements for COMPACT architecture

The main legal challenges regarding the final COMPACT technology relate to privacy and data protection 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[2] and relevant member states' implementation legislation. However, from May 25th 2018 a new General Data Protection Regulation (hereafter: GDPR)[3] will become applicable, setting out uniform rules for the entire European Union.

Data protection legislation applies when 1) personal data are 2) being processed.

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 (Art. 4(1) of the GDPR).

Processing of personal data means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Art. 4(2) of the GDPR).

The **data controller** is defined as 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 (Art. 4(7) of the GDPR).

[2] 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.

[3] 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).

The **data processor** is defined as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Art. 4(8) of the GDPR).

In the WP3 activities, the data subjects will be the LPA employees and citizens, whose personal data is processed by COMPACT technology. As defined above, personal data is defined by the possibility of identifying a natural person from certain information. The definition of the data controller/data processor is important in order to determine with which requirements a partner has to comply when processing personal data. This assessment will be done on a case-by-case basis.

COMPACT technology will be based on **data protection by design and by default**. According to Art. 25 of the GDPR, data protection must be included from the onset of the designing process, rather than as a later addition. **The data controller** must implement appropriate technical and organisational measures (e.g. pseudonymisation, and privacy-enhancing techniques in general) in order to implement the data protection principles such as data minimisation. In particular, it must be ensured that by default personal data are not made accessible to an indefinite number of people.

The legal requirements of data protection by design were identified in D2.5.[4] Here we summarise them in a graphic for clarity:

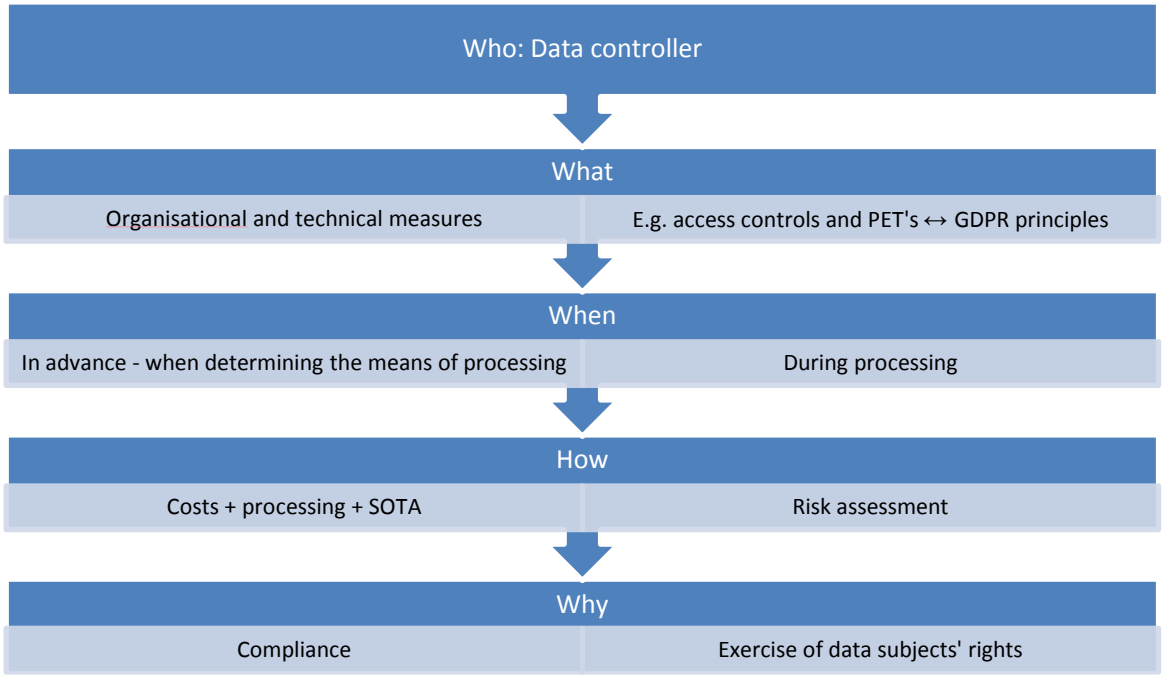

Figure 2: Article 25(1) of the GDPR: Data protection by design

[4] See Danaja FABCIC POVSE, D2.5 'S.E.L.P. Framework', especially chapters 2.7 and 4.3.

