Grant Agreement Number: 825225

Safe-DEED

www.safe-deed.eu

D3.2 Legal and Ethical Requirements for Personal Data Use Case

Deliverable number	*D3.2*
Dissemination level	*Public*
Delivery date	*30 November 2019*
Status	*Final*
Author(s)	*Alessandro Bruni, Aleksandra Kuczerawy, Arina Gorbatyuk*

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement n° 825225).

Changes Summary

Date	Author	Summary	Version
14.10.2019	Alessandro Bruni	First draft	0.1
28.10.2019	Arina Gorbatyuk	First draft	0.2
28.10.2019	Aleksandra Kuczerawy	First draft	0.3
08.11.2019	Alessandro Bruni	Second draft	0.4
12.11.2019	Arina Gorbatyuk	Second draft	0.5
14.11.2019	Ioannis Markopoulos	Peer review	0.6
15.11.2019	Lukas Helminger	Peer review	0.7
18.11.2019	Alessandro Bruni	Adjustments	0.8

1 Contents

Contents 3
List of Tables 4
1 Executive summary 5
2 Deliverable Structure 5
3 Introduction 6
4 Summary of the Principles Relating to the Processing of Personal Data 8
4.1 GDPR 8
4.1.1 Lawfulness, Fairness and Transparency principles 8
4.1.2 Purpose limitation principle 10
4.1.3 Data Minimisation 12
4.1.4 Accuracy 12
4.1.5 Accountability 13
4.2 E-privacy Requirements 14
4.2.1 Rules on Tracking Technologies 14
5 Specification of the Legal Requirements 15
5.1 Overview of the Legal Requirements 15
5.2 Privacy and Data Protection Law Requirements for the Safe-DEED Platform 15
5.3 Privacy and Data Protection Law Requirements for the WP6 use case 18
6 Ethical requirements for the processing of Personal Data 24
7 Conclusion 26
8 References 27
8.1 Legislations 27
8.2 Others 27

List of Tables

Table 1 Clarification on the purpose limitation principle 11
Table 2 Concrete Security measures 13
Table 3 Definition of roles 15
Table 4 Controller and Processor relation 16
Table 5 Fairness principle 16
Table 6 Information to be provided to Data Subjects 17
Table 7 Data Accuracy principle 17
Table 8 Monitoring activities 17
Table 9 Transparency and Accuracy principles 18
Table 10 Transparency and Accuracy principles (2) 18
Table 11 Security and confidentiality 19
Table 12 Security and confidentiality (2) 19
Table 13 Definition of roles 19
Table 14 Accuracy principle 20
Table 15 Accountability Principle 20
Table 16 Identification of a data controller 20
Table 17 Appointment of a DPO 21
Table 18 Purpose specification principle 21
Table 19 Lawfulness principle 21
Table 20 Lawfulness principle (2) 22
Table 21Data Minimisation principle (general) 22
Table 22 Data minimisation (social media) 22
Table 23 Storage limitation principle 22
Table 24 Data subject's rights 23
Table 25 Data Protection by default 23
Table 26 Ethical issues 24

2 Executive Summary

Deliverable D3.2 is the second legal and ethical deliverable of KU Leuven- CITIP, in the Safe-DEED Project. It aims at providing a clear overview of the EU privacy and data protection legal and ethical requirements that Consortium's partners should take into account. In particular, D3.2 substantiates the otherwise abstract principles developed in D3.1 by providing a comprehensive list of the requirements that should be considered by all Safe-DEED's partners involved in the project. The requirements elaborated upon in D3.2 intend to support the activities of the Safe-DEED partners, providing them with a clear and understandable overview of the measures they must implement to ensure compliance of their activities with all the relevant EU Data Protection regulatory frameworks with respect to personal data usage.

To provide a clear and concrete overview, specific attention is paid to those requirements explicitly linked to the deployment of the Forthnet use-case (WP6). Currently, the trial phase of the WP6 use case (D6.1) has been initiated, and the specific requirements listed in D3.2 are developed in parallel to the initial WP6 demonstrator and trials.

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 provide guidance in the identification of the technical and legal aspects that need to be implemented with appropriate compliance measures.

The requirements listed in D3.2 will be implemented in the upcoming deliverable, such as D6.2. In light of such approach, the future deliverables of the WP3 and WP6 will assess whether the requirements listed in D3.2 have been performed or not. Based on such findings, the listed requirements may be amended, performed or deleted.

3 Deliverable Structure

D3.2 is divided into three main parts.

The *first one* (section 4), provides an overview of the essential EU Data Protection principles that have been identified as the most relevant in the EU Data Protection framework and listed in D.3.1.

The *second one* (section 5) offers a concrete list of the EU data protection and privacy legal requirements. Specific and concrete privacy and data protection requirements for the Safe-DEED platform and in particular, for the WP6 use case, described under D6.1 are provided.

Finally, the *third part (section 6)* includes a detailed list of recommendations that should be taken into account to fulfil ethical obligations by the partners involved in the management of personal data.

4 Introduction

The general concept and principles of the EU privacy and data protection legal framework are analysed in D3.1 and substantiated in the current deliverable, D3.2.[1] Furthermore, D3.2 incorporates a list of concrete legal requirements that should be taken into account by Safe-DEED's partner when dealing with personal data. This list will provide Safe-DEED partners, in particular those responsible for the development of the WP6 use case, with clear guidelines. The listed requirements also take into account the most recent developments of the ethical principles made by the European Data Protection Supervisor (EDPS) through the Ethical Advisory Board.

