Grant Agreement Number: 825225

Safe-DEED

www.safe-deed.eu

Legal Frameworks and Ethical Issues

Deliverable number	*D3.1*
Dissemination level	*PU = Public*
Delivery date	*31.05.2019*
Status	*Final*
Author(s)	*Aleksandra Kuczerawy, Amandine Léonard, Alessandro Bruni*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825225.

Abstract

Deliverable 3.1 (D3.1) provides a high-level description of the EU legal frameworks that apply to the Safe-DEED project. The analysis will take into account the legislative initiatives already implemented and those that are still in the approval stage. D3.1 identifies the main requirements that should be taken into account in Working Packages 2, 4, 5 while an in-depth legal analysis of main requirements for the use cases in WPs 6 and 7 will be provided in the upcoming deliverables (D.3.2 and D 3.3).

Table of Contents

List of abbreviations

Art	Article
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
DCD	Digital Content Directive
EC	European Commission
ECHR	European Charter of Fundamental Rights
ECtHR	European Court of Human Rights
ePD	e-Privacy Directive
EPR	E-Privacy Regulation
FFNPDR	Free Flow of Non-Personal Data Regulation
FRAND	Fair, Reasonable and Non-Discriminatory

GDPR	General Data Protection Regulation
IPRs	Intellectual Property Rights
NIS	Network and Information Security Directive
NRA	National Regulatory Authority
P2BR	Platform to Business Regulation
R&D	Research and Development
Rec	Recital
TFEU	Treaty on the functioning of the European Union
WP29	Article 29 Working Party

Executive Summary

This deliverable has been drafted taking into account **Safe-DEED** project characteristics, activities and context following a tailored approach. Considering that the upcoming Deliverables (D3.2 and D3.3) will provide a precise specification on the legal and ethical requirements that need to be taken into account for the development of WP6 and 7 use cases, D3.1 will mainly focus on mapping the legal and ethical aspects that can be considered within the Safe-DEED project.

One of the primary purposes of the project is the improvement of the exploitation of Privacy enhancing technologies. Thus, it is important to provide a focus on the EU privacy and data protection legal and ethical framework considering it as a standard when it comes to privacy and data protection. Within the first chapter, primary attention will be paid to the two main legislation in this area, i.e., the General Data Protection Regulation and the e-Privacy Directive. Chapter 2 provides an overview of the ethical principles that should be taken into account throughout the development of the project. Specific emphasis will be put in this chapter on the ethical aspects involving the management of personal data and on AI latest initiatives.

Another goal of the **Safe-DEED** Consortium concerns the development of new Multi-Party computational methods that require the creation of a multi-party platform. Therefore, an overview is provided of the latest legislative initiatives that have been taken by the European Commission (EC) on the topic of interoperable platforms and free flow of non-personal data. Specific attention will be paid to the latest regulation on the Free Flow of Non-Personal Data and the so-called "Platform to Business" proposal. Additionally, the **Safe-DEED** consortium should also take into account specific security and competition law aspects which may stem from the current EU framework.

Lastly, even if the setup of the **Safe-DEED** project does not foresee a direct involvement of consumer at this stage, some implications and novelties coming from consumer protection laws need to be considered. One particular implication is notably the latest legislative attempt by EU to regulate contracts involving the use of personal data. Thus, the Digital Content Directive and the concept of personal data as a form of payment for concluding agreements will be reviewed. This will be conducted in light of the relationship between the directive and the EU framework on privacy and personal data.

1 Privacy and Data Protection

Introduction

The exploitation of Privacy Enhancing Technologies[1] by multiple private entities is one of the **Safe-DEED** main goals. Consequently, the first chapter analyses the legal requirements that should be taken into account by each member of the Consortium when carrying out activities involving individuals' personal data. In particular, these will be taken into account in the development of the two use-cases.
This section is divided into three parts: the first one introduces the concept of privacy and data protection and aims at clarifying the differences and similarities that may exist between overlapping concepts. The second parts deals with the current applicable privacy and data protection legal regimes. In particular, the General Data Protection Regulation (GDPR) and the e-Privacy Directive (ePD). The last part of the first chapter describes the latest proposal from the EC to replace the ePD by the e-Privacy Regulation (EPR).

Considering the hierarchy of the sources, the deliverable will first analyse the European Convention of Human rights,[2] and the Charter of Fundamental Rights of the European Union.[3] Next, the deliverable will describe the binding EU legislative initiatives in the area of privacy and data protection.

1.1 Clarifications Regarding Privacy and Data Protection

First, it is necessary to make a clear differentiation between privacy and data protection. These two notions may seem to overlap, but they, nonetheless, differ in scope and meaning. To make a clear differentiation between the two concepts, the following sections highlight their similarities and differences.

1.1.1 European Convention of Human Rights

Both privacy and data protection are fundamental rights. While the former is recognized by Art 8 of the European Convention of Human Rights (ECHR) and Art 7 of the Charter of Fundamental Rights of the European Union (CFREU), the latter has no references in the ECHR, but is, nonetheless, mentioned in Art 8 CFREU. Despite the lack of explicit reference to data protection in the text of the ECHR, the European Court of Human Rights (ECtHR) has made a reference to the right of data protection when interpreting Art 8 ECHR. Besides, even if the right to data protection is not part of the ECHR, the Council of Europe has included such right in the Convention 108 on the Protection of Individuals concerning the automatic processing of personal data.[4]

[1] The term **Privacy Enhancing Technologies (PETs)**, which covers the broader range of technologies that are designed for supporting privacy and data protection, ENISA Report, *'A tool on Privacy Enhancing Technologies (PETs) knowledge management and maturity assessment'*, March 2018, available < https://www.enisa.europa.eu/publications/pets-maturity-tool/at_download/fullReport> accessed 26 April 2019.
[2] European Convention of Human Rights, Council of Europe, 1953.
[3] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407.
[4] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

Art 8 ECHR, which recognises the right to respect for private and family life, states: *'1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.*

The case law developed by the ECtHR based on Art 8 ECHR has interpreted the Convention as prescribing negative and positive obligations upon contracting parties. On the one hand, positive obligations require from States to take all the necessary measures to protect each citizen against any unjustified restriction of their fundamental rights. On the other hand, negative obligations require that States do not have to hamper the enjoyment and exercise of fundamental rights, such as the right to privacy and data protection, unless a reason makes the interference necessary. When a conflict occurs between two competing fundamental rights, a fair balance must be found.

1.1.2 Charter of Fundamental Rights of the European Union

The CFREU has become a source of primary law in Europe following the entry into force of the Lisbon Treaty (TFEU) in 2000.[5] At that time, the fundamental rights included in the Charter have been recognised as fundamental rights in the EU normative order.[6] Since then, EU bodies and Member States have to guarantee the protection of the Charter rights also when implementing EU legislation.[7]

1.1.2.1 Similarities and Differences between Privacy and Data Protection

Both the ECHR and the CFREU recognise the possibility to interfere with the right to privacy and data protection when it is justified. According to the Court of Justice of the European Union (CJEU), an interference with the right to privacy occurs when information related to private life is collected, stored, or disclosed, regardless if '*the information is sensitive or whether the person concerned has been inconvenienced in any way*'.[8] Therefore, we can assume that since the processing of data by individuals is likely to interfere with their right to privacy and data protection, it requires a legal justification. Art 8(2) CFREU explains that data have to be processed '*fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law*'.[9] In substance, Art 8(2) CFREU develops the so-called three-step test that should be applied when it is necessary to verify

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

[6] Gloria González Fuster, 'EU Fundamental Rights and Personal Data Protection', *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, Cham 2014) p.192 <https://link.springer.com/chapter/10.1007/978-3-319-05023-2_6> accessed 24 April 2019.

[7] Art 52(1) CFREU: '*The provisions of this Charter are addressed to the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers.*'

[8] CJEU, *Österreichischer Rundfunk and Others*, C-456/00 para 75.

[9] Joined Cases *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, para. 49.

if interference is justified: 1) it must be foreseen by the law, 2) it pursues a legitimate interest 3) it is necessary for a democratic society.[10]

Regarding the first condition, the CJEU has repeatedly stated that an interference can occur when it comes from a national legislative act that does not have a sufficient degree of foreseeability.[11] Indeed, a general provision that does not provide guarantees and limitations for the collection and processing of data, does not meet the criteria laid down in Art 8(2) CFREU.

The second condition that should be met is linked to the broad notions of '*national security*', '*public safety*', '*economic well-being of the country*', '*prevention of disorder or crime*', '*protection of health or morals*' or – even wider – '*the protection of the rights and freedoms of others*'. Considering also Art 52(1) CFREU, which covers objectives of general interests defined by the Union, any interference should be justified under one of those grounds.[12]

The third condition that must be fulfilled to justify interference with fundamental rights is that it should be '*necessary in a democratic society*'. In addition, Art 52(1) recalls the general principle of proportionality, which requires that '*the content and form of Union action shall not exceed what is necessary to achieve the objectives of the treaties*'.[13] This last condition is linked to the second condition, and implies that the interference has to answer a '*pressing social need*'.[14] Therefore, it has to be supported by sufficient reasons and be proportionate to the aims identified at the occasion of the second and third step of the test. When assessing the necessity of the interference, States benefit from a wide margin of appreciation whose scope largely depends on the legitimate aim pursued and the means used to achieve it.[15][16]

The principal distinction between data protection and privacy concerns their scope. According to Art 8 ECHR and Art 7 CFREU, the concept of privacy is linked to '*private and family life, home and correspondence/communications*.'[17] The concept of data protection, on the other hand, is related to the concept of '*personal data'*, which has been defined by the Convention 108 as '*any information relating to an identified or identifiable natural person*'. Even if there are many envisaged similarities between these two concepts, they do not always collide. Though in the majority of cases an interference in the processing of personal of the data subject will also affect his or her privacy, there might be the cases where only one of these two rights is affected.

[10] These requirements come from Art 8(2) ECHR and Art 52(1) CFREU. Even though phrased differently, they prescribe a similar test.
[11] ECtHR, Rotaru v. *Romania*, n. 28341/95, para. 52, ECHR 2000-V; ECtHR, *S. and Marper v. the United Kingdom*, n. 30562/04 and 30566/04, para. 95, ECHR 2008; Kennedy v. the United Kingdom, no. 26839/05, para. 122 and 123.
[12] In the Digital Ireland cases the CJEU stated '*the retention of data for the purpose of allowing the competent authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest*' (CJEU cases C-293/12 and C-594/12, para. 44).
[13] Art. 5(3) of the Treaty establishing the European Union, *O.J.U.E.*, 26 October 2012, C326, pp.13-390.
[14] ECtHR, *Sunday Time v. The United Kingdom*, n. 6538/74, para. 50c.
[15] ECtHR, *Leander v. Sweden*, n. 9248/81, para. 59.
[16] Pierre Dewitte, Aleksandra Kuczerawy, Peggy Valcke, CUTLER D1.1. Legal Taxonomy of Data Sets, < https://www.cutler-h2020.eu/>, accessed 26 April 2019
[17] European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights' <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed 24 April 2019.

Consequently, an interference with the right to privacy may have to be assessed in light of Art 8(2) ECHR and Art 52(1) CFREU, while an interference with the right to data protection may have to be assessed in light of Art 8(2) ECHR, as well as Art 8(2) and 52(1) CFREU.[18]

The activities of collection and processing of data sets that include personal data and are carried out by the **Safe-DEED** partners determine that their undertakings fall within the scope of application of both Art 8 of the CFREU and Art 8 of the ECHR. Therefore, the collection and processing of these data have to be considered as and interference with these fundamental rights. Consequently, these activities need to be justified in light of Art 8(2) and 52(1) CFREU for what concern the right to data protection, and regarding Art 8(2) ECHR and 52(1) CFREU for the right to privacy.

1.2 General Data Protection Regulation

1.2.1 Introduction

The Regulation 2016/679 (General Data Protection Regulation - **GDPR**)[19] entered into force on the 25th of May 2018. The GDPR, whose legal basis has been identified in Art 16 (2) of the Lisbon Treaty (TFEU)[20] regulates the protection of individuals about the processing of personal data and the free movement of such data.

The GDPR replaces the Directive 95/46 on the protection of individuals about the processing of personal data and the free movement of such data.[21] The EU policymakers deemed to move from a directive, which has to be implemented by the Member States through national legislation, to a regulation – the GDPR –which is directly applicable across all EU Member States. The main reason for this shift was that the Directive 95/46/CE *'ha[d] not prevented fragmentation in the implementation of data protection across the Union'*. Also, achieving *'effective protection of personal data requires the strengthening and the setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data'*. [22]

The GDPR represents the cornerstone of the new Data Protection Framework, it sets a higher standard for what concerns the protection of individuals. It is expected the that new regime will enhance business opportunities for EU entities and, consequently, boost the EU Digital Single Market. By broadening the

[18] Paul De Hert and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' [2017] Computer Law & Security Review <http://www.sciencedirect.com/science/article/pii/S0267364917303333> accessed 24 April 2019.
[19] 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] *O.J.E.U.*, L119/1.
[20] Art 16(2) TFEU: *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*
[21] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data [1995] *O.J.E.U.*, L281/31.
[22] Rec 9 -11 GDPR.

scope of the Directive 95/46, the GDPR allocates duties and responsibilities, provides indications to data subjects on how to exercise their rights, clarifies which national law applies and consequently the national supervisory authority that should be competent in a case involving the processing of personal data.

Even if the GDPR is directly applicable, Member States keep a limited margin of appreciation in the implementation of determined matters (such as age threshold governing child's consent, the processing of sensitive data, the exceptions to some of the data subject's rights, the provisions dealing with the data protection officer and the rules on data transfers).[23]

In the context of the **Safe-DEED** project, the initial question stemming from the privacy and data protection framework, is whether the data collected and/or processed by relevant stakeholders in the project, can be qualified as personal data, and if they do, which rules should be applied.

1.2.2 Scope

Art 2(1) of the GDPR states that the regulation applies to *'the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system'*.[24]

Even if the notion of personal data is essential with regard to its application, there are also other important elements related to GDPR provisions that should be considered to tailor its scope of application.

1.2.2.1 Material Scope: Processing of Personal Data

Art 4(2) GDPR defines the activity of **processing**, and consequently the material scope of application, as *'any operation or set of operation which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'*. This broad definition describes all possible activities concerning data, from the initial collection to their erasure.

Anticipating such approach, the CJEU – referring to Art 2(b) Directive 95/46 which defines the processing of personal data – had already interpreted extensively the concept of processing. For example, the Court recognized that the activities carried out by a search engine must be classified as processing, *'although the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data*'.[25] In

[23] See Winfried Veil's map on the opening clauses in the GDPR <https://www. flickr.com/photos/winfried-veil/24134840885/in/dateposted> accessed 10 May 2019.
[24] Art 2GDPR.
[25] Case C-131/12 Google v. Agencia Española de Protección de Datos (AEPD): '*Therefore, it must be found that, in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as 'processing' within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data*.'.

another case, the Court also clarified that '*the operation of loading that page onto a server and the operations necessary to make that page accessible to people who are connected to the internet'*, has to be considered a processing operation.[26] Lastly, the CJEU also declared that the publication of data that has already been published in the media, in an unaltered form, falls within the definition of processing.[27]

Art 4(1) GDPR defines '***personal data***' as '*any information relating to an identified or identifiable natural person ('data subject')*'. It also explains that '*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*'.

To support Member States application of the provision, the Article 29 Working Party (WP29) – now European Data Protection Board (EDPB) – has adopted an Opinion clarifying the concept of personal data. [28]

The WP29 Opinion builds upon the notion of 'personal data', inherited from the Council of Europe's Convention 108, and specifies which information encompasses **'any information**.