5. Achieving legal compliance in WP3

In the D1.2, checklist 'S.E.L.P. by design'[5] we identified four main risks, related to COMPACT technology:

(1) Potentially severe impact of research results on human rights of individuals or groups (e.g. privacy issues, discrimination, stigmatisation)
(2) Potential abuse or misuse of research results
(3) Non-compliance with data protection by design and by default
(4) Disclosure of confidential information

Those risks were, for the most part, addressed in D1.2. However, with the definition of COMPACT architecture,[6] non-compliance risks (3) become more specific and need more specific measures to counter them. Additionally, D3.1, D3.2 and D8.3 will set out measures to reduce the risk of potential abuse or misuse of research results (2).

Other risks remain unchanged, therefore the questions contained in the checklists also remain the same as before but are replicated here from D1.2 for clarity.

The main legal requirements of WP3 are **implementation of data protection by design and by default**, including implementation of PETs, adopting anonymisation measures and implementing the principle of data minimisation; and adopting **relevant safeguards when implementing profiling mechanisms** for detecting potential intrusions.

Furthermore, the partners involved in WP3 are also required to carry out a more detailed DPIA. As explained in D1.2,[7] a DPIA is required, if the processing is likely to result in 'high risks' to individual rights and freedoms.
This is especially the case when processing includes systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling; large-scale processing of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or a systematic monitoring of a publicly accessible area on a large scale.
Additionally, the Article 29 Working Party (WP29) has released guidelines on when the 'high risk' criterion is met. The whole list is contained in D1.2, the general rule is

[5] See Yung Shin VAN DER SYPE, Danaja FABCIC POVSE D1.2 'S.E.L.P. Management Plan (v1)', p 26.
[6] See Almerindo Graziano et al., D3.1 'Services and Contents Specifications'; EIB et al., D3.2 'Overall COMPACT Architecture'.
[7] See Yung Shin VAN DER SYPE, Danaja FABCIC POVSE D1.2 'S.E.L.P. Management Plan (v1)', p 9.

that if at least two criteria are met, the data controller is required to carry out a DPIA. Since WP3 activities will include systematic monitoring and profiling of employees, **the partners involved in those deliverables are required to carry out a DPIA per each deliverable**.

5.1. Data protection by design

Implementing data protection by design is a data processing exercise which **falls under the scope of the GDPR**. Therefore, **the GDPR applies wholly**, as to any other data processing activity. This means that, inter alia, all the data processing principles, such as data minimisation and data confidentiality and integrity, and the data subjects' rights apply.

In order to enhance compliance, Recital 84 of the GDPR specifically advises the controller and the processor to carry out a DPIA.[8] The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data is GDPR-compliant. Therefore, in order to mitigate this risk, the deliverables D3.1, D3.2, D3.3 and D3.5 should also contain **a data protection impact assessment (DPIA)**.

Additionally, those deliverables should also answer the questions, laid out in Chapter 6 in order to aim for legal compliance.

5.2. Profiling

Because COMPACT aims for a high level of automation, profiling is likely to be a part of the intrusion detection tools and services.

Profiling is defined as '**automated processing** of **personal data** consisting of the use of personal data to **evaluate certain personal aspects** relating to a natural person' (Art. 4(4) of the GDPR). If such profiling produces **legal effects concerning an individual**, or other significant effects, and is reached by **an automated decision**, then it falls under the scope of the GDPR and must meet certain requirements. (Art. 22 of the GDPR)

Schematically: profiling falls under GDPR requirements if:
1. There is automated processing (no human in involved) 2. It involves the use of personal data 3. It evaluates a human person's personal aspects 4. It produces legal effects or significant effects

[8] Recitals are the non-binding introductory part of any EU legislation and serve as a guidance and interpretation document.

All four criteria must be met. If one criterion is not met, we are talking about processing, not profiling.
For example, simple categorisation of threats and non-threats, which does not evaluate the user's behaviour, is NOT profiling in the sense of the GDPR; but it IS processing.

