Safe-DEED

www.safe-deed.eu

Legal Requirements for Processing of Non-Personal Data

Deliverable number	*D3.3*
Dissemination level	*Public*
Delivery date	*24 February 2020*
Status	*Final*
Author(s)	*Alessandro Bruni, Arina Gorbatyuk*

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

Changes Summary

Date	Author	Summary	Version
15.01.2019	Alessandro Bruni	First draft	0.1
16.01.2020	Arina Gorbatyuk	Second draft	0.2
05.02.2020	Alessandro Bruni	Third draft	0.3
06.02.2020	Arina Gorbatyuk	Fourth draft	0.4
07.02.2020	Mark de Reuver (TUD)	Internal review 1	0.5
10.02.2020	Ioannis Markopoulos	Internal review 2	0.6
10.02.2020	Petr Knoth	Internal review 3	0.8
17.02.2020	Alexander Georg	Internal review 4	1.1
20.02.2020	Patrick Ofner	Internal review 5	1.2
24.02.2020	Alessandro Bruni	Final version	1.3

1 Contents

2 List of Tables

3 Executive Summary

Deliverable D3.3 contains the overview of the specific legal requirements for the use cases developed by KU Leuven CiTiP within the Safe-DEED Project. The previous Deliverable D3.2 focused on the processing of personal data. Like D3.2, D3.3 intends to describe critical legal requirements of those EU legislative initiatives that touch upon processing of non-personal data. Specifically, D3.3 aims to analyse the key aspects of non-personal data (Section 6.2) and analyse the relevant provisions of EU competition law (Section 6.3), which has been originally articulated in D3.1. D3.3 also provides a list of good practices for negotiating data usage agreements relevant, when the project will be over, for the deployment phase of the project (Section 6.3.2). The requirements elaborated upon in D3.3 will support not only the activities of Safe-DEED during the duration of the WP7 trial phase, but may also be useful for the deployment phase of Safe-DEED's project. As a matter of fact, the listed requirements should be taken into account by all those partners that want to use the technologies developed within the Safe-DEED project.

Compliance with legal requirements is an on-going process. For this reason, an enduring dialogue between KU Leuven and other Safe-DEED partners, especially those involved in WP6, has been established and reinforced. The aim is to guide the identification of the technical and legal aspects that need to be implemented with appropriate compliance measures.

The legal requirements listed in D3.3 might be subject to implementation if upcoming EU legislative initiatives will touch upon Safe-DEED project's activities. Future WP3 deliverables might have to be updated, taking into account forthcoming legislative initiatives proposed at EU and national levels (e.g. concerning the European Electronic Communication Code national implementation). The deliverable D3.3 includes a specific section on the newly appointed EU Commission working plan for the upcoming years.

The identification of legal requirements listed in D3.2 and D3.3 has been carried out considering challenges and results of the trials' phases in WP6 and WP7. While WP6 focuses on processing activities of non-personal data, WP7 demonstrator involves data that have been previously anonymised and consequently are non-personal data. Nonetheless, upcoming challenges originated in the context of the two use cases might involve both categories of data, personal and non-personal. It is crucial, therefore, to read the two documents, D3.2 and D3.3, together.

The listed requirements have been presented in a clear and unambiguously manner. Nonetheless, due to their legal nature, the possibility to have additional legal requirements, such as those originated by the implementation process of EU legislative initiatives in the national frameworks, should always be taken into account by partners.
While at the EU level, an *ad hoc* legislation that touches upon enabling technologies for platforms do not exist, multiple non-binding initiatives have been produced in the last years.

Besides, in the context of processing non-personal data, the EU has recently approved a Regulation (Regulation (EU) 2018/1807)[1] on the free flow of such data. The Regulation, clarifying the nature and characteristics of data that fall in the scope of application of the regulation, requires the drafting of a code of conduct and ad hoc procedure to allow data portability of such data.

Since the activities that characterise WP7 touch upon binding and not binding legislative initiative, deliverable D3.3 specifies the binding and non-binding legal requirements that should be taken into account in the context of enabling technologies for platforms. D3.3 provides legal guidelines that should be followed not only by partners during the demonstrator stage but also by those entities that intend to use Safe-DEED technologies in the deployment stage.

4 Deliverable Structure

D3.3 is divided into three main parts.

The *first part* (section 6) summarises (1) key aspects related to legal frameworks that have been identified as relevant in the context of activities involving the processing of non-personal data and (2) legal considerations related to competition law and negotiation of data usage agreements, originally described in D3.1.

Based on the analysis of the first part, the *second part* (section 7) develops an easy-to-read list of concrete actions that parties involved in WP7 need to considered while performing their trials.

The *third part* (section 8) includes a brief overview of key legislative initiatives that the new Commission intends to develop during its five-year mandate.

In addition, Annex I provides an overview of all legal requirements that have been listen in D3.2 and D3.3.

1 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59–68.

5 Introduction

The EU privacy and data protection legal framework analysed in D3.1 and substantiated in D3.2 is not the only legislative framework that should be considered by Safe-DEED partners. The whole supply-chain of data management activities that constitute the Safe-DEED project involve other crucial EU legislative initiatives. Using as a baseline the EU legislations described in the deliverable D3.1, deliverable D3.3 summarises the critical aspects of the legislative initiatives initially described in D3.1 and offers a list of detailed legal requirements that should be taken into account by Safe-DEED partners when carrying out activities that do not involve the processing of personal data. To assess which are the legal requirements that should be taken into account a preliminary analysis of the WP7 has been carried out. The description of the use case lead by Infineon aims to define, first of all, the nature of the data (personal, non-personal) that will be processed. In concrete, we refer personal-data as those data that, by nature or because properly anonymised, do not include any information of an identifiable or identified person.

While the list of requirements is tailored and developed using WP7 and its trials as a baseline, it is useful for all Safe-DEED partners to take into account the legal requirements described in this deliverable.