The WP29 Opinion clarifies that the nature of an information is not relevant to determine if it is personal or not: any information or statement that identify a person can be considered as personal data. Also, to determine if an information is personal, there is no difference if it is related to an individual's private sphere or concerns his professional activity. Lastly, the format or medium where the information is contained (paper or digitally stored) does not make any difference for the qualification. The CJEU, in the *Nowak* case, has also echoed such a conclusion.[29] In the end, similarly to the concept of processing, such a broad approach leaves the door open for the identification of personal data to a vast amount of data.

After having analysed the concept of 'information', WP29 explains that the term **'relating to'** means that there must be a relationship between a piece of specific information and a person. Such a link can be clear and direct but can also be not so self-evident. Therefore, to classify an information as 'relating to', the WP29 considers: content (i.e. when the information is about a person), purpose (i.e. when the data are used or are likely to be used with the purpose to evaluate, treat in a certain way or influence the status or behaviour of that person) or result (i.e. when the data used are likely to have an impact on that person's rights and interests) element must be present.

Finally, the information must be related to an **'identified or identifiable'** person. According to the WP29 Opinion, an individual is identified when it is possible to pinpoint this individual within a group of people and distinguish him from the rest of the group. On the contrary, an individual is identifiable when he has not yet been identified but can be identified. Such identification process can occur directly, through the name (or additional information if the individual is not the only one with that name) or indirectly, using different pieces of information that combined make possible to identify a specific individual. Rec 26 GDPR states that '*account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly*'. In turn, the means reasonably likely to be used must be assessed in light of '*objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*'.

[26] Case C-101/01 *Bodil Lindqvist,*, para. 25.
[27] Case C-73/07, Satakunnan Markkinapörssi and Satamedia, para. 48-49.
[28] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (WP136).
[29] Case C-434/16, *Nowak v. Data Protection Commissioner*.

Concurring with this provision, the CJEU has ruled that dynamic IP addresses, despite their randomness, constitute a piece of information that can allow the identification of the user by the internet service provider.[30] Hence, an analysis of the factual situation is necessary to evaluate the applicability of the GDPR.

Another concept that should be explained in relation to the activities that are going to be carried out by the **Safe-DEED** partners is related to the **pseudonymisation**.

Pseudonymisation is defined by Art 4(5) as '*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*'. The WP29 specifies that such process makes it possible to disguise the identity of data subjects in a way that makes possible to collect information without knowing the subject names. Pseudonymisation can be done in a retraceable or untraceable way, usually through the use of algorithms. In the former case, individuals can be identified, and consequently, these pseudonymised data fall into the scope of GDPR's scope of application. In the latter case, process creates **anonymized data** and is un-retraceable, in the sense that the identity of the subject is cannot be discovered or even deleted.

To sum up, the possibility to identify the subject marks the difference between pseudonymisation and anonymisation process. Therefore, Rec 26 GDPR states that '*the principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable*'. Therefore, a case-by-case analysis should be carried out to assess the context where data are processed, the techniques that have been used to anonymise data and ultimately, if these methods make the identification of data subjects no longer possible. If this is the case, the anonymised data fall out of the GDPR's scope of application.[31] The above mentioned WP29 Opinion acknowledges keeping anonymised data valuable, is a challenging exercise. Anonymisation, in the way it has been defined in the WP29 Opinion, is an evolving process that will be affected by the relevant technologies, but also by the environment in which data are being processed.

This discussion is crucial and has appeared in many contexts, for example in the context of the blockchain technology, where the current technology architecture makes it problematic to have anonymised data within the chain.

In **Safe-DEED**, large amounts of data will be gathered from different sources and combined using analytics technologies. Therefore, anonymisation techniques are going to be fundamental. As has been demonstrated on several occasions, it is not so difficult to link anonymised or partially anonymised data to a specific individual. [32] Nonetheless, it should be stressed that one of the fundamental purposes of the

[30] Case C-582/14CJEU, *Patrick Breyer v. Bundesrepublik Deutschland*, , para. 31-49.

[31] On identifiability: Stijn Storms, 'Identify Me If You Can – Identifiability and Anonymisation' (*CITIP blog*) <https://www.law.kuleuven.be/citip/blog/identify-me-if-you-can-identifiability-and-anonymisation/> accessed 20 March 2018.

[32] In practice, it has already been demonstrated that very basic, or at least partially 'anonymised' data, may be linked to a person without much efforts. In that sense, see *a.o.*: Larry Hardesty, 'It's Surprisingly Easy to Identify Individuals from Credit-Card Metadata' (*MIT News*, 29 January 2015) <https://news.mit.edu/2015/identify-from-credit-card-metadata-0129> accessed 8 February 2018; Latanya Sweeney, 'Simple Demographics Often Identify People Uniquely' Carnegie Mellon University, Data Privacy Working Paper

Safe-DEED project is the valuation of the information that is possible to extract from the data gathered, rather than the identification of individual as such.

The last pillar analysed by WP29 relates to the notion of **'natural person.'** To fall into the scope of application of the GDPR, data must be related to a living person.

1.2.2.2 Subjective scope: Processor and Controller

The GDPR, enhancing and expanding what was already established in the Directive 95/46, lays down specific rules and obligations concerning actors involved in the processing of personal data, namely, controller and processor. According to the different role they have in the processing of personal data, the GDPR allocates responsibility for compliance and imposes specific rules to ensure security and confidentiality of the processing.

The WP29 had published an Opinion on the role of controller and processor before the GDPR entered into force.[33] In this Opinion, the WP29 indicates the elements that should be taken into account when determining the role of the actors involved in the data processing. Precisely, the following elements should be considered: the level of instruction received by the data controller, the monitoring activity carried out by the controller, the visibility given by the data controller to the data subjects together with their expectations when identifying who is responsible for the compliance with data protection rules. Finally, taking into account what was stated by Art 28(10) GDPR, it is important to stress that when a processor determines the purposes and means of processing, he should be the one considered as a data controller.

1.2.2.2.1 Controller

Art 4(7) of the GDPR defines a controller as '*the natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data*.'

First, the WP29 Opinion explains that if a natural person is appointed to deal with data protection in a given company, he should be considered as acting on behalf of the company, while the company is considered the controller. Consequently, the responsibility to comply with GDPR's rule falls on the company, not on his employer, regardless of his role.

Second, the controller is the one that has to '*determine the means and purposes'* of the personal data processing. The factual ability to control the processing should nevertheless be assessed since there might be cases where the decision and activities carried out by the controller might be done by someone else. When evaluating whether or not an entity has the ability to determine purposes and means of the processing, the WP29 recognises three circumstances which are typically linked to the concept of

<https://dataprivacylab.org/projects/identifiability/ paper1.pdf> accessed 19 March 2018; Arvind Narayanan and Vitaly Shmatikov, 'Robust De-Anonymization of Large Sparse Datasets' (IEEE 2008) <http://ieeexplore.ieee.org/document/4531148/> accessed 19 March 2018; John Bohannon, 'Credit Card Study Blows Holes in Anonymity' (2015) 347 Science 468; JK Trotter, 'Public NYC Taxicab Database Lets You See How Celebrities Tip' (*Gawker*) <http://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546> accessed 19 March 2018.

[33] Article 29 Working Party, 'Opinion 1/2010 on the concepts of controller and processor' (WP169).

control: legal competence, implicit competence, and factual influence to control the natural or legal person that is empowered to make decisions.[34]

Third, the WP29 Opinion highlights situations where multiple parties are involved as controllers with different degree of participation. There are cases where several parties jointly decide the purpose and means of the processing. When this happens, the responsibility must be considered equally shared among the parties. In other cases, multiple actors might be involved within the same process but pursue different purposes through independent means. Moreover, the degree of collaboration between the partner controllers might vary, leading to situations where 'collaborating single controllers' and 'partly joined controllers' occur. In those cases, a clear definition of role and responsibility of the entities is necessary.

Within the **Safe-DEED** project, it is necessary to identify the entities that are involved in the different processing operations, their purposes and means. Each partner that processes personal data for the purposes and through the mean uniquely determined by its activity has to be considered as an autonomous controller. The relevant key requirements that need to be fulfilled in compliance with GDPR provisions, according to the different tasks that will be carried out by Consortium partners for the processing of personal data, will be provided in the next deliverable (D3.2.).

1.2.2.2.2 Processor

The notion of processor is described in Art 4(8) GDPR. According to this provision, a processor is the *'natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller.'*[35] Controllers usually assign parts of the operation to one or more processors, while in some cases they can also delegate the determination of the means of the whole process to them. Considering the characteristics of the activities carried out by a processor, the EU legislator has imposed on them only limited obligations.

Art 28(3) GDPR specifies that a contract, or a legally binding act, between controller and processor, should govern their relationship. Such a contract has to clarify the subject and duration of the processing, nature and purpose, type of personal data, together with the rights and obligations of the controller.

1.2.3 GDPR General Principles

The GDPR expands upon the fundamental principles already enunciated and introduced by the Convention 108 and the Directive 95/46.

The list of data protection principles includes:

- Lawfulness, fairness, and transparency;

[34] Article 29 Working Party, 'Opinion 1/2010 on the concepts of controller and processor' states that '*a last characteristic of the concept of controller is its autonomy, in the sense that, although external legal sources can help identifying who is a controller, it should be interpreted mainly according to data protection law*'. It then adds that '*the concept of controller should not be prejudiced by other - sometimes colliding or overlapping - concepts in other fields of law, such as the creator or the right holder in intellectual property rights; being a right holder for intellectual property does not exclude the possibility of qualifying as "controller" as well and thus be subject to the obligations stemming from data protection law*'.

[35] Art 4 GDPR.

- Purpose limitation;
- Data minimization;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality;
- Accountability.

Data controllers, while performing their activities, have to comply with these principles. Considering this, a brief overview of the enumerated principles will be given in the following section, while an in-depth analysis of potential implications and requirements will be carried out in the next deliverable (D3.2.).

1.2.3.1 Lawfulness, fairness and transparency

According to Art 5(1)(a) GDPR, personal data have to be *'processed lawfully, fairly and in a transparent manner about the data subject'*[36]. These three characteristics are complementary and require to be clarified separately.

To be **lawful**, the processing of personal data has to be carried out on the basis of one of the six legal grounds listed in Art 6(1) of the GDPR: consent, the performance of a contract, legal obligation, the vital interest of individuals, public interest and the legitimate interest.

In the **Safe-DEED** context, the data subjects' consent and controllers' legitimate interest are likely to be the most appropriate legal grounds for processing datasets provide for the use cases, at the core of the Safe-DEED project.

Fairness principle aims to balance potential power asymmetries between the data controller and data subject striking a '**fair balance**' when applying data protection rules to a given situation. Concretely, personal data must not be processed in a way which unreasonably infringes the fundamental rights and freedoms of data subjects and, in particular, their right to the protection of personal data. Therefore, fairness should be achieved through compliance while having in mind controllers' obligations and subjects' rights.

Transparency principle is strictly linked to the fairness one. To fulfil the transparency requirement, each activity characterising the processing must be executed transparently. To accomplish the purpose, Arts 12, 13 and 14 GDPR set the modalities and the necessary information that should be provided to a data subject by a controller when processing personal data. Information that needs to be provided refers to the purpose for which the personal is used and the legal basis for the processing.[37]

1.2.3.2 Purpose Limitation

Art 5(1)b GDPR, which embeds the **principle of purpose limitation**, foresees that personal data shall be '*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest,*

[36] Art 5(1)a GDPR.
[37] Art 14(2)f GDPR.

scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes'. The WP29 has described the purpose limitation principle considering two components.[38]

First, personal data have to be collected for *specified, explicit and legitimate* purposes: there must be a correspondence between the collection of data and the purpose activity when they are processed. The purpose has to be specified to permit the implementation of data protection safeguards and to delimit the scope of the processing. The purpose has to be explicit to delimit the scope of the activity, avoiding any untailored activity by the controller. Lastly, legitimacy, which should not be confused with the lawfulness basis for processing, refers to the legitimate expectations of the data subject that should be respected.

Moreover, the purposes identified for collecting data and the purpose for processing the data must be compatible. Art 5 GDPR refers to further processing and applies to any operation after the collection of personal data. To assess the compatibility between the initial purpose and the subsequent ones, Rec 50 GDPR lists several criteria that should be met:

- The relationship between the purposes for which data have been collected and the purpose that leads the subsequent data processing activities;
- The context in which data have been collected and the subsequent expectations of the data subject regarding their further use;
- The nature of personal data and the impact of further use on the data subject;
- Safeguards put in place by the controller to ensure fair processing. [39]

Second, when carrying out an activity whose purpose is listed in Art 5(1)b GDPR, the compatibility with the original purpose is assumed. Nonetheless, the GDPR does not give a definition of scientific and statistical research, leaving space to legal uncertainty.[40] Contrary, when data have been initially collected with the primary purpose of scientific or statistical analysis, the legal basis for processing should be found in one of the cases listed in Art 6 GDPR, presumably, the legitimate interest of the controller.[41]

1.2.3.3 Data minimization

Art 5(1)(c) GDPR requires that the processing of personal data should be *'adequate, relevant and limited to what is necessary about the purposes for which they are processed.'* To comply with this requirement a necessity and proportionality test is indispensable.[42] When it comes to necessity, the data minimization principle requires that the controller should only use data that are reasonable for achieving the specified purposes of his activity. Therefore, the proportionality requirement enshrines the idea that controllers have to assess whether their purposes could be achieved with either fewer data or with properly

[38] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (WP 203).
[39] Similarly, Art 6(4) GDPR.
[40] Rec 159 GDPR: '*the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research*'.
[41] On that point, see: Natalie Bertels, 'Scientific Research under the GDPR: What Will Change?' <https://www.law.kuleuven.be/citip/blog/scientific-research-under-gdpr-what-will-change/> accessed 23 March 2018; Gabe Maldoff, 'How GDPR Changes the Rules for Research' <https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/> accessed 24 April 2019.
[42] Article 29 Working Party, 'Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector' (WP211).

anonymised datasets. Consequently, it requires controllers to tailor the amount of collected data and their retention period, to the identified purposes.[43]

1.2.3.4 Accuracy

Art 5(1)d GDPR states that personal data shall also 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'*. Therefore, when collecting and processing data subjects' data, controllers need to verify the correctness of the data. Similarly to the previous principles, the purpose and the context of the controller's activities determine the fairness of the measures he or she implements.

1.2.3.5 Storage limitation

When it comes to the storage limitation principle, Art 5(1)e GDPR states that personal data shall be *'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject'*. Therefore, the controller has to identify the purpose of the processing and consequently the data retention period. Once the purpose has been fulfilled, data have to be securely anonymised or deleted. Nonetheless, the same data can be used for a different purpose and in that case, instead of being removed or anonymised, they can be retained for the time strictly necessary for achieving the new purpose. On the other hand, Art 5(1)e GDPR foresees that *'personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes'*.[44]

1.2.3.6 Integrity and Confidentiality

The principles of integrity and confidentiality are embedded in Art 5(1)f GDPR which states that personal data shall also be *'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures'*. In the context of security and confidentiality requirements, this article has to be read in combination with Art 32 GDPR on security measures,[45] and Art 33 GDPR on data breach. Concretely, when processing data, and in order to comply with the principles of integrity and confidentiality, mitigation strategies and risk analysis should be developed at the technical and management level.

[43] Rec 39 GDPR: (data minimisation) '*requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum*'.
[44] Rec 39 GDPR: (data minimisation) '*requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum*'.
[45] Art 32 GDPR describes the technical measures that can be used to ensure integrity and confidentiality such as encryption protocols.

