COMPACT

CYBERSECURITY FOR PUBLIC ADMINISTRATIONS

D2.5 S.E.L.P. Framework

Work Package:	WP2		
Lead partner:	KU Leuven (KUL)		
Author(s):	Danaja Fabčič Povše		
Due date:	31st October 2017		
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	3/7/2017	Danaja Fabčič Povše	Initial table of contents
0.2	20/10/2017	Danaja Fabčič Povše	Final version (pre-review)
0.3	04/12/2017	Danaja Fabčič Povše	Final version (post-review)

Quality Control

Role	Date	Who	Approved/Comment
Internal review	29/11/2017	Ricardo Madeira Simões	Approved
Internal review	4/12/2017	Nadezhda Ilina	Approved

Disclaimer:

Table of Contents

List of Tables

Definitions and acronyms

CIA	Confidentiality, integrity and availability
COMPACT	COmpetitive Methods to protect local Public Authorities from Cyber security Threats
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECHR	Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)
EGE	European Group on Ethics in Science and New Technologies
ENISA	European Union Agency on Network and Information Security
EU	European Union
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)
IP/IPR	Intellectual property, intellectual property rights
ISO/IEC	International organisation for standardisation, International electro technical commission
NIS Directive	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
PET's	Privacy-enhancing techniques
PLD	Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products
PSI Directive	Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, amended by Directive of the European Parliament and of the Council of 26 June 2013
S.E.L.P.	Security, Ethics, Legal and Privacy
TFEU	Treaty on the Functioning of the European Union

1. Introduction

Cyberattacks pose a serious threat to public authorities, whose agencies are regularly targeted by hackers. 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.

S.E.L.P. stands for security, ethics, legal and privacy. It builds upon D1.2, entitled 'S.E.L.P. Management Plan (v1)'. However, while D1.2 addressed the *management* of S.E.L.P. challenges and project compliance, the D2.5 deals with the legal and research ethics compliance of the project research activities and the technological output.

Compliance of the COMPACT architecture will later be assessed in more detail in D3.4 'S.E.L.P. by design in COMPACT' by month 12 of the project.

This opinion is structured as follows:

In Section 2 'Overview', the relevant legal framework is defined, covering the topics of privacy and data protection, security, intellectual property, liability regimes and ethics, which are likely to come up in the COMPACT project activities. The normative framework consists of European legislation, international standards and experts' opinions and non-binding recommendations, referred to as 'soft law'.

Section 3, S.E.L.P. challenges in the COMPACT project, explains the importance and the relevance of data processing in the project. User studies will be carried out in order to assess employees' level of cyber-awareness, and the resulting trial results may contain personal data. Furthermore, LPA's already possess data both on their employees and citizens, which will be integrated into the COMPACT architecture, and there may also be re-use of public sector information for those purposes.

Sections 4, S.E.L.P. challenges for COMPACT technology, and 5, S.E.L.P. challenges for psychological studies and trials, apply the legal requirements of data processing to COMPACT's specific situations. The most important principles of data processing in the project are data minimisation, purpose limitation, transparency and data security. They must be adhered to at all times when processing personal data, therefore a delineation between personal data and anonymised data, to which data protection legislation does not apply, is provided. Those two sections focus on privacy by design as a means of implementing those principles, especially by means of a data protection impact assessment (DPIA), and the implementation of research ethics into user studies.

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

2. Overview of the applicable legal and research ethics framework

The law of the European Union applies because the COMPACT project will take place in the EU and the resulting technology will be used by European LPA's. The analysis therefore takes into account primary EU law (i.e., the Lisbon Treaty, [2] which consists of the Treaty on the EU and the Treaty on the functioning of the EU, as well as the Charter of fundamental rights), secondary law (applicable directives and regulations),[3] as well as certain soft law instruments, such as standards, opinions and recommendations,[4] and international legal instruments, by which member states of the EU are bound.[5]

National law applies to COMPACT activities insofar as it transposes European legislation into domestic legal orders.

First, the legislation transposing the Directive 95/46/EC, applies to, inter alia, consent in the countries where the trials will take place, i.e. Italy, Spain, Portugal and Germany, unless the GDPR will have become enforceable by then. From May 25th 2018, only the GDPR will apply and national legislation will not apply any more.[6]

Second, member states are likewise required to implement the Network and Information Systems Directive[7] by May 2018, and by doing so may expand its scope to include additional subjects or sectors. They have to report any expansions to the Commission, whose future reports on the subject will be taken into consideration for the purposes of this project.

This section of the deliverable will set out the relevant legal framework for main challenges for privacy and data protection, security, intellectual property rights, liability of project partners for their project activities, and research ethics that are likely to arise with regards to the COMPACT project. It focuses on general principles, whose specific application will be discussed in the following sections.

---

[2] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306, 17.12.2007, p. 1–271.

[3] Predominantly 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, 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) and 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] See Section 2.2.1.

[5] Such as the European Convention on Human Rights and Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, no. 108, accessible at http://www.echr.coe.int/Documents/Convention_ENG.pdf and https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 respectively.

[6] Article 99(2) of the General Data Protection Regulation (GDPR).

[7] 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 (NIS Directive).

2.1. Privacy and data protection

The main privacy and data protection issues within the COMPACT project might arise due to the fact that the LPA's hold and/or process personal data both on their employees and their citizens, including the potential monitoring of the LPA's' employees during the COMPACT activities.

Main EU legal instruments are on privacy and data protection are Treaty on the Functioning of the European Union (TFEU),[8] Charter of Fundamental Rights,[9] General Data Protection Regulation (GDPR)[10] and the Directive 95/46/EC,[11] and the Network and Information Systems Directive (NIS Directive).[12]

All EU member states are also signatories of the European Convention on Human Rights (ECHR)[13] as well as the Convention no. 108 on Automatic Processing of Personal Data.[14]

Regarding privacy within the workplace, the following opinions and recommendations must also be considered: Recommendation No. 89 (2) on the Protection of Personal Data used for Employment Purposes issued by the Council of Ministers of the Council of Europe,[15] the International Labour Organisation's Office Code of Practice on protection of workers' personal data,[16] and the relevant opinions of the Article 29 Working Party.[17] These documents are non-binding, but nevertheless relevant as they interpret and explain the law, as well as provide guidance and present best practices in the field.

[8] Treaty on European Union and the Treaty on the Functioning of the European Union, 2010, C 83/01.
[9] Charter of fundamental rights of the European Union, 30 March 2010, C83/389.
[10] 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), OJ L 119, 4.5.2016.
[11] 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, Official Journal L 281 , 23/11/1995. Despite the GDPR's repeal of the Directive, certain provisions, such as notification duty, remain in force. See Section 2.1.2.1.1.
[12] 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, OJ L 194, 19.7.2016.
[13] Convention of the Council of Europe of 4 November 1950 for the Protection of Human Rights and Fundamental Freedoms (ECHR), available at http://www.echr.coe.int/Documents/Convention_ENG.pdf.
[14] Convention of the Council of Europe of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.
For list of signatories, see https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=ReHrHQ1f.
[15] Recommendation No. (89) 2 of the Council of Europe on the protection of personal data used for employment purposes, adopted by the Committee of Ministers on 18 January 1989, available at http://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf.
[16] International Labour Organisation, Protection of workers' personal data, an ILO code of practice, available at http://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/normativeinstrument/wcms_107797.pdf.
[17] The Article 29 Working Party (also referred to as WP29) was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy.

2.1.1. Right to respect for private life in international legal instruments

According to the Article 8 of the ECHR, everyone has the right to respect for his or her private and family life, home and correspondence.[18] An interference with this right by a public authority is allowed only in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[19]

The notion of private life is broad and the definition cannot be definitive.[20] Regarding COMPACT activities, the collection of information on individuals by public authorities always falls within the scope of Article 8,[21] as well as communications within the workplace.[22] Workers have a reasonable expectation of privacy within the workplace and an employer's instructions cannot reduce private life to zero, although it may be restricted as far as necessary.[23]

There are also two non-binding documents issued on the international level, by the International Labour Organisation and the Council of Europe, respectively.

The *Code of Practice on protection of workers' personal data*[24] focuses on basic principles, recommending that be data processing only be carried out if it's done lawfully and fairly, and only for reasons directly relevant to the employment of the worker;[25] used only for the purposes for which they were originally collected,[26] and in case of re-use, used in a manner that is not incompatible with the original purpose,[27] if automated processing is put in place, it should not control the behaviour of workers[28] nor should it be the only basis for a decision,[29] especially an assessment of work performance.[30] An employer should not collect sensitive data unless there is a legal obligation to do so, either in law or

[18] Article 8(1) of the ECHR.
[19] Article 8(2) of the ECHR.
[20] Costello-Roberts v. the United Kingdom, judgment of the ECtHR of 25 March 1993, para. 36.
[21] See Council of Europe, Guide to Article 8, p. 15.
[22] Bărbulescu v. Romania, judgment of the ECtHR of 5 September 2017, para. 81.
[23] Bărbulescu v. Romania, judgment of the ECtHR of 5 September 2017, para. 80.
[24] International Labour Organisation, Protection of workers' personal data. An ILO code of practice, available at http://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/normativeinstrument/wcms_107797.pdf.
[25] Principle 5.1 of the ILO Code of Practice.
[26] Principle 5.2 of the ILO Code of Practice.
[27] Principle 5.3 of the ILO Code of Practice.
[28] Principle 5.4 of the ILO Code of Practice.
[29] Principle 5.5 of the ILO Code of Practice.
[30] Principle 5.6 of the ILO Code of Practice.

collective agreement.[31] If a worker refuses to provide data according to their rights, then his or her employment should not be terminated.[32]

Recommendation No. 89 (2) on the Protection of Personal Data used for Employment Purposes[33] stresses the need to focus on the respect for employees' privacy and human dignity regarding the processing of personal data in the workplace.[34]

Employees should be informed or consulted before measures are put into place, including measures aiming to improve productivity.[35] The collection of personal data should be relevant and not be excessive bearing in mind the type of employment as well as the evolving information needs of the employer.[36] Data, collected for employment purposes, should on principle not be used for other purposes, unless adeuate safeguards are adopted to prevent further processing, incompatible with the original purpose.[37] Employees should have the right to access their data, and correct it if necessary.[38]

2.1.2. EU law

2.1.2.1. General Data Protection Regulation (GDPR)

Regulation (EU) 2016/679 of the European Parliament and of the Council 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, GDPR), was adopted on 27 April 2016.[39]

The GDPR will enter into force on May 25, 2018. Until then, national legislation implementing the Directive 95/46/EC still applies. In order to preserve continuity, it contains an explicit provision in its Article 94(2) that any references to the repealed Directive shall be construed as references to the GDPR.

The GDPR protects *natural persons* with regard to the processing of *personal data* and rules relating to the free movement of personal data.[40] It applies to the *processing* of personal data wholly or partly *by automated means* and to the processing other than by

[31] Principle 6 of the ILO Code of Practice.
[32] Principle 6.8 of the ILO Code of Practice.
[33] Recommendation No. (89) 2 of the Council of Europe on the protection of personal data used for employment purposes, adopted by the Committee of Ministers on 18 January 1989, available at http://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf.
[34] Article 2 of the Recommendation (89) 2.
[35] Article 3 of the Recommendation (89) 2.
[36] Article 4.2 of the Recommendation (89) 2.
[37] Article 6 of the Recommendation (89) 2.
[38] Article 12 of the Recommendation (89) 2.
[39] 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).
[40] Article 1(1) of the GDPR.

automated means of personal data which form part of a filing system or are intended to form part of a filing.[41]

A natural person is an individual human being, as opposed to a legal person, which is an organisation, to whom data protection does not apply. In the COMPACT project, there will be two types of data subjects, the citizens under the LPA's jurisdictions, and the LPA's' employees.

Personal data is defined 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.[42]

There are two categories of personal data at stake – personal data as such, and sensitive data, called special categories of personal data by the GDPR. *Sensitive data* is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

In the COMPACT project, both types of personal data may be collected and processed. It is likely that health-related data will be at stake, especially if the LPA's are linked to the provision of healthcare services.

A *controller* is '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'.[43]

A *processor* is 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.[44]

It is important to distinguish between the controller and the processor, as they have different obligations and different tasks to carried out. This is further explained in Sections 2.1.2.1.4, 2.1.2.1.6 and 2.1.2.1.7.

2.1.2.1.1. Principles of data processing

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

[41] Article 2(1) of the GDPR.
[42] Article 4(1) of the GDPR.
[43] Article 4 (7) of the GDPR.
[44] Article 4 (8) of the GDPR.

limitation and integrity and confidentiality. According to the accountability principle, the controller is responsible for showing compliance with these principles.[45]

Personal data must be processed **lawfully, fairly and in a transparent manner** in relation to the data subject.[46] Lawfulness refers to processing having appropriate legal grounds, as set out in Article 6, and explained below in Section 2.1.2.1.2.

Purpose limitation means that data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[47] This principle establishes 'the boundaries within which personal data collected for a given purpose may be processed and may be put to further use.'[48] It consists of two building blocks:

- data is collected for specified, explicit and legitimate purposes,
- further processing of collected data must not be done in a way incompatible with those purposes (Article 5(1)b).

Specific purpose means that the purpose must be 'sufficiently defined to enable the implementation of any necessary data protection safeguards, and to delimit the scope of the processing operation'. An explicit purpose is one that is 'sufficiently unambiguous and clearly expressed'. Legitimate purpose requires legal grounds for data processing, which go beyond the scope of privacy rules and refer to the legal system as a whole.[49]

Purpose limitation is related to concepts such as data transparency (visibility of purpose), predictability of data processing and user control, i.e. giving data subjects certain rights regarding the collected data.[50]

Further processing for research purposes or statistical purposes is not considered to be incompatible with the initial purposes.[51]

Data must be collected 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.[52]

Under the **accuracy** principle, 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.[53]

According to storage **limitation principle**, data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which

[45] Article 5(2) of the GDPR.
[46] Article 5(1)a of the GDPR.
[47] Article 5(1)b of the GDPR.
[48] Article 29 Working Party, Opinion on Purpose Limitation, p. 4.
[49] Article 29 Working Party, Opinion on Purpose Limitation, p. 12.
[50] Article 29 Working Party, Opinion on Purpose Limitation, p. 13-14.
[51] Article 5(1)b of the GDPR.
[52] Article 5(1)c of the GDPR.
[53] Article 5(1)d of the GDPR.

