“Building the Next Generation Personal Data Platforms”
G.A. n. 871370

DELIVERABLE D7.2

Legal requirements for the PIMCity platform and its components

H2020-EU-2.1.1: PIMCity

Project No. 871370

Start date of project: 01-12-2019

Duration: 30 months

Revision: 01

Date: 24-05-2020

Document Information

Document Name: Legal requirements for the PIMCity platform and its componentsWP7 – Title: Platform specification and demonstration

Task 7.2

Revision: 01

Revision Date: 24-05-2020

Author: Alessandro Bruni, Aleksandra Kuczerawy, Viltė Kristina Steponėnaitė (KUL).

Dissemination Level

Project co-funded by the EC within the H2020 Programme		
PU	Public	☑
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

(Tick the corresponding dissemination level of the deliverable according to Annex I).

Approvals

	Name	Entity	Date	Visa
Author	**Alessandro Bruni, Aleksandra Kuczerawy, Viltė Kristina Steponėnaitė**	**KUL**	**01-05-2020**	☑
WP Leader	**Viltė Kristina Steponėnaitė**	**KUL**	**01-05-2020**	☑
Coordinator	**Marco Mellia**	**POLITO**	**03-06-2020**	☑

Document history

Revision	Date	Modification
Version 1	24-05-2020	V1

LIST OF ABBREVIATIONS

Abbreviation	Meaning
CDSM	Directive on Copyright and related rights in the Digital Single Market
CJEU	Court of Justice of the European Union
Database Directive	Directive on the legal protection of databases
Deliverable D7.2	Deliverable D7.2 of the PIMCity project
DPIA	Data protection impact assessment
DPO	Data protection officer
EU	European Union
GDPR	General Data Protection Regulation
ePD	e-Privacy Directive
InfoSoc	Directive on the harmonisation of certain aspects of copyright and related rights in the information society
KUL	KU Leuven – CiTiP
NPD Regulation	Regulation on the free flow of non-personal data
PIMCity project	Horizon2020 project PIMCity (Building the next generation Personal Data Platforms), Grant Agreement No. 871370
TFEU	Treaty on the Functioning of the European Union
Trade Secrets Directive	Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure

EXECUTIVE SUMMARY

The deliverable D7.2 is the second deliverable (hereinafter as the Deliverable) of KU Leuven – CiTiP (hereinafter as KUL) in the PIMCity project. The deliverable D7.2 provides an overview of the key and potentially relevant legal requirements from the most relevant European Union (hereinafter as the EU) legal frameworks such of privacy, data protection and intellectual property rights that should be taken into account in the light of the PIMCity project. D7.2 also clarifies the general principles and requirements that have been identified as potentially relevant in the deliverable D1.1.

Some more detailed guidelines are also provided as ANNEXES to the deliverable D7.1, in particular guidelines for consent management and privacy policies as well as template informed consent form and template privacy policy.

Taking into account the stage of the project, it is not clear yet whether certain legal requirements or guidelines such as Ethics Guidelines for Trustworthy AI[1] will be applicable. The requirements listed in deliverable D7.2 result from the enduring dialogue among the partners and their relevance is subject to change. An extensive overview of the relevant legal requirements can only be defined and refined at the later stages of the PIMCity project when partners will be able to clarify the particular intentions and technical nuances in detail. KUL will consequently determine the relevance of certain requirements relying on the information provided by the Project partners and update the requirements accordingly.

DELIVERABLE STRUCTURE

The Deliverable consists of two main parts: the first one provides an overview of the key and potentially relevant legal requirements stemming from the most relevant identified EU legal frameworks, while the second one provides a list of particular recommendations.

The deliverable D7.2 also includes two annexes. ANNEX A provides guidelines that shall help the PIMCity partners to identify their roles under the EU privacy and data protection legal framework. ANNEX B provides recommendations for the PIMCity partners responsible for the project website(s).

[1] European Commission High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI, 8 April 2019, available at <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>, accessed 30/05/2020.

LIST OF CONTENT

LIST OF TABLES

INTRODUCTION

Given the information provided to KUL at the current stage, it is clear that the activities undertaken in the context of the PIMCity project shall be subject to the requirements stemming from multiple legal frameworks. In particular, those stemming from the EU privacy, data protection legal frameworks and legal frameworks governing intellectual property rights.

Therefore, the deliverable D7.2 provides an overview of the legal requirements stemming from the following EU regulations and directives: (i) the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[2] (hereinafter as the GDPR); (ii) the Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector[3] (hereinafter as the ePrivacy Directive or the ePD); (iii) the Regulation on the free flow of non-personal data[4] (hereinafter as the NPD Regulation); (iv) the Directive on the harmonisation of certain aspects of copyright and related rights in the information society[5] (hereinafter as the InfoSoc Directive); (v) the Directive on Copyright and related rights in the Digital Single Market[6] (hereinafter as the CDSM Directive); the Directive on the legal protection of databases[7] (hereinafter as the Database Directive); the Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure[8] (hereinafter as the Trade Secrets Directive). Finally, the deliverable D7.2 provides guidelines and a list of particular recommendations.

To identify the particularly relevant legal requirements, it is crucial to have a clear understanding of the characteristics of each and every activity and process. However, taking into account the initial stage of the process, the provided list should be considered as an initial attempt based on the information gathered by KUL from the other PIMCity partners. The PIMCity partners should carefully consider the list of provided legal requirement and assess their relevance taking into account the particular activities and processes at stake.

[2] Regulation 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) [2016] OJ L 119, 4.5.2016, p. 1–88.
[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2009] OJ L 201, 31.7.2002, p. 37–47.
[4] Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303/59 28.11.2018, p. 59–68.
[5] Directive 2001/29/EC of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L 167/10 22.6.2001, p. 10–19.
[6] Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L130/92 17.5.2019, p. 92–125.
[7] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L77/20 27.3.1996, p. 20–28.
[8] Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L 151/1 15.6.2016, p. 1–18.

OVERVIEW OF THE RELEVANT LEGAL FRAMEWORKS

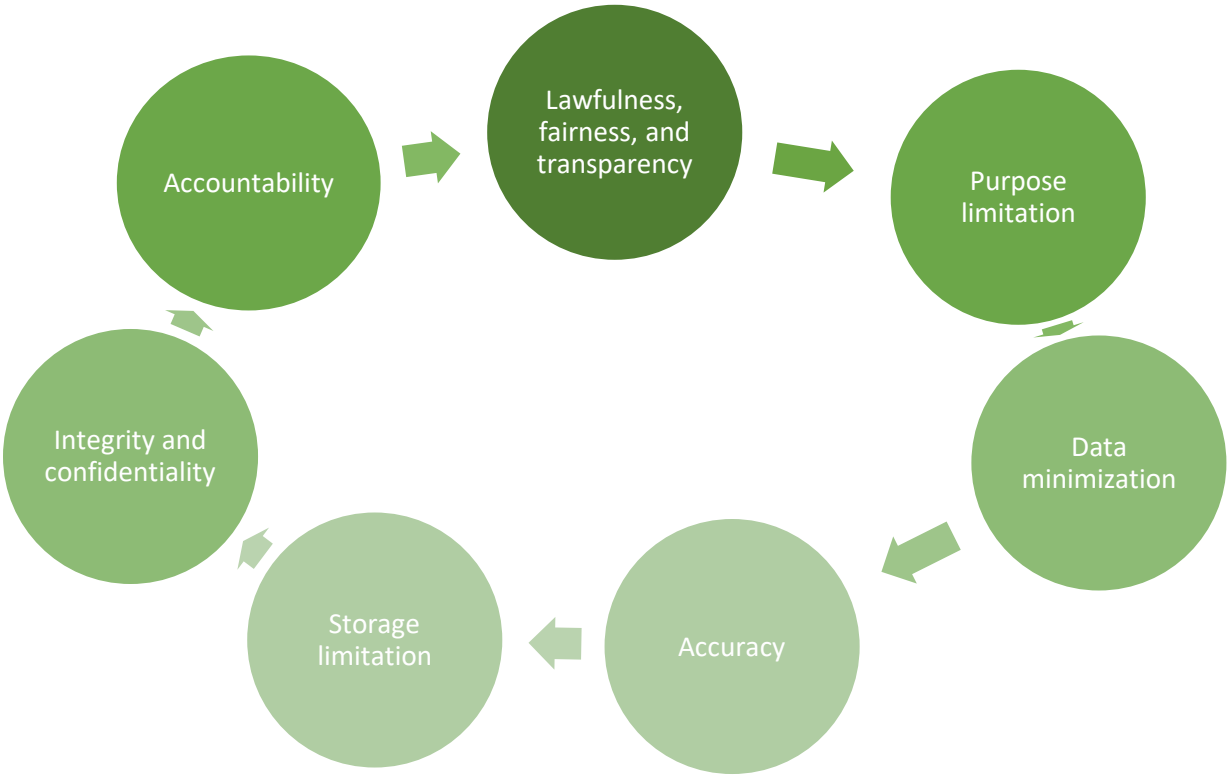
EU Privacy and Data Protection Framework

An overview of the EU data protection framework has been provided in the deliverable D1.1. The analysis provided in this section focuses on the EU data protection principles that are highly likely the most relevant in the context of the PIMCity. In particular, the section provides an overview of the certain requirements stemming from the GDPR and the e-Privacy Directive.

The General Data Protection Regulation (GDPR)

In this section, specific emphasis is given to the GDPR and the privacy and data protection principles, listed in Art. 5 GDPR,[9] embedded in it. PIMCity partners should pay particular attention to such principles for ensuring compliance of their activities with the EU privacy and data protection framework

GDPR PRINCIPLES



Lawfulness, Fairness and Transparency principles

First of all, personal data have to be processed lawfully, fairly and in a transparent manner.[10]

The **fairness principle** requires data controller to assess data subjects' interests carefully and to meet reasonable expectations with regard to the processing activity.

[9] Art. 5 GDPR.
[10] Art. 5(1)(a) GDPR.

The **principle of transparency** can be considered as a prerequisite to ensure the fairness of a process involving personal data. Transparency principle ensures that data subjects can exercise their rights. For them to be able to do so, data controllers have to process individuals' data transparently.

To comply with **the lawfulness principle**, the entity that is acting as data controller has to process data lawfully, using a legal basis substantiated in Art. 6-10 GDPR.

Art. **6(1) GDPR** provides six legal bases to lawfully process personal data: the consent (of the data subject), the performance of a contract, a legal obligation, the vital interests of individuals, the public interest and the legitimate interest of the controller.[11]

The lawful basis for processing data may be different depending on the activity carried out by each partner of the PIMCity project. For example, data gathering might come from different sources and therefore, may require a different legal basis. Given the information provided by partners at this stage of the project, three legal bases may be considered for data processing, in particular ***contract***, ***legitimate interest*** and ***consent***.[12]

Contract

The performance of a contract is one of the six grounds listed in Art. 6(1)b GDPR for lawfully processing personal data.[13] In the context of contract execution, the data processing must be necessary for the performance of the contract at stake. Which personal data are necessary must be determined on a case-by-case basis. The contract has to define the amount of personal data that can be lawfully processed, limiting it to the strictly necessary amount.