Why is profiling considered to be risky? Due to categorisation, it may lead to **illegal or unethical discrimination** if certain attributes are used (e.g. age, gender …). Since COMPACT is dealing with LPA employees, profiling could cause unfair dismissal or other type of discrimination in the workplace (e.g. someone could be branded a bad employee based on their cyber-unaware behaviour).

Further, due to the automated decision-making, the data subject may be **unaware how and why** a certain decision was reached – this is referred to as **information asymmetry**. This can sometimes lead to confusion and decreased trust between the employer and the employee, which COMPACT seeks to avoid.

False negatives and false positives may also occur. This is especially important, when profiling leads to legally significant effects in the employment context (denied raise or a dismissal based on false categorisation).[9]

In order to counter such risks, the data controller is required to adopt suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. The minimum requirement is to enable **the right to obtain human intervention** and for the data subject to **express his or her point of view** and to **contest the decision**. Additionally, the data subject must be provided with information, as set down in Articles 13 and 14 of the GDPR. This information must include **a meaningful description of the logic behind profiling**.
Profiling is also one of the situations which require the data controller to carry out a DPIA. In that case, the controller must consult with the DPO, if it is required to appoint one. In COMPACT, the LPAs are required to have a DPO, but the requirement may not apply to all the partners and all the processing activities.[10]
Therefore, the D3.1, D3.2, D3.3 and D3.5 should contain a **data protection impact assessment (DPIA)**, and answer the questions, set out in Chapter 6.

6. S.E.L.P. by design for WP3

Risk	Requirement

[9] See Bart H.M. Custers and Bart W. Schermer, Responsibly Innovating Data Mining and Profiling Tools: A New Approach to Discrimination Sensitive and Privacy Sensitive Attributes, in: J. van den Hoven et al. (eds.), Responsible Innovation 1: Innovative Solutions for Global Issues, Springer Science Business Media Dordrecht 2014, pp. 338-340.
[10] Who is required to appoint a DPO? See Danaja FABCIC POVSE, D2.5 'S.E.L.P. Framework', p 24.

Potentially severe impact of research results on humans due to privacy risks or potential discrimination (e.g. re-identification of participants, stigmatisation - being branded as a 'bad employee' due to past cyber behaviour)	• Risk assessment (fill in the DPIA) • Use appropriate methods for results interpretation and dissemination (e.g. pseudo-anonymisation) • 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 legislation when implementing profiling	• Risk assessment (fill in the DPIA)
Please justify your measure(s):	

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

Risk	Requirement
Non-compliance with data protection legislation regarding the exercise of data subjects' rights	• 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 • If applicable, store copies of personnel security clearances • State that partners complied with non-disclosure agreements and internal contracts in relation to research data
Please justify your measure(s):	

7. Data Protection Impact Assessment (DPIA) for WP3 activities

7.1. General

Name of organisation:

Role: is your organisation **a data controller or a data processor**?
Data controller is defined as the entity which 'determines the purposes and means of the processing of personal data'.
Data processor 'processes personal data on behalf of the controller'.

Names of personnel involved in the process:

Will the Data Protection Officer's (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:

7.2. Personal data

7.2.1. Collection of personal data

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

If yes, please continue.

Describe the types/categories of personal data that will be collected (e.g. age, gender, level of education, etc.):

Explain the purpose(s) of data collection:

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

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)?		

7.2.2. 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?		

7.3. 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 in the sense of Art. 40 of the GDPR?[11]

7.4. Automation

	YES	NO
Is your processing activity fully automated, i.e. no human is involved in the processing?		

If yes, please continue.

Does your processing activity include categorisation?[12] If yes, please explain:

[11] See Article 40 of the GDPR – such codes of conduct must be approved by the competent Data Protection Authority.

[12] 'Categorisation' refers to the use of classify methods, i.e. classification or clustering.

According to which criteria will categories be created? Does this criteria in any way include personal data, as defined in the GDPR?[13]

Does it include sensitive personal data, such as health, political orientation, etc.?[14]

Can data subjects contest their inclusion in a certain category? What is the procedure if they do so?

Can data subjects ask for information on why and how they were included in a certain category?