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).[54]

Integrity and confidentiality principle requires data to 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.[55]

The application of these principles to the COMPACT tehcnology is explained in Section 4, and in Section 5 for user studies.

2.1.2.1.2. Lawfulness of processing

Article 6 sets out the criteria under which processing of personal data is lawful. Criteria are alternative, therefore fulfilling one criterion is sufficient for lawfulness.

Data processing is lawful if the data subject has given *consent*,[56] or processing is necessary for the *performance of a contract* to which the data subject is party,[57] or processing is necessary for *compliance with a legal obligation* to which the controller is subject,[58] or processing is necessary in order to *protect the vital interests* of the data subject or of another natural person,[59] or processing is necessary for the performance of *a task carried out in the public interest or in the exercise of official authority* vested in the controller,[60] or processing is necessary for the purposes of the *legitimate interests* pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[61]

Although the last paragraph does not apply to processing carried out by public *authorities in the performance of their tasks*,[62] the internal managament of an LPA cannot be considered a performance of its task. Therefore, legitimate interests can be relied upon even in an LPA context. Cyber-security is explictly set out as a legitimate interest in Recital 49 of the GDPR. However, the processing must be *necessary* in order to achieve such legitimate interests. Specifically, when implementing cyber-security measures, the

[54] Article 5(1)e of the GDPR.
[55] Article 5(1)f of the GDPR.
[56] Article 6(1)a of the GDPR.
[57] Article 6(1)b of the GDPR.
[58] Article 6(1)c of the GDPR.
[59] Article 6(1)d of the GDPR.
[60] Article 6(1)e of the GDPR.
[61] Article 6(1)f of the GDPR.
[62] Last sentence of Article 6(1) of the GDPR. Emphasis added by the author.

processing must be kept to the extent strictly necessary and proportionate for the purposes of ensuring network and information security.[63]

If processing is necessary for compliance with a legal obligation to which the controller is subject or necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, then it requires legal basis in Union or national law. Legislation setting out such an obligation or task must have a legitimate aim and be proportional.[64]

In the COMPACT project, legal grounds will be consent, or a legal obligation, especially obligations stemming from the Network and Information Security Directive (see Section 2.2.2), or from the GDPR itself (see Section 2.2.3), or if the processing is necessary for the performance of tasks carried out in the public interest or if it is necessary for legitimate interests of the data controller.

In the COMPACT setting, consent is likely to be legal grounds for the user studies.

Article 7 sets out conditions for valid consent. First, it is the controller who has the burden of proof that consent has been given.[65] Consent has to be explicitly set out even if it's given within the context of an unrelated written declaration.[66] The data subject has the right to withdraw his or her consent at any time and he has to be informed of this right beforehand. The withdrawal of consent only affects future processing. Withdrawing consent must be as easy as giving it.[67] When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[68]

For the processing of special categories of data,[69] such as health, sexual and political orientation, a data subject's explicit consent required.

However, EU or national law may provide that the prohibition may not be lifted by the data subject. If there is such a provision, then even though the data subject has consented to processing, such consent is invalid due to the prohibition and other legal grounds must be sought.[70]

2.1.2.1.3. Data subject's rights

GDPR grants the following rights to the data subject:

[63] Recital 49 of the GDPR.
[64] Article 6(3) of the GDPR.
[65] Article 7(1)a of the GDPR.
[66] Article 7(2)a of the GDPR.
[67] Article 7(3)a of the GDPR.
[68] Article 7(4)a of the GDPR.
[69] Article 9(1) of the GDPR.
[70] Article 9(2)a of the GDPR.

- right to information,[71]
- right of access,[72]
- right to rectification,[73]
- right to erasure,[74]
- right to restriction of processing,[75]
- right to data portability,[76]
- right to object.[77]

1. Right to information

The data controller must provide the data subject with all of the following information:

- the identity and the contact details of the controller,
- the contact details of the data protection officer,
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing,
- the categories of personal data concerned,
- the recipients or categories of recipients of the personal data, if any,
- if applicable, information about transfers to third countries.[78]

It must also provide the following information, which contributes to the principle of fairness and transparency of processing:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
- if processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

[71] Articles 13 and 14 of the GDPR.
[72] Article 15 of the GDPR.
[73] Article 16 of the GDPR.
[74] Article 17 of the GDPR.
[75] Article 18 of the GDPR.
[76] Article 20 of the GDPR.
[77] Articles 21 and 22 of the GDPR.
[78] Articles 13(1) and 14(1) of the GDPR.

- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[79]

The data controller must provide the data subject with the same information regardless of whether the personal data have been obtained from the data subject (Article 13) or otherwise (Article 14). However, the timing of the informing is different for the two situations:

If personal data have been obtained from the data subject, then the information has to be provided at the time they are obtained.[80]

If personal data have not been obtained from the data subject, then there are three possibilities:

- This information must be provided within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed.
- In case the personal data are to be used for communication with the data subject, information must be provided at the latest at the time of the first communication to that data subject.
- If a disclosure to another recipient is envisaged, information must be provided at the latest when the personal data are first disclosed. This will be especially the case in user studies, as different organisations will have access to personal data. [81]

It is not necessary for the data controller to notify the data subject of his or her rights if:

- the data subject already has the information,
- the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
- obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

[79] Articles 13(2) and 14(2) of the GDPR.
[80] Article 13(1) of the GDPR.
[81] Article 14(3) of the GDPR.

- if the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.[82]

If the personal data have been obtained directly from the data subject, then the notification is not required only if the data subject already has the information. Inversely, it is required in all other situations.[83]

2. Right of access

The right of access of the data subject means that the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data, as well as the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- 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;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- 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;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[84]

This information is identical to the information that the data controller has to provide to the data subject under Articles 13 and 14 of the GDPR. The difference is the timing and the initiative for notification – whereas under Articles 13 and 14 the controller has to notify the data subject as set out above, according to Article 15 there is no specific timeline ('the data subject shall have the right to obtain'). Therefore, the data subject can exercise his or her right of access at any time.

[82] Article 14(5) of the GDPR.
[83] Article 13(4) of the GDPR.
[84] Article 15(1) of the GDPR.

If the data subject exercises the right to access, the controller must provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. If the request is made electronically, and unless otherwise requested by the data subject, the information must be provided in a commonly used electronic form.[85] If possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data.[86]

The exercise of right to obtain a copy must not affect the rights of others in an adverse, negative way.[87] This refers to rights, such as trade secrets or intellectual property and in particular the copyright protecting the software.[88]

3. Right to 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.[89]

4. Right to erasure (the right to be forgotten)

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.[90]

[85] Article 15(3) of the GDPR.
[86] Recital 63 of the GDPR.
[87] Article 15(4) of the GDPR.
[88] Recital 63 of the GDPR.
[89] Article 16 of the GDPR.
[90] Article 17(1) of the GDPR.

If the personal data have been made public by the controller, then it is still obliged to erase them and, taking account of available technology and the cost of implementation, must take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.[91]

The right to be forgotten does not apply if processing is necessary for:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health;
- for research purposes in so far as the right to be forgotten is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defence of legal claims.[92]

5. Restriction of processing

The data subject has the right to obtain from the controller the restriction of processing if

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.[93]

If the data subject has requested restriction of processing, then further processing of such personal data is allowed only with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.[94]

[91] Article 17(2) of the GDPR.
[92] Article 17(3) of the GDPR.
[93] Article 18(1) of the GDPR.
[94] Article 18(2) of the GDPR.

A data subject who has obtained restriction of processing must be informed by the controller before the restriction of processing is lifted.[95]

6. Right to data portability

The data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

The right to data portability applies if the legal grounds for processing is the data subject's consent (Article 6(1)a) or if it is necessary for the performance of a contract (Article 6(1)b), and if the processing is carried out by automated means.[96]

The data subject has the right to have the personal data transmitted directly from one controller to another, if technically feasible.[97]

The right to data portability might conflict with the right to be forgotten. In that case, the right to data portability applies without prejudice to the right to be forgotten - which in that case will not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.[98]

Exercising the right to data portability must not adversely affect the rights and freedoms of others.[99]

The right to portability is unlikely to be at stake in the COMPACT project, unless there is a change in consortium, or a new, different division of tasks which would result in several data controllers dealing with the same personal data.

7. Right to object and automated processing

Articles 21 and 22 of the GDPR grant the data subject the right to object, and the right not to be subject to a decision based solely on automted processing, respectively.

The data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on carrying out a task in the public interest or for the legitimate interests of the data controller, including profiling based on those provisions. The controller must then no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the

[95] Article 18(3) of the GDPR.
[96] Article 20(1) of the GDPR.
[97] Article 20(2) of the GDPR.
[98] Article 20(3) of the GDPR.
[99] Article 20(4) of the GDPR.

processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.[100]

Similarly, the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. That right does not apply, if automated processing is necessary for entering into, or performance of, a contract between the data subject and a data controller; if it is authorised by EU or national law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or if it is based on the data subject's explicit consent.[101]

Automated processing is likely to be relevant in the COMPACT project in the implementation phase. Specifically, it is relevant, if the resulting technology will function by detecting cybersecurity threats on an automated basis. In that case, following an objection from the data subject (either an employee or a citizen), the controller must show that it has compelling legitimate interests, such as the necessary functioning of the cyber-security system, which out-weigh the interests of the data subject.

Regarding the right not to be subject to an automated decision, it is unlikely that this right will be relevant for COMPACT activities. Setting up a secure system is an obligation under EU law[102] to which the LPA's are subject, and therefore the right does not apply.[103] Nonetheless, in order to counter the risks posed by automated processing, the law must lay down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.[104]

2.1.2.1.4. Data controller's general obligations

The data controller is 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. If the means and purposes of processing are set out in EU or national law, then such law also determines the controller or the specific criteria for its nomination.[105]

Determining the purposes and means of data processing refers to defining the 'why and how' of the operation.[106] The why's and how's mean determining the following:

[100] Article 21(1) of the GDPR.
[101] Article 22(1,2) of the GDPR.
[102] See Section 2.2 Security on the legal grounds for setting up cyber-security.
[103] Article 22(2)b of the GDPR.
[104] Article 22(2)b of the GDPR.
[105] Article 4(7) of the GDPR.
[106] Information Commissioner's Office, Data Controller and Data Processor: what the difference is and what the governance implications are, p. 8. Available at https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

- Adopting the decision to collect the personal data and the legal grounds to do so,
- The content of the personal data to be collected,
- The purpose(s) of the use of the collected data,
- Who are the data subjects - whose personal data will be collected,
- The possible disclosure of personal data to third parties,
- Possible restrictions to data subjects' rights, as provided for in the GDPR,
- The duration of data storage and possible future amendments to those data.

The controller can do that on its own or together with other controllers, in which case they are considered joint controllers.[107]

Data controllers in the COMPACT project are those partners dealing with personal data, who determine the means and purposes of processing by defining the above criteria. Additionally, LPA's are already data controllers, as they possess personal data pre-dating the project. Those personal data refer to citizens and employees.

It is important to differentiate between a data controller and a data processor as the two have different obligations and responsibilities. Generally, if an entity does not define the above criteria on its own, then it is considered a data processor. The difference is explained in greater detail in Section 2.1.2.1.7.

According to the **accountability principle**, the data controller is responsible for showing that its actions are GDPR-compliant.[108] It carries the responsibility for implementing appropriate technical and organisational measures to ensure and to demonstrate that its processing activities are compliant with the requirements of the GDPR, including adopting an appropriate privacy policy.[109] Moreover, the Regulation requires the controller to adopt 'data protection by design and by default',[110] i.e. use techniques like anonymisation, pseudonymisation, protocols for anonymous communications, access control and encryption in order to ensure application of basic processing principles, such as data minimisation. The implementation of this principle is set out in greater detail in Section 4.3.

The data controller must maintain a record of its processing activities and the following information related to it:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;

[107] Article 26 of the GDPR. On Joint Controllership, see Section 2.1.2.1.5.
[108] Article 5(2) of the GDPR.
[109] Article 24 of the GDPR.
[110] Article 25 of the GDPR.

- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- if possible, the envisaged time limits for erasure of the different categories of data;
- if possible, a general description of the technical and organisational security measures referred to in Article 32(1).[111] [112]

GDPR also lays down the controller's obligation to cooperate with the competent authority in performance of the latter's tasks, if the authority requests the controller to do so.[113]

Additionally, the controller has certain obligations regarding security of data processing,[114] such as notification duty, further explained below in Section 2.2.3, and it is under certain circumstances obliged to carry out a data protection impact assessment (DPIA)[115] and appoint a data protection officer (DPO).[116]

A controller is required to appoint a DPO when any of the following conditions are fulfilled:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- 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
- the core activities of the controller or the processor consist of processing on a large scale of sensitive personal data and personal data relating to criminal convictions and offences.

As a public authority, LPA's are required to appoint a data protection officer (DPO) according to Article 37(1)a. Other partners, which will have the role of a data controller, must appoint one if they meet either of the other two criterions. While it is unlikely that sensitive personal data or data relating to criminal convictions will be processed on a large scale, the implementation of cyber-security and carrying out cyber-security awareness studies are likely to involve regular and systematic monitoring of data subjects. However, the GDPR only requires that a DPO be appointed if such processing is carried out on a large scale.

[111] Article 30 of the GDPR.
[112] For an analysis of Article 32, see Section 2.2.3.
[113] Article 31 of the GDPR.
[114] Articles 32-34 of the GDPR.
[115] Article 35 of the GDPR.
[116] Articles 37-39 of the GDPR.