In relation to the **Safe-DEED** project, specific mention should be given to personal data breach. According to Art 33 GDPR *'the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Art 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay'*. In case of activities that are carried out by the processor, the processor should inform the controller about the data breach.

1.2.3.7 Accountability

According to Art 5(2) GDPR, '*controllers shall be responsible for, and be able to demonstrate compliance with*' all the above-mentioned principles.[46] In addition, Art 25 GDPR requires that the controller, taking into account all the elements of processing, puts in place adequate technical and organisational measures, which have also to be demonstrated, to prove that the processing has been carried out in compliance with the GDPR requirements.

The Accountability principle constitutes a significant novelty of the GDPR, as compared to Directive 95/46. Nonetheless, this is not a new concept and references can be found, among others, in a WP29 Opinion[47], in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[48] and other international agreements[49].

1.2.4 Data Controllers' obligations

The controller must comply with various obligations. First of all, it has to execute its tasks in compliance with the principles described in the previous section. It means that every processing activity has to be based on one of the lawful grounds listed in Art 6 GDPR and it has to be carried out following a specified, explicit and legitimate purpose. As for the accountability principle, the controller must adopt and demonstrate that appropriate technical and organizational measures have been taken and implemented during the whole process.

It is crucial for the controller, when carrying out its activities, to choose processors '*providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'*.[50] Also, allocation of responsibilities as well as clear definitions of the tasks assigned to the processor, should be defined in a written contract, as stated in Art 28(9) GDPR (this can also be done electronically). To comply with the transparency requirement, the controller has to keep a record of the

[46] Art 5(2) GDPR
[47] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173).
[48] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 2013, C(80)58/final, <https://www.oecd.org/sti/ieconomy /2013-oecd-privacy-guidelines.pdf accessed 24 April 2019.
[49] See a.o. International Standards on the Protection of Personal Data and Privacy (The Madrid Resolution), International Conference of Data Protection and Privacy Commissioners, 5 November 2009 <https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_en.pdf> accessed 27 April 2019 2018.
[50] Art 28 GDPR

processing activities that are carried out, which has to include at least the elements that are listed in Art 30(1) GDPR.[51] [52]

Following Art 32 GDPR, controllers also have to ensure a level of security that is adequate to the risk for the rights and freedoms of data subjects that can occur during processing activities. Therefore, Art 32(1)a-d GDPR lists measures that can help the controller in fulfilling such obligation.[53]

1.2.5 Data Subjects Rights

Data subjects have specific rights regarding activities that involve the processing of their personal data. The modalities for the exercise of these rights are listed in Art 12 GDPR. For example, Art 12 requires that any communication issued by the controller to data subjects should be *'concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.'*

The right to access represents the first essential right that is granted by the GDPR to data subjects for exercising their rights in the context of personal data processing. Without access to personal data, many rights granted to data subjects could not be claimed. The right to access can also be introductory to verify data controller compliance with GDPR provisions. Art 15 GDPR gives data subject the right to obtain information from the controller as to whether his or her data are processed. If this is the case, the data subject has the right of access the data and the following information: *(1) the purposes of the processing, (2) the categories of personal data concerned, (3) the recipients or categories of recipients to whom the*

[51] Art 30(1) GDPR: *Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:*
(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
(b) the purposes of the processing;
(c) a description of the categories of data subjects and of the categories of personal data;
(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
(f) where possible, the envisaged time limits for erasure of the different categories of data;
(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

[52] Art 30(5) GDPR foreseen exception to this obligation: *'The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.'*

[53] Art 32(1) GDPR: *1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

personal data have been or will be disclosed, (4) the retention period, (5) the existence of the right to rectification or erasure, (6) the right to lodge a complaint with a supervisory authority, (7) the source of the personal data and (8) the existence of automated decision-making.[54]

The right to rectification (Art 16 GDPR) gives data subjects the right to request *'the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement'*.[55] This right is complementary to the principle of accuracy of personal data.

Art 17 GDPR gives data subject **the right to erasure of data**. This right, also known as 'the right to be forgotten', gives data subjects the possibility, under certain circumstances, to *'obtain from the controller the erasure of personal data concerning him or her without undue delay'.* Besides, the controller has the obligation to inform the data subject when the requirement has been fulfilled and the requested data erased. The same article foresees exceptions to the right in specific cases, namely, '*when the processing is necessary (1) for exercising the right of freedom of expression and information, (2) for compliance with a legal obligation, (3) for reasons of public interest in the area of public health, (4) for archiving purpose in the public interest, scientific or historical research purposes or statistical purposes and (5) for the establishment, exercise or defence of legal claims*'.[56]

Data subjects also have **the right to the restriction of the processing** of their data when one of the conditions listed in Art 18 GDPR is met.[57] As a result of the restriction, *'personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State'*.[58]

The right to data portability (Art 20 GDPR), represents another novelty of the GDPR. This right gives data subjects the right to receive their data from a controller '*in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means'*.[59] Also, the right to data portability gives data subjects the possibility, where technically feasible, to have personal data transmitted directly from one controller to another. With this right, the legislator intends to avoid lock-in situations by individuals. Nonetheless, the wording used in this provision has led to questions about the real effectiveness of the provision.[60]

Art 21 GDPR gives data subjects **the right to object** to the processing of their personal data, for reasons related to their specific situation. To overcome such objection, the controller has to demonstrate

[54] Art 15 GDPR.
[55] Art 16 GDPR.
[56] Art 17 GDPR.
[57] Rec 67 GDPR implies that compliance with this provision can be reached '*temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website*'.
[58] Art 18 GDPR.
[59] Art 20 GDPR.
[60] On Article 20: Paul De Hert and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' [2017] Computer Law & Security Review <http://www.sciencedirect.com/science/article/pii/S0267364917303333> accessed 24 April 2019.

compelling legitimate grounds overriding the interests, rights and freedoms of data subjects for the establishment, exercise or defence of legal claims.

Reinforcing data subjects' rights, the GDPR introduces a one-month time limit for the controller to address the requests made by data subjects, with possible extension to two months if the complexity of the claim requires more time.[61] Also, controllers have to provide data subjects with the requested information about the processing free of charge, unless the requests are manifestly unfounded, in particular, because of their repetitive character. Nonetheless, the controller bears the burden of demonstrating the manifestly unfounded or excessive nature of the request. When the controller has reasonable doubts concerning the identity of the person making the request, the controller may seek additional information to confirm the identity of the data subject making the request.

Lastly, according to Art 22 GDPR, data subjects have *'the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'.* Nonetheless, the same article foresees a specific exception to this provision. In particular, the right is not applicable when the decision is (1) necessary for entering into, or performance of, a contract between the data subject and a data controller, (2) authorised by Union or Member States law or (3) based on the data subject's explicit consent. In the first and last scenario described in Art 20(2) the controller has to put in place measures that ensure data subject's rights and freedoms and legitimate interest, *'at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision'*.[6263]

1.3 e-Privacy Directive

The provisions of the GDPR apply horizontally to all sectors, without any differentiation. However, at the beginning of 2000, the EU legislator, taking into account the technological developments which occurred in the electronic communication sector, started developing vertical legislation to regulate '*the processing of personal data in connection with the provision of publicly available electronic communication services in public communications networks in the community'.* [64] Doing so, the EC intended to provide rules for the respect of users' right to privacy and confidentiality in the electronic communication context. The ePrivacy Directive (ePD) was approved in 2002 and amended in 2009. Before the GDPR was adopted, the ePD was complementary to the Data Protection Directive (DPD), regulating privacy and confidentiality aspects that were not covered by the DPD. Due to the nature of the directive, its implementation slightly differs across EU Member States.

ePD obliges providers of publicly available electronic communications services to ensure, through appropriate organizational and security requirements, the privacy and confidentiality of electronic communications.[65] State security, public defence, and activities that are carried out by states, are out of the scope of the directive.[66]

[61] Art 12(3) GDPR.
[62] Art 20(2) GDPR.
[63] Pierre Dewitte, Aleksandra Kuczerawy, Peggy Valcke, CUTLER D1.1. Legal Taxonomy of Data Sets, < https://www.cutler-h2020.eu/>, accessed 26 April 2019
[64] 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).
65 Art 4 ePD.
66 Art 1 (3) ePD.

Even if the ePD addresses and targets electronic communication service providers, some provisions are generally applicable, such as the one on the storage of the so-called cookies on devices[67], and the one on unsolicited communications[68].

The ePD imposes obligations not only on electronic communication providers but also on Member States. In particular, Art 5 states that they have to guarantee that *'the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing'*.[69]

1.3.1 Types of data

There are different types of data in the electronic communication environment. Due to their characteristics, each category has been labelled with a different level of confidentiality. The differentiation determines various obligations for electronic communication providers. In particular, the ePD lists three different types of data that can be generated during communication, namely, content, traffic and location data.

1.3.1.1 Content Data

Content data are generated during electronic communication and are strictly confidential. Consequently, Member States have to prohibit the listening, tapping, storage or other kinds of interception or surveillance measures of communications without the consent of the users concerned. Nonetheless, '*this shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary to provide an information society service explicitly requested by the subscriber or user'*.[70]

1.3.1.2 Traffic Data

Traffic data are those processed for conveying communication on an electronic communication network, or for billing purposes.[71] Traffic data are related to routing, duration, time or volume of communication. Since they are considered personal information, the ePD foresees the same level of protection for content data.[72] Accordingly, Member States shall prohibit the listening, tapping, storage or other kinds of interception or surveillance of communications by persons other than users, without the consent of the users. Nonetheless, an exception to this rule occurs when such interception or surveillance measures are carried out for billing purposes and technical storage, or because it is necessary for the conveyance of

[67] *A cookie is a small piece of data that a website asks your browser to store on your computer or mobile device. The cookie allows the website to "remember" your actions or preferences over time.* European Commission, Information Providers Guide, available http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm accessed 25 April 2019.
[68] Art 13 ePD.
[69] Art 5 ePD.
[70] Ibid.
[71] Art 2(b) ePD.
[72] Ibid.

communication. In this regard, when data are no longer necessary for the transmission, the service provider has to erase or make them anonymous.

The provision dedicated to cookies (Art 5(3) ePD) requires explicit consent by the user for storage or access to information stored on a user's terminal equipment. The electronic communication provider, before receiving the consent by the user or subscriber, has to inform him about the type of traffic data that are processed and the duration of such services. [73] Also, the provider has to ensure that traffic data are only processed for marketing purposes for the provision of value-added services.[74]

Finally, Art 6 ePD specifies that the activity of processing of traffic data must be restricted to persons acting under the authority, and consequently the responsibility, of providers of electronic communications and networks. In addition, such activity has to be restricted to what is necessary for their tasks.

1.3.1.3 Location Data

Location data are defined as '*any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*'.[75] Specifically, this category includes information regarding the longitude, altitude or the latitude of the terminal equipment. Art 9 ePD states that the provider of electronic communication services can process these data only if they are made anonymous or if these data have been obtained with the consent of the data subject regarding the extent and duration necessary for the provision of a value-added service. To get the consent, the provider should inform the subscriber, or data provider, about the nature of the data needed, the purpose, the duration of the processing, and if the data will be transmitted to third parties to provide value-added service. According to Art 9(1) ePD, data subjects can withdraw their consent to process location data (other than traffic data) at any time. Moreover, according to Art 9(2) ePD, the electronic communication service providers have to give the user or the subscriber the possibility of temporarily refusing the processing of such data for each connection to the network or each transmission of a communication.[76] [77]

1.3.2 Security Aspects

Within the **Safe-DEED** project, the security aspects embedded in the ePD that should be taken into account. In this regard, the upcoming deliverable (D3.2) will provide clarifications about security aspects that have to be ensured when processing personal data. According to ePD provisions, when processing data, providers of electronic communication services have to ensure appropriate technical and organisational measures to safeguard the security of their services.[78] Moreover, when a risk of data breach on the network system security occurs, the provider must inform the user about such risk.

[73] Art 6 (4) ePD.
[74] Art 6 (5) ePD.
[75] Art 2 (c) ePD.
[76] Art 9 (2) ePD.
[77] Pierre Dewitte, Aleksandra Kuczerawy, Peggy Valcke, CUTLER D1.1. Legal Taxonomy of Data Sets, < https://www.cutler-h2020.eu/>, accessed 26 April 2019
[78] Art 4 (1) ePD.

1.4 e-Privacy Regulation Proposal

The EC, aware of the rapid development and an ever-growing volume of data used in the electronic communications environment, has decided to amend the e-Privacy Directive and is currently working on a new e-Privacy Regulation (EPR).[79] The EC has focused its action on broadening the scope of the Directive regulating entities that were not regulated by the ePD. The proposed text aims at reinforcing the regime of protection for users and subscribers of electronic communications services, as part of the EU Digital Market Strategy. In particular, the text aims at ensuring proper enforcement by introducing new compliance obligations and sanctions in situations of non-compliance.[80] Also, the proposed Regulation intends to update the current global standards regarding the confidentiality of communications.[81] Taking into account the development in this field, the new EPR should be considered complementary to the GDPR. Indeed, contrary to the ePD, and similarly to the GDPR, the proposed EPR will be directly applicable within the EU.

1.4.1 Timing

The initial idea of the EC was to get an overall approval of the proposed EPR by May 2018, to have an alignment with the GDPR. Nonetheless, while the European Parliament voted and approved its Report, the Council has not yet reached a common position on the text (so-called General Approach). Considering the end of the Parliament's and the Commission's mandate in May 2019, the approval of the text before the elections is questionable.

Consequently, the current analysis should be taken into account while having in mind that the text is not yet finalised and could be significantly amended.

1.4.2 Scope of the Regulation

Presumably, the EPR attempts to broaden the scope of application of the ePD by including services and activities that were not foreseen in the text of the directive. This assumption is confirmed by analysing the subjective and objective scope of application of the EPR proposal.

At the current stage of development, Art 2(1)(a) specifies that the EPR proposal applies to '*the processing of electronic communications content in transmission and electronic communications metadata carried out in connection with the provision and the use of electronic communications services.'* A recent European Electronic Communication Code (EECC), which is going to repeal four different Directives in the field of telecommunication, states that *'**electronic communications service**' means a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content*

79 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Comittee and the Committee of the Regions, Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century, COM(2012) 9 final, 25 January 2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_en.pdf., accessed 24 April 2019.
80 Factsheet on Data Protection Reform, Why do we need an EU data protection reform?, available at http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf., accessed 24 April 2019.
81 Hunton & Williams, EU Data Protection Regulation Tracker, available at https://www.huntonregulationtracker.com/, accessed 24 April 2019.

transmitted using electronic communications networks and services, the following types of services: (a) 'internet access service' as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120; (b) interpersonal communications service; (c) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting'.[82]

In addition, Art 4(3)c EPR underlines that '**electronic communications metadata**' encompass '*data processed by means of electronic communications services for transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication*'.

Looking at the two definitions, the EPR's scope of application appears to be broader than the scope of the ePD, as it covers services and activities that were not included in the directive.

1.4.3 E-Privacy Regulation General Principles

The GDPR is a horizontal legislation that seeks to ensure the protection of data subjects' fundamental rights regardless of the specific sector where the processing of personal data occurs. The EPR is a vertical legislation that complements and particularises GDPR's rules in the context of electronic communications services. Contrary to the GDPR, the EPR covers data that are not necessarily personal. When electronic communication data are also personal data, due to its nature of *lex specialis*, EPR provisions shall take precedence.

The classification of data gathered and generated by the **Safe-DEED** Consortium will be investigated in the upcoming deliverable (D3.2). At this stage, it is useful to mark the distinction between the different legislation that might apply within the project.