Within the demonstrator phase, KU Leuven displays the legal requirements that should be taken into account when processing non-personal data, which are the ones used by Infineon within WP7 nature of datasets used.
Infineon is aiming to implement a new business model for the order process towards its customers. Therefore, a new dynamic pricing strategy based on the customers' requested lead times (Lead time-based pricing) is developed. Throughout the Safe-DEED project, a demonstrator order process will be developed. It will involve Infineon promoting a mock-up order platform where customers can place their orders and bids. Infineon will also provide the pricing algorithm to compute the adjusted price, as well as a dummy ATP level of the plants with meaningful, but not real data, so not data that fall into the definition of personal data given by the GDPR.
It is useful to clarify that, throughout the process, Infineon analyses the order data internally. Such data includes customer names and customer number (SoldToName and SoldTo number), order numbers, customer wish dates, confirmed dates by Infineon, contractually agreed order lead times, product names and product groups. Since order data are personal, Infineon develops synthetic data derived from the real data by using statistical distributions and giving out sample data to the project partners (especially regarding lead times). Order entry dates will be therefore anonymized by taking out exact dates and only providing the month the order was placed in. Customer names and numbers, as well as products name and group, are fully encoded and shared only as continuous figures. In conclusion, demonstrator carried out by Infineon concerns only non-personal data.
Such analysis on the data processed should also be carried out by the entities that will be using the SAFE-DEED platform capabilities in the deployment stage when the project will be

over. The listing and classification of datasets, to be preliminary activities in the context of processing data, facilitate the entities processing data concerning the applicable legal framework. Thus, every single dataset must be qualified according to the nature of data it embeds (personal data or non-personal data).

6 Relevant EU Framework Applicable to WP7

6.1 European Commission Communication "Building a European Data Economy"

D3.1 provides an in-depth analysis of the European Commission Communication on "Building a European Data Economy"[2]. The EC Communication focuses on the development of the EU data economy. Thus, this Communication should be considered as one of the legislative cornerstones of the Safe-DEED project, since it directly points at the project's general goals. In the Communication, the EC not only provides crucial definitions (e.g. the definition of data market place) but also sets the legislative agenda for the legally binding initiatives that have been taken in the context of the EU data economy. In particular, one of the most important legislative initiatives for this project is the Regulation on free-flow of non-personal data.[3] The Communication and the Regulation on free-flow of non-personal data aim at paving the way for the enhancement of cooperation between different actors involved in the data market place increasing the economic opportunities for the actors involved.

Even though the Communication is not legally binding, it is essential to highlight the definition of a data market place as a 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'*.[4] Based on the provided definition, it is possible to affirm that the Safe-DED enabling technologies for platforms falls into the scope of Communication and, therefore, the legal provisions specified in the Communication and involving the processing of non-personal data should be considered as a building block of the Safe-DEED legal architecture.

Together with the data marketplace definition, the EC Communication recognises four barriers to data mobility within the EU market:

- Data localisation restrictions put in place by Member States' public authorities that does not allow certain data to leave the country;
- Obstacles put in place by IT systems' vendors;

2 "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 04/02/2020.

3 *Ibid.*

4 *Ibid.*

- Complex EU legal patchwork that leads to legal uncertainty;
- Lack of trust due to security risks and concerns about the cross-border availability of data for regulatory purposes.

The removal of the legal obstacles is not only considered as a prerequisite for enhancing the economy, but also for boosting innovation in this area. On the one hand, some of these barriers, such as the one on localisation restriction, have been addressed by the EU legislator in the Regulation on free-flow of non-personal data. Others, such as the one tackling security risks, might be fulfilled through the correct implementation of key legislative initiatives, such as the EU Privacy and Data Protection framework. On the other hand, the removal of the additional barriers coming from Member States restrictions and listed by the EC is a task that should be carried out by the legislator at EU and, in the implementation phase, also by Member States in order to facilitate free flow of data.

6.2 Free Flow of Non-Personal Data Regulation

To achieve the ambitious goals set in the EC Communication "Building a European Data Economy", the EC published a legislative proposal for a Free Flow of Non-Personal Regulation in 2017. Following the ordinary legislative process, the new Regulation entered into force at the end of December 2018 and is applicable since May 2019. The Free Flow of Non-Personal Regulation (FFNPDR) data aims to remove existing barriers to data that have been put in place at a national level.

A non-exhaustive list of what could constitute non-personal data is provided in Rec. 9 FFNPDR. In particular, it could be considered as non-personal data those personal data that have been fully anonymized and those resulting from industrial production processes. In addition, specific example of non-personal data might include (1) aggregated and anonymised datasets used for big data analytics; (2) data on precision farming that can help to monitor and optimise the use of pesticides and water; or (3) data on maintenance needs for industrial machines.[5] In principle, non-personal data could be any *data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679.*[6]

6.2.1 Scope of Application and General Principles

The FFNPDR applies to those entities that deal with the processing of non-personal data. In particular, it refers to (a) service providers offering their services to users residing or having an establishment in the Union, regardless of where the service provider is located; (b) carried out by a natural or legal person living or having an establishment in the Union for its own needs.[7]

The services offered by the Safe-DEED enabling technologies for platform as a whole should be considered within the scope of application of the FFNPDR. Therefore, compliance with the

5 Rec. 9 FFNPDR.

6 Art. 3(1) FFNPDR.

7 Art. 2(1) FFNPDR.

FFNPDR provisions should be considered not only by those entities involved in WP7 activities but by all members of the Safe-DEED consortium.

The FFNPDR stresses its complementarity with the GDPR. In particular, Rec. 10 FFNPDR highlights the interaction between the two Regulations and confirms their shared goal of providing a coherent set of rules that aims to enhance the free movement of different type of data. As a result of the interaction between the FFNPDR and GDPR, crucial provisions of the recent initiative mirror the ones provided for the same activity by the GDPR (Art. 3(1) FFNPDR). Another example of the complementarity is provided by Rec. 10 FFNPDR. Similarly to the GDPR (Art. 23), Rec. 10 FFNPDR prohibits the Member States to put in place measures that limit or prohibit the free movement of non-personal data within the Union in the absence of public security reasons.[8]

Art. 2(2) FFNPDR clarifies that when a set of data includes personal and non-personal data, the FFNPDR will only apply to non-personal data. However, when personal data is processed the GDPR and ePrivacy Directive apply. If this differentiation is impossible, the FFNPDR should not prejudice the application of the GDPR nor impose an obligation to store the different data separately.[9]

To remove the barriers that have been hampering the free movement of non-personal data, the FFNPDR identifies three main actions that have to be fulfilled by Member States and end-users: (1) prohibition of mandatory data localisation requirements; (2) guarantee of data availability for competent authorities; and (3) facilitation of data porting by users. While the first action (prohibition of compulsory data localisation requirements) has to be fulfilled at a national level by competent regulatory bodies, the other two activities have to be ensured by those private entities that fall within the scope of application of the FFNPDR.

6.2.1.1 Guarantee of data availability for competent authorities

Art. 5 FFNPDR foresees measures that will facilitate the cross-border access to non-personal data by public authorities. In particular, the FFNPDR stresses that the measures to enhance the exchange of 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'*.[10] Consequently, *'access to data by competent authorities may not be refused on the basis that the data are processed in another Member State'*. The same article foresees a procedure to enforce the access request through sanctions if the service provider does not comply with such requests.