'Large scale' refers to a large number of data subjects, to the volume of data, the duration/permanence of the processing activity, or its geographical extent.[117] COMPACT technology may very well fall under these criteria, especially since the resulting platform will contain personal data of a large number of a population living in a local community, as well as a large number of the LPA employees.

A DPO is involved in all issues, relating to the protection of personal data. A LPA (and its processors) must support it by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.[118]
He or she must be independent from both the controller and the processor. That means that the DPO must not receive any instructions regarding the exercise of those tasks, must not be dismissed or penalised by the controller or the processor for performing his tasks. The DPO reports directly to the highest management level of the controller or the processor.[119]
Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under the GDPR.[120]
DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with EU or national law.[121] He or she may fulfil other tasks and duties. The controller or processor must ensure that any such tasks and duties do not result in a conflict of interests.[122]

2.1.2.1.5. Joint controllership

Article 26 sets out the requirements for joint controllership.
Joint controllership is defined as two or more controllers jointly determining the purposes and means of processing.[123] They must conclude an arrangement among themselves, in order to demonstrate their GDPR compliance in a transparent way. In particular, they must demonstrate compliance with notification duties set down in Articles 13 and 14. [124] The arrangement must also take into account additional requirements, to which the joint controllers may be subject under EU or national law. It may designate a contact point for data subjects.[125]
The arrangement must also reflect the respective roles and relationship of the joint controllers vis-à-vis the data subjects, to whom its essence must be made available.[126]

[117] Article 29 Working Party, Opinion on Data Protection Officers, p. 7.
[118] Article 38(1-2) of the GDPR.
[119] Article 38(3) of the GDPR.
[120] Article 38(4) of the GDPR.
[121] Article 38(5) of the GDPR.
[122] Article 38(6) of the GDPR.
[123] Article 26(1) of the GDPR.
[124] See Section 2.1.2.1.3, especially the subsection on 'the right to information'.
[125] Article 26(1) of the GDPR.
[126] Article 26(2) of the GDPR.

The data subject may exercise his or her rights, granted by the GDPR, in respect of and against each of the controllers, regardless of the inner arrangement among the joint controllers.[127]

Joint controllership allows for some flexibility among controllers – for example, one controller determines the means and purposes only partly, and the other(s) substantively but not exclusively. This could be the case in user studies, as the LPA's and the partner carrying out the tests have a common purpose for processing, i.e. assessing the level of cyber-knowledge among the workforce, though only one of them will determine to the means to do so. Alternatively, the partners can decide for a data controller/data processor relationship, which is described below in Section 2.1.2.1.8.

2.1.2.1.6. Processor's general obligations

A processor carries out the processing operation on behalf of the controller.[128]

The GDPR only contains a few rules regarding the processor.

First, the processor can only be appointed if it meets certain criteria. According to Article 28(1) of the GDPR, the controller must use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

A processor can subcontract its processing activities to another processor, but not without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, which gives the controller the opportunity to object to such changes.[129]

There is also a restriction on the the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, not to process those data except on instructions from the controller. If the controller's staff or the processor or its staff are required to process data by EU or national law, then they do not need to abide by the controller's instructions.[130]

Like the controller, the processor is required to cooperate with the supervisory authority, if the latter so requests.[131] It is also required to adopt certain security measures, as explained further in Section 2.2.3. Unlike the data controller, it is not required to carry out a DPIA, although it is required to appoint a DPO if it meets either of the following criteria:

[127] Article 26(3) of the GDPR.
[128] Article 4(8) of the GDPR.
[129] Article 28(2) of the GDPR.
[130] Article 29 of the GDPR.
[131] Article 31 of the GDPR.

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- 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
- the core activities of the controller or the processor consist of processing on a large scale of sensitive personal data and personal data relating to criminal convictions and offences (Article 10 of the GDPR).[132]

The processor is required to appoint a DPO under the same conditions as the controller and the same legal requirements apply as in the case in which the controller appoints one.[133]

The data processors in the COMPACT project will typically be entities, to whom the above-mentioned tasks are subcontracted as a part of business strategy, including that of the LPA's, of outsourcing tasks to specialised organisations. For example, an LPA can appoint a specialised IT firm to store its personal data as a way of lowering costs.

The COMPACT partners should therefore choose their processors in a diligent and careful manner, and regulate their relationship as set out in Section 2.1.2.1.8.

2.1.2.1.7. How to differentiate between a data processor and a data controller

The main difference between the two is that the controller is the one to determines the means and purpose(s) of processing. The two are mutually exclusive; the same organisation cannot function as controller and processor for the same processing operation.

It is impossible to be a data processor and a data controller at the same time, for the same processing operation. As set out above, they have different obligations and responsibilities, so it is important to draw a distinction between the two of them.

As it is the controller who determines the purposes and means of data processing, the processor generally holds a more 'technical' role, such as data storage, data retrieval or data erasure.[134]

Typical decisions that a data controller undertakes, are whether to collect the data and the legal basis thereof, which data to collect, the purpose(s) of collection, whose data to collect, etc. A processor decides, on the basis of its contract with the controller ('processor terms'),

[132] Article 37(1) of the GDPR.
[133] See Section 2.1.2.1.4, and Articles 37-38 of the GDPR.
[134] Information Commissioner's Office, Data Controller and Data Processor: what the difference is and what the governance implications are, p. 5. Available at https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

which IT systems or other methods to use for collection, how and where to store data, the means for transferring data and for retrieving, disposing or deleting them, etc.[135]

2.1.2.1.8. The relationship between a processor and a controller

The controller and the processor can regulate their relationship by concluding a contract to that end. This is sometimes referred to as 'processor terms'. GDPR sets out their minimum content, and an example of them has recently been made available by the DLA Piper law firm.[136]

Processor terms must legally bind the processor to the controller's instructions and set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.[137]

According to the GDPR, the processor terms must stipulate, in particular, that the processor:

- processes 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 EU or national 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;
- ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- takes all measures required under Article 32, relating to security of processing (see the section on security)
- respects the conditions for engaging another processor, referred to in paragraphs 2 and 4, i.e. not without the authorisation of the controller, and only if sufficient guarantees are put in place.
- taking into account the nature of the processing, assists 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 (the right to information,[138] the right of access,[139] the right to rectification,[140] the right to

[135] Information Commissioner's Office, Data Controller and Data Processor: what the difference is and what the governance implications are, p. 6-7. Available at https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf
[136] https://www.dlapiper.com/en/uk/insights/publications/2017/08/example-gdpr-ready-processor-terms
[137] Article 28(3) of the GDPR.
[138] Articles 13 and 14 of the GDPR.

erasure,[141] the right to restriction of processing,[142] the right to data portability,[143] the right to object[144]);

- assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 on security of data processing and data protection impact assessment, taking into account the nature of processing and the information available to the processor;
- at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
- 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. The processor must immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

The processor can engage another processor for carrying out specific processing activities on behalf of the controller.

In that case the same legal obligations set out above apply to the new processor either by way of contract or another legal act. Such an act must provide, in particular, *sufficient guarantees* to implement appropriate technical and organisational measures in a way to make sure the processing will meet the requirements of the GDPR.

Meeting the sufficient guarantees threshold is important for the original, initial processor. It remains fully liable to the controller for the performance of the other processor's obligations unless the guarantees are met.[145]

'Sufficient guarantees' can be demonstrated by adherence by either processor to an approved code of conduct, as set down in Article 40 of the GDPR, or a certification mechanism under Article 42.[146]

Processor terms can be based, wholly or partly, on standard contractual clauses, which the Commission or another supervisory authority will adopt.[147] They must be in writing, including in electronic form.[148]

---

[139] Article 15 of the GDPR.
[140] Article 16 of the GDPR.
[141] Article 17 of the GDPR.
[142] Article 18 of the GDPR.
[143] Article 20 of the GDPR.
[144] Articles 21 and 22 of the GDPR.
[145] Article 28(4) of the GDPR.
[146] Article 28(5) of the GDPR.
[147] Article 28(6-8) of the GDPR.
[148] Article 28(9) of the GDPR.

The processor can never determine the means and purpose of processing.

If the processor does that, then it is considered to be the controller, and liable for infringement in the same way that the controller is.[149]

In the DLA Piper processor terms example, the above requirements are not entirely set out. The assumption seems to be that the subject matter, the duration, nature and purpose of processing, as well as the types of personal data to be processed and the data subjects to which they relate, will be clarified in the main contract, to which the processor terms are an addendum.

The example lays down the rights and obligations binding either party in Sections 3-5. These implement the personnel requirement of Article 29 and the security requirements of Article 32, respectively. Section 6 sets out the requirements for subprocessing – in the GDPR wording, engaging another processor pursuant to the meaning of Article 28(2). They also set out data subjects' rights, especially in the event of a data breach, and specify the storage limitation principle in its Section 10 – personal data must be deleted or returned to the controller on cessation date.

The DLA-Piper example is not binding; nonetheless, as the first publically available document of its kind it is useful as an example of good practice.

2.1.2.1.1. Notification duty under the Directive 95/46/EC

Until the GDPR becomes enforceable in less than a year, the Directive 95/46/EC and its implementing legislation still apply. Especially relevant is the Article 18, which requires that the controller or his representative, if any,[150] must notify the competent supervisory authority before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2.1.2.2. Public sector information directive

The Public Sector Information Directive[151] is relevant to the COMPACT project due to the inclusion of LPA's.
'Public sector information' refers to documents held by public sector bodies.[152] Access to these documents is allowed under certain conditions.

[149] Article 28(10) of the GDPR.
[150] According to Article 4(1)c of the Directive 95/46/EC, a controller whose place of establishment was outside the Community (EU) territory, had to appoint a representative within the member state, in which it was using equipment for the purpose of data processing.
[151] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, amended by Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013, *hereafter: the PSI Directive*.
[152] Article 1 of the PSI Directive.

Obliged entities under the PSI Directive are the State, regional or local authorities, bodies governed by public law and associations formed by one or several such authorities or one or several such bodies governed by public law.[153] As a local authority, LPA's fall under this definition.

The PSI Directive leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of data protection legislation.[154] While access to personal data is not prohibited *per se*, there are some exceptions to the access. Access under the PSI does not apply to the following situations:

- documents access to which is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data,
- parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data.[155]

If these documents contain anonymised data, such data is accessible according to the PSI Directive, but if it has not been anonymised, then it is personal data, and falls under the provisions of the GDPR or the Directive 95/46/EC and implementing legislation until May 25th 2018. However, in that case data must be completely anonymised in a way that absolutely prevents re-identification of data subjects, as opposed to data which had been manipulated so as to mitigate the risk of re-identification.[156] In that case, the principle of purpose limitation[157] may limit further processing of data held,[158] but as COMPACT is a research project, such re-use is compliant with the principle.[159]

Public sector information can be re-used for commercial or non-commercial purposes.[160]

2.2. Security

COMPACT is a (cyber)security project, addressing security challenges from two points of views; security of the IT systems and security of personal data. As the latter are kept within the former, they are both addressed in this section, however, different legislation might apply.

[153] Article 2(1) of the PSI Directive.
[154] Article 1(4) of the PSI Directive.
[155] Article 1(2) of the PSI Directive.
[156] Article 29 Working Party, Opinion 06/2013 on open data and public sector information ('PSI') reuse, p. 12-13. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf
[157] Article 5(1)b of the GDPR.
[158] Article 29 Working Party, Opinion no. 03/2013 on purpose limitation. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
[159] See Section 2.1.2.1.1.
[160] Article 3(1) of the PSI Directive.

There is no single definition of cyber-security in applicable legal framework. Moreover, the instruments use different terminology (security of network and information systems, information security etc.).

According to 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 (NIS Directive),[161] 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.[162]

According to the ISO/IEC Standard 27000, Section 3.2.3, information security ensures the confidentiality, availability and integrity of information. It involves the application and management of appropriate controls that involves consideration of a wide range of threats, with the aim of ensuring sustained business success and continuity, and minimizing consequences of information security incidents.[163]

The GDPR does not define security of processing as such, but connects the notion to the controller's obligation to implement 'technical and organisational measures'.[164]

Setting up cybersecurity has implications for the system as a whole, as well as for the personal data kept in it.

A cybersecurity system is likely to face the following risks:

- destruction of information and/or other resources;
- corruption or modification of information;
- theft, removal or loss of information and/or other resources;
- disclosure of information; and
- interruption of services.[165]

There is some EU-level legislation on security aspects, as well as standards and recommendations. Standards reflect consent of the actors in the field. Unlike legislation, standards are non-binding and compliance with them is voluntary. However, complying with standards is nonetheless recommended, because failure to comply can bring market-access issues. Recommendations are likewise non-binding.

[161] 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, OJ L 194, 19.7.2016, p. 1–30 (the NIS Directive).
[162] Article 4(2) of the NIS Directive.
[163] Section 3.2.3 of the ISO/IEC Standard Series 27000.
[164] Article 32 of the GDPR.
[165] International Telecommunications Union, Recommendation No. ITU-T X.1205 (04/2008)

2.2.1. Standards

IT standards are relevant due to the wording of Article 32 of the GDPR, which refers to 'the state of the art'. They reflect consensus and are updated regularly so as to present the best practices in the industry.

Security in IT systems is standardised under the following standards.

The International Standardising Organisation (ISO), together with The International Electro-Technical Committee, published the ISO/IEC 27000-series[166] in October 2013. Especially important are ISO/IEC 27001[167] and 27002, which specify a management system and control objectives, necessary to implement IT security.

Another important series is ISO 15408-series, relating to security techniques and providing evaluation criteria in IT security. There are three standards in the series, namely ISO/IEC 15408-1:2009,[168] ISO/IEC 15408-2:2008[169] and ISO/IEC 15408-3:2008.[170] These provide for a general model of cybersecurity, security functional components and security assurance components.

Further, there are TR 103 series standards on cyber security,[171] published by the European Telecommunications Standards Institute (ETSI). They relate to horizontal security regarding privacy by design, security controls, network and information security and critical infrastructures; information security indicators; to securing technologies and systems, and to security tools and techniques, such as cryptography.

