CYBERSECURITY FOR LOCAL ADMINISTRATIONS

D3.4 S.E.L.P. by Design in COMPACT

Work Package:	WP3 COMPACT Architecture		
Lead partner:	KU Leuven (KUL)		
Author(s):	Danaja Fabcic Povse (KUL)		
Contributors:	Erik Kamenjasevic (KUL), Anton Vedder (KUL), Paolo Roccetti (ENG), Luigi Sgaglione (CINI), Filipe Apolinario (INOV), Nelson Escravana (INOV), Almerindo Graziano (SIL), Ion Larranga (S21SEC), Daniela Wurfoher (AIT), Cornelia Gerdenitsch (AIT), Nadezhda Ilina (KSP)		
Due date:	April 2018		
Version number:	1.0	**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	March 7 2018	Danaja Fabčič Povše (KUL)	Shared ToC with partners
0.2	April 6 2018	Danaja Fabčič Povše (KUL)	KUL input
0.3	May 2 2018	Danaja Fabčič Povše (KUL)	Input from other partners
0.4	May 14 2018	Danaja Fabčič Povše (KUL)	Consolidated version
0.5	May 23 2018	Danaja Fabčič Povše (KUL)	Amended according to ENG comments

Quality Control

Role	Date	Who	Approved/Comment
Internal reviewer	May 18 2018	Ioana Cotoi (ENG)	Approved with minor comments
Internal reviewer	June 2	Nelson Escravana (INOV)	Approved with minor comments

Disclaimer:

This document has been produced in the context of the COMPACT Project. The COMPACT project is part of the European Community's Horizon 2020 Program for research and development and is as such funded by the European Commission. All information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability with respect to this document, which is merely representing the authors' view.

Table of Contents

List of figures

List of Tables

Definitions and acronyms

COMPACT	COmpetitive Methods to protect local Public Administration from Cyber security Threats
DPIA	Data protection impact assessment
DPO	Data protection officer
GDPR	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)
LPA	Local public administration
S.E.L.P.	Security, ethics, legal, privacy
WP29	Article 29 Working Party, advisory body to the Commission on data protection

Executive Sumamry

COMPACT Deliverable 3.4 outlines the work done in Task 3.4 of the COMPACT project. Specifically, it contains an overview of the technical implementation of the privacy and data protection requirements in the COMPACT architecture. Its primary role is to provide an assessment from S.E.L.P. (security, ethics, legal and privacy) point of view and to recommend further course of action in the technical work. Further, the deliverable will contribute to suggesting possible solutions to other European project's legal and ethical challenges in the field of cyber-security research. Finally, it provides recommendations for future work in COMPACT.

The document is structured as follows. First, we focus on the evaluation of the COMPACT platform through the lens of privacy and data protection framework. The evaluation is twofold: technical requirements are assessed per specific COMPACT tool, and organisational requirements are assessed holistically. Further, policy guidelines are given for future work in COMPACT, and policies are suggested for specific project pilots. In Annex I and II, questionnaires to facilitate interaction between technical and legal partners are provided. In Annex III, a controller-processor agreement template is given, which can be used during the COMPACT research phase, and adapted for future adoption.

1. Introduction

Cyberattacks pose a serious threat to public authorities, whose agencies are regularly targeted. The authorities collect numerous data on citizens but often keep 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.[1]

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.

According to the DoW, this report has two purposes:

(1) Legal validation of D3.2 against legal requirements, identified in D2.5
(2) Policy recommendations for future work in COMPACT

S.E.L.P. stands for security, ethics, legal and privacy. This deliverable assesses the compliance of the COMPACT platform, defined in deliverables D3.1 Services and Contents Specifications and D3.2 Overall COMPACT architecture v1, against the requirements of the **EU legislation** defined in D2.5 S.E.L.P. Framework.

Specifically, it will focus on implementing GDPR requirements,[2] data protection and privacy procedures and create general purpose policies, adapted for each trial pilot. Employees' privacy and data protection rules are also contained in collective labour agreements on member state level. However, such agreements will not be checked in this deliverable, and their compliance with EU legal order will be assumed.

Neither will this deliverable assess COMPACT architecture against the requirements of the NIS Directive[3]. The NIS Directive as such applies to operators of essential services, which may include LPA's. However, the technical deliverables of the WP3 do not implement any of the measures, required in the NIS Directive, therefore this directive will not be considered in this report.

Regarding liability and intellectual property issues, it is too early in the development of the project to give a definitive answer on them. Therefore, they will not be addressed in this deliverable. Guidance of the whole consortium towards legal and ethical compliance will continue through S.E.L.P. management as an ongoing task, through checklists defined in D1.2 and D1.4.[4]

[1] As set out in the COMPACT Grant Agreement no. 740712, Part B, p. 3.

[2] 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).

[3] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[4] COMPACT D1.2 S.E.L.P. Management Plan (v1), D1.4 S.E.L.P. Management Plan (v2).

2. S.E.L.P. evaluation

2.1. Legally and ethically relevant issues in COMPACT architecture

The most likely S.E.L.P. challenges to arise in COMPACT were identified in D2.5 S.E.L.P. Framework.[5] It outlined the possible issues in both technology and user studies. In WP3, the architecture for the COMPACT platform was defined in D3.1[6] and D3.2.[7]

The COMPACT platform will include the processing of personal data, and represent an interference with the employees' right to privacy and protection of personal data. Therefore, it is important to assess how far the interference goes and whether it is proportionate and compliant with the legal framework.

Since employees are considered a vulnerable group in data protection law,[8] this has implications for their ability to give consent, but it also represents a 'high risk' in the sense of Art. 35,[9] which means that the data controller must take additional measures to protect them.

2.2. Evaluation methodology

Theoretical work in D3.4 is based on the legal state of the art. It takes into account the legal framework identified in D2.5, i.e. mostly the GDPR, but also the new opinions by the Article 29 Working Party (WP29), released since the submission of the previous deliverable (especially the Opinion 2/2017 on Data processing at work[10]).

The empirical work in this deliverable is based on filled-in checklists from the D1.2, D1.4, and updates on technical work progress from consortium meetings in the first year of the project.

In order to facilitate dialogue between the technical and the legal partners in COMPACT, two questionnaires were drawn up by KUL (see Annex I: Technical partners questionnaire; Annex II: Questionnaire on the exercise of data subject rights), which were then filled in by most of the partners. The questionnaires refer to the technical and organisational measures, adopted by the partners; whether the COMPACT tools, for which they are providing technology, process personal data, and if yes, which ones. Further, the questionnaires contain questions on the data quality principles, necessity of processing and data storage. They were very helpful in identifying personal data flows and the use of datasets in the future COMPACT platform.

[5] COMPACT D2.5 S.E.L.P. Framework.

[6] COMPACT D3.1 Services and Contents Specifications.

[7] COMPACT D3.2 Overall COMPACT architecture (v1).

[8] WP29, Opinion 2/2017 on data processing at work: WP 249, p. 6-7.

[9] WP29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679: WP 248, p. 7-9.

[10] WP29, Opinion 2/2017 on data processing at work: WP 249.

3. Evaluation of the COMPACT platform: privacy and data protection

The COMPACT platform consists of tools, most of which already exist and are marketed and function on their own as separate products. These tools are integrated into the COMPACT platform. This deliverable represents a legal evaluation report of the *integration and grouping* of already existing tools into the COMPACT platform, as suggested by the technical partners. *The way the already existing tools work on their own, outside the COMPACT platform, will not be assessed* as this is outside the scope of the project.

The partners' tools are grouped into four classes of COMPACT tools, which form the COMPACT platform. The classes of COMPACT tools are:

(1) Risk assessment

(2) Security awareness training

(3) Cyber security monitoring

(4) Knowledge sharing services

(1) Data protection in COMPACT

Data processing in COMPACT is subject to the General Data Protection Regulation (GDPR).[11]

Employees' personal data will be processed by the COMPACT platform. Employees are data subjects vis-à-vis the data controller or processor.