8 Rec. 10 FFNPDR: *"Under Regulation (EU) 2016/679, Member States may neither restrict nor prohibit the free movement of personal data within the Union for reasons connected with the protection of natural persons with regard to the processing of personal data. This Regulation establishes the same principle of free movement within the Union for non-personal data except when a restriction or a prohibition is justified by public security reasons. Regulation (EU) 2016/679 and this Regulation provide a coherent set of rules that cater for free movement of different types of data. Furthermore, this Regulation does not impose an obligation to store the different types of data separately".*

9 Art. 2(2) FFNPDR.

10 Art. 5 FFNPDR.

According to Art. 3(1) FFNPDR, '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'*. Unfortunately, no clarifications are provided regarding these authorities, leaving each Member State with the possibility to assess which bodies are entitled to request such data from service providers.

6.2.1.2 Porting of data

Mirroring the GDPR approach, Rec. 29 FFNPDR stresses the importance of removing commercial practices that do not facilitate data porting for enhancing trust in all stakeholders, and transparency in the process. Therefore, Art. 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. Safe-DEED partners should develop a code of conduct covering all aspects listed in Art. 6 FFNPDR.[11] [12]

6.3 Data Usage Agreements and Competition Law in the Context of a Closed (Safe-DEED) Project

In this section, we review the main (potentially) relevant competition law concerns related to the Safe-DEED project and data usage agreements. Safe-DEED partners may consider entering in the near future with those entities that might be interested in using the technologies developed within the project. Those concerns were initially specified in D3.1 and will be briefly revisited and elaborated upon in Section 6.3.1 of the current report. Considering that competition law assessment generally relies on a case-by-case analysis and depends on various circumstances and factors, it is not feasible at the moment to assess whether future practices established by the Safe-DEED partners will be in line with EU competition law and will not raise the attention of relevant competition authorities. Several factors may play a role is diverse and includes, in particular, the type of data shared, the form of the arrangement and the market position of the parties involved in sharing. Some of those factors, especially the market definition and the assessment of the market share, require complex economic analysis which cannot be conducted within the framework of this study.

Instead, our objective is to provide an overview of the (potentially) relevant legal aspects of data sharing in a B2B context that should be considered by the partners when setting up their data usage agreements (Section 6.3.2). The suggested considerations are, in principle viewed as pro-competitive as highlighted by the European Commission in their Staff Working Document 'Guidance on sharing private sector data in the European data economy'.[13] It must be stressed that the European Commission specifies in this document that '*it does not bind the*

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

12 For further explanation about key elements that should be taken into account when drafting a code of conduct please have a look to section seven, Table 1.

13 Commission Staff Working Document – Guidance on sharing the private sector data in the European data economy. (COM (2018) 232 final).

Commission as regards the application of the EU law, in particular with regard to the competition rules in Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU)'.[14] Thus, the Safe-DEED partners should view the (contractual) considerations identified in Section 6.3.2 as suggestions or good practices and not as a legal advice that guarantees that no competition law-related concerns may arise in the future.

6.3.1 Introduction: B2B Data Sharing and (Potentially) Relevant Competition Law Concerns

6.3.1.1 B2B Data Sharing

Prior to conducting the legal analysis, it is essential to identify the relevant terminology and concepts. The accurate terminology and concepts will ensure that the provided analysis is concrete and tailored to the type of data sharing conducted within the Safe-DEED platform.

Safe-DEED is a B2B data-sharing platform. The supply and (re-)use of data in the B2B context can be done in various forms. In the Staff Working Document 'Guidance on sharing private sector data in the European data economy' three main models of B2B data sharing are identified, namely (1) an open data approach; (2) data monetization on a data marketplace; and (3) data exchange in a closed platform.[15]

Open data approach – Under this data-sharing model, the data is made available to the broad number of (re-)users by the data supplier. The approach is considered 'open' since the data supplier sets a very limited amount of restrictions for potential (re-)users to obtain access to the shared data. Furthermore, the access to data is granted for free or for a very limited remuneration. The Safe-DEED platform cannot be classified as 'open' since, at this stage, the 'open' access to data is not envisioned.

Data monetization on a data marketplace – According to this data-sharing model, data monetization occurs through '*a data marketplace as an intermediary on the basis of bilateral contracts against remuneration*'.[16] This model may be of interest to stakeholders which do not aspire to engage in data sharing themselves but would be interested to generate additional profits by 'outsourcing' the task to a data marketplace as an intermediary. The data supplier authorises the marketplace to license their data on their behalf following defined (FRAND) terms and conditions.[17] Thus, the data is generally accessible to interested parties on a bilateral basis at standard conditions. At this stage, the Safe-DEED partners do not follow this model since they do not intend to place their data on a data marketplace.

Data exchange in a closed platform – The third model refers to the data exchange method which occurs in a closed data marketplace. Such closed platforms can be set up, for instance,

14 COM (2018) 232, p. 2.

15 COM (2018) 232, p. 5.

16 *Ibid.*

17 Deichmann, J. et al. (2016) "Creating a successful Internet of Things data marketplace" https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/creating-a-successful-internet-of-things-data-marketplace, accessed 04/05/2020 .

by data suppliers or an independent intermediary. In this case, the data suppliers and/or independent intermediary specify the terms and conditions according to which the data can be shared with third parties. The data sharing may be provided for financial remuneration or as an added-value service.[18] The terms and conditions may be standard or may differ depending on the negotiated contractual terms between the data suppliers and/or an independent intermediary and the interested third party. Based on the provided information from the Safe-DEED partners, it can be concluded that the Safe-DEED platform aims to operate in accordance with this closed platform model.

Thus, the Safe-DEED platform can be classified as a B2B closed platform. As explained in D3.1, the closed platform may, in principle, present a higher number of competition law concerns due to the more restricted nature of data sharing than the other two models. Clearly, in comparison to an open platform or a data marketplace where the terms and conditions of getting access to data are defined and are in general identical for all interested parties, closed platforms may be more restrictive depending on the terms and conditions of data sharing selected by data suppliers or their independent intermediaries. In particular, the Staff Working Document 'Guidance on sharing private sector data in the European data economy' explicitly mentions that when data sharing within closed platforms is conducted on an exclusive basis, it needs to comply with the competition law rules, in particular Arts. 101 and 102 of the TFEU.[19]

6.3.1.2 (Potentially) Relevant Competition Law Concerns

In D3.1 an extensive overview of revenant competition law concerns has been provided. In D3.3 we revisit the main competition law considerations which are relevant for the B2B closed Safe-DEED platform and elaborate upon them.