The Standard of Good Practice for Information Security is published by the Information Security Forum (ISF) and presents a comprehensive list of best practices for information security. The latest version was updated in 2016[172] and provides complete coverage of international standards, such as the ISO/IEC 27002:2013.

[166] ISO/IEC 27000:2016(E), ISO/IEC 27000:2016(F) Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, available at http://standards.iso.org/ittf/PubliclyAvailableStandards/.
[167] ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements, available at http://standards.iso.org/ittf/PubliclyAvailableStandards/.
[168] ISO/IEC 15408-1:2009 – Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model, available at http://standards.iso.org/ittf/PubliclyAvailableStandards/.
[169] Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components, available at http://standards.iso.org/ittf/PubliclyAvailableStandards/.
[170] Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components, available at http://standards.iso.org/ittf/PubliclyAvailableStandards/.
[171] Available at http://www.etsi.org/technologies-clusters/technologies/cyber-security.
[172] Press release and executive summary available upon request at https://www.securityforum.org/tool/the-isf-standardrmation-security/.

2.2.2. Network and Information Systems Directive

The main legislative instrument on security of *IT systems as a whole* is the Network and Information Systems Directive (NIS Directive).[173] The directive requires member states to identify the operators of essential services. The operators are then obliged to take certain measures regarding cybersecurity. It is irrelevant whether the operator is a public or private entity.[174]

LPA's qualify as operators of essential services and are subject to the directive if:

- they provide a service which is essential for the maintenance of critical societal and/or economic activities;
- the provision of that service depends on network and information systems; and
- an incident would have significant disruptive effects on the provision of that service.[175]

Annex II lists essential services for the purpose of this directive.[176]

LPA's, which do not provide the above services, are in principle not subject to the directive and not bound by it. However, as this is a minimum harmonisation directive, member states may choose to expand the scope of the directive to cover other sectors, potentially including those for which the LPA's have competence.[177]

Network and information systems are defined as:

- an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC;[178]
- any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

[173] 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, OJ L 194, 19.7.2016.

[174] Article 4 (4) of the NIS Directive:
'operator of essential services' means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2).

[175] See Article 5(2) of the NIS Directive.

[176] See Annex II to the NIS Directive.

[177] Article 3 of the NIS Directive:
'Without prejudice to Article 16(10) and to their obligations under Union law, Member States may adopt or maintain provisions with a view to achieving a higher level of security of network and information systems.'

[178] Article 2(a) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) defines 'electronic communications network' as:
'transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.'

- digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.[179]

The criterion of 'significant disruptive effects' is to be determined by national legislation, which must take into account at least the following elements:

- the number of users relying on the service provided by the entity concerned;
- the dependency of other sectors referred to in Annex II on the service provided by that entity;
- the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;
- the market share of that entity;
- the geographic spread with regard to the area that could be affected by an incident;
- the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.[180]

Member states must also consider sector-specific factors in order to determine whether an incident would have a significant disruptive effect, if appropriate.[181]

Articles 14 and 15 set out the legal regime for operators of essential services.

If identified as an operator of essential services, a LPA must take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of the network and information systems, which they use in their operations and prevent, having regard to the state of the art, and minimise the impact of incidents, in order to ensure a level of security appropriate to the risk posed as well as continuity of the services.[182]

In case of an incident, it must notify the CSIRT team or the competent authority *without due delay*.[183]

Since the deadline for implementation is May 18th 2018, the member states have not yet reported on having taken any additional measures.

2.2.3. General Data Protection Regulation (GDPR)

GDPR addresses the security requirements of *processing personal data.*

[179] Article 4(1) of the NIS Directive.
[180] Article 7(1) of the NIS Directive.
[181] Article 7(2) of the NIS Directive.
[182] Articles 14(1), 14(2) of the NIS Directive.
[183] Article 14(3) of the NIS Directive.

According to the GDPR, 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 ('integrity and confidentiality').[184]

Articles 32, 33 and 34 refer to security of personal data. They apply to COMPACT partners when they're acting as the controller or the processor.

According to Article 32, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account:

- state of the art
- the costs of implementation
- the nature, scope, context and purposes of processing
- the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The measures must include, inter alia, as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[185]

In assessing the appropriate level of security, the controller and the processor must take into account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.[186]

Compliance with those requirements can be demonstrated through adherence to an approved code of conduct or an approved certification mechanism (Articles 40 and 42 of the GDPR, respectively).[187]

The controller and the processor must ensure that any natural person acting under their authority, who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.[188]

In case of a personal data breach, the controller is required to notify both the supervisory authority and the data subject.

[184] Article 5(f) of the GDPR.
[185] Article 32(1) of the GDPR.
[186] Article 32(2) of the GDPR.
[187] Article 32(3) of the GDPR.
[188] Article 32(4) of the GDPR.

The supervisory authority must be alerted without undue delay (if feasible, not later than 72 after having become aware of the breach), unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.[189] The notification must contain at least the following information:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.[190]

If it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.[191]

The controller must document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with Article 33.[192]

The data subject must be informed without undue delay if the breach is likely to result in a high risk to the rights and freedoms of natural persons. The breach must be communicated in clear language and include at least the above information from points b), c) and d).

There is no need to inform the data subject if:

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Meeting one of the conditions is enough for the notification duty to not apply.[193]

However, the supervisory authority may require the controller to notify the data subject, if it considers the personal data breach likely to result in a high risk.[194]

[189] Article 33(1) of the GDPR.
[190] Article 33(3) of the GDPR.
[191] Article 33(4) of the GDPR.
[192] Article 33(5) of the GDPR.
[193] Article 34(2) of the GDPR.

The processor also has the duty of notification, namely it must notify the controller without undue delay after becoming aware of a personal data breach.[195]

2.2.4. Other soft law instruments

The RFC 2196 Site Security Handbook,[196] published by the Network Working Group with the Internet Engineering Taskforce, provides a general and broad overview of information security including network security, incident response, or security policies. However, it is seriously outdated as it was published in 1997.

Recommendation No. ITU-T X.1205 (04/2008),[197] issued by the International Telecommunications Union, provides a definition of cybersecurity and specifies risks to IT systems, as well as a general overview of cybersecurity technologies, organised by field.

2.3. Intellectual property rights

COMPACT is an innovation project, innovating at the technology and process level. Intellectual property (IP) rights deal with protection and exploitation of inventions. There are two types of inventions involved in the COMPACT projects, the pre-existing ('background') and resulting ones ('results'). Therefore there might be IP rights challenges regarding exploitation and dissemination of COMPACT results.

Background is defined as any data, know-how or information whatever its form or nature, tangible or intangible, including any rights such as intellectual property rights, which is: (i) held by participants prior to their accession to the action; (ii) needed for carrying out the action or for exploiting the results of the action; and (iii) identified by the participants in accordance with Article 45 of the Regulation (EU) No 1290/2013.[198]

Results are defined as any tangible or intangible output of the action, such as data, knowledge or information, that is generated in the action, whatever its form or nature, whether or not it can be protected, as well as any rights attached to it, including intellectual property rights.[199]

Additionally, all partners must take care not to breach third parties' IP rights.

---

[194] Article 34(3) of the GDPR.
[195] Article 33(2) of the GDPR.
[196] Network Working Group, Site Security Handbook, RFC 2196, available at https://tools.ietf.org/html/rfc2196.
[197] International Telecommunications Union, Recommendation No. ITU-T X.1205 (04/2008), available at http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136.
[198] Art. 1(2)(4) of the Regulation (EU) No 1290/2013.
[199] Art. 1(2)(19) of the Regulation (EU) No 1290/2013.

If applicable, the results developed will be protected as patents or copyright under EU law. Key legislation on European level dealing with IP rights are Directive 2001/29/EC on copyright and related rights in the information society,[200] Directive 2009/24/EC on the legal protection of computer programs[201] and from a processual point of view, Directive 2004/48/EC on the enforcement of intellectual property rights.[202]

Grant agreement no. 740712 also contains some rules on IP in its Section 3, entitled 'Rights and obligations related to background and results'. It defines 'results' as any (tangible or intangible) output of the action such as data, knowledge or information – whatever its form or nature, whether it can be protected or not – that is generated in the action, as well as any rights attached to it, including intellectual property rights. Grant Agreement provides for individual as well as joint ownership. Participants are required to protect the results, if feasible.

Consortium Agreement deals with IP issues in Sections 8 and 9. According to Article 8.1, results are owned by the party that they're generated by. Individual ownership is thus the principle, but there are several exceptions provided for joint ownership. Results are jointly owned when they have been generated by several parties and their contributions cannot be ascertained or if it is not possible to separate results when applying for, obtaining or maintaining their protection (i.e., most often a patent).

Access rights to background are set out in Section 9. The parties are only required to ensure access rights to the background identified in Attachment 1. The list of background can be added to at any time; however, approval of the General Assembly is necessary to remove an item from the list.

Each party is solely responsible for ensuring it doesn't knowingly breach a third part's intellectual property rights.

Although the above-mentioned legal instruments set out rights and obligations regarding IP rights, partners are nonetheless encouraged to sign individual agreements with end users of the resulting technology in order to safeguard IP rights resulting from the COMPACT project.

2.4. Liability

Liability refers to 'the state of being bound or obliged in law or justice to do, pay, or make good something'; it is also referred to as legal responsibility.[203] Liability can stem from a faulty performance of a contract – contractual liability, or from other unlawful behaviour, without a contract, which is referred to as tortious liability.

[200] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.
[201] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version), OJ L 111, 5.5.2009, p. 16–22.
[202] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004).
[203] 'liability'. Retrieved from Black's Law Dictionary, http://thelawdictionary.org/liability/

In the COMPACT project, liability issues might arise out of project activities, especially handling of personal data in studies, and the resulting COMPACT technology.

There is no harmonised liability regime as a whole on the EU-level.

However, there is a harmonised liability regime for breach of data protection requirements set down in the GDPR, which applies to both data controller and data processor. Any controller involved in processing is liable for the damage caused by processing which infringes the GDPR. A processor is liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.[204] It can be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

There is also a regime for defective product under the Directive 85/374/EEC on liability for defective products (Product Liability Directive, PLD).[205] The producer is liable for damage caused by a defect in his product.[206] A product is defined as a movable, even though it's incorporated into another movable or into an immovable. The definition explicitly includes electricity and excludes certain agricultural products.[207] Software, despite its *per se* intangibility, has a material interface and material consequences, and according to certain scholars, could as a product for the purposes of product liability directive.[208]

On individual member state level, the national legal systems determine the rules for liability. Due to extensive differences in systems, it is impossible to describe what the specific liability regimes entail. A systemic overview of different tort regimes has been compiled by the European Group on Tort Law,[209] providing an outline on the basic norms (the legal rules), general conditions of liability, such as damage and causation; bases of liability, i.e. fault-based liability, strict liability and libaility for others; defences, rules in case of multiple tortfeasors, i.e. when more than one person has committed a tort, and remedies, i.e. damages. However, there is no such overview of contractual liability.

2.5. Research ethics

Research ethics involve the application of ethical principles to scientific research projects, including the research activities of the COMPACT project. The main ethical issues in the

[204] Article 82(2) of the GDPR.
[205] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.
[206] Article 1 of the PLD.
[207] Article 2 of the PLD.
[208] Triaille, The EEC directive of July 25, 1985 on liability for defective products and its application to computer programs, Computer Law & Security Review, Volume 9, Issue 5, September–October 1993, Page 218.
[209] The European Group for Tort Law, Principles of European tort law: text and commentary, 2005, Berlin: Springer.

COMPACT project relate to use of surveillance technologies and real-time tracking, necessary in order to achieve the desired level of cybersecurity, due to the involvement of human participants in the project's research and the handling of their personal data.

COMPACT is an EU project, funded by the Horizon 2020 Framework. The Horizon 2020 Framework was established by Regulation no. 1291/2013/EU.[210] The rules applicable to participation and dissemination in Horizon 2020 are set out in Regulation 1290/2013/EU.[211]

Article 19 of Regulation 1291/2013 sets out the ethical principles with which all actors in Horizon 2020 projects need to comply. These are the principle of proportionality, the right to privacy, the right to protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the right to ensure high levels of human health protection, as well as the focus on exclusively civil application.

The rules of research ethics in the Horizon 2020 projects are further set out in the self-assessment guidelines, issued by the European Commission.[212]

The involvement of human participants in projects must be completely voluntary on their part. The participants must be able to consent freely to their participation, which requires the research organisation to provide them with information, necessary for informed consent. This is ensured by providing information sheets and informed consent forms.[213] In the COMPACT research, both will be provided.[214] As employees are considered a vulnerable group, whose consent is not entirely free, special safeguards will be provided, as explained in Section 5.1.

Similarly, informed consent must be given before personal data can be processed for research purposes. Only the personal data that are really necessary for research can be collected and processed, lest there be a risk of 'mission creep', i.e. collecting unnecessary data for unrelated, hidden purposes.[215]

Research ethics are also addressed by the COMPACT Grant Agreement no. 740712 in its Article 34.

---

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

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

[212] European Commission, Guidelines: How to complete your ethics self-assessment, July 2016, available at: http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf.

[213] European Commission, Guidelines: How to complete your ethics self-assessment, p. 7.

[214] COMPACT Grant Agreement, Part B, p. 100.

[215] European Commission, Guidelines: How to complete your ethics self-assessment, p. 17.

Section 34.1 requires the participants to carry out action in compliance with ethical standards, including the highest standards of research integrity. Project activities must have an exclusive focus on civil applications. This section also refers to the European Code for Research Integrity as an example of the source of the highest standards of research integrity. Researchers have to comply with basic ethical principles, such as honesty, reliability, objectivity, impartiality, open communication, duty of care, fairness and responsibility for future science generations.