Legal obligation to which the controller is subject

According to Art. 6(c) GDPR the ground for processing personal data may also be processed where it *'is necessary for compliance with a legal obligation to which the controller is subject'*.[14] Such law must comply with the EU data protection law principles (e.g. necessity, proportionality, purpose limitation).

Legitimate interests

To rely on legitimate interests as the legal basis for processing personal data, a data controller has to ensure that the processing activity does not override the fundamental rights of the data subject. The GDPR does not provide an exhaustive list of all contexts or processing activities where the legitimate interest lawful basis can apply. To support data controller in such an evaluation, Article 29 Working Party[15] (hereinafter as WP29) has clarified the examples of legitimate interests.[16] Examples of legitimate interest include (i) direct marketing; (ii) prevention of fraud; (iii) employees' monitoring for safety or management purposes; (iv) physical, IT and network security.

In the PIMCity context, partners that will intend to use legitimate interests as a legal basis for processing personal data shall demonstrate that the processing is *necessary* for these

[11] Art. 6(1)(b) GDPR.
[12] Alessandro Bruni, Amandine Leonard, Aleksandra Kuczerawy SAFEDEED D.3.1. Legal Frameworks and Ethical Issues.
[13] Ibid.
[14] Art. 6(1)(c) GDPR.
[15] On 25 May 2018, it has been replaced by the European Data Protection Board in accordance with the GDPR.
[16] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 27 April 2020, p. 25.

interests. Besides, they shall assess whether there are less intrusive ways to achieve the same result. Such an assessment has to be done carrying out a **balancing test**.

The balancing test requires a context risk-benefit evaluation and an implementation of potential mitigation measures. Crucial elements PIMCity partners should consider: (i) the relationship between the data controller and the individual/data subject; (ii) the individual expectations of the data subject that the data controller will use data subject's data according to what has been reported to him by the controller when fulfilling transparency obligations; (iii) the nature of the personal data processed and whether it is particularly sensitive or private; (iv) the possible impact on individuals/data subjects; (v) whether safeguards can be put in place to minimise the data processing impact.[17]

Consent

The legal basis which is highly likely to be the most relevant for the PIMCity project partners is consent. It is particularly relevant that for the consent of the data subject to be valid, it must be freely given; specific; informed; unambiguous; provided by a statement or by explicit affirmative action.[18]

On 4th May 2020 the European Data Protection Board adopted new guidelines on consent.[19] The new guidelines update the ones provided by WP29 on the same topic.[20] The new guidelines take into account recent CJEU decision on cookies and provide clarifications in regard to consent in the context of internet webpages. In particular, the EDPB clarifies that access to a webpage cannot be subject to the acceptance by the user of the service providers policy on cookies storage on his/her user device. In addition, the guidelines state that scrolling and swiping a webpage do not meet the criteria of clear and affirmative action, necessary to obtain valid consent from the user for processing his/her personal data.

For the detailed guidelines on consent management see Annex B of D7.1.

Purpose limitation principle

The purpose limitation is the second privacy and data protection principle mentioned in the GDPR.[21] According to Art. 5 GDPR personal data must be collected for *"**specified**, **explicit** and **legitimate** purposes and not further processed in a manner that is incompatible with those purposes"*.[22]

WP29 has developed the Opinion 03/2013 to substantiate such a high-level description of the purpose limitation principle.[23] According to WP29 purpose limitation has two building

[17] ICO, Guide to the GDPR – Lawful basis for processing: Legitimate interests, available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>, accessed 14/05/2020. See also Pierre Dewitte, Aleksandra Kuczerawy, Peggy Valcke, CUTLER D1.2. Legal Requirements.
[18] Art. 4(11) GDPR.
[19] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, adopted on 4 May 2020, available at <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf>, accessed 14/05/2020
[20] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, revised and Adopted on 10 April 2018, 17/EN WP259 rev.01, available at <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030>, accessed 14/05/2020
[21] Art. 5(1)(b) GDPR.
[22] Art. 5(1)(b) GDPR. For more details see: Article 29 Working Party, Opinion 03/2013 on purpose limitation, WP 203, adopted on 2 April 2013.
[23] Article 29 Working Party, Opinion 03/2013 on purpose limitation, WP 203, adopted on 2 April 2013.

blocks, briefly illustrated in the table below: i) purpose specification and ii) compatible further use.

Purpose specification principle

Data subjects' personal data have to be collected for a purpose that justifies their collection. The purpose should be sufficiently defined to ensure the implementation of any necessary safeguard measures and delimit the scope of the processing operations. Consequently, the purpose has to be explicit, avoiding any possible ambiguity, and match the legitimate expectations of data subject whose data are processed.[24]

Compatible further use

Personal data that are collected for a specific and identified purposes should not be further processed in a manner which is incompatible with those purposes. Further processing should be interpreted as any processing operation occurring after the initial collection.

In order to ensure purpose limitation, an assessment shall be carried out, taking into account specific criteria listed in Rec. 50 GDPR.[25]

The entity processing personal data shall indicate the purpose(s) for which the data are processed to comply with the purpose limitation principle. Such purpose specification will not only ensure compliance with the purpose limitation principle but will also contribute to fulfilling requirements stemming from the principle of transparency.

Data Minimisation principle

Data controllers have to ensure that processed personal data are '*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*'. In such a way they would ensure compliance with the data minimisation principle.[26]

In PIMCity project context, the amount of data processed by the partners have to be limited to what is necessary to achieve a specific purpose. For example, in case personal data is analysed for marketing purposes, only the particular amount of data which is actually necessary for such a purpose shall be processed.

Accuracy principle

The data accuracy principle requires to process personal data that are '*accurate and, where necessary, kept up to date*'.[27] Therefore, appropriate processing measures have to be put in place by the data controller to check the accuracy of the datasets. Art 5(1)(d) GDPR foresees an exception to the general rule when the processing is carried out for the public

[24] Art. 5(1)(b) GDPR.
[25] Rec. 50 GDPR list the criteria that should be taken into account when assessing the compatibility between the initial processing purpose and the further ones: '(1) the relationship between the purposes for which the data have been collected and the purposes of further processing, (2) the context in which the data have been collected and the reasonable expectations of the data subjects as to their further use, (3) the nature of the personal data and the impact of the further processing on the data subjects and (4) the safeguards applied by the controller to ensure the fair processing and to prevent any undue impact on the data subjects'.
[26] Art. 5(1)(c) GDPR.
[27] Art. 5(1)(d) GDPR.

interest, scientific or historical research purposes or statistical purposes. Nonetheless, in such cases, the data controller has to put in place appropriate technical and organisational measures.[28] The level of accuracy is related to the processing purpose; therefore, it will change depending on the purpose for which personal data are processed.

Integrity and confidentiality

Integrity and confidentiality are two complementary principles. Both principles are linked to the security of processing. The integrity principle requires controllers to ensure appropriate security measures when processing personal data to protecting them against unlawful processing, accidental loss, destruction or damage.[29] In parallel, the principle of confidentiality requires to make personal data available only to those who need them for the processing activities. These two principles, which intend to reinforce data subject security, have been expanded in electronic communications.

In PIMCity context, the entire architecture of the platform and the communication channels established between the platform peer have to take into account the measures suggested in Art. 32-34 GDPR (i.e. encryption) to ensure compliance with these two principles.

Accountability Principle

The accountability principle requires to be able to prove, in a proactive manner, compliance with the obligations provided in the GDPR.[30] The GDPR provides particular obligations that the data controller and data processor have to fulfil to prove their compliance with the GDPR provisions.[31]

In the PIMCity project context, partners have to agree on taking to common appropriate technical and organisational measures to comply with the accountability principle. Such technical and organisational measures include, for example, measures to ensure privacy by design and by default; recording processing activities involving personal data; conducting a data protection impact assessment (hereinafter as a DPIA); appointing a data protection officer (hereinafter as a DPO).[32]

In light of the project activities, PIMCity partners have already selected a DPO and are conducting a DPIA.

[28] Ibid.
[29] Art. 5(1)(f) GDPR.
[30] P. Voigt and A. von dem Bussche, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International 2017.
[31] Chapter IV GDPR.
[32] Alessandro Bruni, Amandine Leonard, Aleksandra Kuczerawy SAFEDEED D.3.1. Legal Frameworks and Ethical Issues.

Directive on privacy and electronic communications (e-Privacy Directive)

Rules on Tracking Technologies

Certain activities may require to meet the requirements stemming from the GDPR and the ePD. The necessity to consider ePD provisions take into account two factors: the development and use, for dissemination purpose, of the PIMCity webpage to web users, the fact that two PIMCity partners, namely Telefonica and Fastweb as electronic communication providers, fall into the application scope of the ePD. Nonetheless, an extensive overview of the particular relevant legal requirements stemming from the ePD can only be defined at the later stages of the PIMCity Project, after partners will have clarified the particular intentions and technical nuances in detail. At this stage, given the information provided to KUL by the PIMCity partners at the current stage project, it is already clear that the requirements of the ePD may be relevant in case partners decide to collect personal data in the PIMCity website(s). Consequently, partners responsible for the website(s) shall carefully examine the requirements stemming from the ePD and the relevant case law accordingly.[33]

Taking into account the activities that will be carried out in the PIMCity project context, it is useful to focus on the ePD provisions and recent EU case law on cookies. Cookies are simple text files that get downloaded onto web-users PC every time they visit a website. The cookie file generally contain two bits of information: the url and a unique user identification number. The cookies allow the provider of the page to know that a specific user has visited its website.[34] Such knowledge can be used for analytic and marketing purpose. Considering their nature since they allow identifying an individual.[35] When the identification, direct or indirect is possible, the GDPR provisions shall apply. The ePD describe which are the legal obligation for the entity managing the website to process such specific type of personal data.[36]

In the context of cookie discussion, it is worth to mention a recent rule of the Court of Justice of the EU (hereinafter as the CJEU).[37] The dispute concerned the fact that ePD does not clarify the notion of consent but refers to the definition provided by the Data Protection Directive (Directive 95/46/EC). The CJEU has resolved the dispute stating that the notion of consent provided in the ePD and in the GDPR should not be differently interpreted.[38] The CJEU has also clarified that consent is not validly constituted if, *'in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent.'*[39] Consequently, consent should be based on affirmative (opt-in).