It defines **personal data** as:
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.
(Art. 4(1))

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))

[11] 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)

Two types of entities carry out the processing activity: they are either the data controller or the data processor, based on which one determines the means and purposes of processing, or how much control it has over the processing[12].

Data controller:
the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law
(Art. 4(7))

Data processor:
a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
(Art. 4(8))

Regarding personal data, it is important to keep in mind that GDPR only stops applying when personal data have become irreversibly anonymised. This is further explained in Section 4.1.1.

(2) Assessment of COMPACT tools

The next sub-section assesses the interaction and implementation of the four classes of COMPACT tools into a platform. The assessment takes into account two main points of view:

1. Personal data processed by the tool, including:
   - Data quality principles and legal grounds for processing and anonymisation techniques recommendations
   - Technical measures to implement data protection policies, according to the privacy by design approach
2. Who are the data controller and the data processor while using the specific tools

Personal data

The four classes of COMPACT tools may process personal data.

Elementary principles of personal data quality in processing are set out **in Art. 5(1) of the GDPR: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality**. According to the

[12] WP29, Opinion 1/2010 on the concepts of "controller" and "processor": WP 169, p. 12-15.

accountability principle, the controller is responsible for showing compliance with these principles[13].

(1) Lawfulness, fairness and transparency principle (Art. 5(1)(a))

Personal data must be processed **lawfully, fairly and in a transparent manner** in relation to the data subject.

(2) Purpose limitation principle (Art. 5(1)(b))

Personal data must be collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes. **Further processing** for statistical purposes, such as the aggregation process is not considered to be incompatible with the initial purposes.

(3) Data minimisation principle (Art. 5(1)(c))

Personal data must be processed in a way that is **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed according to the data minimisation principle.

(4) Accuracy principle (Art. 5(1)(c))

Personal data must be **accurate** and, where necessary, **kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are **erased or rectified** without delay.

(5) Storage limitation principle (Art. 5(1)(d))

Personal data must be kept in a form which permits **identification** of data subjects **for no longer than is necessary** for the purposes for which the personal data are processed. It may be stored for longer periods insofar as it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 89(1).

(6) Integrity and confidentiality principles (Art. 5(1)(f))

Personal data must be processed in a manner that ensures **appropriate security** of the personal data, including protection against **unauthorised or unlawful processing** and against **accidental loss, destruction or damage**, using appropriate technical or organisational measures.

[13] Article 5(2) of the GDPR.

Accountability principle (Art. 6(2)) requires the data controller to show compliance with the six principles. To this end, the partners will jointly carry out a **data protection impact assessment** (DPIA).

Legal grounds for processing were suggested in D2.5 (S.E.L.P. Framework). Here, we repeat in the interest of clarity:

- **Consent** (Art. 6(1)(a), Art. 7) is **not appropriate legal grounds**, since COMPACT includes processing of employees' personal data, who cannot give free consent;
- **Necessary** for **compliance with a legal obligation** (Art. 6(1)(c)) is potential legal grounds, if the LPA is subject to such an obligation, for example the NIS Directive;[14]
- **Necessary** for the purposes of the **legitimate interests** pursued by the LPA (Art. 6(1)(f)), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data – this is also potential legal grounds since ensuring network and information security is explicitly listed as an example of legitimate interests in Recital 47 of the GDPR.

The necessity criterion, common to both legal grounds, was assessed in the questionnaire (see Annex I: Technical partners questionnaire). The criterion can be further subdivided into three questions:

1. What is the purpose of the processing: the objective of the tool?
2. Which data does the tool need to achieve this goal?
3. Could the goal be achieved using fewer data?

According to the question (3), necessity *sensu stricto*, the tools would not work if fewer data were used. Therefore, the criterion is satisfied. Nevertheless, future adopters of COMPACT are **encouraged to continually assess the necessity of processing** in order to comply with legal requirements.

Technical measures to implement data protection policies

In order to follow the privacy by design approach, the architecture must include technical measures to implement data protection policies. The technique chosen is Data Management and Privacy Enforcement (DMPE).[15] It enforces the privacy requirements, resorting to measures such as anonymization and pseudo-anonymization.

[14] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[15] D3.2, p. 9.

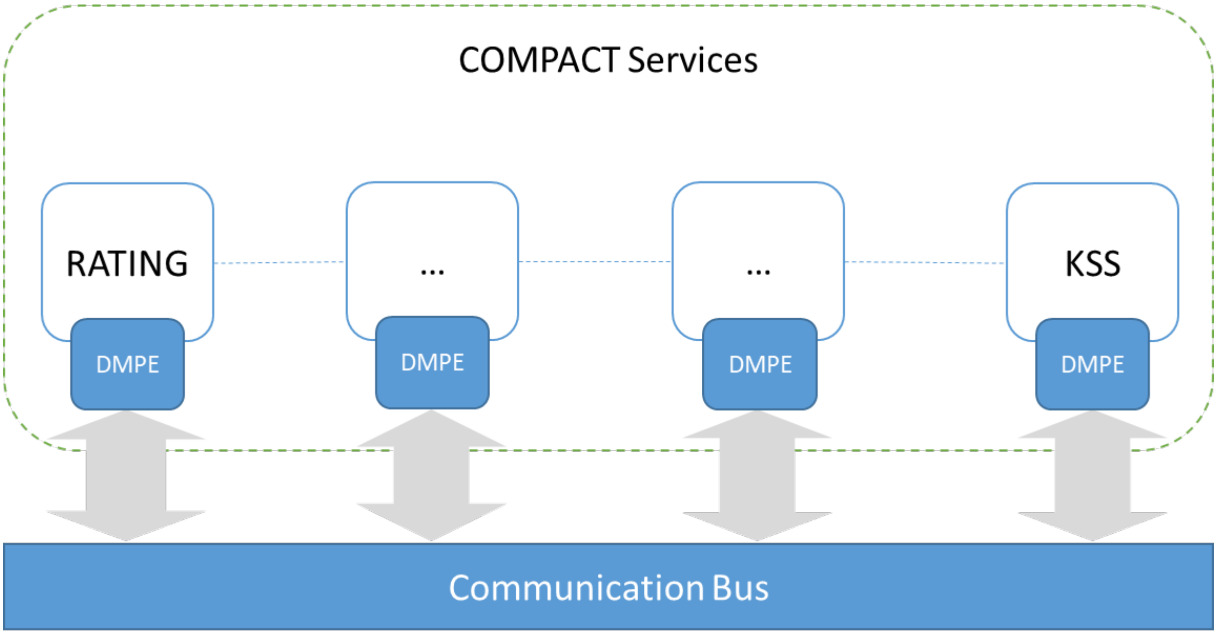


Figure 1: DPME for COMPACT[16]

Privacy enhancing features will be identified in D3.3. According to Art. 25 of the GDPR, such measures are designed to **implement data-protection principles**, such as data minimisation, in an effective manner and to integrate the **necessary safeguards** into the processing. They contribute to **GDPR compliance and protect the rights of employees** as data subjects.

Specific recommendations are laid out in Section 4.1.2 per specific tool.

Data controller and data processor roles

The GDPR sets out different obligations for controllers and processors, as identified in D2.5 (see especially pp. 22-29). Therefore, it is important to know whether COMPACT partners continue to have obligations towards COMPACT implementers and data subjects. Data flows per specific COMPACT tool will be assessed in the next sections in order to determine which entity holds a data controller and a data processor role.

The data controller is generally responsible and accountable for GDPR compliance (Art. 24), especially for complying with data quality principles (Art. 5(2)). It is also responsible for the exercise of data subjects' rights (see Chapter III: Data subject's rights).