There could be three types of data:

1. Electronic communication data that fall under Art 4(3)(a) EPR but are not personal data (Art 4(1) GDPR). In this case, EPR applies to ensure the confidentiality of electronic communication data that otherwise would not be covered.
    - The classic example of electronic communication data that are not personal data is the one related to machine-to-machine communications (M2M);[83]
2. Personal data that fall under the definition of Art 4(1) GDPR but cannot be qualified as electronic communication data. When this situation occurs, the GDPR provisions apply.
    - This is the case of data gathered through participatory platforms;
3. Electronic communications data that fall into the definition of personal data. When this situation occurs, the EPR will prevail over the GDPR. This implies that the legal basis for the processing of data has to be found in Art 6 EPR (and not in Art 6 GDPR).

[82] Art 2(4) EECC.
[83] Rec 14 GDPR: '*this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal persons*'.

- This situation happens, for example, when metadata are transmitted through a smartphone connected to a Bluetooth tracking beacon.[84]

[84] Pierre Dewitte, Aleksandra Kuczerawy, Peggy Valcke, CUTLER D1.1. Legal Taxonomy of Data Sets, < https://www.cutler-h2020.eu/>, accessed 26 April 2019

2 Ethical Guidelines

2.1 Introduction

Legal and ethical principles have been influencing each other for many years. Generally, while the law offers the legislative setting that allows individuals, society and authorities to carry out their activities, ethics provides the basis to build the normative architecture, supporting its interpretation and offering guidance. The overall aim, when it comes to the ethical guidelines, is to ensure the well-being of individuals and society. *'Ethical considerations can play a part in system governance by shaping the actions of people, imposing constraints and providing guidelines for the development and design of technology'*.[85]

The ethical guidelines that will be provided in this deliverable intend to describe the principles that **Safe-DEED** project should follow, and that each partner should take into account when performing its tasks.

2.2 Fundamental Moral Principles

This section provides an overview of the main ethical principles. There are four generally accepted ethical-moral principles developed in the legislative context: autonomy, justice, beneficence and non-maleficence. Additionally, a secondary principle of responsibility will be presented.[86]

The principle of autonomy. According to this principle, every individual has the fundamental right to self-determination. This principle comes with positive and negative obligations. As a negative obligation, the principle of autonomy implies that individual actions should not result in a constraint for others. As a positive obligation, the principle requires respectful treatment when revealing information and taking independent decisions. The respect to privacy and confidentiality of information, together with the request for consent for processing personal information, are considered moral rules or obligations strictly linked to this ethical principle.

The principle of justice. The principle of justice requires that all individuals *'are entitled to have the same degree of attention and moral concern.'*[87] It implies that all persons have to be treated with fairness according to their different needs, contributions, and vulnerabilities. In the privacy and data protection framework, we have seen how the principle of justice and fairness is well represented in the GDPR. This is particularly the case where power asymmetries between data subjects and controllers could lead to potential abuses.

The principle of beneficence. According to this principle, all individuals have to contribute to personal and societal well-being. From a privacy and data protection angle, it implies that those in charge of processing activities have to ensure the security of the individuals that are affected by their activities.

The principle of non-maleficence. This principle originated from Hippocrates' oath (*primum non nocere* – first do not harm) and has been developed from biomedical ethics. The principle implies that

[85] Verhenneman G, Vedder A, WITDOM, D6.1 – Legal and Ethical framework and privacy and security principles, p. 39, 2015, available at: http://www.witdom.eu/deliverables, accessed 24 April 2019.
[86] Ibid
[87] Ibid

individuals have a duty to not cause harm to others insofar as it lies within their power to do so without undue harm to themselves, their vital health and security interests.[88]

The (secondary) principle of responsibility. This principle requires that each partner involved in a given project should behave and fulfil its moral obligations, which stem from its role in a project, at the best of its abilities. Such a principle gives responsibilities to each member of the Consortium for the work they are carrying out and the consequences that might come from it. Also, the principle of responsibility implies that in an interoperable environment, such as the **Safe-DEED** one, the duties have to be equally and fairly divided among the members.

These moral principles have been developed from universal morality and are going to be used as a baseline for developing **Safe-DEED**'s ethical guidelines.[89] At the same time, one of the major ethical issues in the Safe-DEED project stems from the processing of personal data. Therefore, the following section highlights the latest developments in the area of ethical aspects of personal data management.

2.3 EDPS' Ethics Advisory Group 2018 Report, Towards a digital ethics

The European Data Protection Supervisor (EDPS) authority is the EU body in charge of monitoring and ensuring the protection of privacy and personal data in processing activities by EU institutions. Besides this function, the EDPS provides opinions and advices to EU institutions and agencies regarding their legislative initiatives that might have an impact on privacy and data protection.

During the last years, ethics has been a hot topic on the EDPS' agenda. The recent annual meeting organised by this authority has mainly focused on ethics in the management of personal data.[90] Moreover, before the GDPR entered into force, the EDPS published a Report on Ethics.[91] The Report, prepared by the Ethics Advisory Group (EAG), follows the EDPS 2015 Opinion *Toward a new Digital Ethics*.[92] In this document, the EDPS described how the new technological trends are reshaping the relationship between technology and human values. The EDPS also called for a *'big data protection ecosystem: an interactive and accountable assemblage of future-oriented regulation, accountable controllers, privacy-conscious engineering, and empowered individuals*.'[93] To achieve such a purpose, new guidelines regarding digital ethics were deemed necessary.

The 2018 Report describes how new technological trends, such as data market places, are impacting our socio-cultural ecosystem. At the same time, the Report highlights the tensions that may exist between core concepts and principles of data protection and challenges coming from big data exploitation.

[88] Verhenneman G, Vedder A, WITDOM, D6.1 – Legal and Ethical framework and privacy and security principles, p. 6, 2015, available at: http://www.witdom.eu/deliverables., accessed 24 April 2019.
[89] Ibid, p.7
[90] International Conference of Data Protection and Privacy Commissioners, https://icdppc.org/, accessed 26 April 2019
[91] Ethics Advisory Group 2018 Report, *Towards a digital ethics*, available at < https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf>, accessed 25 April 2019.
[92] EDPS, Opinion 4/2015, *Towards a new digital ethics Data, dignity and technology*, 2015, available < https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf> accessed 26 April 2019.
[93] Ibid, p.4.

The EDPS' Report also provides guidelines to policymakers on how to combine ethical principles with challenges coming from digital innovation.[94] The ethical guidelines provided in the Report offer an opportunity to analyse the ethical challenges of our *'digital society, such as its collective ethos, its claims to social justice, democracy and personal freedom.'*[95]

All the questions and guidelines that are provided in the Report are associated with the concept of digital ethics. The concept of digital ethics was traditionally defined as the conglomerate of different ethical approaches as social informatics, computer ethics, but also value sensitive design. The main aim of digital ethics '*is not only to take into account for the present but also to perform a foresight function.'*[96]

2.3.1 Socio-Cultural Shifts of the Digital Age

In the 2018 Report, the EDPS Ethics Advisory Group describes the effects of digital innovation on society and identifies different 'moves' which require the intervention of policymakers. According to the Report, it is possible to observe seven 'moves' where there is a need to redefine digital ethics.

- **From individuals to digital subjects.** The growing trend of profiling through algorithms resulted in a situation where individual identity is defined through digital patterns and constructs rather than through psychological, cultural, moral qualities.[97]
- **From analogue to digital life.** Human life has always been interpreted by reference to specific socio, cultural and political activities. Enhanced reliance on digitalisation and data, leads to the conclusion that the social, cultural and political values, that have contributed to developing personal identity, may not necessarily be taken into account anymore.[98]
- **From institutional governance to governability through data**. In the last decade, a shift in governance has occurred. From a society governed by institutional governments, democratically elected and accountable for their decisions, the governance shifted to algorithms and automated decision-making affecting citizens' life more than institutional governments ever could.[99]
- **From a risk society to scored society.** To address potential societal risks, institutions have always relied on the aggregation of data, even if with different gathering and collecting techniques. Nonetheless, the political decisions taken by government institutions that have been taken so far about certain risks have also taken into account moral principles such as justice and fairness. Nowadays, algorithms can customize the risks and needs of every individual. The role of solidarity is consequently questioned by opaque social and credit scoring that is undermining the social texture of our society.[100]

[94] Ethics Advisory Group 2018 Report, Towards a digital ethics. p.8.
[95] Ibid p.7
[96] *Such a function has many layers. One is an anticipatory function, preparing technology users and policy-makers and providers for potential concerns lying on the horizon and requiring technologies to hold tools and concepts able to confront our evolving digital reality. The other is to develop means for empowering individuals and groups to confront anxieties linked to both the potential weakening of fundamental rights and to technological uncertainty itself.'* Ethics Advisory Group 2018 Report, Towards a digital ethics. p.15.
[97] Ibid, p.11.
[98] Ibid, p.12.
[99] Ibid.
[100] Ibid, p.13.

- **From Human autonomy to the convergence of human and machine.** The new frontier of technology is characterised by 'autonomous machines' that can perform activities without human interactions. Consequently, there is a shift from a period where technological tools were supporting human activities (e.g. GPS) to one where machines decide without human interaction.[101]
- **From Individual responsibility to distributed responsibility.** The availability of large amounts of data is affecting the concept of responsibility. The network and interconnected eco-system that characterise our daily life require to reconsider the idea of responsibility. Moreover, the discussion on algorithmic transparency and accountability is among the most vividly debated themes of our times. At the same time, the discussion on algorithms responsibility should never decrease or alleviate the responsibility of human agents.
- **From Criminal Justice to pre-emptive justice.** One of the main purposes of criminal justice is to ensure security, safeguarding at the same time the human rights of anyone. Nowadays, the latest developments in the criminal justice sector are focusing on techniques to predict criminal behaviour, using the output of big data-driven analysis and smart algorithms. This investigative trend generates concerns in relation to potential drawbacks that it may have on those subjected to investigative and coercive measures.

2.3.2 Policy Recommendations

The ethical analysis made by the EDPS Ethics Advisory Group concludes by providing five political (non-binding) recommendations to support and develop the European values based on the ones embedded in the data protection framework.

- Regardless of the changes that occur in society, the essential and inviolable human dignity has to be preserved;
- Personhood, with his or her moral values and social and cultural characteristics, cannot be taken apart from his or her personal data;
- Freedom of choice has to remain a pillar of the society and autonomous decision making cannot undermine such a principle;
- Accountability, especially in the context of profiling should be fostered to avoid any form of discrimination;
- Data commoditisation can lead to potential tension if human moral values are not taken into account.[102]

In the development of **Safe-DEED** project all these guidelines will be taken into account, not only in personal data management but also when carrying out exploitation activities and platform set up.

2.4 Ethics Guidelines for Trustworthy AI

Debates around Artificial Intelligence (AI) and its exploitation in daily life are characterising the recent global discussion. Even if multiple definitions of AI exist, they are not unanimously accepted.[103] Nonetheless, two characteristics are commonly mentioned to define AI technologies: their ability to

[101] Ethics Advisory Group 2018 Report, Towards a digital ethics. p.13
[102] Ibid. p.20.
[103] See also, Stephanie Rossiello, *Europe's "Trustworthy" AI*, (CiTiP Blog) https://www.law.kuleuven.be/citip/blog/europes-trustworthy-ai-part-1/, accessed 6/05/2019

evolve by learning from experience and their capability to perform complex tasks without human interaction.

The EU strategy on AI aims to create a standard for trustworthy AI that EU businesses could use to capture market opportunities within and outside the EU. The goal is to improve the EU economic competitiveness and turn the EU into a global leader on the matter. In 2018, as part of its strategy on AI, the EC selected a group of experts, giving them the mandate to draft ethics guidelines on AI. On 8th April 2019, the EU's High-Level Expert Group (HLEG) published the "Ethics Guidelines for Trustworthy AI".[104] These Guidelines are the result of over 500 recommendation the group has received on the 'Draft Ethics Guidelines' of 2018.

The Guidelines prepared by the HLEG are not legally binding and do not offer pieces of advice on legal compliance for AI. According to the guidelines, a trustworthy AI must display three characteristics, it must be lawful, ethical, and robust.

Lawfulness as one of the three pillars that are necessary to build a trustworthy AI reflects the "human-centric approach" to AI. In the human-centric approach, the EU Charter and European Convention of Human Rights are considered the basis for developing any legislative initiative in the field of AI.[105]

Robustness refers to the ability of AI to operate in any situation, especially if unpredictable events or malicious attacks occur.

The ethical component of a trustworthy AI requires that technological development of AI must proceed in compliance with EU ethical values, which are listed in the document.[106]

[104] High-Level Expert Group on AI, Ethics Guidelines for Trustworthy AI, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58477, accessed 05/06/2019

[105] High-Level Expert Group on AI, Ethics Guidelines for Trustworthy AI, p.41https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58477, accessed 05/06/2019,

[106] See also, Stephanie Rossiello, *Europe's "Trustworthy" AI*, (CiTiP Blog) https://www.law.kuleuven.be/citip/blog/europes-trustworthy-ai-part-1/, accessed 6/05/2019

3 Platforms, Free Flow of Data and Data Market Place

3.1 European Commission Communication "Building a European Data Economy"

On the 10th January 2017, the EC published a Communication and a Staff Working document on "Building a European Data Economy."[107] The Communication focuses on the main legal challenges that have been hampering the development of the EU data economy and aims at setting the EC legislative agenda to fill the gap. Following the recommendations included in the Communication, the EC has subsequently developed legally binding measures to tackle some data economy issues, for example, national restrictions of data localisation.

First, the EC Communication defines data market place as the market *'where digital data is exchanged as products or services derived from raw data – on the economy as a whole. It involves the generation, collection, storage, processing, distribution, analysis, elaboration, delivery, and exploitation of data enabled by digital technologies'*.[108] According to the EC Communication, if supported with adequate legislative measures, cooperation between different actors involved in the data market place can increase economic opportunities for the involved entities and, as a result, for EU citizens.

The Commission, recognising the potential benefits that can come from the exploitation of data generated by machines, encourages the removal of any national restriction that could limit cross-border access to such data. Concerning the promoted legislative approach, the EC Communication calls for the development of new legislative initiatives to address some of the key barriers related to data economy instead of using existing national and European frameworks.

The recently adopted Regulation on the Free Flow of non-personal data addresses some of the issues raised by the EC. Other potential solutions presented in the Communication, such as the one on data producer's right, mentioned in the EC Staff working document accompanying the Communication, have been included in the Digital Content Directive proposal.

3.2 Free Flow of Non-Personal Data Regulation

In line with the Digital Single Marked strategy, the EC published a legislative proposal on the free flow of non-personal in 2017.[109] In its General Approach on the Free Flow of Non-Personal Data Regulation (FFNPR), the Council defines the EC proposal as a '*balanced compromise that gives Member States flexibility to address core public responsibilities while respecting the principles of the free flow of data*.'[110] The European Parliament on its side also welcomed the initiative. The Committee for the Internal Market and Consumer Protection has defined the free flow of non-personal data as the 5th

[107] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions "Building a European Data Economy" (COM(2017) 9 final), available at < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:9:FIN>, accessed 24 April 2019.
[108] European Data Market study, SMART 2013/0063, IDC, 2016.
[109] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region – Commission Work Programme 2016 – No time for business as usual', https://ec.europa.eu/info/sites/info/files/cwp_2016_en_0.pdf accessed 24 April 2019.
[110] For the version proposal as revised by the Council, see: http://data.consilium.europa.eu/doc /document/ST-15724-2017-REV-1/en/pdf accessed 24 April 2019.

freedom of the EU Single Market after goods, people, services and capitals.[111] After a negotiation phase between the European Parliament and the Council (under EC supervision), an overall agreement was reached, and final approval occurred at the beginning of November 2018. The FFNPDR was signed on the 14th November 2018, entered into force at the end of December 2018 and is applicable from May 2019.[112]

The EC considers the free flow of non-personal data a fundamental building-block of the Digital Single Market Strategy. According to the EC, the FFNPDR, removing the national restrictions to the free flow of non-personal data, will contribute to boosting the EU economy, generating growth of up to 4% GDP by 2020.[113]

The Commission has recognised four barriers to data mobility within the EU market:

(1) Data localisation restrictions by Member States' public authorities;
(2) Obstacle put in place by IT systems' vendors;
(3) Complex EU legal patchwork that leads to legal uncertainty;
(4) Lack of trust due to security risks and concerns about the cross-border availability of data for regulatory purposes.[114]

The removal of the legal obstacles is considered preliminary not only for enhancing the economy but also for boosting innovation (with expected progress in the field of AI, IoT and autonomous systems). Within the **Safe-DEED** project, it will be fundamental to address all the challenges coming from the aforementioned obstacles.