[33] In Annex B of this deliverable D7.2 guidance and recommendation are provided in order to support the identified partners to comply with specific provisions.
[34] Olivia Solon, A simple guide to cookies and how to comply with EU cookie law, Wired Web, available at <https://www.wired.co.uk/article/cookies-made-simple>, accessed 14/05/2020.
[35] Rec. 30 GDPR.
[36] Art. 5(3) ePD: 'Confidentiality of communications'.
[37] CJEU, Case C-673/17: Request for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 30 November 2017 — Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband e. V., OJ C 112, 26.3.2018 ECLI:EU:C:2019:801.
[38] CJEU, Case C-673/17, paragraph 82(2) 'Article 2(f) and Article 5(3) of Directive 2002/58, as amended by Directive 2009/136, read in conjunction with Article 2(h) of Directive 95/46 and Article 4(11) and Article 6(1)(a) of Regulation 2016/679, are not to be interpreted differently according to whether or not the information stored or accessed on a website user's terminal equipment is personal data within the meaning of Directive 95/46 and Regulation 2016/679.'
[39] CJEU, Case C-673/17, paragraph 82(1).

Finally, the CJEU has clarified that service providers must inform website user about the duration of the operation of cookies, and whether or not third parties may have access to those cookies.[40]

In the PIMCity project context, depending on the particular decisions taken by the responsible Project partners, necessary policies and consent forms will be prepared.

Non-personal data (NPD Regulation)

A general overview of the NPD Regulation, including its scope of application, was provided in the deliverable D1.1. The section below focuses on explaining the key and potentially relevant legal requirements in more detail.

Free movement of data within the EU

Firstly, the NPD Regulation prohibits data localisation requirements, only with a minimal possibility of exceptions.

Data localisation requirements stem from legal rules or administrative guidelines or practices that **dictate or influence the localisation of data for its storage or processing**.[41] Such requirements mainly concern accounting documents, invoices, books and records, commercial letters, judicial records, national registries and archives and – broadly speaking – the servers hosting these data.[42] Rec. 18 of the NPD Regulation draws the attention that data localisation requirements represent a clear barrier to the free provision of data processing activities across the Union and to the internal market. As such, they shall be prohibited '*unless justified on grounds of public security in compliance with the principle of proportionality*'.[43] The concept of 'public security', within the meaning of Article 52 TFEU and as interpreted by the CJEU, covers both the internal and external security of a Member State, as well as issues of public safety, in order, in particular, to facilitate the investigation, detection and prosecution of criminal offences. This exception may be applied only in case there is a genuine and sufficiently serious threat. This threat shall be affecting one of the fundamental interests of society, such as the functioning of institutions and essential public services.[44]

Concerning this general prohibition of data localisation requirements, the Member States shall ensure that any existing data localisation requirement that is not compliant with the prohibition mentioned above is repealed by 30 May 2021.[45]

As a result, users of the platform processing non-personal data shall not be bound by any legal rule prescribing mandatory data localisation requirements and shall not face any

[40] Case C-673/17, paragraph 82(3).
[41] For the definition, see: Commission staff working document on the free flow of personal data and emerging issues of the European data economy accompanying the document Communication Building a European Data Economy (COM(2017)9final, 5 <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id= 41247> accessed 30 March 2018.
[42] During a study commissioned by the European Commission, more than 60 restrictions have been identified across 25 States. For a thorough analysis of data localisation requirements among Member States, see: Time.Lex, Spark, Tech4i2, 'Cross-border data flow in the Digital Single Market: data location restrictions' <https://ec.europa.eu/digital-single-market/en/news/cross-border-data-flow-digital-single-market-data-location-restrictions> accessed 30 March 2018.
[43] Art. 4(1) NPD Regulation.
[44] Rec. 19 NPD Regulation.
[45] Art. 4(3) NPD Regulation.

practical obstacles that would have an equivalent effect. Users of the platform shall not be obliged to host their data in a specific Member State or to rely on given facilities within that country unless public security reasons would justify such limitation.

Data availability for competent authorities

Secondly, the NPD Regulation seeks to facilitate cross-border access to non-personal data by public authorities.

The NPD Regulation does not affect the powers of competent authorities to request or obtain access to data under Union or national law. In addition, it states that same competent authorities cannot be refused access to data on the basis that the data are processed in another Member State.[46] In case after requesting access to a user's data, a competent authority does not obtain access and if no specific cooperation mechanism exists under the EU law or international agreements to exchange data between competent authorities of different Member States, that competent authority may request assistance from a competent authority in another Member State.[47]

The notion of competent authority is a broad one and covers any authority '*or any other entity authorised by national law to perform a public function or to exercise official authority, that has the power to obtain access to data processed by a natural or legal person for the performance of its official duties, as provided for by Union or national law*'.[48]

The NPD Regulation also provides the requirements that shall be fulfilled in order to ensure cooperation between authorities.[49]

As a result, users of the platform may be required to provide access to non-personal data by competent authorities of various Member States and shall not refuse to provide access to data on the basis that the data are processed in another Member State.

Porting of data

Thirdly, the NPD Regulation seeks to contribute to the efficiency of switching between service providers. It is assumed that self-regulatory codes of conduct ('codes of conduct') shall be beneficial for these purposes.[50] The NPD Regulation, therefore, provides that the European Commission shall encourage service providers to the complete the development of such codes by 29 November 2019 and to implement them by 29 May 2020.[51] Service providers shall be understood as natural and legal persons who provide data processing services.[52]

It is expected that codes of conduct will cover at least the key aspects that are important during the process of porting data, such as (i) the processes used for, and the location of, data back-ups; (ii) the available data formats and supports; (iii) the required IT configuration and minimum network bandwidth; (iv) the time required before initiating the porting process and the time during which the data will remain available for porting; (v) and the guarantees for accessing data in the case of the bankruptcy of the service provider. It is also expected

[46] Art. 5(1) NPD Regulation.
[47] Art. 5(1) NPD Regulation.
[48] Art. 3(6) NPD Regulation.
[49] Art. 7 NPD Regulation.
[50] Rec. 29-30 NPD Regulation.
[51] Arts. 6(1), Article 6(3)) NPD Regulation.
[52] Art. 3(4) NPD Regulation.

that such codes will make clear that vendor lock-in is not an acceptable business practice, will provide for trust-increasing technologies, and will be regularly updated to keep pace with technological developments.[53]

The European Commission shall ensure that the codes of conduct are developed in close cooperation with all relevant stakeholders, including associations of small and medium-sized enterprises and start-ups, users and cloud service providers.[54]

[53] Rec. 29-31 NPD Regulation.
[54] Art. 6(2) NPD Regulation.

EU Intellectual Property Right Framework

Copyrighted data (InfoSoc Directive, CDSM Directive)

A general overview of the EU copyright legal framework, in particular of the InfoSoc Directive and the CDSM Directive, including their scope of application, was provided in the deliverable D1.1. The section below focuses on explaining the key and potentially relevant legal requirements.

General principles

Copyright grants the right holder, the exclusive prerogatives to (1), reproduce, (2) communicate to the public and (3) distribute the protected work.[55] Before performing any of these acts, third parties should, therefore, seek authorisation from the author, or rely on one of the **various exceptions** listed in the InfoSoc Directive or the CDSM Directive. It should also be noted that, while copyright is initially granted to the author of the work – *i.e.* the natural person who expressed its creativity – it may subsequently be transferred or licensed. Transferring or licencing can be done either *in bulk* or by fractioning the components of the copyright among different transferees/licensees, by limiting the territorial scope of the transfer/license to definite territories or by stipulating specific exploitation modalities for each component.

Exclusive rights of the author

First, the author has the exclusive right to '*authorise or prohibit direct or indirect, temporary or permanent **reproduction** by any means and in any form, in whole or in part*'.[56] As often emphasised by the case-law of the CJEU, the notion of 'reproduction' must be interpreted as to encompass the mere reproduction for technical purposes (*e.g.* cache copies, conversion in a different format, back-up copies preventing data loss, screen buffer, etc.)[57] If the PIMCity partners are to process copyrighted data, it is reasonable to assume that there will be 'reproductions'.[58] Reproductions will have to be authorised by the author or the relevant right holder. Alternatively, if possible, the partners may rely on one of the exceptions foreseen by the InfoSoc Directive or the CDSM Directive (see *infra*). Second, the author also has the exclusive right to '*authorise or prohibit any **communication to the public** of his/her work, by wire or wireless means, including the making available to the public in such a way that members of the public may access them from a place and a time*

[55] Arts. 2, 3, and 4 InfoSoc Directive, respectively.
[56] Art. 2 InfoSoc Directive.
[57] See, for instance: CJEU, Case C-5/08 Infopaq International v. Danske Dagblades: Judgment of the Court (Fourth Chamber) of 16 July 2009, ECLI:EU:C:2009:465, paragraph 51: '*an act occurring during a data capture process, which consists of storing an extract of a protected work comprising 11 words and printing out that extract, is such as to come within the concept of reproduction in part within the meaning of Article 2 of Directive 2001/29'*. See also: CJEU, Case C-403/08 Football Association Premier League Ltd and Others v QC Leisure and Others and Karen Murphy v Media Protection Services Ltd (C-429/08): Judgment of the Court of (Grand Chamber) of 4 October 2011, ECLI:EU:C:2011:631, paragraph 159: '*the reproduction right extends to transient fragments of the works within the memory of a satellite decoder and on a television screen, provided that those fragments contain elements which are the expression of the authors' own intellectual creation*'.
[58] E.g. where platform relies on algorithms its proper functioning may require technical acts of reproduction such as the mere import of these data in the system.

individually chose by them'.[59] Third, the author has the exclusive right to '*authorise or prohibit any form of* ***distribution*** *to the public by sale or otherwise*'.[60]

Relevant exceptions to the rights of the author

The InfoSoc Directive and the CDSM Directive stipulate several potentially relevant exceptions, i.e. cases in which authorisation of the right holder may be not necessary to perform the relevant actions. However, it shall be noted that not all of the exceptions are mandatory under the EU law, i.e. not all of the exceptions will be present in the national laws of the EU Member States. Besides, the EU Member States have implemented some provisions differently. In relation to this, the partners shall examine carefully what is the content of the particular exception in the, particularly relevant Member State. The Partners who may want to rely on a particular exception for their activities involving copyrighted data shall take into account the differences in the national laws of the EU Member States.

Temporary acts of reproduction

First, the InfoSoc Directive introduces a mandatory exception for '***temporary acts of reproduction which are transient or incidental and an integral and essential part of a technological process*** *whose sole purpose is to enable (1) a transmission in a network between third parties by an intermediary or (b) a lawful use*'.[61] This exception only applies when the temporary acts of reproduction have no independent economic significance. It mainly covers caching and browsing operations which, otherwise, would be conditional upon the authorisation of the author of the work which is cached or displayed.[62]

Illustration for teaching or scientific research

Second, the InfoSoc Directive also gives the Member States the possibility to introduce other exceptions to the exclusive reproduction right of the author. It offers the possibility to limit or restrict this right in case the copyrighted work is used '*for the sole purpose of illustration for teaching or* ***scientific research****, as long as the source, including the author's name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved*'.[63] However, it shall be recalled that not every Member State has transposed this optional provision in its national legislation, and, for those that did, significant divergences exist.[64] Additionally, the requirement that the copyrighted work must be used 'solely' for scientific research might prevent from the benefit from this exception. Similarly, the 'non-commercial' criteria might also raise problematic issues. This applicability would need to be analysed on a case-by-case basis, taking into account the copyrighted work at stake and the scope of the exception as implemented in national legislation and interpreted by domestic courts.