Since participants will be tracked in the course of studies, using surveillance technology, Opinion No. 28 on Ethics of Security and Surveillance Technologies[216] and Opinion No. 26 on Ethics of Information and Communication Technologies[217] by the European Group on Ethics in Science and New Technologies must also be considered.
They both stress the need for data protection and privacy-enhancing measures, as well as consent and transparency.[218] These form an integral part of the COMPACT architecture and user studies. Privacy-enhancing techniques are one of the building blocks of privacy by design (see Section 4.3.1), while consent and transparency will be taken into account throughout the conduct of user studies, as the study participants will be notified of their rights and given relevant information about the processing of their data at all times, as explained in Section 5.

2.6. Overview of applicable legal instruments

Table 1: Overview of applicable legal instruments

Subject-matter	Main applicable legal instruments
Privacy and data protection	International law European Convention on Human Rights, Convention no. 108 of the Council of Europe on Automatic Processing of Personal Data, Code of Practice of the International Labour Organisation on protection of workers' personal data, Recommendation No. 89 (2) of the Council of Ministers of the Council of Europe on the Protection of Personal Data used for Employment Purposes.

[216] European Group on Ethics in Science and New Technologies, Opinion No. 28 - 20/05/2014 on Ethics of Security and Surveillance Technologies, available at http://bookshop.europa.eu/en/ethics-of-security-and-surveillance-technologies-pbNJAJ14028/.
[217] European Group on Ethics in Science and New Technologies Opinion No. 26 - 22/02/2012 on Ethics of information and communication technologies, available at http://bookshop.europa.eu/en/ethics-of-information-and-communication-technologies-pbNJAJ12026/.
[218] See EGE Opinion no. 26, p. 59-65 and EGE Opinion no. 28, p. 87-91.

	<u>European Union legislation</u> Treaty on the Functioning of the European Union, Charter of Fundamental Rights, General Data Protection Regulation, Directive 95/46/EC, Network and Information Systems Directive, Opinions of the Article 29 Working Party.
Security	<u>European Union legislation</u> Network and Information Systems Directive, General Data Protection Regulation. <u>Standards</u> ISO/IEC 27000-series, ISO 15408-series, TR 103 series. Network Working Group /Internet Engineering Taskforce RFC 2196 Site Security Handbook, Recommendation of the International Telecommunications Union No. ITU-T X.1205 (04/2008).
Intellectual property	Regulation 1290/2013/EU laying down the rules for participation and dissemination in 'Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)', Directive 2001/29/EC on copyright and related rights in the information society, Directive 2004/48/EC on the enforcement of intellectual property rights, Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version), COMPACT Grant Agreement no. 740712, COMPACT Consortium Agreement.
Liability	Directive 85/374/EEC on liability for defective products,

	General Data Protection Regulation, Principles of European Tort Law. National legal sources.
Research ethics	<u>European Union legislation</u> Regulation 1290/2013/EU laying down the rules for participation and dissemination in 'Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)', Regulation 1291/2013/EU of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC. <u>Opinions of the European Group on Ethics in Science and New Technologies</u> Opinion No. 28 on Ethics of Security and Surveillance Technologies, Opinion No. 26 on Ethics of Information and Communication Technologies. Grant Agreement no. 740712.

2.7. Overview of legal obligations under the GDPR

Data controller: determines the purposes and means of the processing of personal data – Art. 4(7); i.e. the why's and how's of data processing operation	Accountability principle – demonstrate compliance, Art. 5(2) Implement technical and organisational measures to comply with GDPR – Art. 24 Data protection by design and by default – Art. 25 Maintain a record of processing activities – Art. 30 Security requirements – Art. 32-34 DPIA – Art. 35, required if: - Activity on the data protection authority's list - One of the situations in 35(3) (likely) - General clause: high risk to the rights and freedoms of natural persons (likely) DPO – Art. 37, required if: - Public body (LPA's)

	- Regular and systematic monitoring of data subjects on a large scale (likely) - Processing of sensitive data or personal data relating to criminal convictions and offences (unlikely)
Data processor: carries out the processing operation on the data controller's behalf – Art. 4(8)	Sufficient guarantees to show GDPR compliance – Art. 28(1), demonstrated by: - Compliance with a code of conduct – Art. 28(4), Art. 40 - Compliance with an approved certification mechanism – Art. 28(4), Art. 42 - Case-by-case assessment Can only engage another processor if authorised by controller – Art. 28(2) Conclude an agreement with controller (processor terms) – Art. 28(3) Appoint a DPO under the same conditions as the controller – Art. 37(1)
Joint controllers: two or more controllers jointly determine the purposes and means of processing – Art. 26	Conclude an agreement – Art. 26: - Show GDPR compliance in a transparent way - Notification duties (Art. 13, 14) - Roles and relationship towards data subjects

Table 2: GDPR obligations for COMPACT partners

3. S.E.L.P. challenges in the COMPACT project

This section will define the most important legal and ethical challenges related to setting up a cyber-secure system for LPA's, by creating cyber-secure platforms and by assessing the level of cyber-knowledge through user studies.
The challenges are twofold, and relate to protection of already existing personal data that LPA's control and its proper protection in a functioning cybersecurity system, which will involve processing personal data, as well as data, gathered in user trials. Since the COMPACT project deals with LPA's, which are subject to the PSI directive, the access to public sector information presents another challenge. The information related to employees and citizens is considered personal data, unless it has been fully anonymised. Therefore, it is important to implement such anonymisation measures, which irreversibly prevent re-identification of the original data subjects (citizens and employees).[219]
As set out in Section 2, both the employees and the citizens have a right to respect for private and family life, according to the Article 8 of the ECHR, and they enjoy the safeguards of the GDPR. Due to the LPA's' cybersecurity-mandated actions, their personal data will be processed and there may be an intrusion on their privacy. Therefore, there is a potential conflict between the security and privacy or data protection requirements.

3.1. Personal data on citizens

Regarding personal data that LPA's possess on their citizens, the main challenges relate to the LPA's' obligations under the GDPR and the NIS directive. Citizens have a legitimate interest in having their personal data protected and in having control over them, but it is also in the public interest to have functioning and secure network and information systems for the provision of essential services, performed by the LPA's. While the NIS directive explicitly excludes processing of personal data from its scope, setting up a cyber-secure system under the COMPACT project may involve processing personal data, so a proper balance between the requirements of the one and of the other must be found.
Setting up a secure information network is set out as an example of legitimate interest in the GDPR.[220] However, as public authorities cannot rely on their legitimate interest for the processing of personal data in the performance of their tasks for the setting up of a secure system, they must rely on another legal grounds for data processing. As explained in Section 2.1.2.1.2, the legal grounds are either consent, compliance with security requirements or the exercise of tasks in the public interest. However, as explained in Section 4.3, citizens are unlikely to be able to freely consent to data processing.
As data controllers, COMPACT partners must meet their obligations under the GDPR, e.g. they must appoint a data protection officer, implement privacy by design, carry out a data protection impact assessment in certain circumstances.

[219] Article 29 Working Party, Opinion 06/2013 on open data and public sector information ('PSI') reuse, p. 12.
[220] Recital 49 of the GDPR.

LPA's need to comply with the GDPR before it becomes enforceable on May 25th 2018. However, not all of them are ready yet, as a survey by the Information Commissioner's Officer has shown.[221]

3.2. Personal data on employees

The concept of 'employee', who can enjoy the personal data protection, is understood broadly. The term 'employee' encompasses all situations in which there is an employment relationship, regardless of whether or not an employment contract exists.[222]

Employees of any organisation, including LPA's, can expect a reasonable amount of privacy in their workplace.[223] They must be made aware of any privacy-encroaching mechanisms that are put in place. In the COMPACT project, the employees must be notified about the existence of tracking as part of cyber-resilience programme. However, as they have a subordinate position vis-à-vis the LPA both as a public authority and their employer, they cannot consent to the intrusive measures being put in place, unless there are special safeguards. These special safeguards are explained further in this opinion.[224]

On the other hand, the LPA has legal obligations both in EU and national law to set up a cyber-secure IT system, which may involve processing employees' data.[225] A secure system is necessary in order to enable LPA's to conduct their tasks and activities in a safe and secure manner as well as provide a safe working environment for their own employees. LPA's will thus implement measures and policies, with which the employees will comply according to their contractual and statutory obligations.

Since the employees cannot reasonably refuse workplace surveillance nor consent to their data being processed, necessary safeguards and applicable principles will be defined and analysed. Specifically, the workers have the right to information and consultation within the undertaking, of which they are part, according to Article 27 of the Charter of Fundamental Rights. An employer must carry out a proportionality test before undertaking any processing, possibly as a part of the DPIA (data protection impact assessment).[226]

In all situations, an employer must consider the following before starting a processing operation: the necessity and legal grounds of the processing, whether the processing is fair to the employees, proportionate to the concerns raised, and transparent.[227]

In accordance with existing legal framework, a proper balance must be found between the interests of security and privacy. Special attention must be paid to the principle of proportionality so as to prevent the measures going beyond what is necessary to achieve the appropriate level of cybersecurity.

---

[221] https://iconewsblog.org.uk/2017/03/20/information-governance-survey/, accessed on July 27, 2017. Please note that this study only takes into account certain British local communities. Since there has been no EU-wide study yet, it is impossible to assess the general level of GDPR-readiness of local public authorities.

[222] Article 29 Working Party, Opinion 2/2017 on data processing at work, June 8 2017, WP249, p. 4.

[223] ECtHR judgment of Barbulescu v. Romania. See Footnotes 22 and 23.

[224] See Section 5.1 for studies participants, and Section 4.3.1 for the personal data already held by the LPA's.

[225] Articles 4(4) and 14 of the NIS Directive.

[226] Article 29 Working Party, Opinion 2/2017 on data processing at work, June 8 2017, WP249, p. 10 and the following.

[227] Article 29 Working Party, Opinion 2/2017 on data processing at work, June 8 2017, WP249, p. 11.

Apart from the personal data that the LPA's already control, they will also collect and process new personal data in the user studies.

Through user studies, the COMPACT project will assess the level of cyber-awareness among the workforce of specific LPA's. Using gamification and training techniques, the studies will focus on LPA employees' preparedness for a cyber-attack. Since not all the employees will participate in trials, it is important that the procedures, according to which they are chosen, are appropriate and do not exclude or include participants on a discriminatory basis. All participants must consent to their participating in the trials.

The studies will include tracking and surveillance of employees, which may constitute an interference with their private lives beyond the workplace.

Certain data on their employees that LPA's already own, such as their identification number, e-mail address, their role etc., will be used in order to determine which employees should take part in the cyber-resilience programme. This is referred to as *secondary use*. As a research project, processing for the COMPACT purposes is on principle not incompatible with the purpose limitation principle.[228]

Regarding trial participation, all participants must give their consent to it. Data that will be gathered through trials must be handled in accordance with the GDPR. Consent must be informed, and participants have to receive information sheets and consent forms before the trials start. The trials will be performed by a third party, to whom personal data must be disclosed. In this case, special attention will be paid to legal grounds for participation,[229] as there must be certain safeguards before employees can consent to such processing; as well as the principle of proportionality.[230]

3.3. Public sector information

Public sector information may also be processed in the context of setting up a cyber-security system by virtue of being held by the LPA's. Such information may concern both citizens and employees. It may be held in an anonymised, aggregated form, or it may be held as personal data. Anonymised data is not subject to the GDPR requirements. However, as perfect anonymisation is difficult to achieve,[231] a lot of public sector information may fall under the personal data regime. Such personal data must therefore be dealt with accordingly, as either employee data or citizen data.

[228] A clearer application of that principle is provided in Sections 2.1.2.1.1 and 4.3.1.
[229] Article 6(1)f of the GDPR.
[230] Article 29 Working Party, Opinion 02/2017 on data processing at work, p. 21.
[231] See Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014.

4. S.E.L.P. challenges for COMPACT technology

While the previous section outlined the challenges of the COMPACT project, this section will focus on the analysis of elements for setting up the COMPACT architecture. It will in particular focus on concepts such as privacy by design and default and security by design. Those two concepts require security and privacy to be considered in all stages of the engineering process, not only at the end but from the very beginning. All COMPACT technology will be designed in a way, which aims to comply with those two concepts.

According to Article 24 of the GDPR, the controller is responsible for implementing appropriate technical and organisational measures in order to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. It must take into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons when designing such measures, which must be reviewed and updated when necessary.[232] Such measures must also include the implementation of appropriate data protection policies, in a manner proportionate to processing activities.[233]
It is possible to demonstrate compliance with those requirements by adhering to an approved code of conduct, referred to in Article 40 of the GDPR, or approved certification mechanisms, according to Article 42.[234] The European Commission has not yet given general EU-wide validity to any certified code of conduct pursuant to Article 40(9), however there might be approved codes on national levels.

4.1. Data minimisation

The principle of data minimisation is defined in Article 5 of the GDPR as a requirement that the personal data be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[235] There is not much information available on what specifically this means in practice, but the consent among various authorities seems to be that only directly relevant and necessary data are allowed to be processed, and kept no longer than necessary to achieve a specific goal.[236]

The specific goals in the COMPACT context are related to the implementation of cyber-security enhancing technology. Each individual tool is not necessarily a specific goal of its own – rather, the notion of specificity refers to defining purpose(s) in a manner that is sufficiently detailed to define which technology needs to be implemented, and how, in order

[232] Article 24(1) of the GDPR.
[233] Article 24(2) of the GDPR.
[234] Article 24(3) of the GDPR.
[235] Article 5(1)c of the GDPR.
[236] See European Data Supervisory Authority, 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/

to reach those purposes.[237] Tools that pursue a similar goal can therefore be considered to fall within the same 'specific purpose'. Accordingly, the adequacy, necessity and relevance of personal data will be determined for each such specific purpose.

Regarding COMPACT technology, data minimisation is specifically set out as one of the most important principles which should be adhered to during the processes of design and implementation. This is important for both citizens and employees as data subjects.

There are three building blocks in the data minimisation principle: adequacy, relevance and necessity.[238]

Adequacy is assessed based on the context of processing and on the data subjects group to which the data refer. However, special care should be taken that data are not insufficient, or of poor quality. If they are poor quality, then they are no use and cannot be adequate. An example given by the ICO is low-resolution videos in a CCTV surveillance system[239] - such data do not contribute anything towards the goal of their collection and are not considered adequate.