The data processor carries out the processing operation on behalf of the controller. Only processors, who provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject, can be lawfully engaged by the controller.

[16] D3.2, p. 9.

The data controller determines the how and why of data processing; the processor will carry out the activity on the controller's behalf.

If both controller and processor are engaged, then they must conclude a binding agreement (called controller-processor agreement, or processor terms). This is an organisational requirement, which is further explained in Section 3.5.4.

3.1. Risk assessment (AIT, ENG, SIL)

3.1.1. Personal data (including data quality principles)

The risk assessment tool processes, inter alia, the following personal data: **name, role, email, answers, scores, security compliant behaviour**. The **purpose of their processing** is:

(1) User authentication and for gauging user risk assessment. All collected data are necessary to estimate LPA risk. If the user is no longer an employee of the LPA, his data are not necessary and will be anonymised. They can be used to see the trend of risk assessment. All data collected during the project will be deleted at the end of it. In an operational environment, the data previously collected are deleted at the end of each individual assessment.

(2) To get insights about which trainings will be necessary to increase cyber-secure behaviour.

This fits the 'purpose specification' principle, which states that data must be collected for a specified, explicit and legitimate purpose.

The 'data minimisation' principle requires that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

All data are potentially useful. The quality of the data is ensured due to the fact that they are inserted by the data subject. Each data subject can see their own data and the result of the assessment. When possible, validated scales are used. Reliability analyses show the quality of the data.

Nevertheless, future adopters of COMPACT should ensure that the processing of employees' personal data **actually contributes to risk assessment**, and (manually) filter and delete data that do not.

Once the data are no longer useful (at the end of the project, for the trial data generated during the project lifetime), they will be anonymized in order to calculate statistics for the LPA, a functionality that emerged during the interaction with the LPA representatives and is reported in section 5.2 of D2.4 and D2.11 – LPA Community Model.[17]

[17] See section 5.2 of the D2.4 and D2.11 – LPA Community Model.

<u>The 'storage limitation' principle states that data must be kept in a form which permits identification of data subjects for no longer than is necessary</u> for the calculation of risk assessment. Currently, the tools do not enable such an assessment and there is no deadline for deletion or anonymisation. A **specific time limit** must be defined, **in which data must be anonymised or deleted** (e.g., a month, six months etc.).

The 'accuracy' principle requires that the data must be <u>accurate</u>, and where possible,<u> kept up to date.</u> Concerning the overall LPA risk profile, as well as individual profiles, the risk assessment tool will show the most updated profile available, i.e. the one based on the latest input from the LPA users. This provides that data displayed are the most updated ones, providing the input data are correct. There is no easy way for the risk tool to detect mistakes in the personal data input to the tool. Partly, accuracy in calculating scores is dealt consistently across users since all questions are automatically marked against the sample solution.

The 'integrity & confidentiality' of data requires <u>an appropriate security of processing</u>, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. In the risk assessment tool, only authorised users can access, but there are no specifications regarding which actions they can take. Therefore, future adopters of COMPACT are encouraged to grant authorisations to a minimum number of people for specific actions only, in order to comply with this principle. Namely, if all the authorised personnel can perform any action with the data over which they are authorised, this is too broad for compliance.

3.1.2. Controller and processor roles

Data will be hosted by individual COMPACT partners. The provider of the original tool will remain the host after the COMPACT platform is deployed. It will not process data on its own and will not determine the means of purposes of its processing. Most likely, the partner will be considered a **data processor**.

Developers and future adopters are encouraged to conclude a **controller-processor agreement** with the host (see Organisational requirements).

3.2. Security awareness training (AIT, SIL, ENG, KSP)

3.2.1. Personal data (including data quality principles)

The security awareness tool processes, inter alia, the following personal data: **names, email addresses and other unique identifiers, roles/positions within the company**. Further, the security awareness tool will process information about attended training and the individual results (**answers and individual scores)** that employees will achieve, as well as the development of an individual's competences over a period of times by further interacting with the platform. The **<u>purpose of their processing</u>** is first to enable **logging into** the game, and secondly to create a **personalised learning environment**. Either emails or instant tokens can be used for identification of users. The scores can be either individual or group. The individual training results are needed to measure the employees' preparation against cyber threats. The purpose is following the progress and optimisation of a training program. This fits the 'purpose specification' principle, which states that data must be collected for a specified, explicit and legitimate purpose.

The 'data minimisation' principle requires that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The purpose is to assess the risk exposure of the LPA.

All data are **potentially** useful. Whether they are relevant and adequate, is evaluated by **comparing user's answers and correct ones**. Each user has access to their own data. The tool could not work as well with fewer personal data.

Nevertheless, future adopters of COMPACT should ensure that the processing of employees' personal data **actually contributes to security awareness training**, and (manually) filter and delete data that do not.

Further, there is a mechanism, which enables the employee, who leaves his or her job, to ask for their data to be deleted. Since it is irrelevant to process the information of ex-employees in order to assess risk exposure, this also contributes to the 'data minimisation' principle.

Once the data are no longer useful, they will be anonymised in order to calculate statistics for the LPA, similarly to the approach taken for the Risk Assessment results.[18]

The 'storage limitation' principle states that data must be kept in a form which permits identification of data subjects for no longer than is necessary security training. Future adopters are encouraged to determine a specific time limit, in which data must be anonymised or deleted.

The 'accuracy' principle requires that the data must be accurate, and where possible, kept up to date. In part, this cannot be checked by the system. Partly, the accuracy is ensured by the data subjects themselves, who can check and report about changes and inaccuracies in their personal data, such as email address, online ID etc. The employees can notify inaccuracies to training managers, who input such data.

The 'integrity & confidentiality' of data requires an appropriate security of processing, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. In the security awareness tool, only authorised users can access data due to access controls. However, future adopters of COMPACT are encouraged to **grant authorisations to a minimum number of people for specific actions only**, in order to comply with this principle. Namely, if all the authorised personnel can perform any action with the data over which they are authorised, this is too broad for compliance.

[18] See section 5.2 of the D2.4 and D2.11 – LPA Community Model.

3.2.2. Controller and processor roles

For certain partners, it is not yet determined, whether the partner remains the data host, or whether the game data will be stored on LPA premises. In cases where the COMPACT partner remains the host, they **will most likely be considered a data processor**. This is especially the case if the host cannot do anything further with the data apart from hosting. However, it is **too early to determine** whether all partners involved in the security awareness training tool will be considered controllers or processors.

Developers and future adopters are encouraged to conclude a **controller-processor agreement** with the host (see section on Organisational requirements).

3.3. Cyber security monitoring (SIL, CINI, S21SEC, INOV)

3.3.1. Personal data (including data quality principles)

It is not possible to tell in advance which personal data cyber security monitoring tools will process, due to the way the tool is configured. **Potentially any or no personal data can be processed**.

What makes it impossible to predict in the current stage of the COMPACT project is its configuration, that dictates which data is captured by the tool, and highly varies depending on the installation scenario chosen in for demonstration trials.

The configuration of the tool dictates which data will be collected by the tool. Since this configuration is dependent on the characteristics of the environment where the tool deployed, the personal data captured by the tool can only be predicted by understanding its environment. E.g., Do the computers monitored by the tool have personal data? Is the tool configured to inspect storage (for instance sensitive files or folders) or communications that contain personal data?

During the trials setup task, data and environment scenarios will be defined and it will be clearer, whether or not personal data will be processed, and if so, which types of personal data.

There are different **purposes of their processing**:

- Demonstrate compliance with GDPR: i.e., gathering evidence that GDPR procedures (such as, the right to be forgotten) are being carried out in the LPA, by monitoring its IT systems.
- Identify non-compliance with the LPA's procedures caused by unexpected activities that compromise the ongoing business processes (GDPR procedures or other processes carried out in the LPA). The unexpected activities are not directly caused by malware, since they can be originated by wide range of causes such as: human errors; natural disasters; or intruders that all sort of malicious tools to disrupt the IT systems.
- Analysing the website in search of malware.