[59] Art. 3 InfoSoc Directive.
[60] Art. 4 InfoSoc Directive.
[61] Article 5(1) InfoSoc Directive.
[62] In that sense, Recital 33 of the InfoSoc Directive goes as follows: '*this exception should include acts which enable browsing as well as acts of caching to take place, including those which enable transmission systems to function efficiently, provided that the intermediary does not modify the information and does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information*'.
[63] Art. 5(3)a InfoSoc Directive.
[64] See on that point: Jean-Paul Triaille and others, *Study on the Legal Framework of Text and Data Mining (TDM).* (Publications Office 2014) 368–370 <http://bookshop.europa.eu/uri?target=EUB:NOTICE:KM0313426:EN:HTML>.

Since the adoption of the CDSM Directive, it is relevant that certain provisions of the InfoSoc Directive shall be interpreted **without prejudice to the exceptions and limitations newly provided by the CDSM Directive**.[65] Hence it is necessary to clarify the regime introduced by the CDSM Directive. Besides, the latter document establishes some other potentially relevant exceptions. Both issues are further addressed below.

Reproductions made by research organisations to carry out text and data mining of works or other subject-matter for the purposes of scientific research

Firstly, it is clarified by the CDSM Directive that Member States **shall provide** for an **exception to the exclusive right to authorise reproduction** as revealed above[66] for reproductions and extractions ***made by research organisations*** *and cultural heritage institutions in order* ***to carry out, for the purposes of scientific research, text and data mining of works or other subject-matter to which they have lawful access***[67]. In this context it is relevant that 'research organisation' shall be understood as *university, including its libraries, a research institute or any other entity****, the primary goal of which is to conduct scientific research or to carry out educational activities involving also the conduct of scientific research***: (i) *on a not-for-profit basis or by reinvesting all the profits in its scientific research*; or (ii) *pursuant to a public interest mission recognised by a Member State*; *in such a way that the access to the results generated by such scientific research cannot be enjoyed on a preferential basis by an undertaking that exercises a decisive influence upon such organisation*.[68] Conversely, organisations upon which commercial undertakings have a decisive influence allowing such undertakings to exercise control because of structural situations, such as through their quality of shareholder or member, which could result in preferential access to the results of the research, should not be considered research organisations for the purposes of this Directive.[69] Research organisations shall benefit from such an exception **also when their research activities are carried out in the framework of public-private partnerships**. It is explicitly provided that research organisations shall be *able to rely on their private partners for carrying out text and data mining, including by using their technological tools*[70].

Digital use of works and other subject-matter for the sole purpose of illustration for teaching

In addition, **Member States shall provide for an exception or limitation to the exclusive right to authorise reproduction to allow the digital use of works and other subject-matter for the *sole purpose of illustration for teaching, to the extent justified by the non-commercial purpose to be achieved***, *on condition that such use: (i) takes place under the responsibility of an educational establishment, on its premises or at other venues, or through a secure electronic environment accessible only by the educational establishment's pupils or students and teaching staff; and (ii) is accompanied by the indication of the source, including the author's name, unless this turns out to be impossible*[71]. However, Member States may provide for some exceptions to this exception or limitation[72].

[65] Article 5(3)a InfoSoc Directive; Article 24(2)b CDSM Directive.
[66] Article 2 InfoSoc Directive.
[67] Article 3(1) CDSM Directive.
[68] Article 2(1) CDSM Directive.
[69] Recital 12 CDSM Directive.
[70] Recital 11 CDSM Directive.
[71] Article 5(1) CDSM Directive.
[72] Article 5(2) CDSM Directive.

The recitals clarify that exception or limitation provided should benefit all educational establishments and emphasise that it *should apply only to the extent that the uses are justified by the non-commercial purpose of the particular teaching activity*. While deciding whether the activity is non-commercial, the organisational structure and the means of funding should not be the decisive factors.[73] The use of works or other subject matter under the exception or limitation *should be limited to what is necessary for the purpose of such activities*.[74]

Reproductions and extractions of lawfully accessible works and other subject-matter for the purposes of text and data mining

Besides, Member States **shall provide** for **an exception or limitation to the exclusive right to authorise reproduction for reproductions and extractions of lawfully accessible works and other subject-matter for the purposes of text and data mining**.[75] The latter exception or limitation shall apply on the condition that the use has not been expressly reserved by their right holders in an appropriate manner, such as machine-readable means in the case of content made publicly available online.[76]

It remains to be seen whether the PIMCity partners will be able to benefit from these exceptions, depending on their status (e.g. on whether they qualify as 'research organisations'), activities (e.g. whether the activities are 'non-commercial'), access to work at stake (e.g. whether it is 'accessed lawfully'), transposition in the Member States, including but not limited. All of the circumstances will need to be analysed and assessed in the light of the criteria on a case-by-case basis.

The data that is, or may be, processed during the PIMCity project as well as during the exploitation phase, may be protected by copyright. The processing of data may, therefore, infringe on the exclusive rights of copyright holders. It may be necessary for the partners to seek for authorisations of the right holders or to rely on one of the exceptions provided by the InfoSoc Directive and/or CDSM Directive, as implemented in the national laws accordingly.

Recommendations regarding certain actions are provided in the second part of the deliverable D7.2.

[73] Recital 20 DCSM Directive.
[74] Recital 22 DCSM Directive.
[75] Article 4(1) CDSM Directive.
[76] Article 4(2) CDSM Directive.

Protection of databases (Database Directive, CDSM Directive)

The PIMCity partners might be interested in processing data contained in a **database**, *i.e.* a '*collection of independent works, data or other materials arranged in a systematic or methodological way and individually accessible by electronic or other means*'.[77] In relation to this, provisions of the Database Directive and the CDSM Directive with regard to databases may be relevant.

Different kinds of protection (rights) for authors and makers of a database

In particular, there are different kinds of protection provided by the Database Directive. ***First***, databases which, '*by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright. No other criteria shall be applied to determine their eligibility for that protection*'.[78] The copyright protection of databases provided for by the Database Directive shall not extend to their contents and shall be without prejudice to any rights related to the contents. ***Second***, in case the maker of a database shows that there has been '*qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database*', such maker shall have *sui generis right* with regard to such database.[79] The Database Directive provides rights for both authors of a database and makers of a database as well as exceptions to their rights (copyright and *sui generis* right respectively). Key provisions are revealed in detail below.

Protection by copyright

When it comes to the **copyright** protection, it shall be noted that the ***author of a database shall have the exclusive right*** *to carry out or to authorize* (a) *temporary or permanent reproduction by any means and in any form, in whole or in part*; (b) *translation, adaptation, arrangement and any other alteration*; (c) *any form of distribution to the public of the database or of copies thereof*. *The first sale in the Community of a copy of the database by the rightholder or with his consent shall exhaust the right to control resale of that copy within the Community*; (d) *any communication, display or performance to the public*; (e) *any reproduction, distribution, communication, display or performance to the public of the results of the acts referred to in (b)*.[80]

Exceptions to restricted acts

Exceptions to restricted acts provided in the Database Directive include certain acts by the lawful user of a database[81] as well as certain acts that may be provided by the Member States, i.e. Member States shall have the option of providing for limitations on the exclusive rights mentioned above in the following cases: (a) *in the case of reproduction for private purposes of a non-electronic database*; (b) *where there is use for the sole purpose of illustration for teaching or scientific research, under certain conditions*; (c) *where there is use for the purposes of public security of for the purposes of an administrative or judicial procedure*; (d) *where other exceptions to copyright which are traditionally authorized under national law are involved, without prejudice to points (a), (b) and (c).*[82]

The CDSM Directive provides for additional copyright exceptions. To remind, the rules provided by this instrument shall be implemented by Member States by 7th June 2021. In

[77] Article 1(2) Database Directive.
[78] Art. 3 Database Directive.
[79] Art. 7(1) Database Directive.
[80] Article 5 Database Directive.
[81] Article 6(1) Database Directive.
[82] Article 6 Database Directive.

particular, with regards to database which is protected by copyright the CDSM Directive provides that Member States shall provide for an exception to the exclusive author's right to carry out or to authorize temporary or permanent reproduction[83] *for reproductions and extractions made by research organisations and cultural heritage institutions in order to carry out, for the purposes of scientific research, text and data mining of works or other subject matter to which they have lawful access*.[84] Secondly, Member States shall provide for an exception or limitation to exactly the same right as just revealed above[85] for reproductions and extractions of lawfully accessible works and other subject matter for the purposes of text and data mining.[86]

Member States shall provide for an exception or limitation to this right[87] as well as to some other rights as revealed further in this paragraph *in order to allow the digital use of works and other subject-matter for the sole purpose of illustration for teaching, to the extent justified by the non-commercial purpose to be achieved*, on condition that such use: (i) *takes place under the responsibility of an educational establishment, on its premises or at other venues, or through a secure electronic environment accessible only by the educational establishment's pupils or students and teaching staff*; and (ii) *is accompanied by the indication of the source, including the author's name, unless this turns out to be impossible*.[88] The other rights that shall be addressed by this exception or limitation are author's of a database exclusive rights to carry out or to authorize (i) translation, adaptation, arrangement and any other alteration,[89] (ii) any communication, display or performance to the public[90] and (iii) any reproduction, distribution, communication, display or performance to the public of the results of translation, adaptation, arrangement and any other alteration.[91] To summarise, the latter exception or limitation shall be provided to the rights provided for in Article 5(a), (b), (d) and (e) Database Directive. However, Member States may provide for some exceptions to this exception or limitation.[92]

Protection by sui generis right

In contrast to copyright protection provided by the Database Directive as revealed above, the ***sui generis* right on database** grants the right holder exclusive prerogatives in relation to a database that demonstrates that there has been a qualitatively and/or quantitatively **substantial investment** in either the **obtaining**, **verification** or **presentation** of its content.[93] On the one hand, the 'substantial investment' *may consist in the deployment of financial resources and/or the expending of time, effort and energy*.[94] On the other hand, the said investment must concern either the obtaining, the verification or the presentation of the data. In that sense, the CJEU has made clear that the resource used for the creation of materials which make up the content of the database does not constitute a valid