The context is processing for the needs of setting up cyber-security. Since the technology has not yet been designed, specific requirements cannot yet be defined, but they may include the implementation of encryption and other PET's (see Section 4.3.1). In this case, adequacy refers to implementing PET's to cover enough data to ensure a smooth and working cyber-security system.

The two large groups of data subjects are employees and citizens. The adequacy of data should be assessed separately for each, and if necessary the groups should be divided into smaller sub-groups, for whom a new, separate adequacy assessment must be carried out.

Relevance means that data, which are not linked to the goal of the processing, must not be processed. In COMPACT terms, data which are irrelevant for cyber-security and do not contribute anything to it, should not be integrated in the resulting technology, for example data relating to personal and family lives of employees.

Necessity is similar to relevance in the sense that data, superfluous to the goal, should not be processed. If the data do not contribute towards the goal, and if there is a less invasive measure possible, i.e. not including those data in the processing operation, then they should not be processed. If data are no longer necessary for a specific purpose, they must be erased.[240]

An example are personal data, already available publically on the LPA's' websites, such as the name of the employee, their e-mail address and/or their position within the organisation – they might not need to be included in the cyber-security implementation due to their

[237] See Article 29 Working Party, Opinion 03/2013 on purpose limitation, p. 12. While the opinion deals with purpose limitation rather than data minimisation, the recommendations apply by analogy to the latter as well, due to the identical wording in Article 5, which refers to 'specific purposes' in both cases.
[238] See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-3-adequacy/
[239] https://ico.org.uk/for-organisations/guide-to-data-protection/principle-3-adequacy/
[240] Article 17(1)a of the GDPR.

already being publically available. Another example is, if the location needs to be determined, it can be done through GPS positions – but since a less intrusive option exists, i.e. determining location through wifi connection, then the latter must be used, due to the necessity requirement. If the inclusion of these data in the technology does not contribute towards its implementation, then they should not be included.

Data minimisation is one of the building blocks of privacy by design and by default, and it also contributes to overall security of data subjects' private lives, because in the case of a security incident, fewer data can leak out.

Data that do not meet the criteria of data minimisation, must not be kept and must be erased.

4.2. Data subjects' rights

Section 2.1.2.1.3 set out the rights a data subject has according to the GDPR. Regarding COMPACT technology, the most important rights will be the right to information,[241] the right of access,[242] the right to rectification[243] and the right to erasure.[244]

The right to information means that the data subject has the right to be informed about the means and purposes of processing, the possible exercise of GDPR rights and certain other information.[245]

The right to access means that the data subject can obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed. If they are indeed being processed, certain information must be provided.[246]

The right to information refers to being informed at the time of the obtaining of the personal data, whereas the right to access does not have a specific timeset, and can be exercised by the data subject at any time.

The data subjects must be informed about:

- the identity and the contact details of the controller, i.e. the COMPACT partner, which determines the means and purposes of data processing,
- the contact details of the data protection officer, which the LPA's are required to appoint (see Section 2.1.2.1.4),
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing,
- the potential recipients or categories of potential recipients of the personal data,

[241] Articles 13 and 14 of the GDPR.
[242] Article 15 of the GDPR.
[243] Article 16 of the GDPR.
[244] Article 17 of the GDPR.
[245] Articles 13 and 14 of the GDPR.
[246] Article 15 of the GDPR.

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period,
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability,
- the right to lodge a complaint with a supervisory authority.[247]

Since the COMPACT cyber-security will involve two types of data subjects, it might be a good practice to provide employees and citizens with separate information, because different personal data may be processed regarding each group.

The right to rectification gives data subjects the right to obtain from the data controller without undue delay the rectification of inaccurate personal data concerning them. The data subject also has the right to have incomplete personal data completed, including by means of providing a supplementary statement.[248] In the COMPACT project activities, both employees and citizens may want to rectify their personal data. There are no exceptions from this rule, the data controllers must always rectify personal data but the implementation of cyber-security as the purpose of processing must be taken into account when correcting.

Regarding the right to have their personal data erased – or 'the right to be forgotten',[249] data subjects can obtain the erasure of their data if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, if the personal data have been unlawfully processed, or if the personal data have to be erased for compliance with a legal obligation in EU or national law to which the data controller is subject.
This also applies to data that has been made public, for example the employees' names and positions within their LPA's, which is sometimes put on their websites. In that case, the data controller following the request for deletion, has to inform the controller(s)[250] of the request, taking into account the state of the art and the costs of implementation.
An example of personal data, which have to be erased because they are no longer necessary, might be keeping data on residents, who have moved out of the community, or former employees' personal data.

If the data subject has requested to have their personal data rectified or erased, the LPA must not process the personal data while the rectification or deletion is being carried out,

[247] Article 13(1) and (2) of the GDPR. Articles 14 and 15 require the disclosure of the same information, but in different circumstances. See Section 2.1.2.1.3.
[248] Article 16 of the GDPR.
[249] Article 17 of the GDPR.
[250] The controller in this scenario is the entity running the platform on which the data has been made public, e.g. the website or physical medium.

unless it does so with the data subject's consent or to protect the interests of third parties.[251]

The above rights only apply to personal data. As soon as the personal data have been completely and irreversibly anonymised, the rights do not apply any more. However, as the process of implementing cyber-security involves the processing of personal data, the GDPR, and the rights it grants, will apply throughout the process of anonymisation. GDPR will not apply as soon as irreversible anonymisation is complete.

4.3. Data protection by design and by default

Data protection by design and privacy by default are among the general obligations of the controller, codified in the GDPR. They contribute to the principle of accountability, under which the data controller must be able to show its compliance with the requirements of the GDPR. Measures undertaken should be in line with the current state of the art and adopted with the aim of complying with the data controllers' obligations.[252]

Article 25(1), which sets out the **data protection by design** obligation, requires that data protection be included from the onset of the designing of systems, rather than as a later addition. The data controller must implement appropriate technical and organisational measures (e.g. pseudonymisation) in order to implement the data protection principles such as data minimisation (only processing data that is necessary for the purpose). Data minimisation applies to amount of data, its period of storage and its accessibility. In particular, it must be ensured that by default personal data are not made accessible to an indefinite number of people.

Article 25(2), which sets out the **data protection by default** obligation, requires the controller to implement appropriate technical and organisational measures, which ensure that by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, those measures must ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

The specific obligation for the data controller is therefore to adopt measures, which implement data protection principles: data minimisation, purpose limitation, storage limitation and integrity and confidentiality.

GDPR suggests the adoption of the following measures, which contribute to privacy by design: minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing and enabling the controller to create and improve security features.[253]

[251] Article 18 of the GDPR.
[252] See Recital 78 of the GDPR.
[253] Recital 78 of the GDPR.

Data protection by design is conceptually similar to the idea of privacy by design – the difference being that they focus on data protection and privacy, respectively. The Court of Justice of the European Union seems to treat the right to privacy and the right to data protection as two sides of the same coin,[254] so it is reasonable to assume that the tenets of privacy by design also apply to Article 25.

A privacy-by-design compliant system follows three privacy-specific protection goals: *unlinkability, transparency,* and *intervenability*, and three security-specific goals: *confidentiality, integrity,* and *availability* (also referred to as CIA).[255]

Privacy by design is based on the following seven principles: proactive, not reactive; privacy as the default setting, privacy embedded into design, full functionality (full-sum instead of zero-sum), end-to-end security, visibility and transparency, respect for user privacy.[256]

Proactivity means anticipating privacy risks and acting before they happen, rather than remedying risks that have actually materialised.

With **privacy as the default setting**, an individual need not do anything to protect their own privacy and personal data, as they are already protected automatically.

Privacy embedded into an IT system means that it is an essential component of the system, as opposed to a later addition. It is integral to the system without diminishing its functionality.

Full functionality repudiates the false dichotomy of privacy versus security, and encourages implementing all legitimate interests and objectives in a way that avoids unnecessary trade-offs.

End-to-end security builds upon privacy embedded into the system, emphasizing the importance of security for privacy. It means that data is securely retained from the first collection onwards throughout the entire cycle of the operation.

According to **visibility and transparency** principle, the business practice or technology involved is subject to an independent verification, and its components and operations must remain visible and transparent to the users and providers.

User-centric privacy-by-design respects users' privacy requires the controller of the system to keep the interests of the data subjects foremost in their considerations, providing various privacy-friendly measures, such as appropriate notice, privacy defaults and user-friendly options.[257]

[254] See judgments of the Court of Justice of the European Union, Joined Cases C-468/10 and C-469/10, ASNEF and FECEMD v. Administración del Estado, 24 November 2011, para. 42; and Joined Cases C‑92/09 and C‑93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, para. 52. The Court deals with them together, without clearly delineating one right from another.

[255] ENISA, Privacy and Data Protection by Design – from policy to engineering, December 2014, p. 12.

[256] The seven principles were originally developed by dr. Ann Cavoukian in the early 2000's. See Privacy by Design, The 7 Foundational Principles, 2011, Information and Privacy Commissioner of Ontario, available at https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[257] Cavoukian, Ann. Privacy by Design, The 7 Foundational Principles, 2011, p. 2, available at https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

> Privacy by design consists of two main elements: incorporating substantive privacy protections into an organisation's practice and keeping up comprehensive data management procedures during the life cycle of a service or product.[258]

The key is therefore to focus on both legal compliance and on risks from computer enginering point-of-view. It is especially important that privacy by design is not understood as solely an IT solution to the privacy risks, but also in a processual manner, encompassing compliance, computer engineering, business and organisational processes.[259]

4.3.1. Implementation of privacy-enhancing techniques

The incorporation of privacy-enhancing techniques (PET's) into the technology minimises the privacy risks to individuals. Through their development and integration, it is ensured that privacy is considered through the entire life-cycle of a system.[260]

Typical PET's include measures such as communications anonymisation, right to access to personal data, authentication and pseudonymity. An especially important PET is anonymisation, as anonymised data falls outside the scope of the GDPR, according to its Recital 26:

'The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.'

There is no prescribed standard of anonymisation in the EU legislation, nor a specifically prescribed technique.

The state of anonymisation must be as final and as irreversible as erasure, [261] which might be difficult given that computational power has increased and re-identification is possible despite previous anonymisation. Potential identifiability depends on specific circumstances analysis – what are the costs of re-identification, which means does the controller have at its disposal and how reasonably likely it is to employ them. If there is no potential linkability between data in a dataset or in different datasets, then the data is considered anonymised and GDPR does not apply any more.[262]

---

[258] Regulating privacy by design.(privacy enhancing technologies)(Technology: Transforming the Regulatory Endeavor), Rubinstein, Ira S., Berkeley Technology Law Journal, Summer, 2011, Vol.26(3), p. 1411.

[259] Tsormpatzoudi, Pagona; Berendt, Bettina; Coudert, Fanny, Privacy by design: From research and policy to practice – the challenge of multi-disciplinarity, in: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2016, Vol.9484, p. 203.

[260] ENISA, Privacy and Data Protection by Design – from policy to engineering, December 2014, p. 11.

[261] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, Adopted on 10 April 2014, p. 6. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[262] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, Adopted on 10 April 2014, p. 8-9.

PET's are essential for setting up a cyber-secure system. However, as their implementation is a data processing operation, it must also meet the requirements of the GDPR.

The integration of PET's must be in accordance with the principles of data processing, set out in Article 5 of the GDPR.

First, it must be done *lawfully, fairly and in a transparent manner* in relation to the data subject. Legal grounds for implementation are discussed below.

According to the *purpose limitation principle*, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Processing for research purposes is not considered incompatible with the original purposes, which are either in the context of the employment or collection of citizens' data carried out as part of the LPA's' public tasks.

Therefore, the personal data which is already held by the LPA's can be processed without the need for new consent, as long as it is done for research purposes.

The notion of 'research' is broad, and it encompasses technological development and applied research such as the one in the COMPACT project.[263]

Data minimisation principle requires that the processing of personal data be adequate, relevant and limited to what is necessary in order to implement PET's. Personal data that do not meet these criteria cannot be processed. This principle and its importance in the COMPACT project are further explained in Section 4.1.

Personal data must be *accurate and kept up to date*. If data are inaccurate, every reasonable step must be taken to ensure that they are erased or rectified without delay, according to the accuracy principle. Both data pre-dating the PET implementation as well as post-implementation must be accurate. In case of irreversible anonymisation, the data is not considered personal data anymore, and GDPR does not require them to be erased or rectified in case of inaccuracy, although it may be in the data controller's interest to do so.

According to *storage limitation principle*, personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of PET implementation. It may be stored for longer periods only if it will be processed for scientific research purposes. While this exception applies to further user studies in the COMPACT project, it cannot be useful after the implementation of the PET's. Personal data must therefore be changed into a form, which does not permit identification, as soon as the PET's have been implemented.

Finally, according to the *integrity and confidentiality principle*, 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. *In concreto*, this means that during

[263] See the second sentence of Recital 159 of the GDPR: For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.

the incorporation of the PET's data safety must be considered not only as the ultimate goal but also as a means to that goal.

PET implementation is *lawful* if it based on any of the legal grounds identified in Section 2.1.2.1. Concurrent legal grounds are also possible. They are either consent[264] or a legal obligation under EU or national law,[265] or the exercise of tasks in public interest.[266]

Consent as legal grounds is unlikely.
LPA's are in a position of authority over both employees and citizens whose data will be processed in order to implement PET's. While this weakens the 'free' in freely given consent, the latter is still possible if there are sufficient guarantees. If a meaningful alternative without additional costs is possible, then consent is still free.[267] Working Party gives some example when a meaningful alternative is not possible: if the alternative means extra costs for the data subject, such as having to pay extra to have a non-digitised service, or if refusal to submit to a privacy invasion causes suspicion on the authorities' part, such as refusing to submit to a body scan, or if by not consenting, certain services are denied, as in the case of e-ID cards.
Regarding PET implementation, consent as legal grounds is thus not possible, since citizens do not have a meaningful alternative at their disposal – if they do not consent to their personal data being processed for security purposes, such a system cannot be set up, as it needs to be comprehensive in order to be functional.