This fits the 'purpose specification' principle, which states that data must be collected for a specified, explicit and legitimate purpose.

The 'data minimisation' principle requires that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

This principle means that data controllers should collect and use only the personal data that they really need for a specific goal, and they should only keep it for as long as they need it.[19] The fact that any data may be processed by the tool is not necessarily in conflict with the principle. It is important that they must contribute to the goal: in this case, it is data security and malware detection. Data that do not contribute to security interests, must be deleted.

Specifically, only the structure of the web pages that belong to the LPA is analysed. All these pages have to be analysed, as any of them may contain malware, but no external pages will be analysed, apart from those directly linked from the LPA's web site (these have to be analysed because as they can affect the way the LPA's pages are shown, they can end up infecting visitors to the LPA's website, but only those directly linked are analysed). Only URLs containing malware will be reported, and this information is sent to the SOC, who stores it for as long as necessary.

It is not clear whether there is a mechanism that deletes data that are processed but are not relevant to the goals. Nor is it clear for how long the data will be stored, since 'necessity' must be clearly defined. It is important that once the goal is reached, for example the tool has found out an individual's browsing habits and does not need any additional data, it stops collecting data. If a dataset does not bring any additional useful information, it should be deleted.

The 'storage limitation' principle states that data must be kept in a form which permits identification of data subjects for no longer than is necessary for monitoring. The only exception is if an LPA employee leaves their job, in which case the account will be disabled, while the data will be frozen, but still available for a period of time, then anonymised. Future adopters are encouraged to determine a specific time limit for other instances, in which data must be anonymised or deleted.

The 'accuracy' principle requires that the data must be accurate, and where possible, kept up to date. For example, if due to a calculation error in a user's browsing habits, a false positive is found, there must be a mechanism to correct the mistake. **It has been not fully implemented due to technical constraints**.

This is due to the fact that from the SOC perspective, there is not a threshold approach, but at each "detection" is associated an attack likelihood that can be used to have an indication of the detection relevance.

[19] See European Data Protection Supervisor, https://edps.europa.eu/node/3099#data_minimization and the Information Commissioner https://ico.org.uk/for-organisations/guide-to-data-protection/principle-3-adequacy/

Even if the personal data is incorrect, the detected URL containing malware may be correct. For instance, imagine that there is a web page containing a list of people who have defaulted on payments to the LPA, and some John Doe is incorrectly included in this list. If the COMPACT tool finds malware in the web page regarding the status of John Doe, the malware-containing URL reported to the SOC may be something like:

https://www.lpa.com/defaulters/John_Doe

If John realizes that he has been incorrectly included in the defaulters list, he can request the LPA to modify this information and remove him from the list, but he can't request the SOC to remove or correct the incorrect URL, because it is related to a page that really exists at the moment of malware detection, and that hosts malware. So, even though John Doe is incorrectly listed as a defaulter (he is entitled to ask for a change of this data), the URL really exists and hosts malware. It probably cannot be altered because doing so could prevent SOC operators from removing the malware. Once the issue is correctly closed, this URL is no longer necessary for SOC operators and can be anonymized or deleted but during issue management it's not possible to update this information.

The 'integrity & confidentiality' of data requires an appropriate security of processing, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Since the tools will enable local storage, it is important for the LPA's using the COMPACT platform to define their own access controls. Rules must be put in place, which determine **who** can have **what kind** of access controls – what can security operations centre (SOC) employees do with the data they access. More specifically, locally stored information (reported URLs) can be adapted to the LPA's needs, are only accessible by authorized persons and can be deleted as needed.

3.3.2. Controller and processor roles

LPA will be the data controller. It determines the means and purposes of processing, i.e. it decides to use the cyber security monitoring tool in order to detect intrusions and malware, and the data will be stored on its servers (local storage). The COMPACT partners will not be hosting any data and will not be involved as a data processor.

3.4. Knowledge sharing services (SIL, ENG)

3.4.1. Personal data (including data quality principles)

The knowledge sharing services tool processes personal data.

In the category of personal data, which must be provided, there are the following datasets: name, surname, email address (or another unique identifier), work organisation, role in organisation. Optionally, the users can provide other information, e.g. gender, age etc. The

purpose of data processing is to (a) enable user authentication and identification within the community and (b) share technical information with the rest of the LPA community.

This fits the 'purpose specification' principle, which states that data must be collected for a specified, explicit and legitimate purpose.

The 'data minimisation' principle requires that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

As noted above, this tool allows for two types of personal data, mandatory and optional. The data subject has a choice of revealing the latter or not. It is not clear whether the second category of **optional data** is relevant for user authentication. **Its relevance should be assessed**, and the data deleted if they do not contribute to authentication.

The 'storage limitation' principle states that data must be kept in a form which permits identification of data subjects for no longer than is necessary for the sharing of knowledge.

In practice, when an employee signs up to the platform, he or she becomes its user. As long as the user exists and the platform is operational, this user's personal data will be stored. Deletion of some personal is possible when the user cancels his or her account, due to leaving their job. However, there is no general time limit to delete the data if they become unnecessary. It is recommended to determine the time limit, after which data must be anonymised or deleted.

The 'accuracy' principle requires that the data must be accurate, and where possible, kept up to date. There is a mechanism that allows any registered user to delete or edit content. However, **crowd-sourced** types might still be inaccurate despite (or due to) the large number of users who can edit content.[20] We recommend to monitor and filter for inaccuracies and misleading information in the knowledge sharing tool.

The 'integrity & confidentiality' of data requires an appropriate security of processing, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Only **registered users** can use the knowledge sharing tool. However, as any user can delete or edit content, this may lead to accidental deletion of important data. Therefore, we recommend assessing and potentially limiting how much control a user should have over other user-generated content.

3.4.2. Controller and processor roles

The knowledge sharing tool will allow the disclosing entity to define "what" is being disclosed and to "whom". In this tool, the partner providing the tools will **remain the data controller**, **provided it will host the data and determine its use, the means and purposes of its processing**, i.e. to enable the functioning of the information hub. Should the partner

[20] The most known crowd-sourced encyclopedia, Wikipedia, is often a target of this criticism, see for example: https://www.livescience.com/7946-wikipedia-accurate.html

engage an external data processor, such a processor must provide sufficient guarantees in order to comply with Art. 28(1) of the GDPR, including but not limited to those set down in a processor-controller agreement.

3.5. Organisational requirements

Organisational requirements of the GDPR are legal obligations for the controller, which cannot be implemented in the system due to their nature. Organisational measures are mentioned several times throughout the GDPR, most importantly with regards to the controller's **general responsibility for compliance (Art. 24) and data protection by design and by default (Art. 25).** This section will cover their assessment by the COMPACT partners in the COMPACT architecture.

3.5.1. Ensuring the exercise of data subjects rights

GDPR grants the following rights to the data subject:

- right to information,[21]
- right of access,[22]
- right to rectification,[23]
- right to erasure,[24]
- right to restriction of processing,[25]
- right to data portability,[26]
- right to object,[27]
- right not to be subject to automated decision-making, including profiling.[28]

The most crucial rights regarding the COMPACT platform are the right to information/the data controller’s notification duties, the right of access, rectification and erasure.

<u>Notification duties, right of access</u>

The data controller must provide the employee with the following information (Art. 13, 14 and 15 of the GDPR):

a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

[21] Articles 13 and 14 of the GDPR.
[22] Article 15 of the GDPR.
[23] Article 16 of the GDPR.
[24] Article 17 of the GDPR.
[25] Article 18 of the GDPR.
[26] Article 20 of the GDPR.
[27] Article 21 of the GDPR.
[28] Article 22 of the GDPR.