[83] Article 5(a) Database Directive.
[84] Article 3(1) CDSM Directive.
[85] As provided in Article 5(a) Database Directive.
[86] Article 4(1) CDSM Directive.
[87] Article 5(a) Database Directive.
[88] Article 5(1) CDSM Directive.
[89] Article 5(a) Database Directive.
[90] Article 5(d) Database Directive.
[91] Article 5(e) Database Directive.
[92] See Article 5(2) CDSM Directive.
[93] Article 7(1) Database Directive.
[94] Recital 40 Database Directive.

investment. Rather, the term 'obtaining' should be understood as referring to the '*resources used to seek out existing independent materials and collect them in the database*'.[95]

General principles

The *sui generis* right introduced by the Database Directive grants the maker of a database the **exclusive right** to prevent extraction and/or re-utilisation of the whole or of a substantial part of a database which fulfils the criteria mentioned above. Third parties should seek the authorisation from the maker of the database before performing any of these acts, or should rely on one of the **exceptions**.[96] It shall be noted that certain provisions of the Database Directive shall be implemented without prejudice to the exceptions and limitations newly provided by the CDSM Directive.[97] It is also important that the *sui generis* right initially grants these exclusive prerogatives to the 'maker' of the database, *i.e.* the person who took the initiative and the risk of investing in it.[98] However, these rights may be transferred or licensed. This may not only be done in bulk, but also by fractioning the components of the *sui generis* right among different transferees/licensees, by limiting the territorial scope of the transfer/license to definite territories or by stipulating specific exploitation modalities for each component. The duration of the *sui generis* right is, in principle, limited to 15 years counting from the date of completion of the database.[99] Yet, any change to its content which would result in the database being considered to be a substantial new investment shall qualify the database resulting from that investment for its own term of protection.[100]

Exclusive rights of the maker of a database

As hinted above, the *sui generis* right allows the maker of the database to **prevent extraction and re-utilisation** of the whole or a substantial part of the database. Extraction, on the one hand, refers to the '*permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form*'.[101] As emphasised by the CJEU, the notion of 'extraction' must be interpreted broadly, so to encompass any unauthorised act of appropriation, via a physical copy or not, of the whole or part of the content of a database.[102] As such, one could reasonably assume that the short-lived transfers necessary for computers to perform any processing operation on

[95] See, on that point: CJEU, Case C-203/02 The British Horseracing Board Ltd and Others v. William Hill Organisation Ltd: Judgment of the Court (Grand Chamber) of 9 November 2004, ECLI:EU:C:2004:695, paragraph. 42. There are indeed situations where the creation of the individual elements requires a more important investment than their subsequent arrangement into a database. In that case, the data themselves might benefit from the protection afforded by copyright law. Same could be said for the chosen structure. This, however, does not *per se* exclude the database from the *sui generis* right if there has also been an investment in the presentation of the database which is independent from the resources used to create the data.
[96] Article 9 Database Directive.
[97] See, e.g. Article 9(b) Database Directive. Article 24(1)b CDSM Directive.
[98] Recital 41 Database Directive.
[99] Article 10(1) Database Directive.
[100] Article 10(3) Database Directive.
[101] Article 7(2)a Database Directive.
[102] See: CJEU, Case C-203/02, paragraph 51. See also: CJEU, Case C-304/07 Directmedia Publishing GmbH v. Albert-Ludwigs-Universität Freiburg: Judgment of the Court (Fourth Chamber) as of 9 October 2008, ECLI:EU:C:2008:552, paragraph 36: '*The decisive criterion in this respect is to be found in the existence of an act of 'transfer' of all or part of the contents of the database concerned to another medium, whether of the same nature as the medium of that database or of a different nature*'.

databases would fall under that category and, therefore, would require either authorisation from their maker or a valid exception. Re-utilisation covers '*any form of making available to the public all or substantial part of the contents of a database by the distribution of copies, by renting, by online or other form of transmission*' (Article 7(2)b Database Directive).

Both 'extracting' and 're-utilising' only refer to types of acts concerning **the whole or a qualitatively or quantitatively substantial part** of the content of the database at stake. In other words, the *sui generis* right does not grant the right holder the exclusive prerogative over acts performed on the individual elements of the database, or insubstantial parts of it. However, this right does cover the repeated or systematic performance of these acts, as soon as their commutative effect results in extracting or re-utilising a substantial part.[103] The CJEU has, for instance, ruled that the use of metasearch engines or data mining in relation to databases available on the Internet, and the subsequent use of the data collected this way, could, under certain circumstances, lead to an 'extraction' or a 're-utilisation' within the meaning of the Database Directive.[104]

Relevant exceptions to the rights of the maker of a database

Extracting and/or-reutilising insubstantial parts

Database Directive introduces a mandatory exception to the categories of acts that, in principle, require the database maker's authorisation. In relation to a database which is made available to the public, the right holder may not prevent a lawful user from extracting and/or-reutilising **insubstantial parts**, for any purpose whatsoever.[105] This exception is somewhat stating the obvious given that, as a rule, the *sui generis* right only grants the right holder exclusive prerogatives over acts that concern 'substantial' parts of a database (see *supra*). Lawful users may not, however, perform acts which conflict with the *normal exploitation of the database or unreasonably prejudice the legitimate interests of the maker of the database*.[106]

Extraction for illustration for teaching or scientific research

Additionally, the Database Directive lists three optional exceptions Member States may decide to implement into their national laws.[107] Among them, one allows Member States to stipulate that lawful users may extract or re-utilise substantial parts of a database '*in the case of extraction for the purposes of illustration for teaching or* ***scientific research****, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved*'.[108] As revealed above, this provision shall be interpreted without prejudice to the provisions of the CDSM Directive.

[103] Article 7(5) Database Directive.
[104] Article 7(2) Database Directive. CJEU, Case C-202/12 Innoweb v. Wegener ICT media: Judgment of the Court (Fifth Chamber) of 19 December 2013, ECLI:EU:C:2013:850, paragraph. 54. In that case, the activity at stake was '*to provide any end user with a means of searching all the data in a protected database and, accordingly, to provide access to the entire contents of that database by a means other than that intended by the maker of that database, whilst using the database's search engine and offering the same advantages as the database itself in terms of searches*'. See also on that point: Perttu Virtanen, 'Innoweb v Wegener: CJEU, Sui Generis Database Right and Making Available to the Public – The War against the Machines' (2014) 5 European Journal of Law and Technology <http://ejlt.org/article/view/361>.
[105] Article 8 Database Directive.
[106] Article 8(2) Database Directive.
[107] Article 9 Database Directive.
[108] Article 9(b) Database Directive.

Not every Member State has transposed this optional provision of the Database Directive in its national legislation, and, for those that did, significant divergences exist.[109] One could, however, highlight a crucial difference between the optional exception foreseen by relevant article of the InfoSoc Directive[110] and the relevant text of the Database Directive.[111] While the former requires the copyrighted work to be used 'solely' for research purposes, the latter omits that term and seems, *a priori*, more flexible.

Text and data mining for the purposes of scientific research

Besides, the CDSM Directive provides for additional exceptions. In particular, Member States shall provide for an exception to the right of the maker of the database[112] *to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database*[113] for *reproductions and extractions made by research organisations and cultural heritage institutions in order to carry out, for the purposes of scientific research, text and data mining of works or other subject matter to which they have lawful access*.[114]

Exception or limitation for text and data mining

Secondly, Member States shall provide for an exception or limitation to exactly the same right as just revealed above[115] for reproductions and extractions of lawfully accessible works and other subject matter for the purposes of text and data mining.[116]

Use of works and other subject matter in digital and cross-border teaching activities

Besides, Member States shall provide for an exception or limitation to this right[117] in order to allow the digital use *for the sole purpose of illustration for teaching, to the extent justified by the non-commercial purpose to be achieved, on condition that such use*: (i) *takes place under the responsibility of an educational establishment, on its premises or at other venues, or through a secure electronic environment accessible only by the educational establishment's pupils or students and teaching staff*; and (ii) *is accompanied by the indication of the source, including the author's name, unless this turns out to be impossible*.[118]

The relevant databases may be protected by copyright or by *sui generis* right as provided in the Database Directive and revealed above. Certain actions of PIMCity partners may, therefore, infringe on the rights of the author or the maker of the databases. It may be necessary for the partners to seek for authorisations of the right holders or to rely on one of the exceptions provided by the Database Directive and/or CDSM Directive, as implemented in the national laws accordingly. Recommendations regarding certain actions are provided in the second part of the Deliverable.

[109] See on that point: Triaille and others 79–84.
[110] Article 5(3)a InfoSoc Directive.
[111] Article 9(b) Database Directive.
[112] Which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents (Article 7(1) Database Directive).
[113] Article 7(1) Database Directive.
[114] Article 3(1) CDSM Directive.
[115] As provided in Article 7(1) Database Directive.
[116] Article 4(1) CDSM Directive.
[117] Article 7(1) Database Directive.
[118] Article 5(1) CDSM Directive.

Data protected by trade secrets (Trade Secrets Directive)

In addition to the traditional intellectual property rights, special protection for trade secrets is granted by both international and national legal frameworks.[119] The EU Trade Secrets Directive aimed to address the fragmented legal framework[120] and provided general principles for the EU level.

Trade Secrets Directive protects information which (1) is secret in the sense that it is not generally known or readily accessible to persons within the circles that normally deal with the kind of information in question, (2) has commercial value because it is secret and (3) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.[121] When it comes to data as such, the protection established for trade secrets will expand to every piece of information that fulfils the protection requirements.[122] Beneficiary-wise, this protection is granted to the trade secret holder, who is the '*natural or legal person lawfully in control of a trade secret*'.[123]

General principles

Compared to traditional intellectual property rights such as copyright and the *sui generis* right on databases, the Trade Secrets Directive does not grant trade secret holders exclusive prerogatives over the protected items. Instead, it allows right holders to take action following any **unlawful acquisition**, **use** and **disclosure** of trade secrets.