Instead, legal grounds stem from a legal obligation.
The integration of PET's is a part of a wider obligation to implement privacy-by-design into an IT system.[268] Therefore, it is a legal obligation stemming from EU law, which meets the criterion of Article 6(1)c of the GDPR.
Article 6(3) of the GDPR further specifies the criteria that legislation, from which the obligations stem, must meet. Specifically, it must set out the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing. It must also be proportionate to the goal pursued.
While the GDPR obviously meets its own criteria, they are nonetheless relevant in case the processing obligation (i.e. implementing PET's) were to stem from another EU or national legal act. If so, only the legislation meeting such criteria could be considered valid legal grounds for data processing.

[264] Article 6(1)a of the GDPR.
[265] Article 6(1)c of the GDPR.
[266] Article 6(1)e of the GDPR.
[267] Article 29 Working Party, Opinion 15/2011 on the definition of consent, Adopted on 13 July 2011, p. 14-15.
[268] The sole implementation of a few specific PET's does not achieve the overall goals of privacy-by-design as an overarching privacy-friendly measure. See ENISA, Privacy and Data Protection by Design – from policy to engineering, December 2014, p. 9.

Additional legal grounds for PET implementation is carrying out a task in the public interest or in the exercise of official authority vested in the controller.[269] Making data held by LPA's more secure by implementing PET's is definitely in the public interest, and it is a basis for carrying out other tasks, such as provision of water or health services, as well as the traditional administrative tasks. When implementing PET's on the basis of Article 6(1)e, the data controller must also take into account:

- The link between the original purpose for which the data have been collected and the implementation of PET's,
- The context of the original collection and the relationship between the LPA and the employees or citizens,
- Whether sensitive data, or data related to criminal convictions and offences are being processed,
- The possible consequences of the intended further processing for employees and citizens as data subjects,
- The existence of appropriate safeguards, which may include encryption or pseudonymisation.

Another legal grounds is implementing PET's as a part of the LPA's' legitimate interests, as set out in Article 6(1)f of the GDPR and Recital 49. While this alinea does not apply to LPA's' processing personal data in the performance of their tasks, it can be said that a public organisation orders its internal functioning the same way that a private organisation does.[270] If the PET implementation is done on this basis, then the following requirements must also be met:

- Processing must be necessary for achieving those legitimate interests,
- Legitimate interests at stake are either those pursued by the controller or the third party, the LPA being the third party unless they are acting as the data controller,
- The legitimate interests of PET implementation must be overridden by the interests or fundamental rights and freedoms of the data subject, especially if the data subject is a child.

The necessity of processing refers to there being no measure which would be less intrusive for the data subjects' privacy.

Concurrent legal grounds are possible under EU law, as long as they are used in the right context.[271] Implementing PET's as a way of ensuring privacy by design seems to be the right context for all applicable legal grounds.

[269] Article 6(1)e of the GDPR.
[270] See e.g. Lane, Jan-Erik. New public management, London : Routledge, 2000.
[271] Article 29 Working Party, Opinion 15/2011 on the definition of consent, Adopted on 13 July 2011, p. 8.

4.3.2. Data protection impact assessment

A **data protection impact assessment/privacy impact assessment** (DPIA/PIA) is one of the starting points for the data controllers to apply the requirements of privacy by design to the actual technology.[272] A DPIA is carried out as a part of the design phase. It is meant to identify the stakeholders (and consult with them), the risks, solutions and recommendations, implement those recommendations as well as provide for review, audit and accountability measures.[273]
The DPIA assesses the impact of the envisaged processing operations on the protection of personal data for a single operation or a set of similar processing operations that present similar high risks.
Carrying out a DPIA is required in three situations:

(1) The data controller is explicitly required to do so by the GDPR in the following cases:

   a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

   b. processing on a large scale 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

   c. a systematic monitoring of a publicly accessible area on a large scale.[274]

(2) If the processing activity is on the list, published by the national supervisory authority.[275]

(3) If the processing is likely to result in a high risk to the rights and freedoms of natural persons, especially if new technologies are used.[276]

The DPIA template has already been provided in the Deliverable 1.2 ('S.E.L.P. Management v1'). It sets out risks, defined as 'high risks' for the purposes of the DPIA, as identified by the Article 29 Working Party;[277] generally, if at least two risks are met, then the LPA as the data controller is required to carry out a DPIA.
While defining specific risks that may occur throughout the duration of the COMPACT project is within the remit of the project partners, the most likely risks to materialise that can be defined at this stage are the following ones: systematic monitoring, processing of

[272] See Cavoukian, Ann. Privacy by design in law, practice and policy, 2011, p. 15, available at http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf
and ENISA, Privacy and Data protection by design, 2014, p. 12 and the following.
[273] ENISA, Privacy and Data protection by design, 2014, p. 12.
[274] Article 35(3) of the GDPR.
[275] Article 35(4) of the GDPR.
[276] Article 35(1) of the GDPR.
[277] 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, pp. 7-9. Available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

sensitive personal data as defined in Article 9 of the GDPR, and processing of data of vulnerable groups, especially employees.

The obligations of a data controller, if at least two risks are likely to materialise, are therefore the following:

- First, it must carry out a DPIA, according to the methodology, set out in the Deliverable 1.2 ('S.E.L.P. Management v1'). It must periodically review the DPIA and the processing it assesses, at least when there is a change of the risk posed by processing the operation.
- It must document the decision it takes with regards to the DPIA.
- It must inform the competent authority if required to do so.[278]

The data controller is also required to notify the competent supervisory authority if the DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate such a risk.[279] If the supervisory authority considers such processing to be a potential infringement of the GDPR, especially if the controller has insufficiently identified or mitigated the risk, then the authority will provide written advice. It may also act according to Article 58 of the GDPR, which grants it investigative, corrective, authorisation and advisory powers.

According to Article 35(7), a DPIA must contain at least the following:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The contents of a DPIA are further specified in the DPIA Guidelines: [280]

1. <u>Systematic description</u>

Data controllers must define and take into account the *nature, scope, context and purpose* of processing, according to Recital 90 of the GDPR; they all refer to setting up a

[278] 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, p.21

[279] Article 36(1) of the GDPR.

[280] This section is wholly based on: Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA), p. 21.

cyber-secure system within an LPA. The description of the processing operation must be functional.
Next, it must describe which personal data will be processed in this operation. Since the COMPACT architecture will encompass the whole IT systems of LPA's, this will mean all personal data stored on LPA's' servers, such as e-mail addresses, names, employees' positions; as well as all the personal data regarding citizens. It must also define the recipients of those data, i.e. the partners who will be developing the cyber-security system, as well as the duration for which they will be stored, which according to the Grant Agreement, must not be longer than 6 months after the end of the project.
Another requirement is identification of the assets, on which personal data rely, such as software, hardware, networks, people, paper or paper transmission channels.
Finally, this section must take into account potential compliance with approved codes of conduct.

2. Proportionality and necessity

When assessing proportionality and necessity according to Article 35(7)b and Recital 90, the data controller must take into account the following: on the one hand, measures contributing to the proportionality and the necessity of the processing, based on the principles of data processing, and on the other hand, measures contributing to the rights of the data subject.
The principles that must be taken into account, are specified, explicit and legitimate purpose; lawfulness of processing, data minimisation and storage limitation.
Measures must contribute to rights such as the right to be informed according to Articles 12, 13 and 14 of the GDPR, the right of access and portability, the right to rectify, erase, object to and restrict processing. They must also include the definition of recipient(s) of personal data, and processor, if applicable. In case of transfer of data to third countries, they must include certain safeguards. Prior consultation with the competent authority according to Article 36 of the GDPR must also be considered.

3. Risk management

Risk management section of a DPIA must address the risks to the rights and freedoms of data subjects, specifically it must define the origin, nature, particularity and severity of the risks. For risks, such as *illegitimate access, undesired modification, and disappearance of data*, it must, from the perspective of the data subjects, take into account the risk sources, potential impact on the rights and freedoms of natural persons, potential threats that could lead to such risks, as well as their likelihood and severity.
It must also determine measures, envisaged to treat those risks.

4. Involvement of interested parties

In order to protect legitimate interests of interested parties, the data controller must seek the advice of the data protection officer when carrying out the DPIA, as well as seek the views of data subjects or their representatives, if appropriate. This means consulting the representatives of employees as well as citizens. Such consultation is inappropriate if it

harms the protection of commercial or public interests or the security of processing operations.[281]

A single DPIA may address a set of similar processing operations that present similar high risks. According to Recital 92 of the GDPR, this is the case for public authorities when setting up an across-the-board platform, especially if it is more reasonable and economical to carry out a single project instead of partial DPIA's. However, if during the implementation of the COMPACT architecture risks to employees and risks to citizens prove to be too diverse, then the processing operations are not similar any more, and two separate DPIA's must be carried out.

4.4. Data protection officer

As a public authority, LPA's are required to appoint a data protection officer (DPO) according to Article 37(1)a.

An appropriate DPO is one with a good level of expertise, which depends on the sensitivity and amount of the data processed and the complexity of the processing operation. He or she must have expert knowledge of EU data protection laws, as well as the basic tenets of the processing operation. Since LPA is a public organisation, the DPO must also have a 'sound knowledge of the administrative rules and procedures of the organisation'.[282] He or she may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.[283]

The appointed DPO must be independent from the LPA. This means the DPO must not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing their tasks.[284] This is a requirement for both internal DPO's as well as in the case of outsourcing the task.[285] A DPO is autonomous in carrying out their tasks, but that does not mean they have decision-making powers beyond Article 39, i.e. giving advice on data processing, monitoring compliance with the GDPR, advising on the implementation of the DPIA, cooperating with the supervisory authority, and act as the main contact point for prior consultation under Article 36.

If the DPO disagrees with the controller's activities, then he or she may object to them, and must not be dismissed on the basis of such disagreement. Neither can they be subject to any sort of direct or indirect penalties resulting from the conduct of their work. The Article 29 Working Party recommends that a DPO only be dismissed for gross misconduct, such as theft or work harassment.[286]

[281] Article 35(9) of the GDPR.
[282] Article 29 Working Party, Guidelines on data protection officers (DPO), WP243, 13/12/2016, p. 11. Available at http://ec.europa.eu/newsroom/document.cfm?doc_id=43823.
[283] Article 37(6) of the GDPR.
[284] Article 38(3) of the GDPR.
[285] Article 29 Working Party, Guidelines on data protection officers (DPO), WP243, 13/12/2016, p. 14.
[286] Article 29 Working Party, Guidelines on data protection officers (DPO), WP243, 13/12/2016, p. 15.

Additionally, while a DPO is allowed to carry out other tasks, there must not be any conflicting interests between such activities.[287] This could interfere with the DPO's independent functioning, especially if he or she were also the person determining the means and purposes of processing. This is an issue especially in smaller LPA's, which might not have enough personnel to designate separate roles. A solution could be to outsource the role of a DPO to an external consultant or consultancy company. Generally, a top administrative position and the position of a DPO carry a conflict of interest between themselves. Guidelines on data protection officers (DPO)[288] cites typical corporate roles, such as CEO, CFO, head of IT, marketing director etc. On LPA level, those are the mayor, heads of relevant departments and similar positions. Therefore, the DPO cannot be chosen from among these positions.

While a DPO monitors the compliance, the overall responsibility to comply with the GDPR remains with the data controller, or its processor, according to the accountability principle.[289]

The contact details of the DPO must be published and notified to the supervisory authority[290] in order to ensure that the DPO may be contacted confidentially and discreetly by both data subjects and the authorities. The Article 29 Working Party opinion also recommends informing the workforce about the DPO's name and contact details as a good practice.[291]

4.5. Security by design

Security by design means taking into account security considerations from the very beginning of the engineering process.
According to Article 24 of the GDPR, the data controller is required to implement appropriate technical and organisational measures to ensure and to demonstrate that processing is performed in a GDPR-compliant manner. One of those are security measures, which have to be implemented according to Article 32, as described in Section 2.2.3. They contribute to confidentiality, integrity and availability as security-specific goals of an IT system.[292]

Privacy and security by design must not be seen as mutually exclusive. In fact, they both contribute to the same goal: a fully-functioning cyber-security system that ensures data confidentiality and security while not encroaching on the employees' private lives more than is necessary.

[287] Article 38(6).
[288] Article 29 Working Party, Guidelines on data protection officers (DPO), WP243, 13/12/2016, p. 16.
[289] Article 5(2) of the GDPR.
[290] Article 37(7) of the GDPR.
[291] Article 29 Working Party, Guidelines on data protection officers (DPO), WP243, 13/12/2016, p.13.
[292] ENISA, Privacy and Data protection by design, 2014, p. 16, available at https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

5. S.E.L.P. challenges for psychological studies and trials

This section will set out the legal requirements for involving human participants in the COMPACT trials and studies. It will focus on the legal requirements for user studies on how the LPA personnel understand and behave regarding cyber-security. These trials will be carried out in accordance with Task 2.1, 'Conduction of behavioural studies', using advanced social scientific methods. The studies present two types of challenges, both of which relate to privacy in the workplace: [293]

1. Challenges related to the involvement of human participants, such as consent, recruitment process, HR data,
2. Challenges related to protection of personal data during and after the studies.

At least two partners will carry out the trials. Each processing activity, regarding the same personal data, will be a joint effort between partners, either as joint controllership or a data controller/data processor relationship. What the actual roles will be, will become clear later in the project. It will depend on whether the parties will determine the means and purposes of processing jointly, together; or if one of the parties will process data on behalf of the other. In the former case, that is a case of joint controllership, in the latter instance, one of the partners will act as the data controller and the other will be its processor.