General – As it was explained in D3.1 the goal of competition law is to establish and protect '*a system ensuring that competition is not distorted*'.[20] Competition on the market is protected as means of enhancing consumer welfare and ensuring an efficient resources allocation. In order to assess the degree of competitiveness between undertakings on a market, one needs to first define that market and then assess the market power of a particular undertaking on that defined market. Generally, the market power is determined based on the market shares held by an undertaking at stake on a specific market.[21] The market definition and the assessment of the market power on the defined market, especially in the digital market, is a very complicated matter that requires economic analysis. The definition of the market may significantly affect the outcome of whether a certain undertaking is dominant in a specific market or not. In particular, the narrower the market is defined, the higher is the likelihood that a certain undertaking may be considered dominant.

Competition law and online platforms - The European Commission acknowledges the importance of online platforms for the digital market and specifies, in particular, that '*online*

18 COM (2018) 232, p. 5.

19 *Id*., p. 5.

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

21 For more detailed information see D3.1, Section 5.1.

platforms are key enablers of digital trade'.[22] However, '*there might be room in the market for only a limited number of platforms*'[23], which may raise competition law concerns. According to the European Commission '*it is essential to protect competition "for" the market* and '*to protect competition on a dominant platform*'.[24]

Dominant platforms play a form of regulatory role and, thus, they '*have a responsibility to ensure that their rules do not impede free, undistorted, and vigorous competition without objective justification*'.[25] Non-dominant platforms also play a regulatory role but, according to the European Commission, it is far-reaching to impose conduct rules on all platforms, regardless of their market power, since many types of conducts may have pro-competitive effects.[26] Thus, the European Commission is primarily concerned with the effects on competition on the market of types of conducts exercised by dominant platforms.

At this stage, it is outside of our competences to assess whether the Safe-DEED platform is a dominant player in the market. Nonetheless, we provide some relevant observations vis-a-vis Arts. 101 and 102 of the TFEU[27] that Safe-DEED partners should consider in their practices and when drafting underlying agreements.

Article 101 TFEU – Art. 101(1) prohibits parties from engaging in agreements that have '*as their object or effect the prevention, restriction or distorting of competition within the internal market*'. Such agreements are automatically void according to Art. 101(2) of the TFEU. However, Art. 101(3) of the TFEU suggests that the prohibition specified in Art. 101(1) may be declared inapplicable when agreements between undertakings 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. In the past, stakeholders were obliged to notify their agreements to the European Commission. However, that notification requirement no longer exists, and parties currently need to do a self-assessment. Nonetheless, further guidance is provided to stakeholders that will help them evaluate whether their agreements may be potentially anti-competitive.[28] In D3.1 it has been concluded that the activities included in the Safe-DEED project would unlikely lead to establishment of vertical

22 European Commission (2018) "Proposal for a regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services", COM/2018/238 final < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018PC0238&from=EN>, accessed 04/05/2020.

23 European Commission (2019) "Competition policy for the digital era" , p. 5, available at https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf, accessed 04/05/2020 .

24 European Commission (2019) "Competition policy for the digital era" , p. 5 https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

25 *Id.* , p. 6.

26 *Ibid.*

27 Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390, available at < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN>, accessed 05/02/2020

28 For instance, 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.* For more information see D3.1, Section 5.2.

agreements. For this reason, in this Section we only focus on horizontal co-operation agreements.

Market definition and market power under Art. 101 TFEU – When assessing the market power in the framework of horizontal co-operation agreements under Art. 101 TFEU, the combined market share of the parties to such an agreement is assessed. If the parties have a low combined market share, the horizontal co-operation agreement is unlikely to give rise to restrictive effects on competition in the market within the meaning of Art. 101(1). If a combined market share is low, normally, the agreements are not considered anti-competitive. The definition of the 'low combined market share' depends on the type of agreement. In particular, the 'safe harbor' thresholds may differ depending on the agreement concluded between parties. Furthermore, the threshold often differs depend on whether the parties to an agreement are (potential) competitors or not. For instance, in the Commission Notice on agreements of minor importance which do not appreciably restrict competition under Art. 81(1) of the Treaty establishing the European Community ('the *De Minimis* Notice') it is specified[29,30] :

> '*The Commission holds the view that agreements between undertakings which may affect trade between Member States and which may have as their effect the prevention, restriction or distortion of competition within the internal market, do not appreciably restrict competition within the meaning of Article 101(1) of the Treaty:*
>
> *(a) if the aggregate market share held by the parties to the agreement* ***does not exceed 10 % on any of the relevant markets affected by the agreement****, where the agreement is made between undertakings which* ***are actual or potential competitors*** *on any of those markets (agreements between competitors); or*
>
> *(b) if the market share held by each of the parties to the agreement* ***does not exceed 15 % on any of the relevant markets affected by the agreement****, where the agreement is made between undertakings which* ***are not actual or potential competitors*** *on any of those markets (agreements between non-competitors).*'

Thus, Safe-DEED partners, when engaging in horizontal co-operation agreements, should consider (1) the combined market share; (2) the type of actor they intend to cooperate with. If Safe-DEED partners establish a horizontal co-operation agreement with a (potential) competitor and their combined market share is below 10%, there is in principle no need to be concerned about the horizontal agreement being considered anti-competitive under Art. 101 TFEU. Similarly, if Safe-DEED partners establish a horizontal co-operation agreement with a non-competitor and their combined market share is below 15%, the agreement should also not be considered anti-competitive.

29 OJ C 368, 22.12.2001, p. 13.

30 Other more type of an agreement-specific thresholds are indicated in various Block Exemption Regulations, e.g. the Commission Regulation (EU) No 316/2014 of 21 March 2014 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of technology transfer agreements, *OJ L 93, 28.3.2014, p. 17–23.*

Potential anti-competitive practices under Art. 101 TFEU – As was indicated in D3.1 there are three major competition concerns that may arise from horizontal co-operation agreements under Art. 101 TFEU:

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

Furthermore, according to the Commission guidelines on the applicability of Art. 101 TFEU to horizontal co-operation agreements, there is a general assumption that cooperations between various stakeholders are pro-competitive, unless they lead to:

(1) Reduction in price competition;
(2) Hinderance of emergence of innovative technologies;
(3) Exclusion of, or discrimination against, certain companies by preventing their effective access to the technology (which can include data).[31]

In the framework of the digital economy, one of the potentially anti-competitive practices that comes to mind is creation of oligopolies between competing platforms (market leaders) with high market power by concluding various types of horizontal cooperation agreements. Matching platforms could enable a collusive outcome on the market. Furthermore, the cooperation between competing stakeholders in a particular platform can also lead to exclusion, for instance, of other actors not involves in the platform, or lock-in. Furthermore, it is essential to consider which type of data is exchanged between competitors. The exchange of strategic data (e.g. individualized data, younger data) is much more likely to be anti-competitive under Art. 101 TFEU than the exchange of other type of data (e.g. aggregated data, older data).