3.2.1 Regulation's Scope of application

According to Art 2 FFNPDR, the provisions foreseen in this text apply to '*the processing of electronic data other than personal data in the Union, which is: (a) provided as a service to users residing or having an establishment in the Union, regardless of whether the service provider is established or not in the Union; or (b) carried out by a natural or legal person residing or having an establishment in the Union for its own needs.'*

Art 2(2) and Rec 10 FFNPDR clarify that when a set of data includes personal and non-personal data, the FFNPDR will only apply to non-personal data. If this differentiation is impossible, the FFNPDR should not prejudice the application of GDPR nor impose an obligation to store the different data diversely.

[111] "This regulation *de facto* establishes data as the fifth freedom on the EU Single Market. By removing borders, burdens and barriers such as data localisation rules, we enable a level playing field for European companies to compete globally. This legislation is truly a game changer, potentially providing enormous efficiency gains for both companies and public authorities. It will reduce data protectionism, which is threatening the digital economy, and pave the way for artificial intelligence, cloud computing and big data analysis".
[112]Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union O J L 303, 28.11.2018, p. 59–68.
[113] Deloitte, "Measuring the Economic Impact of Cloud Computing in Europe", final report prepared for the European Commission https://ec.europa.eu/digital-single-market/en/news/measuring-economic-impact-cloud-computing-europe accessed 24 April 2019.
[114] See, for a visualisation and information on the objectives of the proposal: European Commission, 'State of the Union 2017 – Free flow of non-personal data', https://ec.europa.eu/ digital-single-market/en/news/free-flow-non-personal-data accessed 24 April 2019.

Regarding the material scope of application, Art 3 states that, in the context of the regulation, data have to be considered as data other than personal data as referred to in the GDPR.[115] Therefore, only data that do not include any information to an identifiable or identified person fall within the material scope of application of the regulation. Consequently, only non-personal data (by nature or properly anonymised datasets) will be covered by these provisions.[116]

Art 3 FFNPDR defines processing as *'any operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'*[117] This definition mirrors the definition provided for the same activity by the GDPR. Rec 10 makes the correspondence even more explicit by stressing that Member States are prevented from putting in place measures that limit or prohibit the free movement of non-personal data within the Union.

The geographical scope of application of the FFNPDR covers activities carried out by a natural or legal person residing or having an establishment in the EU, regardless of where the natural or legal person is established. Therefore, activities taking place outside the EU fall out of the scope of the regulation.

3.2.2 General principles

To boost the Digital Single Market, the FFNPDR aims to remove all the barriers that are hampering the free movement of non-personal data. Doing so, the FFNPDR identifies three main actions to achieve its purpose: prohibition of mandatory data localisation requirements, guarantee data availability for competent authorities, and facilitation of data porting by users.

3.2.3 Prohibition of mandatory data localisation requirements

Art 3(1)5 FFNPDR defines data localisation requirements as *'any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law, including in the field of public'*. Rec 18 explains that these requirements '*represent a clear barrier to the free provision of data processing services across the Union and the internal market. As such, they should be banned unless they are justified on the grounds of public security, as defined by Union law, in particular within the meaning of Article 52 TFEU, and satisfy the principle of proportionality enshrined in Article 5 TEU'*. In this context, these legal and administrative requirements are mainly related to accounting documents, invoices, commercial letters, criminal records, national registries, and archives.

The only exception to the removal of such a barrier is the Member State's public security prerogative. It should be highlighted that public security has two dimensions, the internal and the external one. The former includes activities related to the investigation, detection, and prosecution of a crime. The latter involves international cooperation with other countries. Taking into account the letter of the text, where

[115] Art 4(1) FFNPDR.
[116] Rec 17 FFNPDR.
[117] Art 3(1) FFNPDR.

no further explanations are provided, it is assumed that the reference to public security notion covers both situations.

Consequently, Member States have 24 months after the Regulation becomes applicable (approx. May 2021) to repeal the national provisions that are not in compliance with the FFNPDR. Member States can put in place data localisation, but if they do so, they have to inform the Commission immediately. Also, Member States are required to communicate all necessary information related to data localisation requirements that are in place.

In the **Safe-DEED** context, once Art 4 FFNPDR becomes applicable, removal of the national provisions on data localisation might result in an advantage. Since there will be no legal boundaries for non-personal data gathered from different Member States, the situation will create a reasonable possibility to transfer data to another country without being obliged to host them in a specific Member State.

3.2.4 Guarantee of data availability for competent authorities

Together with the provisions that will remove national legal and administrative requirements for the free flow of non-personal data, the FFNPDR foresees measures that will facilitate the cross-border access to non-personal data by public authorities. Art 5 states that the measures to enhance the exchange of the data across Member States *'shall not affect the powers of competent authorities to request and receive access to data for the performance of their official duties by Union or national law'*.[118] Consequently, *'Access to data by competent authorities may not be refused on the basis that the data are processed in another Member State'*.[119] If a service provider does not comply with such requests, it will incur sanctions.

According to Art 3(1) 6 FFNPDR, a 'competent authority', is *'an authority of a Member State or any other entity authorised by national law to perform a public function or exercise public authority that has the power to obtain access to data stored or processed by a natural or legal person for the performance of its official duties, as provided for by national or Union law'*.[120] Additionally, to enhance the cooperation and efficiency of their activities, the Regulation foresees cooperation mechanisms, especially regarding the exchange of information and assistance when accessing cross border data.

End-users and/or users exploiting data from the **Safe-DEED** platform might be asked by the competent national authority for access to their non-personal data. Taking into account what is stated in the Regulation, they will have to comply with such request, and they will not be able to refuse such demand on the basis that the requested data are stored in another country.

[118] Member States decision regarding data localisation requirements are usually related such as security, surveillance and economic protectionism. Nonetheless, these restrictions have multiple drawbacks. See on these points: Cathal Flynn, 'Shortcomings of the EU Proposal for Free Flow of Data' (2018) 45 InterMEDIA <https://www.twobirds.com/~/media/pdfs/shortcomings-of-eu-proposal-for-free-flow-of-data.pdf?la=en> accessed 24 April 2019.
[119] Art 5 FFNPDR.
[120] Art 3(1)6 FFNPDR.

3.2.5 Porting of data

Rec 29 FFNPDR stresses the importance of removing commercial practices that do not facilitate data porting, linking this need to the one that has to lead to the right to data portability in the GDPR. Therefore, Article 6 FFNPDR *'encourage and facilitate the development of self-regulatory codes of conduct at Union level ('codes of conduct'), to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards'*. To do so, relevant stakeholders should develop their code of conduct covering four key aspects:

- Best practices in facilitating the switching of providers and the porting of data in a structured, common and machine-readable format allowing sufficient time for professional users actually to switch or port the data;
- Information, which should be detailed, precise and shown in a transparent manner between parties before the contract is concluded;
- Approaches to certification schemes that can facilitate the comparison between different products and services;
- Communications regarding roadmaps to raise awareness of the codes of conduct among relevant stakeholders.[121]

Compliance with these requirements should enhance trust in all stakeholders, and transparency in the whole process. In the **Safe-DEED** context, the idea of developing a code of conduct that would facilitate compliance with the requirements in Art 6 should be discussed.

3.3 Platform-to-Business Proposal

On 26th April 2018, the EC published its Proposal for a Regulation on promoting fairness and transparency for business users of online intermediation services (Platform-to-Business Regulation - P2BR). The Proposal was anticipated by a public consultation and a communication in 2016. On the 14th of February, the Council and the Parliament reached an overall agreement that remains to be approved. Once approved, it will be published in the EU Official Journal to enter into force at the beginning of November 2019.

With this initiative, the EC intends to legislate in the area of business platforms, which has, so far, not been addressed by specific legislative initiatives. Considering that the final approved text is not yet available, this deliverable focuses on the proposal published by the Commission in 2018. If any substantial changes occur, they will be reported and described in the upcoming deliverables.

The P2BR is part of the legislative measures promoted by the EC for the Digital Single Market strategy. The proposal is the first legislative initiative in the field of platforms and focuses only on a specific type of platforms, namely, those offering services or products to the same users of their business clients. The P2BR foresees for them a list of measures ensuring transparency and fairness. Doing so, the EC aims to temper the natural asymmetries that characterise the relationship between platforms and their suppliers, establishing a fair and trustworthy innovation-driven ecosystem.

[121] Pierre Dewitte, Aleksandra Kuczerawy, Peggy Valcke, CUTLER D1.1. Legal Taxonomy of Data Sets, < https://www.cutler-h2020.eu/>, accessed 26 April 2019

3.3.1 Scope of application

The P2BR regulates the area of Business-to-Business relations. Art 2 P2BR describes the requirements of the intermediation services (platforms) that fall into the scope of application of this Regulation: *(a) they constitute information society services within the meaning of the European Electronic Communication Code; (b) they allow business users to offer goods or services to consumers, to facilitate the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded; (c) they are provided to business users based on contractual relationships between, on the one hand, the provider of those services and, on the other hand, both those business users and the consumers to which those business users offer goods or services.*

An online intermediation service falls into the scope of application of P2BR only if all these characteristics are present. The provided definition of intermediaries describes only the services that have a direct relationship with business users and their clients. The P2BR does not foresee a clear threshold, applying indistinctively to all types of platforms that fall in the criteria listed in Art 2 P2BR.

3.3.2 General Principles

The P2BR follows two main principles, namely, transparency and fairness.

The P2BR foresees transparency obligation for providers of intermediation services to inform, through clear, unambiguous and readily available contractual terms and conditions, about the treatment, the criteria used to rank their products and the requirements to suspend or terminate their services.

Moreover, the P2BR aims to achieve fairness through the settlement of effective out-of-court redress mechanisms such as internal handling systems for business users and mediation procedures. To facilitate the process, contractual terms and conditions prepared by the intermediaries have to include a list of independent mediators that can be approached to settle disputes.

Taking into account the **Safe-DEED** project, it is crucial to understand to whom the platform intends to offer its services because it might determine whether it will fall or not within the P2BR scope.

4 Security Aspects

The European Commission has identified Cybersecurity as one of the highest priorities for the EU. Establishing a secure and safe environment is a precondition to enhance trust and consequently support EU private businesses.

The Directive on Security of Network and Information Systems (NIS) and the recently approved Cybersecurity Act are the first two legislative binding measures in this area. These two initiatives are the result of two different action plans put in place by the EC in 2013 and 2017, where potential economic opportunities are explored together with the security challenges.

In addition to these two legislative initiatives, the EC has published different reports and has created an ad hoc Commissioner for Security to coordinate all the actions in the area of cybersecurity horizontally.[122]

The enhancement of security is a priority of the **Safe-DEED project**. Improving security will have a direct impact on all relevant stakeholders, resulting in boosting business opportunities of the **Safe-DEED** platform users. From a legal point of view, the requirements concerning security are mainly coming from the data protection framework, specifically from the GDPR and the ePD. Nonetheless, it is fundamental to understand the latest legislative trends in this area, and in particular the links with the GDPR. It is also relevant to consider potential development of initiatives related to encryption protocols.

4.1 Network and Information Systems Directive (NIS)

The Directive 2016/1148 on the security of network and information systems is the first EU legislative initiative in the cybersecurity area (NIS).[123] The NIS was part of the 2013 EU Cybersecurity strategy, a set of binding and non-binding legal measures aimed at establishing a high standard of security across all EU Member states. The Directive came into force on 6 July 2016 and required Member States to put in place adequate measures foreseen in the text by 9 May 2018.

The NIS establishes standard steps regarding the handling of incidents and notification mechanisms. It is characterised by a minimum level of harmonisation, leaving the possibility to the Member States to adopt or maintain higher standards for securing their network and information systems. At the same time, the NIS specifies that if other EU legislation has already foreseen sector-specific security measures, their provisions should prevail if they are proved to ensure at least equivalent security standards.[124]

[122] Communication from the Commission to the European Parliament and the Council, First progress report towards an effective and genuine Security Union, COM/2016/0670, p.2

[123] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union OJ L 194, 19.7.2016 p. 1–30.

[124] Rec 9 NIS: *'Certain sectors of the economy are already regulated or may be regulated in the future by sector-specific Union legal acts that include rules related to the security of network and information systems. Whenever those Union legal acts contain provisions imposing requirements concerning the security of network and information systems or notifications of incidents, those provisions should apply if they contain requirements which are at least equivalent in effect to the obligations contained in this Directive.'*

4.1.1 Scope of application

The NIS applies to operators of essential services and Digital Services Providers.

Art 4 NIS defines operators of essential services as any private or public entity that falls under one of the categories referred to in Annex II of the NIS. These operators, which should have been identified by the Member states by 9 November 2018, are considered essential for the maintenance of critical societal and economic activities.

Digital Service Providers are legal persons providing a digital service, as enshrined in Art 1(1) Directive 1535/2015[125]. Different Types of Digital Service Providers are listed in Annex III of the NIS. They include online market place, online search engine or cloud computing service. The reason why such providers are included in the list is their cross-border nature. Digital Service Providers have to comply with the security and notification obligations listed in art 16 NIS to ensure the integrity and security of their services. They are subject to ex-post supervisory control by competent national authorities to whom they have to report in case of an incident resulting in a substantial impact on the provision of a service.

Concurrently, Member States have to put in place adequate measures for handling incidents. They have to adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures to achieve a high level of security.[126] Specifically, they have to designate one or more competent authorities to monitor the application of the NIS,[127] identify a point of contact for cross-border cooperation with other Member States,[128] and establish at least one Computer Security Incident Response Teams (CSRITs) to handle incidents at national level, and raise awareness about risks and critical events to all stakeholders.[129]

4.2 Cybersecurity Act

The European Parliament and the EU Council have recently approved the Cybersecurity Act Regulation (Cybersecurity Act), which is going to be published in the EU Official Journal before the end of May.[130] The Cybersecurity Act is the only legislative binding measure included in the Cybersecurity Package, released during the State of the Union on 13 September 2017.

The new Cybersecurity Act follows two main guidelines: the implementation of mandate and scope of the EU Agency ENISA, and the creation of an EU cybersecurity certification scheme for ICT products, ICT services, and ICT processes. Overall, the new Regulation aims to enhance the role of the EU in the global scenario, improving cross-border coordination, implementing EU Member States' common understanding of cyber threats and promoting EU standards. According to the EC strategy, the adoption

[125] The definition included in Directive 1535/2015 refers to: service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.
[126] Art 7 NIS.
[127] Art 8 (1)(2) NIS.
[128] Art 8 (3)(4) NIS.
[129] Art 9 NIS.
[130] Proposal for a Regulation of the Parliament and the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (COM/2017/0477 final - 2017/0225)

of EU standards in the cybersecurity context will enhance trust in EU products, services, and processes and will consequently promote EU companies outside the EU borders.[131]

The EU cybersecurity certifications for ICT products, services and processes will be developed under the EC initiative by ENISA together with relevant stakeholders coming from academia, public and private sector. As foreseen by the Cybersecurity Act text, the recourse to the developed certificates by industries and companies will be initially voluntary. Each cybersecurity certification scheme will foresee different assurance levels that are considered the basis for users' confidence. The different assurance levels will depend *'on the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident.'*[132] The type of assurance level chosen by the applying company will determine the accuracy and the kind of evaluation necessary for granting the certification, but also the marketing value of the certificate.