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with a supervisory authority;

GDPR gives three possible moments, when the information have to be given:

- when the personal data are **obtained** from the employee (Art. 13(1))
- when the employee exercises his or her **right of access** (Art. 15(1))
- if the personal data have **not been obtained from the employee**, then within a reasonable period after obtaining the personal data, but **at the latest within one month**; if the personal data are disclosed to another entity, then at the latest at the **time of this disclosure** (Article 14(3))

The data controllers will most likely obtain personal data directly from the employee, but the other two situations are nonetheless possible. Therefore, controllers must **keep track of when and from who personal data are obtained** in order to provide employees with the proper information.

If the employee exercises his or her right of access, it means the controller has to provide that employee with the confirmation as to whether or not personal data concerning him or her are being processed, along with the above information (Art. 15(1)). This information must be provided **free of charge**. Only for any further copies can the controller charge a reasonable fee based on administrative costs (Art. 15(3)).

In other words, if an employee asks the LPA, what personal data it collects on him or her, and why, and how they are being used, the LPA must be able to provide that information within 30 days of the filing of the request.[29]

Rectification

According to Article 16, the data subject has the right to obtain from the controller the **rectification of inaccurate personal data concerning him or her *without undue delay***. The data subject also has the right to have incomplete personal data completed, including by providing a supplementary statement. When completing personal data, the purpose(s) of processing have to be taken into account.[30]

Some of the COMPACT tools provide for rectification of innacurate data (security awareness training), but the others do not have such a mechanism. If the employee asks to have his or

[29] Including, for example: 'any email that refers to the worker, as well as performance reviews, job interviews, payroll records, absence records, disciplinary records, computer access logs, CCTV footage, and recordings of phone calls to, from or about the person'. See: https://www.theguardian.com/technology/2018/apr/23/europe-gdpr-data-law-employer-employee

[30] Article 16 of the GDPR.

her data corrected, updated or completed, then the controller is bound to do so without undue delay. The controllers (LPA's or technology providing parterns, who remain controllers) are obliged to put this into practice.

Erasure

The data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay. The controller must accordingly erase personal data without undue delay, if:

- the personal data are **no longer necessary** in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based, and there is no other legal ground for the processing;
- the data subject objects to the automated processing according to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in EU or national law to which the controller is subject;
- the personal data have been collected from children according to Article 8(1) of the GDPR.[31]

Since processing of personal data in COMPACT will be based on **necessity for the exercise of legitimate interests**, or **necessity to comply with a legal obligation**, the necessity factor is important. 'Necessity' is part of the broader principle of **proportionality**, which consists of two building blocks: appropriateness and necessity. Necessity must be assessed first.[32] In COMPACT, we decided to assess necessity based on three questions:

1. legitimate objective of the measure (what is the goal of processing?)
2. its scope (which personal data does it process?)
3. its strict proportionality – is it the least restrictive measure available (could it work with fewer data?)

According to the answers given, the four tools seem to comply with the principle, mainly due to the fact the tools could not work with a smaller amount of data. However, as the standard is assessed on a case by case basis, we recommend the COMPACT adopters to set up their own **internal controls** in order to **continually assess the necessity criterion**.

Conclusion: data subject rights

[31] Article 17(1) of the GDPR.

[32] See EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, pp.7-9. https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf

According to the answers given by the partners, not all LPA employees can already exercise their rights. We recommend that the controllers put in place (organisational) measures that enable them. Once they have appointed a DPO (data protection officer), he or she will be the reference point whom the employees can contact, which facilitates the exercise of their rights.[33]

3.5.2. Data protection impact assessment

A data protection impact assessment (DPIA) is a self-assessment exercise, which the data controller must carry 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. Therefore, the criterion of 'high risk' is used when determining whether or not the controller has to carry out a DPIA. A non-exhaustive list of when this criterion is met has been published by the Article 29 Working Party, the general rule being that if more than two criteria are met, the DPIA is obligatory.[34] The envisaged COMPACT platform fits two of the listed criteria: systematic monitoring of a vulnerable group of data subjects (employees are considered vulnerable due to power imbalances between them and the employer).[35] Therefore, **COMPACT data controllers must perform it, and duly follow its procedures and recommendations throughout the processing.**

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

- A systematic description of data processing,
- Assessment of proportionality and necessity of data processing,
- Risk management,
- Involvement of all interested parties.[36]

A DPIA template for WP3 has been provided in D1.4 and is currently being filled out by the partners, following the advice of the COMPACT Ethics Committee (one KUL and one ENG representative).

Since the final COMPACT platform will also involve systematic monitoring of employees, **future COMPACT users should equally carry out a DPIA**. The template from D1.4 can be adapted and used to that end.

If a DPO is appointed, he or she should be consulted in the process of carrying out a DPIA.

[33] According to Art. 38/4 GDPR, a DPO can be contacted by data subjects regarding the exercise of their rights. See Section 3.5.3, Involvement of the data protection officer.

[34] WP29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679: WP 248, p.9.

[35] WP29, Opinion 2/2017 on data processing at work: wp249, p. 7.

[36] WP29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679: WP 248, p. 21.

3.5.3. Involvement of the data protection officer

Certain controllers as well as processors need to appoint a data protection officer (DPO). According to Art. 37 of the GDPR, this is necessary when:

a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

LPA's need to appoint a DPO based on alinea a), since they are public authorities. Other users of COMPACT potentially outside the LPA sector, including COMPACT partners who remain controllers, should self-assess whether they fit either of the two other criteria. For example, CCTV operators and private security firms most likely do fit, and so do hospitals, who deal with sensitive personal data (Article 9 data) on a large scale.

Two or more LPA's can also appoint a common DPO (Art. 37(3)).

A DPO's tasks were already described in D2.5, section 4.4 (Data protection officer). Here we repeat his or her minimum tasks, according to 39(1) GDPR:

a) to inform and advise the controller or the processor and the employees regarding their GDPR obligations
b) to monitor GDPR compliance
c) to provide advice regarding the DPIA and monitor its performance
d) to cooperate with the supervisory authority
e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

A DPO can also be contacted by employees regarding the exercise of their GDPR rights (Art. 38(4)).

According to the answers given by the partners, **not all of them have yet appointed a DPO**. Especially the LPA's are encouraged to do so by May 25 2018 in order to avoid a breach of the GDPR.

3.5.4. Data processing agreements

Certain COMPACT tools will involve processing by a data controller and a data processor. Art. 28(3) imposes a new obligation on them: they must conclude a binding agreement, which governs the processing by a processor. This is sometime referred to as 'processor terms' or a 'controller-processor agreement'. Its minimum content is described as follows:

According to the agreement between them, the processor must:

a) process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
b) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
c) take all measures required pursuant to Article 32;
d) respect the conditions referred to in paragraphs 2 and 4 for engaging another processor;
e) taking into account the nature of the processing, assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
f) assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
g) at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the personal data;[37]
h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

Additionally, the processor must immediately inform the controller of the latter's possible breach of the GDPR. Therefore, also the processor must monitor compliance to a certain extent.

A template has been provided to the partners for research activities, which can be adapted by COMPACT users after the platform is deployed (see Annex III: Controller-processor agreement template). This template is based on a previous project, called EPISECC.[38]

[37] Art. 28(3) of the GDPR.