Thus, the Safe-DEED partners should ensure that they do not conclude agreements with competing platforms which may potentially distort competition by excluding other actors and preventing them from accessing the data, especially if the data is strategic. If such agreements cannot be avoided, the Safe-DEED partners should carefully consider whether the conducted agreements are in line with competition law and assess whether they could benefit from the 'safe harbor' exceptions. In Section 6.3.2. we provide additional recommendations for closed B2B platforms, such as the one of the Safe-DEED project, that could help avoiding establishment of anti-competitive practices.

Article 102 TFEU – Art. 102 prohibits partners from abusing their dominant position. However, the existence of a dominant position needs to be assessed very carefully by evaluating the relevant market and the position of the stakeholder concerned. The actual definition of the market is often quite controversial, in particular for very innovative, new markets. Nonetheless, in case a competition authority defines the market rather narrowly, dominance may be established.[32] Thus, stakeholders with a (potentially) high market power

31 D 3.1, p. 49.

32 For more information, see D3.1, Section 5.1.3. and 5.2.

need to be aware that the conditions that they pursue their agreements with third parties and their conduct vis-à-vis third parties may also be restricted by Art. 102 TFEU.

In sum, the essential questions under Art. 102 TFEU are whether an undertaking at stake has a dominant position and whether the undertaking abuses its dominant position. The dominant position per se is not considered anti-competitive, only the abuse of such position.

Market power under Art. 102 TFEU – According to the 'Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings', '*the assessment of whether an undertaking is in a dominant position and of the degree of market power it holds is a first step in the application of Article 82 [Article 102]. According to the case-law, holding a dominant position confers a special responsibility on the undertaking concerned, the scope of which must be considered in the light of the specific circumstances of each case*'.[33] The dominance is not likely if the undertaking's market share is **below 40 % in the relevant market**.[34]

Thus, Safe-DEED partners should estimate whether their market share in the relevant market is below 40% to approximate whether they could potentially have a dominant position.[35] If the market share is close to 40% or higher, they should be extremely careful in their activities to ensure that their actions and established agreements are not considered abusive.

Forms of abuse under Art. 102 TFEU – As it was mentioned above dominant platforms are seen as regulators and, thus, they have a responsibility to ensure that competition on their platforms is fair, unbiased and pro-users. In general, there are multiple forms of abuse that can take place under Art. 102 TFEU.[36] The forms of abuse can be market specific. For instance, as described in D3.1 four main theories of harm related to data sharing has been identified:

(1) Refusal to share;

33 Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings *OJ C 45, 24.2.2009, p. 7–20*.

34 Rec. 14 of the Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings *OJ C 45, 24.2.2009, p. 7–20*. It must be noted that '*there may be specific cases below that threshold where competitors are not in a position to constrain effectively the conduct of a dominant undertaking, for example where they face serious capacity limitations. Such cases may also deserve attention on the part of the Commission*.'

35 Aleksandra Kuczerawy, Amandine Léonard, Alessandro Bruni, Safe-DEED D3.1: *'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 amarket 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 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'*. For more details on the definition of relevant market see D3.1, p.45-46

36 For more detailed information Section IV of the Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings *OJ C 45, 24.2.2009*.

(2) Abusive discrimination;
(3) Leveraging of customer data;
(4) Exploitation by unlawful processing or unfair term.[37]

If Safe-DEED partners could be considered a dominant player in the relevant market, it is essential to ensure that they do not foreclose access to the (especially strategic) data exchange in the relevant market to interested third parties.[38] The refusal to grant access to data by a dominant undertaking may be considered an abusive practice under Art. 102 TFEU.[39] Thorough analysis though will be required to assess whether such access is truly indispensable.[40]

6.3.2 Data Usage Agreements: Main Principles and Legal Considerations

In this Section we provide specific considerations and recommendations for Safe-DEED partners which they should follow when setting up their data usage agreements for the deployment phase. Whereas it is not possible to conclude with certainty which practices may be considered anti-competitive in the future, the provided considerations and recommendations should lower the risk of anti-competitive and/or abusive practices under Arts. 101 and 102 TFEU. To our knowledge, the Safe-DEED partners only aim at establishing data usage agreements with third parties during the deployment phase, for this reason, we focus only on this type of agreement.

In Section 6.3.2.1, we elaborate upon general guiding principles for agreements conducted within B2B data sharing platforms. In Section 6.3.2.2, we provide an overview of important legal aspects of data sharing through data usage agreements. The analysis is based on the Staff Working Document 'Guidance on sharing private sector data in the European data economy' introduced earlier.

6.3.2.1 General Guiding Principles for Agreements within B2B Data Sharing Platforms

The Staff Working Document specifies five main principles to be considered by B2B data sharing platforms when establishing agreements with third parties, namely (1) transparency; (2) shared value creation; (3) respect for each other's commercial interests; (4) ensure undistorted competition; and (5) minimized data lock-in. Following these principles is essential to ensure fair markets for IoT objects and for products and services relying on data created by such objects.[41] Safe-DEED partners should preferably abide by these general principles when negotiating their data usage agreements with third parties.

37 For more detailed information on data market and see D3.1, p. 52.

38 For more details on the definition of relevant market see D3.1, p.45-46

39 To date, however, there is no relevant case law on the matter, which limits our analysis.

40 European Commission (2019) "Competition policy for the digital era" , p. 9 https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf, accessed 04/05/2020 . Furthermore, '*it is necessary to distinguish between different forms of data, levels of data access, and data uses. In a number of settings, data access will not be indispensable to compete, and public authorities should then refrain from intervention*'.

41 COM (2018) 232, p. 3.

Transparency – It is suggested that the relevant contractual arrangements (including data usage agreements) should be transparent. In particular, the contractual clauses should specify in a transparent and clear manner *'(i) the persons or entities that will have access to the data that the product or service generates, the type of such data, and at which level of detail; and (ii) the purpose of using such data*'.[42]

Shared value creation – It is essential to contractually recognize the co-creation of data where data is generated as a by-product of using a product or service.