The Cybersecurity Act will enter into force in two years from the twentieth day of its publication on the Official Journal (May 2021), almost at the end of the **Safe-DEED** project. Nonetheless, the creation and adoption of cybersecurity certification schemes for ICT products, ICT services, and ICT process might prove useful for one or more partner and consequently for the project as an element that can enhance security and trust in the Safe-DEED platform.

4.3 EU Encryption Framework

The recent discussions on encryption focused on the implications of the use of encryption in the security context by users, law enforcement agencies and criminals. The European Union has recently included provisions related to encryption in different binding legislative initiatives, such as GDPR (Art 32) and the European Electronic Communication Code, but also Reports and Opinion Papers, such as the ENISA Opinion Paper on Encryption.[133]

4.3.1 ENISA Opinion Paper on Encryption

ENISA, the European Union Agency for Network and Information Security, published an Opinion Paper on encryption in 2016.[134] The purpose of the paper was to provide an overview of encryption and decryption protocols for security services.

The ENISA's Opinion delivers key messages about encryption that should be taken into account by policymakers when discussing potential legislative initiatives in this field.

[131] Art 46 (1) Cybersecurity Act *'The European cybersecurity certification framework shall be established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonised approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services and ICT processes'.*
[132] Art 52(1) Cybersecurity Act.
[133] ENISA's Opinion Paper on Encryption https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption, accessed 25 April 2019
[134] Ibid.

In particular, one of the main takeaways of ENISA's Opinion is related to the use of backdoors. The EU Agency strongly argues against the use of backdoors by law enforcement due to their inability to ensure the security and confidentiality of users. Other key messages delivered by ENISA are:

- *"Judicial oversight may not be a perfect solution as different interpretations of the legislation may occur;*
- *History has shown that technology beats legislation and criminals are best placed to capitalise on this opportunity;*
- *Law Enforcement solutions need to be identified without the use of backdoors and key escrow. It is very difficult to restrict technical innovation using legislation;*
- *The experience in the US showed that limiting the strength of encryption tools inhibited innovation and left the competitive advantage in this area with other jurisdictions";*[135]

4.3.2 Eleventh progress report towards an effective and genuine Security Union

In 2016, the EU Commission started publishing monthly series of reports where the progress made in the area of security is described. The reports highlight the areas where additional legislative efforts are necessary. Every report follows the same structure:

- *'tackling terrorism and organised crime and the means that support them;*
- *Strengthening our defences and building resilience against them'.*[136]

The Eleventh report (published on 12th October 2016) was mainly focused on the package of anti-terrorism measures. The report provides a specific section dedicated to encryption and its use. In the report, the EC highlights the difficulties in balancing, on the one hand the interests of citizens in having ensured the confidentiality and security of their personal data (Art 32 GDPR) and, on the other hand, the necessity for law enforcement and judicial authorities in prosecuting and investigating crimes. The report provides a set of measures to support law enforcement and judicial authorities. The measures follow two main guidelines: (a) legal measures to facilitate access to encrypted evidence, (b) technical measures to enhance decryption capabilities. As a result, '*Member State authorities should have a toolbox of alternative investigation techniques at their disposal to facilitate the development and use of measures to obtain needed information encrypted by criminals*.' [137]

The legislative initiatives described in the report relate to the cross-border access to electronic evidence and the development of a platform to exchange information and the standardization of judicial cooperation between Member States (e-evidence Regulation proposal).[138] The report provides seven technical measures to enhance decryption capabilities. The measures focus on increasing the know-how among all Member States and their agencies and on strengthening the cooperation among all relevant stakeholders.

[135] ENISA's Opinion Paper on Encryption, p.5 https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption, accessed 25 April 2019.
[136] Communication from the Commission to the European Parliament, the European Council and the Council. *First progress report towards an effective and genuine Security Union* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0670&from=EN, accessed 25 April 2019.
[137] Ibid, p.9.
[138] Ibid.

4.3.3 European Electronic Communications Code

The Directive 2018/1972 establishing the European Electronic Code (EECC) has been adopted on the 11th of December 2018[139]and have to be implemented in two years (December 2020) by Member States. The EECC is considered crucial for the development of the EU Digital Single Market Strategy.[140] The EECC amends four different Directives[141] and governs all aspects involving providers of electronic communication networks and their competent national authorities.

In the security provisions, the EECC makes a specific reference to encryption protocols and explicitly, to the end-to-end encryption. First of all, it requires providers of public electronic communication networks to inform their users about any potential security threat that might affect their service, and of the measures taken to ensure the security of communications. To comply with the requirement, Rec 96 EECC makes a specific reference to encryption.[142] Moreover, the EECC provides that, where appropriate to guarantee safety and privacy of communication, the adoption of end-to-end encryption should be made mandatory by Member States.[143] At the same time, the EECC leaves such a possibility to the discretion of Member States.[144]

[139]Directive (EU) 2018/1972 establishing the European Electronic Communications Code (Recast) OJ L 321, 17.12.2018, p. 36–214.
[140] Rec 3 EECC.
[141] Specifically, the Code amends Directive 2002/19/EC, 2002/20/EC, 2002/21/EC and 2002/22/EC.
[142] Rec 96 EECC.
[143] Rec 97 EECC.
[144] Art 40 EECC.

5 Competition law

5.1 The goal of competition law and key concepts

The goal of competition law is to establish and protect *'a system ensuring that competition is not distorted*'[145]. For the European Commission, competition on the market is protected as a means of enhancing consumer welfare and of ensuring an efficient allocation of resources. Moreover, the CJEU has, in its case law, emphasised that competition law protects not only the interests of competitors or consumers, but also the market structure, or competition '*as such*'.[146]

Vigorous competition policy enforcement is still a powerful tool to serve the interests of consumers and the economy as a whole. However, specific characteristics of platforms, digital ecosystems, and the data economy require concepts, doctrines and methodologies, as well as enforcement, to be adapted and refined.[147] For example, contrary to non-digital markets where price competition is given a fairly high priority, innovation and quality competition (including questions of access and re-use of data) represent fundamental characteristics of digital markets.[148]

Some concepts are instrumental in the framework of competition law. They will be briefly put forward in this section and considered in light of the challenges brought by the digital economy. These challenges and the specific characteristics of platforms will, in turn, play an important role in the evaluation and determination of legal and ethical requirements, which are paramount to the project.

5.1.1 Consumer welfare

As previously mentioned, enhancement of consumer welfare is considered a goal of competition law. In the digital economy, the term "consumer" encompasses multiple groups of customers. It covers all *direct or indirect users* of products or services offered by an undertaking or covered by an agreement between undertakings. Therefore, business users (such as manufacturers, distributors or other undertaking located at an intermediate level) need to be included in the scope of consumer welfare.

5.1.2 Market definition[149]

In order to evaluate the degree of competitiveness between undertakings on a market, as well as the potentially pro- or anti-competitive effects of certain practices, it is generally required to engage in a market definition exercise. Traditionally, the definition relies on *geographic* and *product* dimensions. If the geographic dimension of market definition is fairly straightforward, its product dimension requires some explanation. A relevant product market comprises all those products and/or services which are

[145] Protocol 27 on the internal market and competition, annexed to the TFEU, *OJC 115, 09.05.2008.*
[146] E.g.: Case C-209/10, *Post Danmark I*, EU:C:2012:172, at para. 44. Case C-23/14, *Post Danmark II*, EU:C:2015:651, at para. 69. Case T-213/01, *Österreichische Postsparkasse v Commission*, EU:T:2006:151, at para. 115. Case T-286/09, *Intel v Commission*, EU:T:2014:547, at para. 105. Case C-280/08 P, *Deutsche Telekom v Commission*, EU:C:2010:603, at para. 182.
[147] A. Ezrachi, "BEUC Discussion Paper – The goals of EU competition law and the digital economy" (2018).
[148] N. Duch-Brown, B. Martens, F. Mueller-Langer, JRC Report, *The Economics of Ownership, Access and Trade in Digital Data* (2017) p. 20. Commission's study on Competition policy for the digital era. Final report (2019).
[149] Commission Notice on the definition of relevant market for the purposes of Community competition law, *OJ L 372, 9.12.1997, p. 5-13.*

regarded as *interchangeable* or *substitutable* by the consumer, by reason of the products' characteristics, their prices and their intended use. The main purpose of market definition is to identify in a systematic way the competitive constraints that the undertakings involved face. Three main competitive constraints are generally identified, i.e. demand substitutability, supply substitutability and potential competition.[150]

In the digital economy, and with regard to the development of platforms in particular, it is more difficult to provide a clear market definition based on the principles of substitutability and interchangeability. The presence of so-called *multi-sided* platforms represents another bottleneck in this endeavour.[151] The essential feature which makes a business multi-sided is the existence of an *indirect network effect* that crosses customer groups. This implies that once more customers join one side of the platform, the value of the platform to its customers on the other side rises (positive network effects) or decreases (negative network effects)[152]. The market definition relating to platforms needs to pay particular attention to the demand-side *as well as* the supply-side.[153] A global, but nonetheless case specific, approach to defining the market is necessary.[154]

5.1.3 Market power

The degree of market power held by an undertaking represents another key concept under competition law. The decisive criterion to determine market power is whether or not an undertaking's scope of action is *sufficiently controlled by competition forces*.[155] As a proxy, market power is traditionally determined based on the market shares held by an undertaking on a specific market. However, other factors may also be relied upon in order to determine market power, therefore, the identification of market power is case specific.

In the digital market, the level of market shares may not always represent the ideal factor to determine market power. They are limited indicators of competitive strength in innovative markets due to the dynamic nature of the market as well as the changes in market shares, which can happen within a short period of time.[156] Alternative ways in which market participants may be protected (and can protect themselves) from competition should, therefore, be taken into consideration. These alternative ways may, for example, include the presence of unavoidable trading partners, intermediation power in the area of platforms, or data not available to market entrants. In particular, the *intermediation power* of platforms is directly related to the multi-sidedness nature of the platforms and means that they allow for direct interaction between two or more distinct groups of users that are connected by indirect network effects.[157]

As for the data available to market players, if it is argued that the alleged ubiquitous and *non-rivalrous* nature of data may make it more difficult for an undertaking to obtain market power, it is not totally implausible. Data represents an important input in the digital market and holding exclusive rights or *de*

[150] Ibid., p.13.
[151] S. Wismer and A. Rasek, "Market definition in multi-sided markets", OECD, DAF/COMP/WD(2017)33/FINAL.
[152] I. Graef, "Market Definition and Market Power in Data: The Case of Online Platforms", *World Competition* 38, no.4 (2015) p. 476 and reference in footnote 14. Bundeskarellamt (BKartA), B6-113/15, Working Paper – The Market Power of Platforms and Networks, June 2016.
[153] As observed in case No COMP/M.7217 – *Facebook/WhatsApp*, 3 Oct. 2014.
[154] I. Graef, "Market Definition and Market Power in Data: The Case of Online Platforms", *World Competition* 38, no.4 (2015) p. 492.
[155] N. Duch-Brown, B. Martens, F. Mueller-Langer, JRC Report, *The Economics of Ownership, Access and Trade in Digital Data* (2017).
[156] I. Graef, "Market Definition and Market Power in Data: The Case of Online Platforms", *World Competition* 38, no.4 (2015) p. 494.
[157] Bundeskarellamt (BKartA), B6-113/15, Working Paper – The Market Power of Platforms and Networks, June 2016. I. Graef, "Market Definition and Market Power in Data: The Case of Online Platforms", *World Competition* 38, no.4 (2015) p. 484.

facto control over data may have to be taken into consideration for the determination of market power. However, the significance of data and data access for competition will depend on an analysis of the *specificities of a given market, the type of data* (e.g. volunteered, observed or inferred data, personal or non-personal data, historical or real time data…), *and data usage* in a given case.[158]

The following factors, related to market power in the digital economy[159], and counter-balancing factors, may be particularly relevant for the **Safe-DEED** project:

- *Pronounced* direct and indirect *network effects*. These may lead to the creation of barriers to entry and high switching costs for customers. As a counter-factor, the possibility of having interoperable platforms may facilitate a potential switch. Additionally, effective data portability is also to be considered as a counter-factor.
- *Economies of scale and of scope*. In digital markets, undertakings have the opportunity to increase their output, as a consequence of constant fixed costs, while reducing their average costs. This is notably due to specialisation, learning processes, high capacity utilisation or batch size economies. These economies may be particularly efficient from a competition law perspective. They can, nonetheless, prevent market entry or make it more difficult for a competitor to enter the market within a short period of time.
- *Single-homing* (i.e. users are affiliated with only one platform) and degree of *differentiation* (i.e. the capacity to address specific groups of users and to accommodate heterogeneous preferences). Single homing can facilitate concentration. As a counter-factor, *multi-homing* possibilities may counteract self-reinforcing feedback loop[160] effects and reduce lock-in effect.
- *Data source (i.e. data as an input) and access to data*. Exclusive control over specific data (or datasets) can represent a barrier to the market entry of competitors.[161] Such exclusive control may be obtained through IPRs, trade secrets and/or *de facto* through technical measures.
- *Innovation potential of digital markets (including input market for data)*. It cannot be assumed that innovative power as well as the disruptive nature of the Internet are sufficient to competitively control the scope of action of certain undertakings. It should be examined whether concentrations or other practices are likely to result in a restriction of innovation competition (e.g. through existing competition or potential competition from innovative businesses). Innovation potential may be hindered due to the presence of barriers to entry which can include significant investment for technically sophisticated product (e.g. development of a database or complex algorithm).

[158] Commission's study on Competition policy for the digital era. Final report (2019) p. 24.
[159] This non-exhaustive list of factors is based on the N. Duch-Brown, B. Martens, F. Mueller-Langer, JRC Report, *The Economics of Ownership, Access and Trade in Digital Data* (2017), the Commission's study on Competition policy for the digital era. Final report (2019), as well as the Bundeskarellamt (BKartA), B6-113/15, Working Paper – The Market Power of Platforms and Networks, June 2016.
[160] Feedback loop effects appear "*where control over some of an individual's data increases the platform's ability to collect more of it. This can, for instance, happen when data interoperability reciprocity agreements are in place, e.g. all companies interconnecting with the platform need to provide a copy of all the collected data back to the platform allowing the platform to collect data on the user's activity outside the platform and centralise the data. In the context of ecosystems, private data APIs between services belonging to the same ecosystem might create a strong advantage for services that belong to the ecosystem, especially when the ecosystem is very large and involves numerous and diverse services*". Commission's study on Competition policy for the digital era. Final report (2019) p. 31.
[161] EPSC, *Enter the Data Economy – EU Policies for the Thriving Data Ecosystem* (Strategic Notes 2017).

5.2 Article 101 of the TFEU

Article 101 TFEU provides that "*all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their **object or effect** the prevention, restriction or distortion of competition within the internal market shall be prohibited as incompatible with the internal market. In particular, those which:*

> *(a) directly or indirectly fix purchase or selling prices or any other trading conditions;*
> *(b) limit or control production, markets, technical development, or investment;*
> *(c) share markets or sources of supply;*
> *(d) apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;*
> *(e) make the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts".*

Any agreements or decisions prohibited pursuant to this Article shall be automatically void (Art 101(2) TFEU). However, under Art 101(3) TFEU, some agreements which may fall within the scope of Art 101(1) may still be compatible with the internal market. It is required that these agreements contribute to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit, and (a) do not impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives and, (b) afford such undertakings the possibility of eliminating competition in respect of a substantial part of the products in question. In other words, agreements which provide *efficiency gains* may still be declared compatible with the internal market.