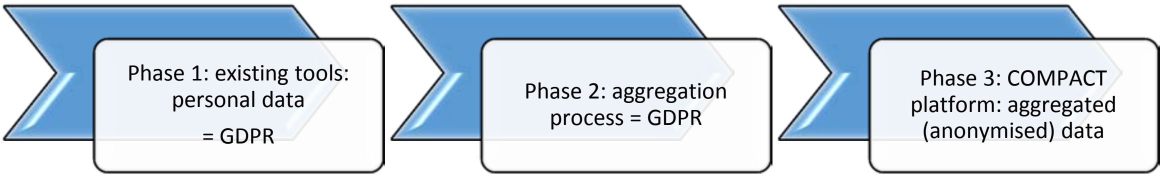
[38] EPISECC project https://www.episecc.eu/ 'EPISECC is a Collaborative Project which will Establish a Pan-European Information Space to Enhance seCurity of Citizens.'

4. Policy guidelines

4.1. Guidelines for further work in COMPACT

4.1.1. Anonymisation of personal data

According to D3.2 and D3.1, the platform represents the only point at which the partners' tools interact.[39] [40] In order to ensure that employees do not suffer adverse consequences, only the host should see individual data, and the LPA only aggregated data. The data flows in COMPACT can be summarised into the following figure:


Phase 1: existing tools: personal data
= GDPR
Phase 2: aggregation process = GDPR
Phase 3: COMPACT platform: aggregated (anonymised) data

As described in D3.2, the following measures may be applied in COMPACT:

- **"Homomorphic encryption**. This encryption allows mathematical operations to be performed on encrypted data without compromising the encryption. In this way sensitive data can be encrypted homomorphically and hence processed in this form
- **Pseudo-anonymization**. It changes sensitive data in such a way that additional information is required to achieve the original data
- **Anonymization**. The sensitive information are completely removed."[41]

Deliverables D3.3/D3.5 will set out aggregation processes and measures, which aim to **anonymise data** in order to prevent singling out individual data subjects. If the processes

[39] D3.2 p. 49.

[40] The sole exception to this being that the LPA Human Resources departments will still be able to see training status of employees and related results (e.g. in Italy this is imposed by law).

[41] D3.2, p. 32.

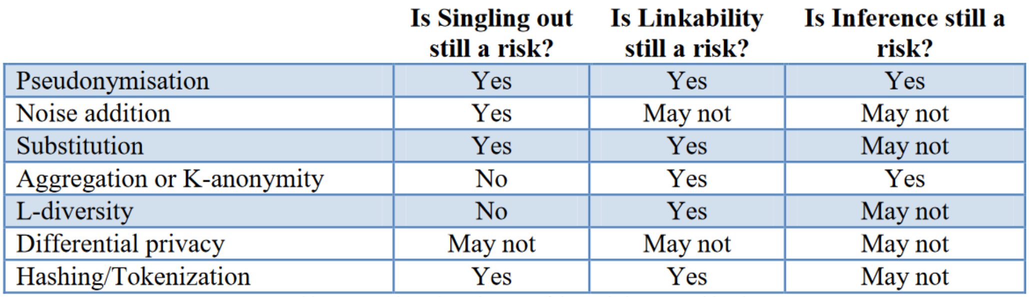
defined in D3.3 and D3.5 **irreversibly anonymise data** at a high enough level of aggregation, then the data will not be considered personal and the GDPR will not apply any more. The standard of 'irreversible anonymisation' of personal data is high, according to the Opinion 05/2014 on Anonymisation Techniques of the Article 29 Working Party.[42] There is no prescriptive technique and different anonymisation techniques may be used.

However, seemingly anonymised data remain personal data if the data subject can be potentially re-identified from them. It must be reasonably unlikely to acquire means by which the individual can be re-identified.[43] Simply removing an identifying element from the dataset is not enough. Data remain personal data if they fit the following criteria:

(i) is it still possible to single out an individual,
(ii) is it still possible to link records relating to an individual, and
(iii) can information be inferred concerning an individual?

In other words, the anonymisation process needs to respond to three risks: singling out, linkability and inference.[44] An overview of how different anonymisation techniques respond to the three risks was provided by the WP29:

Table 1: Residual risks corresponding to different anonymisation techniques



	Is Singling out still a risk?	Is Linkability still a risk?	Is Inference still a risk?
Pseudonymisation	Yes	Yes	Yes
Noise addition	Yes	May not	May not
Substitution	Yes	Yes	May not
Aggregation or K-anonymity	No	Yes	Yes
L-diversity	No	Yes	May not
Differential privacy	May not	May not	May not
Hashing/Tokenization	Yes	Yes	May not

Table 6. Strengths and Weaknesses of the Techniques Considered

(source: WP216, p. 24)

The risks should be continually re-assessed and addressed in order to keep up with the changes of the technical state of the art and increased computing power, which would make re-identification easier.[45]

The risks in COMPACT refer to the LPA ability to have access to their employees' personal data. Therefore, the processes defined in further technical deliverables should aggregate data at as high level as possible in order to prevent the LPA from seeing personal data through singling out, linkability and inference.

[42] See WP29, Opinion 05/2014 on Anonymisation Techniques: WP 216: not every technique is thorough enough to effect irreversible anonymisation, and several might need to be combined and their effectiveness continually assessed.
[43] See Recital 26 of the GDPR, and case C‑ 582/14 Breyer, para. 45 and 48.
[44] WP29, Opinion 05/2014 on Anonymisation Techniques: WP 216, pp. 11-12.
[45] WP29, Opinion 05/2014 on Anonymisation Techniques: WP 216, p. 24.

4.1.2. Technical requirements

This section summarises the technical requirements that need to be implemented into the COMPACT platform with the aim of GDPR compliance.

Table 2: Technical requirements

COMPACT TOOL	RECOMMENDATIONS
Risk assessment	R1: Delete data that are not useful for the risk assessment: can be an additional feature in the platform, or done manually (filtering mechanism) R2: Ensure a mechanism for rectifying incorrect personal data R3: Assess access controls: ensure that a minimal number of people can access personal data on the server ensure that they can take a limited scope of actions the amount of persons and actions must be limited to what is necessary: only if the tool would otherwise not work as well R4: In the research phase: delete data from employees, who decide to opt-out of the research
Security awareness training	R5: Delete data that are not useful for the security awareness training: can be an additional feature in the platform, or done manually R6: Ensure a mechanism for deletion/anonymisation and set a specific deadline, by which data must be anonymised or deleted R7: Assess access controls: ensure that a minimal number of people can access personal data on the server ensure that they can take a limited scope of actions the amount of persons and actions must be limited to what is necessary: only if the tool would

	otherwise not work as well R8: In the research phase: delete data from employees, who decide to opt-out of the research
Cyber security monitoring	R9: Implement a mechanism for data deletion in order to comply with data minimisation principle: if the data are not useful for the objective, they should be deleted (manually or automatically) R10: For stored data, define a date, after which they must be deleted or anonymised If possible, implement a mechanism for correction of inaccurate data R11: Assess and put in place appropriate access controls R12: In the research phase: delete data from employees, who decide to opt-out of the research
Knowledge sharing services	R13: Implement a mechanism to delete data, which are irrelevant and not useful for knowledge sharing R14: Define a specific deadline for anonymisation or deletion of stored data, once they are not useful anymore (apart from the case of former employees) R15: Regarding user-generated content: Implement filtering/monitoring mechanism to ensure quality Re-assess/implement access controls: how much control should a user have over content generated by other users R16: In the research phase: delete data from employees, who decide to opt-out of the research

4.1.3. Organisational requirements

R17: Ensure the data subjects can exercise their rights under the GDPR:

- right to information,
- right of access,
- right to rectification,
- right to erasure,
- right to restriction of processing,
- right to data portability,

- right to object, - right not to be subject to automated decision-making, including profiling.
R18: Carry out a data protection impact assessment according to exiting methodologies and guidelines.
R19: If required to do so, appoint a data protection officer.
R20: Conclude data processing agreements - if processor/controller situation: processor agreement - if joint controllers: joint controllership agreement

4.2. Policies for specific project pilots

The trials in individual LPAs will begin in M13. According to the LPA partners, it is too early and unnecessary to address specific policies in this deliverable. Furthermore, data processing in employment context is very shortly regulated by the GDPR. It gives the member states the competence to regulate it in Art. 88:

> Member States may, **by law or by collective agreements**, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the **performance of the contract of employment**, including discharge of obligations laid down by law or by collective agreements, management, **planning and organisation of work**, equality and diversity in the workplace, health and safety at work, **protection of employer's or customer's property** and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

Such legislation must take into account 'suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights', with a particular focus on transparency (Art. 88(2)). According to the Commission website, most of the member states have not yet adopted such acts.[46]

Nevertheless, the next subsections will provide a short overview of existing legal framework on data protection in an employment context, based on the previous Directive 95/46/EC. The German law, adopted on the basis of 88(2) of the GDPR, is also described in this section in more detail.