Respect for each other's commercial interests – The contractual arrangements should protect the commercial interests as well as trade secrets of data holders and data users.

Ensure undistorted competition – The contractual arrangements should not distort competition and be in line with Arts. 101 and 102 TFEU, as explained above in detail, especially when exchanging sensitive and/or strategic data.

Minimized data lock-in – Stakeholders offering a product or service that generates data as a by-product should allow or enable data portability to the highest possible extent.[43]

6.3.2.2 Legal Considerations for Contractual Arrangements Within B2B Closed Platforms

B2B data sharing is generally done on a contractual basis. It can either be done based on standard (FRAND) agreements or based on agreements that are negotiated separately on a bilateral basis with each interested party. As it was pointed out above, the standard agreements are more transparent and less restrictive since they give third parties the possibility to have access to the data at stake on similar terms and conditions. Safe-DEED peers should consider whether they intend to follow the more 'open' or 'closed' approach when negotiating their data usage agreements. The preference for a certain procedure may be influenced by competition law considerations, especially if the Safe-DEED partners could be considered dominant.

Furthermore, Safe-DEED peers should consider who will be responsible for executing this task. Namely, it is essential to establish a party who will be responsible for negotiating and establishing data usage agreements with third parties. It could be one of the peers or both. However, to ensure that data usage agreements scope is aligned and does not significantly differ, it may be useful to appoint a separate (independent) body within the platform which will be responsible for monitoring the process of data exchange, managing the platform access and commercialising the data.

The principle of contractual freedom generally governs contractual arrangements. This freedom, however, may be limited by mandatory legislative provisions, such as contract law provisions, GDPR or competition law restrictions. Mandatory provisions cannot be contractually modified and have to be followed by the parties in their contractual arrangements. The (non-exhaustive) list of legal considerations that Safe-DEED peers should follow when preparing and/or negotiating data usage agreements are indicated in Section 7.1.

42 *Ibid.*

43 *Ibid.*

7 Specific Legal Requirements for the Safe-DEED processing activities involving non-personal data

Deliverable D3.3 differentiates between general requirements that are applicable to all Safe-DEED partners and those to be only considered by partners involved in the trials lead by Infineon in WP7.
In the tables below (Tables 1-2), tasks that have to be taken into account by all Safe-DEED partners are listed.

Table 1 Code of conduct

GENERAL TASK	TO DO	DESCRIPTION	LEGAL BASIS
Code of Conduct	Draft of a Code of Conduct	To develop a self-regulatory code of conduct that each party has to comply with. Such code should aim to establish a competitive data economy environment within the platform, based on the principles of transparency and interoperability and taking due account of open standards	• Art. 6 FFNPDR
The FFNPR specifies the aspects that such code should cover: *'(a) best practices procedures for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format; (b) minimum information requirements to ensure that professional users are provided, before a contract for data processing is concluded, with sufficiently detailed, clear and transparent information regarding the processes activities, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another service provider or port data back to its own IT systems; (c) approaches to certification schemes that facilitate the comparison of data processing products and services for professional users, taking into account established national or international norms, to facilitate the comparability of those products and services. (d) communication roadmaps taking a multi-disciplinary approach to raise awareness of the code of conduct among relevant stakeholders.'*			
In the Safe-DEED deployment phase, a Code of Conduct should be drafted and signed. In particular, the Code of Conduct should include: (a) *best practices*, which have to be agreed and developed by the platform parties. Regarding point (c), *approaches to certification schemes that facilitate the comparison of data processing products and services for professional users*, partners should specify which are the requirements that should be met with regard to the quality, security, business continuity and environmental aspects of the platform. In addition to the aspects covered by the FFNPR, additional requirements, listed in Table 3 should be also taken into account by Safe-DEED partners in the deployment phase.			

Table 2 Availability of data

GENERAL TASK	TO DO	DESCRIPTION	LEGAL BASIS
Availability for competent authorities	Make data available to competent authorities upon request	Provide relevant authorities with the requested data for the performance of their duties	• Art. 5 FFNPDR • Art. 6 FFNPDR
Art. 5 FFNPDR foresees the possibility for a competent authority, solely or in cooperation with one or more counterparts of other Member States, to request or obtain data from those entities that have such data.			
In the Safe-DEED platform, data will remain stored in the premises of the parties that are using Safe-DEED platform functionalities for extracting data value. Therefore, each partner will be obliged to comply with the requests coming from competent bodies. Such bodies might be the ones of the state where the partner is located or a competent authority from other states if the addressee of the order did not fulfil the initial request.			

7.1 Specific Legal Requirements for the Deployment Stage

The Safe-DEED project aims to develop enabling technologies for platforms. Considering the potential benefit these technologies might have in the market, specific attention has been paid in this section to the crucial elements that should be included in the data usage agreement that will be concluded by those entities that would like to take advantages from the deployed technologies. About the data usage agreement, the listed requirements should be taken into account by partners that intent to use Safe-DEED technologies. The data usage agreement can be developed taking into account different criteria and requirements according to the nature and the scope of the platform that partners want to build.

Table 3: Legal Aspects of Data Usage Agreements[44]

GENERAL TASK	TO DO	DESCRIPTION	PARTIES INVOLVED
Preparation of data usage agreement	To develop rules that have to be followed by those entities that intend to use Safe-DEED project functionalities	Prepare the draft of the agreement that complies with guiding principles and consider competition law restrictions	Safe-DEED partners involved in WP6 and WP7
The data usage agreement has to include the following aspects (not exhaustive): (1) Data availability (2) Data access (3) Re-use of data (4) Technical means for data access and exchange (5) Security measures (6) Liability (7) Parties' rights (8) Duration and termination of the contract (9) Dispute resolution			
Task 1: Data availability – The contractual arrangement has to clearly describe which data is shared (e.g. customer data, diagnostic data). Furthermore, the quality of the data that is provided under the agreement at the moment of contractual negotiations and over time needs to be stated. In particular, one needs to specify whether the data will be updated and how often. The source/origin of data needs to be mentioned and how that data was collected or constructed. It has to be contractually clarified whether the provided data is a data set or a data stream. It is essential to ensure that rights of thirds parties to the data in question are respected and there are no legal obligations that may prevent the data access and exchange. Furthermore, the data protection legislation needs to be carefully consulted. Among other legislative provisions, the shared data has to be in line with the GDPR provisions, as			

44 Based on COM (2018) 232, p. 7.

described in D 3.2.