In case of **joint controllership**, the partners will respectively jointly the purposes and means of data processing. Therefore, the two parties must abide by the GDPR requirements for joint controllership, i.e. conclude an arrangement, which will set out their relationship and respective roles vis-à-vis the study participants and demonstrate GDPR compliance. Data subjects may exercise their rights against each controller, regardless of their inner arrangements.[294]

In particular, the arrangement must show compliance with notification duties of Articles 13 and 14. Participants must be provided with the following information:

- the identity and the contact details of the controller,
- the contact details of the data protection officer of the LPA,
- that the personal data will be processed in order to assess the level of cyber-knowledge, and that the processing is based on consent,
- potential recipients or categories of recipients of the personal data,
- that the data will be stored throughout the duration of the project, and at most six months after it has ended, after which it will be erased using state of the art deletion techniques,

[293] This section is based on European Commission, H2020 – Guidance: How to complete your ethics self-assessment, Version 5.2, 12 July 2016, section Human beings, unless specifically stated otherwise.
[294] See Section 2.1.2.1.5.

- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability,
- that they have the right to withdraw consent at any time and that withdrawal does not affect the lawfulness of prior processing,
- the right to lodge a complaint with a supervisory authority,
- the existence of automated decision-making with regards to cyber-security, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[295]

This information has to be provided at the right time.
If personal data have been obtained from the participant, then he or she has to be notified at the same time that the data are obtained. If the personal data have been obtained elsewhere, for example from the HR department directly, then the participant has to be notified at the latest a month after the obtaining of such data.

In the case of **data controller/data processor** relationship, one party determines the means and purposes of data processing on its own (controller), while the other party processes the personal data on the former's behalf (processor). According to the GDPR, the parties must then conclude an agreement,[296] so-called processor terms, as described above in Section 2.1.2.1.8. Processor terms must stipulate, in particular, that the processor:

- processes the personal data only on documented instructions from the controller,
- ensures that persons authorised to process the personal data within the processor's internal organisation have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality,
- takes all required security measures under Article 32,
- does not engage another processor without the authorisation of the controller, and only if sufficient guarantees are put in place,
- assists the controller by appropriate technical and organisational measures, insofar as this is possible, taking into account the nature of the processing, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights (the right to information,[297] the right of access,[298] the right to rectification,[299] the right to erasure,[300] the right to

[295] Articles 13(1) and 14(1), 13(2) and 14(2) of the GDPR.
[296] Article 28(3) of the GDPR.
[297] Articles 13 and 14 of the GDPR.
[298] Article 15 of the GDPR.
[299] Article 16 of the GDPR.
[300] Article 17 of the GDPR.

restriction of processing,[301] the right to data portability,[302] the right to object[303]),

- assists the controller in ensuring compliance with the obligations regarding security of data processing and data protection impact assessment, taking into account the nature of processing and the information available to the processor,
- at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data,
- 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. The processor must immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

5.1. Participation in the trials

Recruitment details have already been set out in the Annex to the Grant Agreement, Section 5. At this stage it must be repeated that only those employees who actively consent to participation can be invited to take part in the user studies. Consent must be a positive action; passive behaviour does not qualify as consent.[304] Participants are recruited based on personal data, already held by the LPA's' HR departments, such as name, address, position within the LPA etc.

These data were originally collected by LPA's for a different purpose than involvement in study trials. Nonetheless, there is no need to obtain the employees' consent for re-use of these data, because the COMPACT project is a research project in the sense of Article 5(1)b of the GDPR.

By signing the Informed Consent Sheet,[305] employees consent to participate in trials, and to their personal data being processed for research purposes.[306]

Prior to involving human participants in trials, their consent must be obtained. Their consent must be informed and freely given. Informed consent is ensured by providing the trial participants with detailed information sheets and informed consent forms.

[301] Article 18 of the GDPR.
[302] Article 20 of the GDPR.
[303] Articles 21 and 22 of the GDPR.
[304] Article 29 Working Party, Opinion 2/2017 on data processing at work, p. 6-7.
[305] See the COMPACT Grant Agreement, p. 99-100.
[306] There is, legally speaking, a difference between consenting to trial participation, and consenting to the processing of personal data, due to different legal grounds. The legal basis for the latter comes from the GDPR, while the former stems from the respect for human dignity and the individual's right to self-determination. Nevertheless, for the purposes of this report they will be treated identically, as outside the legal academia there is no need for different treatment. In practice, they are usually treated the same way, i.e. one act of consent covers both trial participation and data processing.

According to a recent opinion of the Article 29 Working Party, employees cannot freely consent to the processing of their personal data in the workplace due to their subordinate position vis-à-vis the employer.[307] Nonetheless, their inclusion in the trials is possible, but certain mitigation measures against coerced consent must be put in place, such as detailed description of the type of vulnerability, details of recruitment, inclusion and exclusion criteria and informed consent procedures.
Those measures ensure the employees' fully informed understanding of the implications of participation.

The vulnerability in COMPACT derives from the employer's position of authority. While the existence of an employment relationship does not render consent fully impossible, it may be difficult for an employee to refuse participation, especially if such participation is presented as a part of employment obligations, which may affect work performance. Such pressure includes, inter alia, any kind of reward for participation, both monetary and non-monetary, and vice versa for non-participation, including more severe sanctions such as dismissal.
Concerns can be alleviated through anonymous collection of data. Additionally, opt-out must remain an option even after the studies have started, should the studies prove to be too intrusive, especially in the case of conduct of interviews.
Since the trials will not be carried out by the LPA's themselves, the likelihood of pressure in that regard is small. Nonetheless, the research purposes of the trials should be explained by a person, who does not hold a position of authority over them.[308]
Inclusion and exclusion criteria refer to criteria, used by the LPA's' HR departments to identify potential candidates. They must be described in detail so as to avoid possible discrimination.

The LPA's' human resources departments will monitor the employers' potential pressure on their employees. In case of breach, i.e. undue pressure on employees, the consent will be considered invalid from the moment of the breach, and the employees' data can no longer be collected.

5.2. Personal data in the user studies

This subsection will set out the legal requirements for the handling of personal data, processed in the user studies. Additionally, management techniques of data handling will be addressed in Deliverable 2.6 'Data Management Plan', and its subsequent updates, due to the open data requirements of Horizon 2020 projects.

The processing of study trials data must abide by the basic principles of data processing as set out in the GDPR, as described above in Section 2.1.2.1. However, as the final results will be stored in an anonymised aggregated form, they will not be considered personal data any

[307] Article 29 Working Party, Opinion 2/2017 on data processing at work, p. 6-7.
[308] See the Guidelines of Institutional Review Board for Social & Behavioural Studies of the University of Virginia, available at
http://www.virginia.edu/vpr/irb/sbs/resources_guide_participants_vuln_coerce_employee.html

longer, and the GDPR will not apply. The legal requirements therefore only apply to personal data, collected through user studies *until it has been anonymised*, and throughout the process of anonymisation, in a manner described in Section 4.3.1.

Personal data will be collected through tracking and surveillance, as well as through interviews and online surveys of trial participants. Systematic monitoring of employees as a vulnerable group meets two of the criteria for 'high risk' as defined in Article 35 of the GDPR, thus there is a need for the data controller to carry out a data protection impact assessment. In order to avoid repetition of Section 4.3.2, which describes in detail the structure and requirements for a GDPR-compliant DPIA, this subsection will briefly set out the requirements for user studies.

1. Systematic description of the processing activity

   The scope, nature and context of the processing refer to assessing the level of cyber-awareness within the workforce, by the means of interviews, surveys, tracking and surveillance. The DPIA must define which personal data will be collected and processed, as well as their recipients, and that they will be deleted at the latest six months after the end of the COMPACT project, using irreversible state-of-the-art erasure techniques. Additionally, the DPIA must define measures, contributing to security of the storage of data, describe the processing in a functional manner, identify the assets on which the personal data will rely, such as software, hardware and paper, and potential compliance with approved codes of conduct under Article 40 of the GDPR.

2. Proportionality and necessity

   Tracking and surveillance of employees' activities must not go beyond what is necessary to achieve the cyber-awareness assessment goals. One of the key elements to take into account is *effectiveness* of surveillance– does tracking participants collect and process the data it has been set up for or not? Effectiveness must be monitored regularly. Additionally, if tracking is too intrusive, possible alternatives must be sought,[309] for example monitoring of a smaller number of workplace activities or devices.
   The DPIA must clearly delineate between the activities and devices, for which monitoring is necessary, and those which shall not be monitored.

3. Risk management

   Tracking and surveillance pose a privacy risk, as they may encroach excessively onto the private life of participants, especially if policies such as bring-your-own-device are in place. The DPIA should set out mitigating measures, e.g. oblige the data controller to warn participants that their working environment is being monitored.

4. Involvement of interested parties

   The data controller must seek the advice of the data protection officer when carrying out the DPIA, as well as seek the views of studies participants. If such consultations harms the

[309] EGE Opinion no. 28, p. 87-91.

protection of commercial or public interests or the security of processing operations, then it is considered inappropriate and the data controller is not required to carry it out.[310]

[310] Article 35(9) of the GDPR.

6. Conclusion

This deliverable reported on the security, ethics, legal and privacy framework of the COMPACT architecture and user trials, with the aim of providing guidance for the architecture design and its future implementation within the LPA's. Legal and ethical aspects are an integral part of the project and will be addressed throughout its duration in all aspects.

The importance of personal data in the COMPACT project is twofold.
The implementation of COMPACT technology will process personal data of citizens and employees that the LPA's already possess. The principles of data minimisation and privacy-by-design and by-default must be respected with regards to the implementation. Insofar as the implementation of privacy-enhancing techniques (PET's) will entail anonymisation of data, these data will not be considered personal data any longer, and therefore the requirements of the GDPR will not apply. Data controllers are required to carry out a data protection impact assessment (DPIA) in order to assess and address risks to individuals, stemming from data processing, and in some instances are required to appoint a data protection officer (DPO). LPA's are always required to appoint a DPO. Furthermore, the citizens and employees and data subjects have certain rights vis-à-vis the data controllers, such as the right to information and the right to access, the right to erasure and to rectification of data, the exercise of which must be enabled at all times.

Regarding user studies, the recruiters must ensure that recruitment of participants and their consent is done without duress, lest their consent become forced instead of free. To that end, they must put in place certain measures, such as anonymous collection of data. However, there is no need to obtain the employees' renewed consent to access their HR-data in the selection and recruitment phase, due to the research nature of the data processing.
The partners carrying out the trials will be acting either as joint controllers, or in a controller-processor relationship.
In the case of joint controllership, the parties must conclude an arrangement among themselves in order to determine their respective roles and responsibilities, as well as carry out a DPIA due to the inclusion of tracking and surveillance of trial participants in order to address and assess possible privacy and security risks.
In the case of a controller-processor relationship, the parties must conclude an agreement, referred to as 'processor terms', which ensures that the processing by the processor meets the requirements of the GDPR, without decreasing the safeguards to the data subjects.

7. References

Article 29 Working Party Opinions: available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

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,

Guidelines on data protection officers (DPO), WP243, 13/12/2016,

Opinion 8/2001 on the processing of personal data in the employment context, 13 September 2001, WP 48,

Opinion 15/2011 on the definition of consent, July 13 2011,

Opinion 03/2013 on purpose limitation, April 2 2013, WP203,

Opinion 06/2013 on open data and public sector information ('PSI') reuse,

Opinion 05/2014 on anonymisation techniques, Adopted on 10 April 2014,

Working document on the surveillance of electronic communications in the workplace, 29 May 2002, WP 55.

Cavoukian, Ann, Privacy by design in law, practice and policy, 2011, p. 15, available at http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf,

DLA Piper, Example GDPR ready processor terms, available at https://www.dlapiper.com/en/uk/insights/publications/2017/08/example-gdpr-ready-processor-terms,

European Commission, Guidelines: How to complete your ethics self-assessment, July 2016, available at http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf,

European Data Supervisory Authority, Data minimisation, available at https://edps.europa.eu/node/3099#data_minimization,

European Group for Tort Law, Principles of European tort law: text and commentary, 2005, Berlin: Springer

European Group on Ethics in Science and New Technologies, Opinion No. 28 - 20/05/2014 on Ethics of Security and Surveillance Technologies, available at http://bookshop.europa.eu/en/ethics-of-security-and-surveillance-technologies-pbNJAJ14028/,

European Group on Ethics in Science and New Technologies, Opinion No. 26 - 22/02/2012 on Ethics of information and communication technologies, available at http://bookshop.europa.eu/en/ethics-of-information-and-communication-technologies-pbNJAJ12026/,

European Union Agency on Network and Information Security, Privacy and Data Protection by Design – from policy to engineering, December 2014, available at https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design,

Guidelines of Institutional Review Board for Social & Behavioural Studies of the University of Virginia, available at http://www.virginia.edu/vpr/irb/sbs/resources_guide_participants_vuln_coerce_employee.html ,

Information and Privacy Commissioner of Ontario, Privacy by Design, The 7 Foundational Principles, 2011, available at https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf,

Information Commissioner's Office, Guide to data protection, Principle 3 – adequacy, available at https://ico.org.uk/for-organisations/guide-to-data-protection/principle-3-adequacy/,

Information Commissioner's Office, Data Controller and Data Processor: what the difference is and what the governance implications are, available at https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf,

Lane, Jan-Erik, New public management, London: Routledge, 2000,

Rubinstein, Ira S., Regulating privacy by design (privacy enhancing technologies) (Technology: Transforming the Regulatory Endeavor), Berkeley Technology Law Journal, Summer, 2011, Vol.26(3), pp. 1409-1456,

Triaille, Jean-Paul, The EEC directive of July 25, 1985 on liability for defective products and its application to computer programs, Computer Law & Security Review, Volume 9, Issue 5, September–October 1993, pp. 214-226,

Tsormpatzoudi, Pagona; Berendt, Bettina; Coudert, Fanny, Privacy by design: From research and policy to practice – the challenge of multi-disciplinarity, in: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2016, Vol. 9484, pp. 199-212.