Article 4(2) Trade Secrets Directive considers the **acquisition** of a trade secret unlawful whenever carried out by '*unauthorised access to, appropriation of, or copying any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced*', or by '*any other conduct which, under the circumstances, is considered contrary to honest commercial practices*'.[124] Subsequent **use or disclosure** of the trade secret, on the other hand, is considered unlawful where made by a person who (1) has acquired the trade secret unlawfully, (2) is in breach of a confidentiality agreement or any other duty not

[119] See Article 39 of the TRIPS Agreement. Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, signed in Marrakesh, Morocco on 15.04.1994.
[120] See Recital 8 of Directive 2016/943: '*The differences in the legal protection of trade secrets provided for by the Member States imply that trade secrets do not enjoy an equivalent level of protection throughout the Union, thus leading to fragmentation of the internal market in this area and a weakening of the overall deterrent effect of the relevant rules*'.
[121] Article 2(1) Trade Secrets Directive. This definition follows from Article 39 of the TRIPS agreement (The TRIPS Agreement).
[122] For more details on the notion of 'trade secret', see: Nuno Sousa e Silva, 'What Exactly Is a Trade Secret under the Proposed Directive?' (2014) 9 Journal of Intellectual Property Law & Practice 923.
[123] Article 2(2) Trade Secrets Directive.
[124] The notion of 'honest commercial practices' is substantiated by a footnote in Article 39 of the TRIPS agreement which goes as follows: '*For the purpose of this provision, "a manner contrary to honest commercial practices"16 shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who know, or were grossly negligent in failing to know, that such practices were involved in the acquisition*'. This, of course, will also be subject to interpretation by the CJEU and national courts once the Directive.

to disclose the trade secret or (3) is in breach of a contractual or any other duty to limit the use of the trade secret.[125]

Article 4(4) Trade Secrets Directive also considers the acquisition, use or disclosure of a trade secret as unlawful whenever a person knew or ought to have known that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully. As it appears from the above, the data as such are not protected. Rather, the circumstances under which they have been acquired, used or disclosed entitle secret holders to seek civil redress against potential infringers.[126] These circumstances could, in turn, trigger liability if a subject processes trade secrets that have been unlawfully acquired or disclosed.

Trade Secrets Directive also provides the circumstances under which the acquisition, use and disclosure of trade secrets are deemed **lawful** as well as mandatory **exceptions**.[127]

The relevant information may be protected by the Trade Secrets Directive, as revealed above. Therefore, certain actions of PIMCity partners concerning such information may be considered unlawful. Recommendations regarding certain actions are provided in the second part of the Deliverable.

[125] Article 4(3) Trade Secrets Directive.
[126] According to Article 6 Trade Secrets Directive, it is up to Member States to actually provide the measures, procedures and remedies which are necessary to ensure the availability of these civil redress against the unlawful acquisition, use or disclosure of trade secrets. This is, therefore, addressed by national law and subject to differences between Member States.
[127] Arts. 3, 5 Trade Secrets Directive.

Data portability and intellectual property rights

It may also be particularly important to take into account the rights of the rights of the copyright holders, the sui generis database right and trade secrets protection in the light of the right to data portability which was revealed in the context of the GDPR. The GDPR clearly provides that the right to data portability shall not adversely affect the rights and freedoms of others.[128] Although this right provides incentives to reuse data, it might limit opportunities to create or collect them as well, discussed briefly below.[129] For example, copyright may be held by the data subjects or by the platform. Besides, the copyright ownership may be mixed for the content at stake, or may be held by third parties, such as friends who made pictures.[130] As discussed by scholars, 'most of the platforms do not ask for the transfer of rights or exclusive licenses for user-generated content', hence 'a lot of provided content will be owned by users.'[131] It may be that the data asset such as a text or a picture is copyright protected, and, although copyright law guarantees exclusivity of use to a piece of data, the right to data portability, in contrast, foresees the possibility of its reuse. Secondly, e.g. certain limitations may stem from the sui generis database right[132]. In essence, it may be that opportunity to exercise the right to data portability would be hindered in several circumstances. There are '*a number of open questions regarding the extent to which companies will be able to invoke their IP rights on datasets to preclude data subjects from moving their personal data to another provider.*'[133] Hence, the implementation of the right to data portability '*depends on how its balancing with IP law is conducted in practice. While the GDPR is designed as a general-purpose control mechanism that applies irrespective of the type of reuse of data, the reconciliation of the GDPR with IP rights might again limit the follow-on use of ported data by purpose-specific considerations*'.[134]

Given the particular goals of the PIMCity project, especially in the light of WP4, including but not limited, the PIMCity partners shall assess these challenges in detail. In particular, the partners shall take into account the potential challenges that may arise due to the rights of the copyright holders, the sui generis database right and trade secrets protection and ensure they are adequately addressed.

[128] Art. 20 GDPR.
[129] Inge Graef, Martin Husovec and Nadezhda Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law.* German Law Journal, Volume 19, Issue 6, November 2018, 1359-1398, p. 1374.
[130] Ibid, p. 1378.
[131] Ibid.
[132] Ibid, p. 1381.
[133] Ibid, p. 1398.
[134] Ibid.

SPECIFICATION OF THE LEGAL REQUIREMENTS

The second part of deliverable D7.2 provides a detailed overview of the legal requirements that PIMCity partners should take into account while developing their activities within the project. In particular, each partner shall carefully examine all of the potentially relevant legal provisions and assess their relevance, taking into account the specific activities and processes at stake.

EU Privacy and Data Protection Requirements

The tables below (Tables 1-15) provide the actions that should be taken to comply with the GDPR provisions.

Table 1 – Identification of data controller/s

General Task	*Description*
Definition of roles	Define the roles of the different entities within the project. It shall allow the allocation of responsibilities between the different entities that are part of the project. First of all, it shall be identified who acts as the data controller(s). Besides, data processors and joint controllership cases, if applicable, shall be identified
The allocation of the roles and related responsibility is a necessary activity to comply with the GDPR provisions. Key obligations are allocated to the data controller. The GDPR defines the data controller as the *'natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'*.[135]	
In PIMCity project context, the appointed data controllers should be considered the ones in charge of deciding the purpose and the means related to the processing of personal data. Due to the different activities carried out by PIMCity project partners, there will likely be situations where more than one controller collaborate to achieve common objectives. Such a situation is defined in the GDPR as joint controllership.[136] Additional information and the set of questions that shall help to identify different roles of the Project partners will be provided as Annex A.	

Table 2 - Controller and Processor relation

General Task	Description
Formalising relationships between controller(s) and processor(s)	Define the roles and responsibilities of the entities involved in the processing activities and enter into agreements following the GDPR requirements accordingly. It has to be ensured that controller(s) and processor(s) enter into necessary agreements
According to the GDPR, "*the relationship between a controller and a processor should be determined by an agreement or other legal acts*". In particular, Art. 28(3) GDPR defines in	

[135] Art.4(7) GDPR: '(Definitions) Controller'.
[136] Art. 26 GDPR: 'Joint controllers'.

detail all the elements that such an agreement should contain.[137] Besides, in case of joint controllership, additional agreements would be necessary.[138]
According to the information collected during the DPIA, most of the PIMCity project partners will act as controllers. Some of them may appear to be processors. Other partners might not be involved in data processing activities at all. The appointment of a processor is not necessary. Nonetheless, if the controller delegates part of its processing activities to another entity acting on his behalf, the relationship between controller and processor should be specified in the agreement.

Table 3 – Privacy Policy

General Task	Description
Comply with the transparency principle	Draft privacy policies to ensure data subjects are provided with all the required information regarding the processing of their data.
The GDPR lists the information that have to be provided when personal data are collected from the data subject (Art. 13),[139] or when the personal data have not been obtained from the data subject (Art. 14).[140] Following the requirements of the GDPR, the following information is to be provided, including but not limited: the identity and contact details of the controller, the identity and contact details of the controller's representative (if any), purposes of the processing (in our case marketing and data analytics), legal basis for data processing (contract, the legitimate interest of the controller or consent), recipients, the existence of transfers outside EU, the retention period, the existence of data subject's rights, the right to launch a complain, the presence of automated decision-making processes.	
In PIMCity project context, the privacy policy for PIMCity website(s) is going to be developed. Besides, each partner shall consider the necessity of additional privacy policies and ensure they are in place if necessary.	

Table 4 – Information to be provided to Data Subjects

General Task	Description
Provide all necessary information to the data subject	Data subjects shall be provided with essential information about processing activities to have opportunities to exercise their rights
Arts. 15-22 GDPR[141] list a series of information that should be provided, upon request, to the data subject about the processing of his/her data. In particular, the information provided	

[137] Art. 28(3) GDPR: 'Processor'.
[138] Art. 26 GDPR: 'Joint Controllers'.
[139] Art. 13 GDPR: 'Information to be provided where personal data are collected from the data subject'.
[140] Art.14 GDPR: 'Information to be provided where personal data have not been obtained from the data subject'.
[141] Art.15 GDPR: 'Right of access by the data subject'; Art. 16 GDPR: 'Right to rectification'; Art. 17 GDPR: 'Right to erasure' ('right to be forgotten'); Art. 18 GDPR: 'Right to restriction of processing';

will allow the data subject to exercise, among other his/her: right of access, right to rectification, right to erasure (right to be forgotten), right to restriction of processing, right to data portability, right to object. Art. 5(3) ePD allows the storage and access information stored in the terminal equipment of a subscriber or user (cookies) on condition that the subscriber or user concerned is provided with clear and comprehensive information about the purposes of the processing, and is offered the right to refuse such processing by the data controller.[142]
Within the PIMCity project context, data subjects whose data will be processed shall be able to exercise their rights in accordance with the GDPR. In shall be noted that comprehensive, clear and unambiguous information should also be provided in the Project website(s) privacy policy.

Table 5 – Data Accuracy Principle

General Task	Description
Ensure Accuracy	Ensure data accuracy of data processed
The GDPR requires that personal data shall 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'*. [143]	
In the PIMCity project context, partners that are storing personal data as part of their activities should verify both at the time of the collection and at the time of their processing the accuracy of the data stored. According to the type of activities carried out, each partner should determine the degree of the steps that should be implemented to ensure the accuracy of data processed.	

Table 6 – Transparency and Accuracy principles

General Task	Description
Transparency and Accuracy Principle	Keep a record of processing activities to fulfil data controller obligations and comply with transparency and accountability principle
In compliance with the GDPR provisions,[144] information related to data processing activities should be kept. In particular, such information should include the name and contact details of the controller, the purposes of the processing, the description of the categories of data subjects and personal data, recipients, the existence of transfers outside EU, the technical and organisational measures, including but not limited.	
In the PIMCity project context, each partner acting as a data controller in the context of its tasks should keep a record of any processing activities involving personal data.	

Art.19 GDPR: 'Notification obligation regarding rectification or erasure of personal data or restriction of processing'; Art. 20GDPR: 'Right to data portability'; Art. 21 GDPR: 'Right to object'; Art. 22 GDPR: 'Automated individual decision-making, including profiling'.

[142] Art. 5(3) ePD: 'Confidentiality of information'.

[143] Art. 5(1)(d) GDPR: '(Principles relating to processing of personal data), Accuracy principle'.

[144] Art. 30 GDPR: 'Records of processing activities'.

Table 7 – Security and confidentiality

General Task	Description
Security and confidentiality	Develop necessary measure to ensure security and confidentiality of communications
In compliance with the GDPR, in particular Art. 32[145] and also Art. 4 ePD,[146] security measures have to be implemented, according to the context to address potential risks posed to data subjects' rights and freedoms by the processing activities. Also, the GDPR describes in detail the modalities surrounding the obligation for a controller to notify a national data protection authority and data subjects themselves about a data breach.	
In the PIMCity project context, partners involved in processing activities will have to ensure "*confidentiality, integrity, availability and resilience of processing systems, the ability to restore the availability and access to personal data in the event of a physical or technical incident,"*[147] and a process for testing and evaluating the effectiveness of those measures. Besides, the data controller/s must implement a procedure for managing personal data breaches and notifying a national data protection authority and the data subjects in cases where such notification is mandatory.	