4.2.1. Afragola and Bologna

In Italy, the Personal Data Protection Code[47] contains a few rules on data processing at work in its Chapter VIII, Title III. Distance monitoring of employees is prohibited. The personality and moral freedom of workers who are home-based, must be ensured by the employer.

[46] In fact, the website is outdated and does not mention the GDPR at all: http://ec.europa.eu/social/main.jsp?catId=708&langId=en

[47] Personal data protection code (Legislative Decree no. 196 of 30 June 2003)

Further, home-based workers are required to ensure confidentiality as necessary with regard to all family-related matters.

4.2.2. Amadora

The Portuguese Data Protection Act waives the prior consent requirement, when the processing is required for pursuing the legitimate interests of the data controller (such as the employer) (or third parties to whom the data is disclosed), unless overridden by the individual's (such as an employee's) fundamental rights, freedoms or guarantees.[48]

Since the future deployment of COMPACT is based on legitimate interests or necessity for fulfilling a legal obligation, the consent of employees is not required.

However, during the research and trials phase, employees must still consent to the participation in a research activity and to the processing of their personal data due to the requirements of EC's Research Ethics.[49]

4.2.3. Bremerhaven

In Germany, the data protection framework has already been updated according to the GDPR rules. Section 26 of the Federal Data Protection Act[50] lays down rules for data processing in an employment context. The definition of an employee is wide and includes the following categories (Section 26(8)):

1. dependently employed workers, including temporary workers contracted to the borrowing employer
2. persons employed for occupational training purposes
3. participants in benefits to take part in working life, in assessments of occupational
4. aptitude or work trials (persons undergoing rehabilitation)
5. persons employed in accredited workshops for persons with disabilities;
6. volunteers working pursuant to the Youth Volunteer Service Act or the Federal Volunteer Service Act
7. persons who should be regarded as equivalent to dependently employed workers
8. because of their economic dependence; these include persons working at home and
9. their equivalents
10. federal civil servants, federal judges, military personnel and persons in the alternative
11. civilian service

Further, applicants for employment and persons whose employment has been terminated are also regarded as employees.

[48] Act on the Protection of Personal Data (transposing into the Portuguese legal system 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).

[49] Horizon 2020: Guidance: How to complete your ethics self-assessment, sections 2 and 4.

[50] Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (DSAnpUG-EU) of 30 June 2017.

Their personal data may be processed for employment-related purposes where necessary for hiring decisions or, after hiring, **for carrying out** or terminating **the employment contract** or to exercise or satisfy rights and obligations of employees' representation laid down by law or by collective agreements or other agreements between the employer and staff council (Section 26(1)).

More detailed rules must be negotiated and agreed by social partners, that is employers and employee unions, in a collective labour agreement (Section 26(4)).

4.2.4. Donostia-San Sebastian

The Spanish Data Protection Act and the implementing Regulation[51] contain only a few rules, relevant for data processing in a work context.

First, an employee's consent is not required if the processing of personal data refers to the parties to an administrative, employment or business contract or pre-contract, provided the data is necessary for its performance.

Further, whenever security measures to protect the processing of personal data are put in place, such measures must be described in a security document that also specifies the **obligations of any employees, agents and contractors accessing the data files**, and the structure of the files, including a description of the systems processing them. **In other words, access controls must be defined and described.**

[51] The Data Protection Act (Law 15/1999 on the protection of personal data), and the implementing Regulation (The Regulation developing the Data Protection Act, Royal Decree 1720/2007 of 21 December (Data Protection Regulation)).

5. References

Bibliography

Opinions of the Article 29 Working Party:

- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679: WP 248
- Opinion 1/2010 on the concepts of "controller" and "processor": WP 169
- Opinion 2/2017 on data processing at work: WP 249
- Opinion 05/2014 on Anonymisation Techniques: WP 216

European Commission: Horizon 2020: Guidance: How to complete your ethics self-assessment.

https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

European Data Protection Supervisor: ‘data minimisation’.

https://edps.europa.eu/node/3099#data_minimization

European Data Protection Supervisor: Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit.

https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf

The Information Commissioner: ‘the adequacy principle’.

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-3-adequacy/

Legislation

European Union

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)

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Italy

Personal data protection code (Legislative Decree no. 196 of 30 June 2003)

Germany

Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (DSAnpUG-EU) of 30 June 2017.

Spain

The Data Protection Act (Law 15/1999 on the protection of personal data), and the implementing Regulation (The Regulation developing the Data Protection Act, Royal Decree 1720/2007 of 21 December (Data Protection Regulation))

Portugal

Act on the Protection of Personal Data (transposing into the Portuguese legal system 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)

Case-law

Court of Justice of the European Union, Patrick Breyer v Bundesrepublik Deutschland (Case C-582/14)

Reports (deliverables)

COMPACT D1.2: Yung Shin VAN DER SYPE, Danaja FABCIC POVSE, *S.E.L.P. Management Plan (v1)*, 2017

COMPACT D1.4: Danaja Fabčič Povše, Erik Kamenjašević, Anton Vedder, *S.E.L.P. Management Plan (v2)*, 2018

COMPACT D2.5: Danaja FABCIC POVSE, *S.E.L.P. Framework*, 2017

COMPACT D3.1: Almerindo Graziano, Christos Paraskeva, Georgios Nicolaou, Jessica Testa, Lorenzo Eccher, Barbara Pirillo, Paolo Roccetti, *Services and Contents Specifications*, 2018

COMPACT D3.2: Lorenzo Eccher, Paolo Roccetti, Barbara Pirillo, Jessica Testa, Luigi Coppolino, Salvatore D’Antonio, Luigi Sgaglione, Filipe Apolinário, Almerindo Graziano, Ion Larranaga, Nadezhda Ilina, *Overall COMPACT architecture (v1)*, 2018

6. Annex I: Technical partners questionnaire

Data protection in COMPACT

Author: KU Leuven
Madrid, April 11 2018
Partner name: _________

This questionnaire will help contribute to the legal assessment of COMPACT architecture as part of T3.4. It has three questions. Thanks for filling it in!

QUESTION 1: PERSONAL DATA IN COMPACT
Personal data = (1) any information (2) relating (3) to an identified or identifiable (4) natural person
Example: email address, IP address, name, position, level of education …
Which personal data does each tool use?

TOOL	PERSONAL DATA USED	What is the reason for their use and where is this defined? Deletion/anonymisation system for data that will not be used?	How is the quality and usefulness of data assessed?	Access controls to the data used (authorisation, authentication)?[52]
Risk assessment				
Security awareness training				
Cyber security monitoring				
Knowledge sharing services				

Please answer the following questions only insofar as they use PERSONAL DATA. If the tool does not involve personal data as defined in question 1, please skip.

QUESTION 2: Legal standard of 'necessity': three components

1. Goal – objective of the tool
2. Which data does the tool need to achieve this goal?

[52] Ensured by specific component, not the global platform.