Overall, potentially anti-competitive agreements are those which reduce the parties' decision-making independence. The restrictive effects of these agreements are expected where parties are able to raise prices, reduce output, reduce product quality and/or variety or reduce innovation. Multiple factors must be taken into consideration to assess these restrictive effects (e.g. the nature and content of the agreement, the market power of the parties, the capacity of the agreement to create, maintain or strengthen such market power). The main competition concerns which may arise from horizontal co-operation agreements under 101 TFEU are the following:

- Limited possibilities for parties involved, as well as third parties, to compete;
- The sharing of assets appreciably reduces the decision-making independence of the parties;
- The agreement affects the parties' financial interests which may also reduce the decision-making independence of the parties.

In the digital economy, *innovation competition* has a significance of its own and needs to be considered alongside price competition. The general benchmark related to "not sufficiently controlled scope of action" nevertheless remains the key factor of the assessment.[162]

The presence of *platforms* on the market allowing for (potential) competitors to exchange data or data-related information may lead to *concentration* issues. The exchange of information (in particular sensitive information) may give rise to restrictive effects if it further reduces strategic uncertainty in the market. The main issue is, potentially, that by being able to analyse data from another party and by combining it with one's own data, a company will be able to develop new products or services on a market and gain market power. Matching platforms hold the risk of tight oligopolies as they could facilitate a collusive outcome on the market as it is easier to reach a common understanding and to monitor deviations. In turn, a high level of concentration can lead to monopoly. Next to concentration concerns, the collaboration of (potential competitors) on a platform may also hold risks in terms of

[162] Commission's study on Competition policy for the digital era. Final report (2019).

exclusion, i.e. of competitors not involved in the platform[163] or *lock-in*, i.e. actual or potential competitors will have limited decision-making powers due to the necessity to stay within a specific ecosystem. Some counter factors to the risks of anti-competitive agreements in the digital industry are notably to ensure that the data is limited in scope or aggregated and anonymised. Additionally, *protocol and data interoperability* as well as *access conditions* represent other counter-factors to take into consideration.[164]

On the other hand, *data sharing* and *pooling*[165] may be considered as pro-competitive. Data sharing and pooling present similarities with other types of collaboration agreements which are traditionally seen as pro-competitive, such as R&D collaboration, standard-setting or patent pools. The pooling of data of the same type or of complementary data resources may enable firms to develop new or better products or services or to train algorithms on a broader, more meaningful basis.[166]

Safe-DEED aims to provide a set of tools to facilitate the assessment of data value, thus incentivising data owners to make use of the cryptographic protocols to create value for their companies and clients. Having in mind the objectives of the project, it is potentially unlikely that such technology becomes an anti-competitive tool. However, since competition law assessment generally relies on a case-by-case analysis and depends on various factors such as the type of data shared, the form of the arrangement as well as the market position of the parties involved in the sharing, these elements need to be further explored in detail in the use cases of the projects in order to provide a more tailored analysis.

5.2.1 Commission guidelines on the applicability of Article 101 TFEU to horizontal co-operation agreement[167]

The Commission guidelines apply to horizontal co-operation agreements between actual or potential competitors. The guidelines apply as well to agreements between non-competitors, such as, for example, companies active in the same product markets but in different geographic markets without being potential competitors. They are meant to help competition authorities as well as judicial authorities in applying Art 101 TFEU. The scope of the guidelines is fairly broad and provides an analytical framework for the most common types of horizontal co-operation agreements, i.e. R&D, production (including subcontracting and specialisation), purchasing, commercialisation, standardisation and information exchange.

Agreements included within the scope of the guidelines can lead to substantial economic benefits (e.g. by combining complementary activities, skills or assets). Undertakings can share risk, save costs, increase investments, pool know-how, enhance product quality and variety and launch innovation faster. There is a general assumption that collaboration is pro-competitive, unless it leads to (1) reduction in price competition (2) hinderance of emergence of innovative technologies and (3) exclusion of, or discrimination against, certain companies by preventing their effective access to the technology (which can include data). On the other hand, such agreements may be problematic if they lead to price- or output- fixing, partitioning of the market, or if they enable the parties to maintain, gain or increase

[163] B. Lundqvist, "Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition law in an Internet of Things World – The Issue of Access", *Stockholm Faculty of Law, Research Paper Series no 1*, 2016, p. 4.
[164] Commission's study on Competition policy for the digital era. Final report (2019) p. 20.
[165] B. Lundqvist, "Competition and Data Pools", *EuCML* Iss. 4/2018, 146-154.
[166] Commission's study on Competition policy for the digital era. Final report (2019). OECD, "Roundtable on information exchange between competitors under competition law – Note by the Delegation of the European Union", DAF/COMP/WD(2010)118 (2010).
[167] Communication from the Commission – Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, *OJ C 11, 14.1.2011, p. 1-72.*

market power which is likely to give rise to negative market effects (e.g. on price, output, product quality or variety, or innovation).

The guidelines are highly relevant regarding collaboration between undertakings in the digital economy. The guidelines are also relevant for understanding the concept of *competition in existing markets* as well as *competition innovation,* which generally touches upon future markets or potential markets. For example, in the framework of R&D agreements, the effects of competition in innovation may not always be sufficiently assessed by referring to existing product or technology markets. Therefore, it may be important to identify "R&D poles"[168] aimed at developing future substitutable products or technology. In such agreements, the analysis focuses on whether, after the cooperation, there will be a sufficient number of remaining R&D poles.

Additionally, with regard to exchanges of data (or data-related information) the guidelines may particularly apply to exchanges between competitors of *strategic data*. These exchanges are more likely to be caught by 101 TFEU than exchanges of other types of information as they may reduce the parties' decision-making independence by decreasing their incentives to compete. Strategic data may refer, i.a., to specific individual data, technology data. The strategic usefulness of data depends on its market coverage, frequency, aggregation, age as well as the market context in which the exchange occurs.[169] Information related to *prices* and *quantities* are traditionally considered the most strategic (e.g. discounts, rebates, customer data, production costs, quantities, turnovers, sales, capacities, qualities, marketing plans, risks, investments, technologies and R&D programs and their results).

It is conceivable that the **Safe-DEED** set of tools could be used as a tool for exclusion of, or discrimination against, certain companies by preventing their effective access to the technology. Moreover, one of the functionalities of Safe-DEED will be to help undertakings in realising whether it makes sense to collaborate and combine their data to create a value that exceeds the sum of individual parts. The component will in this case also provide guidance on how to split the revenue resulting from such a data collaboration is a fair manner. Such component may have to be assessed under the rules of competition law, as it will lead to collaboration between (potential) competitors and will touch upon price-related element. However, safe harbours (or counter-factors) envisaged for standard setting in the guidelines may apply to this specific component of the project, i.e. adoption of an *open access* model, *transparency* on the adoption procedure, and the adoption of a *Fair, Reasonable and Non-Discriminatory (FRAND) licensing* model[170]. On the other hand, the technology envisaged under the project could also lead to an increase of exchange leading to an increase in variety as well as quality of products and/or services. This increase in variety and quality would potentially be considered pro-competitive.

[168] R&D Agreement (para 111 et seq). With regards to R&D poles, see. para 120.
[169] B. Lundqvist, "Competition and Data Pools", *EuCML* Iss. 4/2018, p. 151.
[170] FRAND licensing means that the members of a standard setting organisation (SSO) will license their technology to the other members of the organisation as well as third parties under fair, reasonable and non-discriminatory terms. This is particularly relevant for technologies which are protected under so-called standard essential patents (SEPs). These terms facilitate widespread use of a standard and ensure that right holder benefit from a fair return on their investment without gaining an unfair bargaining advantage. Y. Méniére, N. Thumm, JRC Report, "Fair, Reasonable and Non-Discriminatory (FRAND) Licensing Terms" (2015).

5.2.2 Regulation on the application of Article 101(3) TFEU to categories of vertical agreements and concerted practices (Block Exemption Regulation – 330/2010)[171]

This regulation provides that certain types of vertical agreements (by opposition to horizontal agreements) can improve economic efficiency and therefore may benefit from an exemption. The categories of agreements satisfying the condition of Art 101(3) include vertical agreements for the purchase or sale of goods and services where those agreements are concluded between non-competing undertakings, between certain competitors or by certain associations of retailers of goods. It also includes vertical agreements containing ancillary provisions on the assignment or use of IPRs (Recital 3).

Important factors that must be considered in order to benefit from the exemption are: the degree of market power of the parties, the extent to which the parties face competition from third parties outside of the agreement, or whether the goods and/or services are interchangeable and/or substitutable (Recital 7).

With regard to market shares, the Regulation envisages a 30% market share on the relevant market for the vertical agreement to be presumed not to represent an anti-competitive agreement. Above this threshold, the presumption will not be applicable and efficiency gains will have to be demonstrated. Beside this market threshold, the Regulation also stipulates that, to benefit from the exemption, vertical agreements should not contain certain types of clauses considered severe restrictions of competitions (Art 4 – Hardcore restrictions). These restrictions essentially touch upon price-determination issues, market allocation, active or passive sales, cross-supplies in distribution system, and spare parts.

Due to the fact that the parties involved in the project do not engage in concerted actions to purchase, sell or resale goods or services, the activities included in the **Safe-DEED** project will most likely not fall within the scope of this Regulation. The exploitation activities of the project may, nonetheless, lead to another conclusion and will therefore be reviewed more in details during the course of the use cases and their potential outcomes on the market post-project.

5.3 Article 102 of the TFEU

Article 102 TFEU stipulates that: "*Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States.*

Such abuse may, in particular, consist in:

> *(a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;*
>
> *(b) limiting production, markets or technical development to the prejudice of consumers;*
>
> *(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;*
>
> *(d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts*".

[171] Commission Regulation (EU) No 330/2010 of 20 April 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices, *OJ L 102, 23.4.2010, p. 1-7.*

The essential questions under 102 TFEU are whether an undertaking is in a position of dominance and whether this position is abused. Moreover, it is also necessary to enquire whether this abuse can be justified due to efficiency gains. The burden of proof to demonstrate such gains rests on the dominant undertaking. It should be highlighted that, undertakings which are in a position of dominance on a specific market also bear a special responsibility not to distort competition on such market.

In recent years, Art 102 TFEU has been relied upon by competition authorities with regards to practices related to data. Four main theories of harm related to data have been identified: *Refusal to share*, abusive discrimination, leveraging of customer data, and exploitation by unlawful processing or unfair term.

Refusal to share and concerns with regards to *data access* have been the centre of attention under Art 102 TFEU. In particular, the possibility for authorities to rely on Art 102 TFEU to impose on an undertaking (in a dominant position) an obligation to provide access to its data (or datasets) if such data may be considered *indispensable* for competitors to compete. In such instance, the refusal to grant access from a dominant undertaking may be considered an abusive practice under 102 TFEU. The applicability of the "essential facility" or the "exceptional circumstances" doctrine[172] developed by the CJEU to practices related to data, has been questioned. The requirement of indispensability remains hard to prove in a world of ubiquitous and non-rivalrous data.[173] So far, there has been no case where competition authorities have found that data could constitute a competition problem under this approach. It is argued that, in a number of settings, data access will not be indispensable to compete, and public authorities should refrain from intervention.[174] However, it is also argued in literature, that if the data is so vast that it may be *impossible to rebuild a similar data set*, the exceptional doctrine may be applicable.

Similar to the analysis of 101 TFEU, counter-factors may also have to be considered in the assessment of abusive dominance in the digital economy and in particular with regards to access to data. First, a distinction may have to be established between non-anonymous use of individual-level data, anonymous use of individual level data, aggregated data and contextual data. Second, additional factors such as, computing power, software (and their degree of openness), skilled engineers or the degree of market power of data controllers, machine producers or platforms,[175] may affect the analysis.

Depending on the components (technological and non-technological ones) developed by the partners, the tools to facilitate the assessment of data value under the **Safe-DEED** project may also act as counter-factors for firms whose business model is built on the acquisition and monetisation of personal data and which feel the need for keeping their datasets to themselves, and which could, thereby, shield data away from competitors.

[172] Judgment of 6 April 1995, *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd. (ITP) v. Commission of the European Communities*, joined cases C-241/91 P and C-242/91 P, EU:C:1995:98. Judgment of 29 April 2004, *IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG.*, C-418/01, EU:C:2004:257. Judgment of 27 June 2012, *Microsoft Corp. v. European Commission*, Case T-167/08, EU:T:2012:323. Under the case law of the CJEU, four conditions must be met in order for a refusal to license to be considered anti-competitive under 102 TFEU: indispensability, lack of effective competition between the upstream and downstream product, prevention of the emergence of a new product, and no objective reason for the refusal. In *Microsoft*, the GC clarified that the prevention of a "new product" is but one case in which a refusal to license can be found to limit production, markets or technical development to the prejudice of consumers. "Exceptional circumstances" that justify the imposition of a duty to license may likewise exist where a refusal to deal would eliminate *competition for innovation or quality* to the detriment of consumers. N. Duch-Brown, B. Martens, F. Mueller-Langer, JRC Report, *The Economics of Ownership, Access and Trade in Digital Data* (2017) p. 21 et seq.

[173] J. Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition on the European Commission's "Public consultation on Building the European Data Economy" (April 26th, 2017). B. Lundqvist, "Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition law in an Internet of Things World – The Issue of Access", *Stockholm Faculty of Law, Research Paper Series no 1,* 2016.

[174] Commission's study on Competition policy for the digital era. Final report (2019).

[175] I. Graef, "Market Definition and Market Power in Data: The Case of Online Platforms", World Competition 38, no.4 (2015): 473-506.

5.4 Merger Regulation (139/2004)[176]

Competition authorities are particularly attentive to mergers and acquisitions by large companies. They are concerned with the conduct of undertakings who are part of these agreements but also to the possible effects of these agreements on the market structures. A particular concern is the degree of concentration of mergers and their consequences in terms increase in market power. By joining forces, undertakings will potentially increase their market power and, under certain circumstances, may reach (or reinforce) a position of dominance on a specific market.

Contrary to Art 101 and 102 TFEU, which may be relied upon by competition as well as judicial authorities after a particular situation occurs on the market (*ex post* control[177]), the compatibility of mergers and acquisitions with the internal market may have to be assessed before they occur (*ex ante* control).

Under the Merger Regulation, potential mergers and acquisitions of a certain size must be notified to the European Commission for review and approval prior to their implementation (Art 4 Merger Regulation). The Commission's jurisdiction over concentrations is nonetheless limited to mergers with an "EU dimension", i.e. where the parties to the agreements have a substantial size and have a significant turnover within the internal market (see the thresholds provided under Art 1 Merger Regulation as well as Art 5 for the calculation of turnover). For smaller concentrations, a notification to the national competition authorities may be required.

Under Art 3 of the Regulation, a concentration is deemed to arise where a change of control on a lasting basis results from (a) a merger of two or more previously independent undertakings or (b) the acquisition, by one or more persons already controlling at least one undertaking, or by one or more undertakings of direct or indirect control of the whole or parts of one or more other undertakings (this also include the creation of a joint venture). Control is constituted by rights, contracts or any other means which confer the possibility to exercise decisive influence on an undertaking. This include by obtaining ownership or the right to use all or part of the assets of an undertaking.