Table 8 – Accountability Principle

General Task	Description
Accountability Principle	Prove that necessary actions have been taken to comply with the EU privacy and data protection framework
The GDPR requires the controller to comply with the GDPR requirements and be able to prove it. Compliance with some of the obligations laid down in the GDPR, through a DPIA may, *de facto*, lead to ensuring accountability.[148]	
In PIMCity project context, data controllers must comply with the GDPR provisions and have to be able to demonstrate its compliance activity. The controllers must keep detailed documentation of the essential steps that have been taken while processing the data to achieve the results (within the identified scope of data processing activities). To comply with the accountability principle, a DPIA[149] has been launched at the beginning of the project and will be periodically updated.	

Table 9 – Appointment of a Data Protection Officer

General Task	Description
Requirements for the processing of personal data	Appoint a DPO which shall assist the controller or the processor in monitoring internal compliance with the GDPR requirements

[145] Art. 32 GDPR: 'Security of processing'.
[146] Art. 4 ePD: 'Security'.
[147] Art. 32 GDPR: 'Security of processing'.
[148] Art. 5(2) GDPR: '(Principles relating to processing of personal data), Accountability principle'.
[149] Art. 35 GDPR: 'Data Protection Impact Assessment'.

The GDPR requires the designation of a DPO under certain circumstances.[150] In particular, a DPO shall be appointed when *"(i) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (ii) 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 (iii) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Art. 9 GDPR and personal data relating to criminal convictions and offences referred to in Art. 10 GDPR"*.[151]
In compliance with GDPR provision, the PIMCity project partners shall appoint a DPO.

Table 10 – Purpose limitation principle

General Task	Description
Specification of the processing purpose	The purposes of the processing activities should be specified to comply with the purpose limitation principle
According to the GDPR, personal data have to be collected for a specific purpose. To comply with the purpose limitation principle, further processing of the same dataset is allowed only if the processing is compatible with the purpose for which they were collected in the first place. A compatibility assessment needs to be carried out to assess the compatibility of the initial purpose with the further ones.[152]	
In PIMCity project context, the processing of personal data has to be carried out having a specific purpose. An assessment of the compatibility of the initial data processing and the one carried out by PIMCity partners needs to be carried out.	

Table 11 – Lawfulness principle

General Task	Description
Definition of the lawful basis for processing personal data	Identify a suitable legal basis to comply with lawfulness principle.
According to the GDPR, the processing of personal data requires a lawful legal basis. When the controller uses the user consent as a legal basis for processing personal data, the GDPR specifies that the data controller has to fulfil specific requirements stemming from the GDPR. Guidance on the legitimate interests is provided in WP29 Opinion 06/2014.[153]	
In the PIMCity project context, personal data may be only processed by the Project partners if there is at least one of the legal basis provided in the GDPR. For example, in the case of processing that is considered concerning the personal data that would be collected in the PIMCity website, the consent shall serve as a legal basis. Taking into account the recent	

[150] Art. 37 GDPR: 'Designation of the data protection officer'.
[151] Ibid.
[152] Art. 5(1)(b) GDPR: '(Principles relating to processing of personal data), Purpose limitation principle'.
[153] Article 29 Working Party, Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, accessed 28/04/2020 844/14/EN WP 217.

decision taken by the ECJ,[154] consent of website page users' for processing their data should be considered valid when it is given through a proactive action (ticking the box).

Table 12 - Data Minimisation principle

General Task	Description
Requirements for the processing of personal data	Assess the necessity to process a certain amount of data to comply with the data minimisation principle
According to the GDPR, controllers should assess whether their purposes of data processing could be achieved with either fewer data or with appropriately anonymised datasets.[155]	
In PIMCity project context, the collection of data should be restricted to the identified purpose(s), which are limited to the strictly necessary scope, e.g., data analytics for marketing purposes. Each partner should only process personal data that are suitable and reasonable to accomplish the specified goals.	

Table 13 – Storage limitation principle

General Task	Description
Requirements for the processing of personal data	Personal data should be stored for the time it is necessary to perform a specific processing activity, and in line with national provisions concerning data retention periods.
The GDPR establishes that controllers should identify the purposes for which they are processing the data and determine a retention period accordingly to such purposes. Once those purposes have been fulfilled, data must be anonymised or securely deleted, unless there is another legal ground justifying their processing in an identifiable form.[156]	
In the PIMCIty project context, partners involved in processing activities should erase personal data once the identified purposes have been achieved, unless there is another legal ground justifying their processing in an identifiable form. If the same dataset is intended to be used for another purpose not compatible with the initial one, another legal ground that justifies the new processing activity should be found.	

Table 14 – Data subject's rights

General Task	Description
Requirements for the processing of personal data in light of data subjects' rights	Ensure the data subjects can exercise their rights
Art. 12 GDPR sets out the modalities for the exercise of the rights of data subjects. To comply with such provision, also ensuring the respect of the transparency and fairness principles, any communication issued by the data controllers must be phrased in a concise,	

[154] CJEU, Case C-673/17, paragraph 82(1).
[155] Art. 5(1)(c) GDPR: '(Principles relating to processing of personal data), Data minimisation principle'
[156] Art. 5(1)(e) GDPR: '(Principles relating to processing of personal data), Data storage principle'.

transparent, intelligible and easily accessible form, using clear and understandable language. Also, the data controller should support and facilitate the exercise of data subject rights.[157]
In PIMCity project context, the data controller should implement the necessary measures to facilitate data subjects in exercising their prerogatives (access, rectification, erasure, restriction, data portability, object). To comply with such requirement a form that data subjects can use to contact the data controller can be provided.

Table 15 – Data Protection by design and by default

General Task	Description
Requirements for the development of the project activities regarding the processing of personal data	Ensure that measures developed and activities carried out by project partners in the context of the project are the least privacy-invasive for the data subject
According to Art. 25 GDPR *'the controller shall implement appropriate technical and organisational measures for ensuring 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, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons'.*[158]	
In PIMCity project context, partners shall ensure that the least privacy-invasive preferences are selected by default.	

[157] Art. 12 GDPR: 'Transparent information, communication and modalities for the exercise of the rights of the data subject'.
[158] Art. 25 GDPR: 'Data protection by design and by default'.

Free flow of non-personal data

Table 16 - Requirements stemming from the NPD Regulation

General Task	Description
Assess the relevance of the requirements provided in the NPD Regulation	Assess whether the requirements provided in the NPD Regulation may be relevant in the light of the Project activities
The PIMCity partners shall assess whether the requirements provided in the NPD Regulation may be relevant in the light of the Project activities, in particular with regard to the obligation to provide access to non-personal data for competent authorities of various Member States.	

Copyrighted data

Table 17 - Requirements stemming from the InfoSoc Directive and the CDSM Directive

General Task	Description
Ensure there are no violations of copyright	(i) Assess whether the particular data which is relevant for the project may be protected by copyright; and, if yes, (ii) assess what kind of actions are likely to take place in the light of the project (e.g. reproduction of such data, communication to the public, etc.), and (iii) consider the alternatives for lawful processing of such data accordingly such as relying on authorisations or exceptions
The data that is processed during the project as well as during the exploitation phase of the project, may be protected by copyright. The processing of data may, therefore, infringe on the exclusive rights of copyright holders. It may be necessary for the partners to seek for authorisations of the right holders or to rely on one of the exceptions provided by the InfoSoc Directive and/or CDSM Directive, as implemented in the national laws accordingly.	
Overall, the partners (i) need to assess whether the particular data which is relevant for the project may be protected by copyright; and, if yes, (ii) to assess what kind of actions are likely to take place in the light of the project (e.g. reproduction of such data, communication to the public, etc.), and (iii) to consider the alternatives for lawful processing of such data accordingly such as relying on authorisations or exceptions. E.g., in case the PIMCity partners are to reproduce or communicate to the public copyrighted data, authorization from the right holders may be necessary. In relation to this, partners shall consider entering into an agreement with the right holders.	
Similar to the data processed during the project, the use of third-party software may infringe on the exclusive rights of copyright holders. Contractual agreements (i.e. essentially licensing agreement) will have to be considered for the use of third-party libraries.	
The partners shall also assess carefully any use of any other *work* in a broad sense to evaluate whether it may be protected copyright, taking into account not only the legal	

framework but also potentially relevant developments of the case law.[159] If the *works* appear to be protected by copyright, partners shall consider carefully what kind of actions are likely to take place in the light of the project (e.g. reproduction of such *works*, communication to the public, etc.) and consider the alternatives for lawful use of such *works*.

Database protection

Table 18 - Requirements stemming from the Database Directive

General Task	Description
Ensure there are no violations of the rights of the authors and makers of databases	(i) Assess whether the particular database may be protected by copyright and/or *sui generis* right; and, if yes, (ii) assess what kind of actions are likely to take place in the light of the project and (iii) consider the alternatives for a lawful approach such as relying on authorisations or exceptions
The relevant databases may be protected by copyright or by *sui generis* right as provided in the Database Directive and revealed in the first part of the deliverable D7.2. Specific actions of project partners may, therefore, infringe on the rights of the author or the maker of the databases.	
It may be necessary for the partners to seek for authorisations of the right holders or to rely on one of the exceptions provided by the Database Directive and/or CDSM Directive, as implemented in the national laws accordingly.	

Trade secrets protection

Table 19 - Requirements stemming from the Trade Secrets Directive

General Task	Description
Ensure there are no unlawful acquisition, use and disclosure of trade secrets	Assess whether certain *information* in a broad sense, including data, may be considered a trade secret
The relevant information may be protected by the Trade Secrets Directive as revealed above. Therefore, certain actions of project partners about such information may be considered unlawful.	
The project partners have to assess carefully whether certain *information* in a broad sense, including data, may be considered a trade secret; and, if yes, to comply with the requirements as provided in the Trade Secrets Directive as well as in the relevant national laws.	

[159] See, e.g. CJEU, Case C-406/10 SAS Institute Inc. v. World Programming Ltd.: Judgment of the Court (Grand Chamber) of 2 May 2012, EU:C:2012:259.

CONCLUSION

The deliverable D7.2 identifies the requirements for the PIMCity project stemming from the EU privacy and data protection legal frameworks and from legal frameworks governing intellectual property rights. In particular, the deliverable D7.2 identifies that some of the key and potentially relevant requirements stem from the provisions of the GDPR, the ePrivacy Directive, the NPD Regulation, the InfoSoc Directive, the CDSM Directive, the Database Directive and the Trade Secrets Directive. Accordingly, it provides a list of particular recommendations that shall be taken into account by the PIMCity project partners accordingly.