Does the processing activity evaluate a data subject's behaviour? If yes, what kind of evaluation is it? What kind of effects does it create and what does that mean for the data subject?

Will data subjects be informed about the logic of the processing activity in a clear and understandable manner?

7.5. High risk

Will you process data in ways, which are likely to result in a high risk 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		

[13] Definition of personal data in Art. 4(1) 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 online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[14] Sensitive personal data: 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 (Art. 9(1) of the GDPR).

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 with the DPIA.

7.6. Impact on individuals' rights and freedoms

a. Human participation

	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 explain the inclusion criteria of individuals for the project:

Please explain any exclusion criteria of individuals for the project:

d. Inducements

	YES	NO
Will any inducements to participate 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:

7.7. Ethical implications of the research

	YES	NO
Do you expect the processing to lead to discrimination? Discrimination may occur if criteria, such as gender, is used.		

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

	YES	NO
Do you expect the processing to lead to stereotypisation? Stereotypisation may occur due to evaluation carried out by automated tools, such as branding someone a security risk or a costly employee due to his/her poor cyber-behaviour.		

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 (e.g. not use devices, which allow monitoring, or otherwise adapt their actions due to COMPACT activities)		

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

7.8. 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.

Risk	Description	Counter-measures
Illegitimate access to data		
Undesired modification of data		
Disappearance of data		

7.9. 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:

8. Conclusion

The questions and requirements in this deliverable are aligned with architecture defined before Jan 29 2018.

The technical deliverables of WP3, i.e. **D3.1, D3.2, D3.3 and D3.5 must all fill in DPIA and the S.E.L.P. by design checklist**. The filled-in questionnaires must be attached to the deliverables as annexes, or in the case of a deliverable qualifying as other (e.g. a demonstrator), as a separate document. The questions are not to be answered in a yes/no manner, unless it is specifically required to do so.

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

The means for answering questions and follow-up within the consortium remains CC or emails for smaller groups.

9. Annex I: 'Checklist' from D2.1

9.1.1. Legal aspects and privacy concerns

Just like any other powerful technology or service, cyber threat intelligence can be used for both good and evil. For instance, while an organization may use cyber threat intelligence to acquire intelligence that could proactively improve its security posture and inform strategic, operational and tactical decisions with regards to cyber security, an adversary or cyber threat actor may as well use the same information to plan or execute cyber attacks with more precision. A more specific example may include a cyber threat actor who uses cyber threat intelligence technology to search for lost credentials belonging to an organization to gain unauthorized access to the information. At the current rates of cyber threat intelligence products and services it is in fact quite likely that many organizations could either not afford to acquire the capabilities or decide to defer their acquisition to a later stage. A well-motivated and financially capable attacker will instead have easier access to cyber threat intelligence capabilities and thus have more opportunities to carry out effective cyber attacks. Ability to access lost credentials also poses a big concern with regards to people's privacy.

Another legal concern related to cyber threat intelligence is the acquisition of information. Some information is not easy to acquire legally and it may require unorthodox or illegal means. On the other hand, it is difficult if not impossible for the end user of the intelligence to know if the intelligence has been obtained legally.[15]

[15] This Chapter is identical to Chapter 2.5.2 from Mariacarla Staffa et al., D2.1 'Technology Review Update', p 70.

10. Annex II: Data Protection Impact Assessment: WP2 First Online Study

This template is addressed to all the partners. It aims to comply with EU data protection legislation.[16]

10.1. General info

Name and role (data processor/data controller):

Peter Wolkerstorfer

Names of personnel involved in the process:

Cornelia Gerdenitsch, Daniela Wurhofer, Peter Wolkerstorfer

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

No. Only required when audio, video or biometric data will be collected.

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

If yes, please explain:

Subjects can ask questions regarding the survey. For that an E-mail address is located at the end of the survey.

10.2. Personal data

10.2.1. Personal data

	YES	NO
Does the program/change require you to collect any personal data?	x	

If yes, please continue.

Describe the categories of personal data that will be collected.

Variables measuring knowledge about cyber security, work-related variables (e.g. time pressure), individual variables (self-efficacy, self-regulatory focus), organizational variables (e.g., error culture) and demographic information. The questionnaire is provided in the appendix.