Task 2: Data access – The contractual clauses have to clearly specify in a transparent, clear and understandable manner who has a right to access, right to (re-)use and distribute data and under which conditions. The conditions for data re-use and distribution have to be specified (see also Task 3). The right to access and (re-)use of data can be limited. For instance, it can be limited to a certain group or certain purposes of data use.

Task 3: Re-use of data – Contractual clauses should clearly specify what the (re-)user is allowed to do with the acquired data. Concrete contractual clauses on data (re-)use will ensure transparency and increase the trust between the parties. The terms of data usage (the exact usage that can be made of the data) have to be specified as clear and concrete as possible, including the rights on derivatives of the data. If the receiving party does not follow the agreed upon terms of data (re-)use it may lead to a breach of contractual obligations and give the data supplier clear means to start a lawsuit, unless the parties resolve the conflict amicably.

Task 4: Technical means for data access and exchange – The necessary IT security mechanisms should be in place to ensure that data can be accessed and exchanged efficiently. For this reason, the Safe-DEED partners should consider establishing a separate (independent) body that would be responsible for monitoring the data access and exchange processes.

Task 5: Security measures – Contractual parties should ensure that the shared data is protected from any foreseen and unforeseen circumstances, including theft, misuse, technical problem and human error. Failure to provide the necessary level of security measures may lead to liability concerns. Furthermore, if parties exchange trade secrets under the contractual obligations, it is essential that all parties install the necessary secrecy mechanisms to ensure that the trade secret protection is secured.

Tasks 6: Liability – In the context of data usage agreements, parties may include a clause on liability provisions for supplying erroneous data. If the requested data is not provided or it is not up to negotiated standards the receiving party (client) may request the Safe-DEED partners to pay damages. This clause may be considered important by the clients of the Safe-DEED platform since they may want to ensure that the data that is provided to them is of high (agreed upon) quality.

Task 7: Parties' rights – In general, the scope of parties' rights and obligations should be clearly specified in the contract. If one of the obligations are not met by one of the parties it may give rise to a breach of contractual obligations and lead to a lawsuit, unless parties manage to amicably resolve the dispute.

Task 8: Duration and termination of the contract – Parties to an agreement have to specify for how long the negotiated contractual obligations last and under which conditions the contract can be renewed. It is also important to specify under which conditions and

circumstances can a contract be terminated prior to the termination date.

Task 9: (Alternative) dispute resolution – It is important to specify in a separate contractual clause, which law is applicable to the contract. The contract at stake will be governed by the selected applicable law. Furthermore, the parties should specify which dispute resolution mechanism is selected in case a conflict arises. The parties have several choices. First, the parties may decide to litigate in court. In this case, the jurisdiction has to be specified, to ensure that parties are aware in which country the dispute will be litigated. Second, instead of following the tradition litigation route, parties may decide to use the alternative dispute resolution (ADR) mechanisms, e.g. mediation and/or arbitration. The alternative mechanisms may be combined. For instance, one may first try to resolve a dispute through mediation and if the mediation process was unsuccessful turn to arbitration. To ensure that the selection of the ADR institutions is efficient, parties may in advance specify which institution should facilitate the conflict resolution process. There are multiple ADR centers: national, regional, international. One of the renown ADR centers is the ICC.

8 Upcoming EU Policy Actions

The new European Commission President Ursula von der Leyen has recently presented its five-year policy program (2019-2024) to the European Parliament.[45] The working programme puts forward the number of areas on which the new Commission will focus its political and legislative efforts. In the context of the Safe-DEED project, it is useful to concentrate on two identified action points, namely, '*A European Green Deal'* and *A 'Europe fit for the digital age'*.[46]

'A European Green Deal' is a horizontal action point that is to be applied to all sectors which aim at reducing carbon emission reaching in 2050 carbon neutrality. To reach those goals different legislative initiatives will have to be introduced. In the context of Safe-DEED, the future legislative initiatives might have an impact on the selected practices of some of Safe-DEED partners. In particular, partners, which manage or own data centers, may be forced to reduce the emissions such data-hubs currently produce, in case the rules become stricter. On the other hand, the Commission plans to make the EU area the leader in the circular economy and clean technologies. The activities and functionalities developed in the context of the Safe-DEED project will be crucial to support this plan. '*A Europe fit for the Digital Age*' is a sector-specific action point that aims to increase opportunities for EU citizens and companies within safe and ethical boundaries. In particular, the European Commission recognizes the value and opportunities linked to data. The data is considered an essential ingredient to societal challenges, from health to farming, from security to manufacturing. President Ursula von der Leyen explains that '*in order to release that potential we have to find our European way, balancing the flow and wide use of data while preserving high privacy, security, safety and ethical standards.*'[47] We can expect that one of the first legislative initiatives will be a new proposal on privacy and confidentiality in the electronic communication sector (ePrivacy Regulation). The ePrivacy Regulation proposal should have a direct impact on Safe-DEED partners and, in particular, on the set up of platform activities since they will have to run on publicly available electronic communication networks.

Some Member States have already started working on similar legislative initiatives. In particular, the new Austrian government have unveiled an ambitious plan that partially overlaps with the one displayed by the new President of the European Commission.[48] In particular, the government's plan intends to boost innovation through transparency and access to scientific data. The government aims to increase transparency and accessibility of the scientific data by establishing the "Austrian Micro Data Center".

45 President of the European Commission Ursula von der Leyen, *A Union that strives for more: My agenda for Europe*, available at https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf, accessed 15/01/2020

46 Ibid, p.5

47 Ibid, p.13

48 Digitale und soziale Transformation Ausgewählte Digitalisierungs-vorhaben an öffentlichen Universitäten 2020 bis 2024, available at <https://pubshop.bmbwf.gv.at/index.php?rex_media_type=pubshop_download&rex_media_file=digital_uni.pdf>, accessed 05/02/2020

9 Conclusion

Deliverable D3.3 is the third deliverable of the Safe-DEED project that provides legal analysis. D3.2 and D3.3 jointly provide a comprehensive list of essential legal requirements relevant for the Safe-DEED project. Deliverable D3.3 also focuses not only on IT-related aspects but also on the relevant EU legislation (e.g. relevant EU competition law provisions), essential fields for the ICT sector. Furthermore, it describes *ad hoc* requirements resulting from the recently approved Free-Flow of Non-Personal Data Regulation.