At this very early stage of the project (M6) KUL cannot provide an extensive overview of all of the relevant legal requirements. The requirements will be refined once the PIMCIty partners clarify the details related to the tools that are (planned to be) developed during the upcoming stages of the project and the data that are going to be used.

At the current stage of the project the partners shall, including but not limited:

(i) identify their roles in the light of the GDPR;
(ii) identify particular personal data that are (or are about to be) processed;
(iii) identify purposes, legal bases and other nuances related to such data processing as required by the GDPR;
(iv) enter into agreements among each other and with third parties, if necessary, in accordance with the requirements provided by the GDPR;
(v) prepare other necessary documentation such as privacy policies in order to comply with the obligations provided in the GDPR;
(vi) ensure appropriate technical and organisational measures are in place;
(vii) ensure personal data are being processed in accordance with all of the principles and requirements outlined in the GDPR;
(viii) assess whether the requirements provided in the NPD Regulation may be relevant in the light of the Project activities;
(ix) assess whether the particular data which is relevant for the project may be protected by copyright; and, if yes,
    a. assess what kind of actions are likely to take place in the light of the project (e.g. reproduction of such data, communication to the public, etc.), and
    b. consider the alternatives for lawful processing of such data accordingly such as relying on authorisations or exceptions;
(x) assess whether relevant databases may be protected by copyright and/or *sui generis* rights; and, if yes,
    a. assess what kind of actions are likely to take place in the light of the project and
    b. consider the alternatives for lawful approach such as relying on authorisations or exceptions;
(xi) assess whether certain *information* in a broad sense, including data, that is relevant for the Project may be considered a trade secret.

Given the activities undertaken in the light of this Project, it is necessary to conduct a DPIA, initial version of which is provided in the deliverable D7.1. Besides, due to the considered data collection in the PIMCity website(s), it may be necessary to prepare a privacy policy, cookie policy and consent forms for the website(s). The final overview of the legal requirements will be provided in the deliverable D7.5, due date month 30.

ANNEX A

Guidelines for defining partner's role in the light of the GDPR

It is important to identify the particular role of the partner such as *controller, processor* as well as identify specific cases such as *joint controllership* in the light of the GDPR, since depending on these roles the partners will have different obligations under the GDPR. These guidelines provide some basic advice that shall be helpful while determining these roles.

Explanations of the notions provided in the GDPR

A partner shall consider itself a **controller if it is** a 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 the EU or Member State law, the controller or the specific criteria for its nomination may be provided for by the EU or Member State law.

A partner shall consider itself a **processor if it is** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

In other words, the controller is the party that determines the purposes (why) and means (how) of the processing of the personal data. In essence, the controller decides which data will be collected, for which purpose, how the data will be processed and for how long such data will be processed and stored.

The term **processing** is rather broad as it designates any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The **processor** is the party that processes personal data on behalf of the controller(s). In other words, the processor only processes the personal data within the scope as determined by the controller.

It shall be noted that it is also possible that two or more parties jointly determine the purposes and the means of the *processing* of the *personal data*. In this event, the aforementioned parties qualify as ***joint controllers***.

Indicative checklists

The following checklists set out indicators as to whether a particular partner is a *controller* or a *processor* or whether some of them qualify as *joint controllers*. The more boxes a partner ticks, the more likely it is that it falls within the relevant category. The checklists are not to suggest, however, that certain amount of positive or negative answers guarantees certain qualification. Each case has to be analysed carefully on a case-by-case basis.

I. Is the partner a controller?

- The partner has decided to collect personal data.
- The partner has decided what the purpose or outcome of processing should be.
- The partner has decided what personal data should be collected.
- The partner has decided which individuals to collect personal data from.
- The partner obtains commercial gain or other benefits from the processing.
- The partner is processing personal data as a result of a contract between it and the data subject.
- The data subjects are partner's employees.
- The partner makes decisions about the individuals concerned as part of or as a result of the processing.
- The partner has complete autonomy as to how personal data is processed.
- The partner has appointed the processors to process personal data on its behalf.
- The partner decides how long to retain personal data.
- The partner decides regarding the legal basis for the processing of personal data.

II. Is there joint controllership?

- Partner has a common objective with others regarding the *processing* of *personal data*.
- Partner is *processing personal data* for the same purpose as another *controller*.
- Partner is using the same set of *personal data* (e.g. one database, one list with customer details, etc.) for *processing* as another *controller*.
- Partner has designed this process with another *controller*.
- Partner has common information management rules with another *controller*.

III. Is the partner a processor?

- Partner is following instructions from someone else regarding the *processing* of *personal data*.
- Partner was given personal data by a customer or a similar third party or told what personal data to collect.
- Partner does not decide to collect personal data from individuals.
- Partner does not decide what personal data should be collected from individuals.
- Partner does not decide the legal basis for the use of personal data.
- Partner does not decide what purpose or purposes personal data will be used for.
- Partner does not decide whether to disclose personal data, or to whom.
- Partner does not decide how long to retain personal data.
- Partner may make some decisions on how data is processed but implement these decisions under a contract with someone else.
- Partner is not interested in the end result of processing.

ANNEX B

Recommendations for the PIMCity project website

The PIMCity partners responsible for the project website(s) are recommended to begin their assessment the recommended questions listed below, including but not limited.

1. What personal data is collected (e.g. IP address; or also other such as name, first name)?
2. For what purposes are the personal data processed (e.g. analytics; or also for others such as enhanced functionalities, targeted advertising)?
3. Are the personal data shared with third parties (e.g. shared with some other company)?
4. Does the company/institution perform all processing activities itself or does it use third-party processing services? In case it uses third-party processing services, (4.1) please describe them.
5. Are there processors used in a non-EU country?
6. Do any of the processors use the collected personal data for their own purposes?
7. Does the application/website use cookies? If yes, (7.1) what are these, (7.2) do they collect personal data? (e.g. IP address, (7.3) are there any third-party cookies?

It shall be taken into account that in case some of the cookies as listed below is used, it is necessary to obtain the **informed consent** of visitors of the website relating to **the use** of such cookies:

- analytical cookies: cookies that allow tracking the browsing behaviour of visitors to and on the website;
- advertising cookies: cookies that allow tracking the browsing behaviour of internet users, and on that basis, allow the personalization of advertisements that are shown in advertising spaces on the website;
- social media-plug-ins: e.g. the Facebook like button on the website, “follow us on Twitter”, etc.

Overall in such cases, one needs to have at least (i) informed consent; (ii) privacy policy; (iii) cookie policy. Depending on relationships with third parties, various agreements such as *controller-to-controller* agreement, data processing agreement or *joint controller* agreement may be necessary.

References

Legislation

The TRIPS Agreement. Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, Marrakesh, Morocco, 15.04.1994.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L77/20 27.3.1996, p. 20–28.

Directive 2001/29/EC of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society, O.J.E.U. L167/10 22.6.2001, p. 10–19.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002 31.7.2002, p. 37–47.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, OJ L 337, 18.12.2009 18.12.2009, p. 11–36.

Regulation 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 [2016] OJ L 119, 4.5.2016, p. 1–88.

Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L 151/1 15.6.2016, p. 1–18.

Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, O.J.E.U. L303/59 28.11.2018, p. 59–68.

Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, PE/26/2019/REV/1, OJ L 136, 22.5.2019 22.5.2019, p. 1–27.

Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] O.J.E.U. L130/92 17.5.2019, p. 92–125.

Jurisprudence

The Court of Justice of the European Union, Case C-203/02 The British Horseracing Board Ltd and Others v. William Hill Organisation Ltd: Judgment of the Court (Grand Chamber) of 9 November 2004, ECLI:EU:C:2004:695.

The Court of Justice of the European Union, Case C-304/07 Directmedia Publishing GmbH v. Albert-Ludwigs-Universität Freiburg: Judgment of the Court (Fourth Chamber) as of 9 October 2008, ECLI:EU:C:2008:552.

The Court of Justice of the European Union, Case C-5/08 Infopaq International v. Danske Dagblades: Judgment of the Court (Fourth Chamber) of 16 July 2009, ECLI:EU:C:2009:465.

The Court of Justice of the European Union, Case C-403/08 Football Association Premier League Ltd and Others v QC Leisure and Others and Karen Murphy v Media Protection Services Ltd (C-429/08): Judgment of the Court of (Grand Chamber) of 4 October 2011, ECLI:EU:C:2011:631.

The Court of Justice of the European Union, Case C-406/10 SAS Institute Inc. v. World Programming Ltd.: Judgment of the Court (Grand Chamber) of 2 May 2012, EU:C:2012:259.

The Court of Justice of the European Union, Case C-202/12 Innoweb v. Wegener ICT media: Judgment of the Court (Fifth Chamber) of 19 December 2013, ECLI:EU:C:2013:850.

The Court of Justice of the European Union, Case C-673/17: Request for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 30 November 2017 — Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband e. V., OJ C 112, 26.3.2018, ECLI:EU:C:2019:801.

Other sources

Article 29 Working Party, Opinion 03/2013 on purpose limitation, WP 203.

Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

Article 29 Working Party, Guidelines on consent under Regulation 2016/679, revised and Adopted on 10 April 2018, 17/EN WP259 rev.01.

European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, adopted on 4 May 2020.

ICO, Guide to the GDPR – Lawful basis for processing: Legitimate interests, Web.

Alessandro Bruni, Amandine Leonard, Aleksandra Kuczerawy, SAFEDEED D.3.1, Legal Frameworks and Ethical Issues.

Athena Christofi, Els Kindt, Nadia Feci, SMOOTH D2.1, Requirements' Definitions.

Pierre Dewitte, Aleksandra Kuczerawy, Viltė Kristina Steponėnaitė, Peggy Valcke, CUTLER D1.4, Legal Requirements.

Pierre Dewitte, Aleksandra Kuczerawy, Peggy Valcke, CUTLER D1.1, Legal Taxonomy of Data Sets.

Pierre Dewitte, Aleksandra Kuczerawy, Peggy Valcke, CUTLER D1.2. Legal Requirements.

Inge Graef, Martin Husovec and Nadezhda Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law.* German Law Journal, Volume 19, Issue 6, November 2018, 1359-1398.

Olivia Solon, A simple guide to cookies and how to comply with EU cookie law, Wired Web.

Jean-Paul Triaille and others, *Study on the Legal Framework of Text and Data Mining (TDM).* (Publications Office 2014) 368–370 <http://bookshop.europa.eu/uri?target=EUB:NOTICE:KM0313426:EN:HTML>.

Perttu Virtanen, 'Innoweb v Wegener: CJEU, Sui Generis Database Right and Making Available to the Public – The War against the Machines' (2014) 5 European Journal of Law and Technology <http://ejlt.org/article/view/361>.