Due to the fact that **Safe-DEED** will only provide a set of well-orchestrated and coordinated standalone components, including technological and non-technological ones, which will be added to existing data platforms, the concerns at the heart of the Merger Regulation will highly unlikely apply to the project. Overall, Safe-DEED will not affect the fact that the parties to the project will remain independent undertakings, i.e. autonomous economic entities.

5.5 Standardisation and interoperability

The development and adoption of standard(s) within the framework of the project may take into account the founding principles envisaged under the Regulation on European Standardisation (1025/2012).[178] The relevant principles are, namely, *coherence*, *transparency*, *openness*, *consensus*, *voluntary application*, *independence from special interests and efficiency*. Additionally, the Communication from

[176] Council Regulation (EC) No 139/2004 of 20 Jan. 2004 on the control of concentrations between undertakings (the EC Merger Regulations). *OJ L 24, 29.1.2004, p. 1-22.* See also the Commission Regulation (EC) No 802/2004 of 21 April 2004 for the notification procedure.

[177] As envisaged in Council Regulation (EC) No 1/2003 of 16 Dec. 2002 on the implementation of the rules on competition laid down in Arts 81 and 82 of the Treaty, *OJ L 1, 4.1.2003, p. 1-25.*

[178] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 Oct. 2012 on European Standardisation, *OJ L 316, 14.11.2012, p. 12-33.*

the Commission on "ICT Standardisation Priorities for the Digital Single Market"[179] may also provide key principles to be considered in the development of technical standards as envisaged in the project.

The standards envisaged in the Regulation, as well as those referred to in the Communication from the Commission, may ensure that the *interoperability* of digital technologies is guaranteed and therefore help in providing economies of scale, foster research and innovation and keep markets open. Open standards also ensure that market entry barriers are lowered. The presence of standards affects the competition law analysis of the project as it is, presumably, believed that standards provide efficiency gains and have, therefore, pro-competitive effects. As mentioned in the Communication from the Commission, "*interoperable solutions based on open systems and interfaces keep markets open, boost innovation and allow service portability in the Digital Single Market*"[180].

5.6 Key requirements related to the EU competition law framework

The competition law assessment of digital markets requires less emphasis on market definition and more focus on theories of harm and identification of anti-competitive strategies. It is, nonetheless, necessary to keep regular analysis of markets from consumers' perspective if possible. This task should be combined with an analysis of competition on (possible) markets for digital ecosystems.

For the development of a platform, including its essential components such as the set of tools envisaged in the **Safe-DEED** project, it is important that its infrastructure as well as the APIs in place do not represent technical means which would be considered hampering competition.[181] It is not impossible that competitors may not be able to compete on the merit due to e.g. the existence of privileged APIs which could distinguish between competitors and entities part of the service. Under certain circumstances, this could be considered an anti-competitive discriminatory practice.

Due to the fact that the objective of **Safe-DEED** is to provide a set of tools to undertakings but is not meant to provide a specific platforms for trading data directly, it is particularly relevant to analyse the likelihood that other undertakings may have access to similar information or that new entrants are able to benefit from the same competitive tools as the ones developed in the project.

The following table summarily presents the elements forming part of the competition law framework and which may be particularly relevant for the **Safe-DEED** project. These elements will be part of the in-depth analysis relative to the use cases.

Risks related to Art 101 TFEU	Counter-factors
Collusion, exclusion and discrimination, lock-in Reduction of competition innovation Exchange of sensitive data	Pro-competitiveness of collaboration Limited, aggregated, anonymised, non-strategic data Protocol interoperability Data interoperability and portability Degree of openness (software, APIs) and access

[179] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ICT Standardisation Priorities for the Digital Single Market, COM/2016/0176 final.
[180] *Ibid*, p. 3.
[181] B. Lundqvist, "Competition and Data Pools", *EuCML* Iss. 4/2018, p. 149.

	Transparency FRAND (like) licensing
Risks related to Art 102 TFEU	Counter-factors
Refusal to share – issue of access to indispensable data Discriminatory practices, leveraging of customer data Lock-in effects	Threshold for indispensability Differentiation of data (volunteered, observed or inferred) and data portability[182] Openness (software, APIs) Standardisation and interoperability

With regards to data and datasets in particular, a more granular distinction may be relevant for the analysis of the use cases from a competition law perspective:

Data (or data-related factors) presenting more competition law concerns	Data (or data-related factors) presenting less competition law concerns
Individualised data	Aggregated data
Younger data	Older data
Frequent exchange	Not frequent exchange
Non-public data	Genuinely public data
Non-public exchange (closed level of openness)	Genuinely public exchange (high level of openness for competitors and customers)

[182] Commission Staff Working Document – Guidance on sharing private sector data in the European data economy (25.04.2018). Accompanying the communication "towards a common European data space" (COM(2018) 232 final).

6 Consumer Protection Implication

The **Safe-DEED** project aims to develop a platform where a set of tools is implemented to incentivise data owners to create value from the data assets provided by the different providers of the platform. Therefore, the area of consumer protection is out of the scope of this deliverable, since at this stage, no interaction with the consumers is foreseen.

Nonetheless, the latest legislative initiatives in this area might result in having an indirect impact also on **Safe-DEED**. The Digital Content Directive touches upon the concept of personal data as a counter performance in a contractual relationship between the goods or services provider on the one hand, and the consumer on the other one. Hence, this chapter analyses the aspects involving personal data as a value, the interaction with GDPR and current consumer protection provisions.

6.1 Digital Content Directive

On 9th of December 2015, the EC published a proposal for a Directive on certain aspects concerning contracts for the supply of digital content (Digital Content Directive, DCD).[183] After a legislative *iter* of almost four years and many changes, the EU Institutions have reached an agreement on the text, which is going to be published on the EU official journal by the end of May 2019.

Contractual law is an area of Member States competence. Along the years, many Commission's initiatives have failed to harmonise this field. After the negotiation on the Common European Sales Law failed, the EC has slightly changed its approach and has started focusing on tackling contractual law through consumer protection. The first legislative initiative coming from the new approach focuses on '*online and other distance sales of goods*',[184] while the second focuses on '*contracts for the supply of digital content*.'[185]

The Digital Content Directive does not pay attention to digital content ownership but instead on remedies for consumers and personal data providers that are using their personal data as a form of payment when contracting for the supply of digital content.

[183] Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, (COM(2015) 634 final).
[184] Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, COM/2015/0635 final - 2015/0288 (COD) and Amended proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, amending Regulation (EC) No 2006/2004 of the European Parliament and of the Council and Directive 2009/22/EC of the European Parliament and of the Council and repealing Directive 1999/44/EC of the European Parliament and of the Council, COM(2017) 637 final 2015/0288(COD).
[185] Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM(2015) 634 final 2015/0287 (COD).

6.1.1 Purpose and Scope of Application

The DCD aims to harmonise the current framework on contracts for the supply of digital content. The goal is to improve the trust of consumers and consequently to stimulate cross-border purchasing of digital services, and ultimately enhance the EU Digital economy.

Rec 19 and Art 2 DCD clarify what should be considered a digital content or a service. By doing so, the DCD lists a broad range of products and services usually provided by the so-called Over The Top Players (OTT). Indeed, digital content should be considered as data that are produced and supplied in digital form while services allow a consumer to create, process, store, access, share or allow interaction with data. This definition includes, *inter alia, computer programmes, applications, video files, audio files, music files, digital games, e-books or other e-publications, and also digital services,* which allow the creation of, processing of, *accessing* or storage of data in digital form, *including software-as-a-service, such as video and audio sharing and other file hosting, word processing or games offered in the cloud computing environment and social media*.'[186]

According to Art 3 DCD, only contracts for the supply of digital content that are provided for a price or using personal data as a form payment fall into the scope of this Directive. The DCD makes a clear differentiation between personal data provided as a form of remuneration and data *presented to the trader for supplying the digital content or digital service or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process that data for any other purpose'.*[187]

The DCD, dealing with personal data makes clear reference to GDPR. In particular, Rec 38 DCD states that '*any processing of personal data in connection with a contract falling within the scope of this Directive is lawful only if it conforms with the provisions of Regulation (EU) 2016/679 relating to the legal grounds for the processing of personal data'.*[188]

Consequently, the trader, when dealing with personal data, has to comply with the GDPR requirements.[189] The DCD clarifies that in cases where a lack of compliance with the GDPR's requirements occur, it might also affect the conformity requirements of the contract falling into the scope of DCD.[190] The predominance of GDPR over the DCD is also confirmed in the provision that regulates digital content contract termination, where the GDPR requires the discipline of contracts where personal data are used as a form of payment.

[186] Rec 19 DCD.
[187] Art 3 DCD.
[188] Rec 38 DCD.
[189] Rec 69 DCD.
[190] Rec 48 DCD: '…*One example could be where a trader explicitly assumes an obligation in the contract, or the contract can be interpreted in that way, which is also linked to the trader's obligations under Regulation (EU) 2016/679. In that case, such a contractual commitment can become part of the subjective requirements for conformity'.*

7 References

7.1 Doctrine

Clifford D., Ausloos J., "Data Protection and the Role of Fairness" [2017] CiTiP Working Paper Series 13.

De Hert P. et al., "The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services" [2017] Computer Law & Security Review.

Duch-Brown N., Martens B., Mueller-Langer F., JRC Report, "The Economics of Ownership, Access and Trade in Digital Data" [2017].

Ezrachi A., "BEUC Discussion Paper – The goals of EU competition law and the digital economy" [2018].

González Fuster G., "EU Fundamental Rights and Personal Data Protection", The Emergence of Personal Data Protection as a Fundamental Right of the EU [2014] Springer.

Graef I., "Market Definition and Market Power in Data: The Case of Online Platforms" [2015] World Competition 38, no.4.

Lundqvist B., "Competition and Data Pools", [2018] EuCML Iss. 4/2018.

Lundqvist B., "Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition law in an Internet of Things World – The Issue of Access" [2018] Stockholm Faculty of Law, Research Paper Series no 1.

Maldoff G., "How GDPR Changes the Rules for Research" https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research.

Méniére Y., Thumm N., JRC Report, "Fair, Reasonable and Non-Discriminatory (FRAND) Licensing Terms" [2015].

Wismer S., Rasek A., "Market definition in multi-sided markets", OECD, DAF/COMP/WD(2017)33/FINAL.

Bundeskarellamt (BKartA), B6-113/15, Working Paper – The Market Power of Platforms and Networks, June 2016.

Commission Staff Working Document – Guidance on sharing private sector data in the European data economy (25.04.2018). Accompanying the communication "towards a common European data space" (COM(2018) 232 final).

Commission's study on Competition policy for the digital era. Final report (2019)

EPSC, Enter the Data Economy – EU Policies for the Thriving Data Ecosystem (Strategic Notes 2017)

7.2 Case Law

CJEU Case C-101/01 *Bodil Lindqvist*, ECLI:EU:C:2003:596

CJEU Case C-131/12 *Google v. Agencia Española de Protección de Datos (AEPD)*, ECLI:EU:C:2014:317

CJEU Case C-209/10, Post Danmark I, ECLI:EU:C:2012:172

CJEU Case C-23/14, Post Danmark II, ECLI:EU:C:2015:651

CJEU Case C-280/08 P, Deutsche Telekom v Commission, ECLI: EU:C:2010:603

CJEU Case C-418/01, IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG., ECLI:EU:C:2004:257

CJEU Case C-434/16, *Nowak v. Data Protection Commissioner*, ECLI:EU:C:2017:994

CJEU Case C-456/00 *Österreichischer Rundfunk and Others*., ECLI: EU: C: 2003: 294

CJEU Case C-73/07, *Satakunnan Markkinapörssi and Satamedia*, ECLI:EU:C:2008:727

CJEU Case T-167/08, *Microsoft Corp. v. European Commission*, ECLI:EU:T:2012:323

CJEU Case T-213/01, *Österreichische Postsparkasse v Commission*, ECLI:EU:T:2006:151

CJEU Case T-286/09, *Intel v Commission*, ECLI:EU:T:2014:547.

CJEU Joined cases C-241/91 P and C-242/91 P, *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd. (ITP) v. Commission of the European Communities*, ELI:EU:C:1995:98.

CJEU Joined Cases C-92/09 and Case C-93/09 *Volker und Markus Schecke and Eifert*, ECLI:EU:C:2010:662

ECtHR *Kennedy v. the United Kingdom*, no. 26839/05

ECtHR, *Rotaru v. Romania*, n. 28341/95,

ECtHR, *S. and Marper v. the United Kingdom*, n. 30562/04 and 30566/04

7.3 Legislations

Article 29 Working Party, 'Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector' (WP 211)

Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (WP 203)

Article 29 Working Party, 'Opinion 1/2010 on the concepts of controller and processor' (WP169)

Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173)

Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (WP 136)

Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407.

Commission decision COMP/M.7217 – Facebook/WhatsApp, 3 Oct. 2014.

Commission Notice on the definition of relevant market for the purposes of Community competition law, OJ L 372, 9.12.1997

Commission Regulation (EC) No 802/2004 of 21 April 2004 for the notification procedure.

Commission Regulation (EU) No 330/2010 of 20 April 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices, OJ L 102, 23.4.2010, p. 1-7.

Communication from the Commission – Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, OJ C 11, 14.1.2011, p. 1-72.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ICT Standardisation Priorities for the Digital Single Market, (COM/2016/0176 final).

Communication from the Commission to the European Parliament, the European Council and the Council. First progress report towards an effective and genuine Security Union (COM(2016) 670 final)

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, " Building a European Data Economy" (COM(2017) 9 final)

Communication from the Commission to the European Parliament and the Council, First progress report towards an effective and genuine Security Union, (COM/2016/0670) final)

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Comittee and the Committee of the Regions, Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century, (COM(2012) 9 final)

Communication from the Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region – Commission Work Programme 2016 – No time for business as usual' (COM/2015/0610 final)

Council Regulation (EC) No 1/2003 of 16 Dec. 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 4.1.2003, p. 1-25.

Council Regulation (EC) No 139/2004 of 20 Jan. 2004 on the control of concentrations between undertakings (the EC Merger Regulations). OJ L 24, 29.1.2004, p. 1-22.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108)

Directive (EU) 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 OJ L 201, 31.7.2002

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union OJ L 194, 19.7.2016 p. 1–30

Directive (EU) 2018/1972 establishing the European Electronic Communications Code (Recast) OJ L 321, 17.12.2018, p. 36–214

Directive (EU) 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data OJ L 281, 23.11.1995 p. 31–50

EDPS Ethics Advisory Group 2018 Report, Towards a digital ethics.

ENISA's Opinion Paper on Encryption 2016.12.12

European Convention of Human Rights, Council of Europe, 1953.

Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, (COM/2015/0635 final)

Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, (COM(2015) 634 final)

Proposal for a Regulation of the Parliament and the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (COM/2017/0477 final - 2017/0225)

Protocol 27 on the internal market and competition, annexed to the TFEU, OJC 115, 09.05.2008.

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 Oct. 2012 on European Standardisation, OJ L 316, 14.11.2012,

Regulation (EU) No 2018/1807 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59–68

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, p. 1–88

7.4 Others

European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights'

Hunton & Williams, EU Data Protection Regulation Tracker.

Natalie Bertels, 'Scientific Research under the GDPR: What Will Change?' (CITIP blog)

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

OECD, "Roundtable on information exchange between competitors under competition law – Note by the Delegation of the European Union", DAF/COMP/WD(2010)118 (2010)

Stephanie Rossiello, *Europe's "Trustworthy" AI*, (CiTiP blog)

Stijn Storms, 'Identify Me If You Can – Identifiability and Anonymisation' (CITIP blog)

Verhenneman G, Vedder A, WITDOM, D6.1 – Legal and Ethical framework and privacy and security principles [2015].