3. Could the goal be achieved using less data?

TOOL	Objective	Which data	Less data?
Risk assessment			
Security awareness training			
Cyber security monitoring			
Knowledge sharing services			

<u>QUESTION 3: PERSONAL DATA FLOWS</u>: data controllers and data processors
When the COMPACT platform is implemented, does any data flow through your organisation? Or does the data processed by the COMPACT platform stay there, and does not pass through the systems, or servers etc., of your organisation?

This will affect the legal obligations your organisation will have regarding users of the COMPACT platform: depending on whether it is involved in the processing and how much control it will have over the personal data, it may be a DATA CONTROLLER or a DATA PROCESSOR.

TOOL	WHERE WILL THE DATA BE STORED? WILL THE DATA AT ANY MOMENT BE STORED ON YOUR SERVERS?	HOW MUCH CONTROL DO YOU HAVE OVER THE DATA FLOW? WHAT CAN YOU DO WITH THESE DATA DURING TRANSIT? CAN YOU ACCESS IT?
Risk assessment		
Security awareness training		

Cyber security monitoring		
Knowledge sharing services		

7. Annex II: Questionnaire on the exercise of data subject rights

Data protection in COMPACT

Author: KU Leuven
Madrid, April 11 2018

LPA name: ________
This questionnaire will help contribute to the legal assessment of COMPACT architecture as part of T3.4. It has one question. Thanks for filling it in!

QUESTION: EXERCISE OF DATA SUBJECT RIGHTS
GDPR gives the data subjects certain rights, some of which are relevant for COMPACT.
Right to access, information requirements, right to rectification, right to be forgotten
The exercise of rights must be enabled both during research and after the project is finished. If it cannot be ensured in the system, then the implementer of the COMPACT platform has to enable it.

If an employee comes up to the your LPA as implementer of the platform, can they ask for the following, with regard to the COMPACT platform:

1. Do you hold any personal data about me? (R2A, Art. 15)
2. What personal data do you hold about me? (R2A, Art. 15)
3. How and why are these personal data being processed? (R2A, Art. 15)
4. These personal data are inaccurate, please update them! (R2R, Art. 16)
5. It is unnecessary to keep these personal data about me, please delete them! (R2BF, Art. 17)

Will the employees be notified that the platform is processing their personal data? If yes:

1. When
2. By whom
3. What kind of information do they receive?

Refresher: the definition of personal data
Personal data = (1) any information (2) relating (3) to an identified or identifiable (4) natural person
Example: email address, IP address, name, position, level of education …

8. Annex III: Controller-processor agreement template

Controller - Processor Agreement

Name of controller – Name of processor

Agreement

Between:

____(Name and address of controller), duly represented by ____ (name) acting as _____________________________ function),

Hereinafter: the Controller,

And:

____ (name and address of processor), duly represented by ____ (name) acting as ______________________________(name and function),

Hereinafter: the Processor,

Whereas

The parties to this agreement are partners involved in the user studies on cyber-security awareness organised within the framework of the COMPACT project, funded by the European Commission under the Horizon 2020 programme, Grant Agreement no. 740712. The user studies will take place in October 2017, and will continue throughout the project. They will involve the processing of personal data, including but not limited to the name and position within the company, age, gender, etc. in order to assess the level of cyber-awareness among the workforce of the local public authorities. The research results of such studies will be used to feed into further COMPACT project activities.

In the user studies _____ will fulfil the role of data controller since they are the entity responsible for the overall project management and the coordination of the user studies. Consequently, they have a decisive voice in determining the purpose of the data processing, which is the assessment of cyber-awareness. The other project partners involved in the user are considered to be data processors acting on behalf of the data controller. This means that the other project partners will only process the data concerned on instructions of the data controller and will commit vis-à-vis the data controller to process the data in a secure and privacy-respecting way. The end-responsibility for the secure data processing and compliance with the applicable data protection legislation will lie with the data controller, but in case a data processor does not fulfil its obligations under this agreement, the data controller can seek compensation from the party in breach.

Therefore, it has been agreed as follows:

Article 1 – Definitions

1.1. “Personal Data”, “Controller”, “Processing”, “Personal Data” shall have the same meaning as in Article 4 of the 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 (hereafter: General Data Protection Regulation, GDPR).

1.2. "The research activity" shall refer to the use of personal data, including but not limited to the name and position within the company, age, gender, etc., in the user studies by AIT in order to assess the level of cyber-awareness among the workforce of the local public authorities in the context of the COMPACT project, resulting in research results that will be used to aid in compilation of future reports, which will further the COMPACT activities, as well as benefit the general public.

1.3. "Data Subjects" refers to the participants in the user studies, as described in Article 1.2, whose Personal Data will be processed.

Article 2 - Subject

This commitment governs the processing of Personal Data undertaken by the controller and the other project partners in the context of the research activity that will be executed in the framework of the COMPACT project, a project funded by the European Commission under the Horizon 2020 programme. It regulates the roles, duties and responsibilities of the Controller and the Processor.

Article 3 – Duties and obligations of the Controller

The Controller agrees and guarantees that throughout the duration of the Processing it will issue instructions to the Processor in accordance with the GDPR.

Article 4 – Duties and obligations of the Processor

4.1. The Processor agrees and guarantees that it will only act on (and in accordance with) the instructions of the Controller and will process the Personal Data only on the Controller's behalf.

4.2. The Processor agrees and guarantees:

to prevent unauthorized persons from gaining access to data processing systems for processing or using Personal Data (access control),

to prevent data processing systems from being used without authorization (access control),

to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that Personal Data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),

to ensure that it is possible after the fact to check and ascertain whether Personal Data have been entered into, altered or removed from data processing systems and if so, by whom (input control),

to ensure that Personal Data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),

to ensure that Personal Data are protected against accidental destruction or loss (availability control),

to ensure that data collected for different purposes can be processed separately.

Such technical and organisational measures shall ensure, having regard to the state of the art and the cost of their implementation, and the nature, scope, context and purposes of Processing, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of its employees who have access to the Personal Data.

4.3. The Processor further agrees that it shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorization by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to its processing of the Personal Data for the research activity and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of this Personal Data.

The Processor will also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law, (2) any accidental or unauthorized access, and (3) any request received from the data subjects with regard to the processing of those Personal Data pursuant to this Agreement.

In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorization to do so from the Controller.

4.6 Taking into account the nature of the Processing, the Processing shall assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller’s obligations to respond to requests to exercise Data Subject rights under the GDPR.

4.7. The Controller reserves the right to monitor the data processing activities and the Processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data of the stakeholders when requested to do so by the Controller or by the data subject as well as after the work has been carried out.

4.9. The Processor shall notify the Controller the cases of violation by the Processor or its employees of provisions to protect Personal Data or of the terms specified by the Controller.

4.10. The Processor shall not involve another processor in the Processing without prior specific written authorisation of the controller. In this case, the newly-engaged processor must abide by the same Duties and Obligations as the Processor pursuant to this Agreement. If the newly-engaged processor does not abide by the same Duties and Obligations, the Processor remains fully liable to the Controller for the performance of the other processor's obligations.

4.11 At the request of the Controller, the Processor shall delete or return all the Personal Data to the Controller after the end of the provision of services relating to processing, and delete existing copies unless European Union or Member State law requires storage of the Personal Data.

4.22 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Agreement and Article 28 of the GDPR, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

Article 5 – Term and Termination

5.1 The Agreement is concluded for the duration of the COMPACT project.

5.2 Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and failed to remedy such default within fourteen (14) days after due notice.

5.3 Parties agree that on the termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents it from returning or destroying such data. In that case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

Article 6 – Applicable law, Mediation and Jurisdiction

6.1. The laws of _________ shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in ________.

Done in ______________, on __________ (date), in two copies, each party having received one.

The Processor
______________ (name and function)

______________ (name and function)
The Controller
______________ (name and function)
______________ (name and function)