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

[16] 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).

Data will be collected in October and November via an online survey implemented with LimeSurvey. The information sheet and informed consent form are presented at the starting page of the survey and need to be confirmed by participants.

Please fill in the following.

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

10.2.2. Previously collected personal data

~~If the program/change does not require you to collect any new personal data, please fill in the following:~~

	~~YES~~	~~NO~~
~~Does the program/change 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?~~		

10.3. Data processing

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

The data will be quantitatively analysed to assess the effect of psychological variables (e.g., knowledge, motivation) on cyber-secure behaviour of LPA's employees. Data is processes accumulated that no conclusions on the individuals are possible.

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

We do not record personal data. No analyses will be published where individuals can be directly or indirectly identified.

How does the processing operation function?

The data will be stored in a folder by the AIT research team and only used for research purposes related to the evaluation of the COMPACT online study. Data will be processed using statistical programs such as SPSS.

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

Data is stored only internally in our facilities with provide state of the art IT security. State of the art IT security measures and company policies mitigate most of the risk of illegitimate access. Firewalls (to prevent illegitimate access from outside) and a rights-based-file system (to prevent illegitimate access from inside) are the countermeasures against this risk.

Does the processing comply with any approved code of conduct?[17]

There is no approved code of conduct at our institution. Data processing will be in a way that anonymity of data is approved. No analyses will be published where individuals can be directly or indirectly identified.

[17] See Article 40 of the GDPR.

10.4. High risk

Will the program/change 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, including profiling and predicting	x	
Automated-decision making with legal or similar significant effect		x
Systematic monitoring		x
Processing of sensitive data	x	
Processing of data on a large scale		x
Matched or combined datasets		x
Data concerning vulnerable data subjects	x	
Innovative use or applying technological or organisational solutions		x
Data transfer across borders outside the European Union		x
Processing that by itself prevents data subjects from exercising a right or using a service or a contract		x
Other similar measures		x

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

10.5. Impact on individuals' rights and freedoms

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

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

Group	Number
LPAs of end user organisations CMA, CDA, BOL, DSS, BIT	> 100

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

	YES	NO
Children under 18		x
Adults with learning or other disabilities		x
Very elderly people		x

Individuals in a subordinate relationship to investigators		x
Other vulnerable groups	x	

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

Employees as vulnerable group. Employees of LPAs are included in the study, because they are the target group of the project

h. Inclusion and exclusion criteria

Please indicate, with reasons, the inclusion criteria for the project

LPAs are included in the study, because they are the target group of the project and part of the project. All employees of the end user organizations CMA, CDA, BOL, DSS, BIT are potentially included in the study.

Please indicate, with reasons, any exclusion criteria for the project

Participants who do not work for the LPAs are not included, because they are not the target group of the project.

i. Will any inducements be offered? If 'Yes', please describe

No.

j. Please describe how and where recruitment will take place

The link to the online study will be sent by the end user organisations CMA, CDA, BOL, DSS, BIT to their employees – participation is voluntary.

k. 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:

Not applicable – information sheet and consent form is provided.

10.6. Ethical implications of the research

Do you expect the processing to lead to discrimination? If yes, please explain, including any counter-measures your organisation will undertake:

No, we do not expect discrimination, as the data is processed accumulated and no conclusions about individual persons are possible.

Do you expect the processing to lead to stigmatisation? If yes, please explain, including any counter-measures your organisation will undertake:

No, we do not expect stigmatisation, as the data is processed accumulated and no conclusions about individual persons are possible.

Do you expect the processing to lead to stereotypization? If yes, please explain, including any counter-measures your organisation will undertake:

No, we do not expect stereotypization.

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):

No, we do not expect data subjects to change their behaviour.

10.7. 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:

State of the art IT security measures and company policies mitigate most of the risk of illegitimate access. Firewalls (to prevent illegitimate access from outside) and a rights-based-file system (to prevent illegitimate access from inside) are the countermeasures against this risk.

Undesired modification:

Same as illegitimate access.

Disappearance of data:

Same as illegitimate access.

10.8. Other

Does the program/change contain any other measures that may affect privacy or other rights or freedoms of individuals?

If yes, please explain:

No.