The first part of the deliverable D3.3 provides an overview of main legislative initiatives that touch upon the processing of non-personal data. In the second section D3.3 suggests a list of concrete actions that should be taken into account by Safe-DEED partners, especially for those involved in the development of the trials in WP7. In particular, D3.3 reviews relevant legal provisions of EU competition law and provides a list of good practices for negotiation data usage agreements, relevant for the deployment phase of the project. Besides, the deliverable includes a summary of the future policy goals of the newly appointed Commission. The action points described by the President of the Commission, such as the ones described in the 'A Europe fit for the digital age' section of her working programme, might become concrete legal requirements in the forthcoming EU legislative initiatives. As a result, upcoming legislatives might affect actions of the Safe-DEED partners.

It has to be considered that compliance with legal requirements is an on-going process. Thus, the continuous collaboration between KU Leuven and Safe-DEED partners during the development of the different use cases will have a beneficial effect on the project outcomes.

10 Annex to D3.2 and D3.3

To facilitate the understanding of the main legal and ethical requirements provided in D3.2 and D3.3 this Annex provides a summary of all the relevant legal frameworks as well as the actions that are necessary to be fulfilled by Safe-DEED partners to comply with the identified requirements. The development of the annexes considers not only the Safe-DEED project demonstrator stage, but also the deployment one where the technologies and functionalities developed within the project will be used by entities that are not part of the project.

MATERIAL SCOPE	TYPE OF REQUIREMENT	TASK	LEGAL BASIS	TO DO	STAGE
PERSONAL DATA	**LEGAL AND ETHICAL**	Comply with the transparency and accuracy principles	• Art. 13-22 GDPR	Draft Privacy policy to provide all necessary information to the data subject so that they can exercise their rights	• DEMONSTRATOR • DEPLOYMENT
			• Art. 12 GDPR • Art. 15-22 GDPR	Provide a form for data subjects to exercise their rights	• DEMONSTRATOR • DEPLOYMENT
			• Art. 30 GDPR	Keep a record of processing activities	• DEMONSTRATOR
			• Art. 28(3) GDPR	Draft a controller/processor agreement to define roles, tasks and responsibilities	• DEPLOYMENT
			• Art. 4(8) GDPR • Art. 28(1) GDPR	Ensure that the processors (if any) have implemented adequate measures to ensure compliance with the GDPR requirements	• DEMONSTRATOR • DEPLOYMENT
			• Art. 5(1) d/f GDPR	Verify the accuracy of data stored in the platform not only at the time of their collection, but also at the time of their processing	• DEMONSTRATOR • DEPLOYMENT

			• Art. 4(8) GDPR • Art. 28(1) GDPR	Ensure that processor activities are in compliance with the GDPR requirements	• DEMONSTRATOR • DEPLOYMENT
		Comply with the Accountability principle	• Art. 24(1) GDPR • Art. 25(1) GDPR	Prove that necessary actions have been taken to comply with the EU data protection framework	•DEMONSTRATOR •DEPLOYMENT
		Comply with the Purpose specification principle	• Art. 5(1)(b) GDPR	Prove that data collection and further processing purpose are compatible through a compatibility process	• DEMONSTRATOR • DEPLOYMENT
		Comply with lawfulness principle	• Art. 4(11) GDPR • Art. 5(1)(a) GDPR • Art. 6(1)(f) GDPR • Art. 7 GDPR	Prove that processing of personal data has been carried out having a lawful legal basis	• DEMONSTRATOR • DEPLOYMENT
		Comply with data minimisation principle	• Art. 5(1)(c) GDPR	Prove that an assessment on whether the scope of the processing activity could be achieved with either fewer data or with appropriately anonymised datasets	• DEMONSTRATOR • DEPLOYMENT
		Comply with the storage limitation principle	• Art. 5(1)(e) GDPR	Controllers have identified the purposes for which they are processing the data and have determined a retention period accordingly to such purposes	• DEMONSTRATOR • DEPLOYMENT
		Ensure data	• Art.	Prove that the less	• DEMONSTRA

		protection by design	25(2) GDPR	privacy-invasive preferences are selected by default	TOR • DEPLOYMENT
		Appoint a Data Protection Officer (DPO)	• Art. 37 GDPR • Art. 38 GDPR • Art. 39 GDPR	Appoint a DPO to assist the controller or the processor in monitoring internal compliance with the GDPR requirements	• DEMOSTRATOR (for the entity involved in the processing activity) • DEPLOYMENT (platform)
		Define the controller	• Art. 4(7) GDPR • Art. 24(1) GDPR • Art.82 GDPR • Art. 5(2) GDPR	Appoint, within the consortium or outside of it (third party) to allow the allocation of responsibilities between the entities that are part of the project for compliance, non-compliance and accountability for the implemented measures	• DEPLOYMENT
		Ensure security and confidentiality of communication	• Art. 32 GDPR • Art. 33 GDPR • Art. 34 GDPR • Art.5 ePrivacy • Art.6 ePrivacy	Develop ad hoc procedures to ensure security and confidentiality of communication (also through procedures to ensure data breach notification). The level of security should be appropriate to the risk raised by the processing operation	• DEMONSTRATOR • DEPLOYMENT
NON-PERSONAL DATA		Make data available for competent authorities	• Art 5 FFNPR • Art 6 FFNPR	Make data available to competent authorities upon request	• DEPLOYMENT
		Draft of a Code of Conduct	• Art 6 FFNPDR	To develop a self-regulatory code of conduct that each party has to comply with	• DEPLOYMENT

PERSONAL AND NOT-PERSONAL DATA		Preparation of data usage agreement	• Commission Staff Working Document – Guidance on sharing the private sector data in the European data economy. (COM (2018) 232 final)	Prepare the draft of the agreement that complies with guiding principles and consider competition law restrictions	• DEPLOYMENT

11 References

11.1 Legislation

Commission Regulation (EU) No 316/2014 of 21 March 2014 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of technology transfer agreements, OJ L 93, 28.3.2014, p. 17–23

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC OJ L 130, 17.5.2019, p. 92–125.

Directive (EU) 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, p. 20–28.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59–68.

11.2 Other documents

Commission Staff Working Document – Guidance on sharing the private sector data in the European data economy. (COM (2018) 232 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).

Deichmann, J. et al. (2016) "Creating a successful Internet of Things data marketplace".

Digitale und soziale Transformation Ausgewählte Digitalisierungs-vorhaben an öffentlichen Universitäten 2020 bis 2024.

European Commission (2018) "Proposal for a regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services".

European Commission (2019) "Competition policy for the digital era".

Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings OJ C 45, 24.2.2009.

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

President of the European Commission Ursula von der Leyen (2019) A Union that strives for more: My agenda for Europe.

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