The activities involving the gathering and use of data, relevant for the Safe-DEED project, are subject to numerous regulatory frameworks. It is essential to analyse the nature of the provided datasets since partners involved in the given use-case use will have to understand and assess which framework applies to the different Safe-DEED's activities. For this specific deliverable, contrary to D3.1, the legal and ethical requirements listed in the following sections focus exclusively on the EU privacy and data protection framework namely, the Regulation (EU) 2016/679[2] (General Data Protection Regulation) and the Directive 2002/58[3] (Directive on privacy and electronic communications (ePrivacy Directive)). Other EU legal frameworks that touch upon the management of personal data, such as the Directive 2019/770[4] (Digital Content Directive), are considered indirectly. In particular, Rec. 38[5] and Art. 3(8)[6] - 16(2)[7] of the Digital Content Directive consider compliance with the GDPR and the ePrivacy Directive (ePD) to be a necessary precondition for the conclusion of a contract in exchange for costumer's personal data. Therefore, providing a clear list of such requirements will ensure that the Safe-DEED partners comply with the Digital Content Directive provisions that tackle the management of personal data.

To extract value from the Safe-DEED platform, Forthnet, which leads WP6 activities, will have to combine its datasets with the open data provided by EURECAT. EURECAT provides the data-valuation software. Forthnet - and all entities that will be using the SAFE-DEED platform capabilities in the future - should have a clear overview of all the data that will be processed. In practice, datasets have to be identified, listed and classified to have a clear understanding of the type of data, the entity in charge of collecting the data, their format, their intended use, etc. The identification, listing and classification of datasets will facilitate the entities processing data with regard to the applicable legal framework.

---

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

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

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

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

5 Rec. 38: '[…] *As a consequence, any processing of personal data in connection with a contract falling within the scope of this Directive is lawful only if it is in conformity with the provisions of Regulation (EU) 2016/679 relating to the legal grounds for the processing of personal data'.*

6 Art. 3(8): *'[…] this Directive shall be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC. In the event of conflict between the provisions of this Directive and Union law on the protection of personal data, the latter prevails'.*

7 Art. 16(2): *'In respect of personal data of the consumer, the trader shall comply with the obligations applicable under Regulation (EU) 2016/679'.*

Thus, every single dataset must be qualified according to the nature of data it embeds personal data or non-personal data which hinges upon the scope of application of all the potentially applicable legal frameworks. Within D6.1. initial pilot, two datasets have been used to test the Safe-DEED platform potentialities: Customer Relationship Management (CRM) data and Live Events data. The detailed analysis of the provided datasets has demonstrated that the data of the CRM do not fall into the definition of personal data, whereas the data of Live Events does. In particular, the CRM comprises of the non-personal customer data because all identifiers had been taken out. On the contrary, live streams event data, are gathered by Facebook and YouTube. Consequently, while activities involving the CRM data fall out of the scope of application of the GDPR and the ePD, those related to the live stream events data have to follow the requirements listed in the EU privacy and data protection legal framework.

Within the trial phase, the qualification of datasets is provided under the guidance of KU Leuven together with Forthnet. Once the Safe-DEED project is completed, each entity involved in the platform's activities has to ensure that the preliminary guidance provided in this deliverable is in line with the circumstances surrounding each specific case.

5 Summary of the Principles Relating to the Processing of Personal Data

In this section the EU Data Protection principles that are considered to be the most relevant in the Safe-DEED project context are reviewed. Accordingly, each one of such principles should be taken into account by the Safe-DEED partners involved in personal data processing activities such as the one that characterises WP use case. The identified principles are: lawfulness, fairness and transparency, accuracy, integrity and confidentiality, and accountability. These principles are listed in the GDPR. In addition, the specific requirements listed in the e-Privacy Directive are also described.

5.1 The General Data Protection Regulation (EU) 2016/679 (GDPR)

The extensive overview of the EU data protection framework has been provided in D3.1. In particular, specific emphasis has been given to the GDPR and the principles embedded in it. The EU Data Protection principles are listed in Art. 5 GDPR.[8]

5.1.1 Lawfulness, Fairness and Transparency principles

The first set of fundamental principles listed in the GDPR - lawfulness, fairness and transparency - requires the personal data is to be processed lawfully, fairly and in a transparent manner when it concerns the individual.[9]

On the one hand, the GDPR prescribes that, to comply with the lawfulness principle, the entity appointed as a data controller has to process its data lawfully, using a legal basis substantiated in Art. 6-10 GDPR. To comply with the fairness principle, controllers have to ensure that personal data are processed considering the interests and reasonable expectations of data subjects.

In addition to the lawfulness and fairness principles, the GDPR includes the principle of transparency, which can be considered as a prerequisite to ensure the fairness of a process involving personal data. The transparency principle requires data subjects (individuals) to have control over their personal data, to ensure that they are able to exercise their rights. To be in compliance with the transparency principle, controllers have to be transparent about the personal data processing.[10]

8 Art. 5GDPR : *'Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) 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, 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 ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('dataminimisation'); (d) 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 ('accuracy'); (e) 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 ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')'.*

9 Art. 5(1)(a) GDPR.

10 The transparency obligations and specific information that controllers have to communicate to individuals are listed in details in Art. 12-14 GDPR.

5.1.1.1 Lawfulness and the need for an appropriate lawful basis

In order to process the data, the data controller needs to have a valid legal basis. Art. 6(1) GDPR provides six legal bases on which the data controller can rely: the consent (of the data subject), the performance of a contract, a legal obligation, the vital interests of individuals, the public interest and the legitimate interest of the controller.

Each one of these legal bases for processing personal data has been analysed in detail in D3.1. Considering the nature of datasets that have been used for the initial trial, it is clear that not all of them are relevant for WP6 use-case. In particular, the lawful basis for processing data might change depending on the specific use-case and the source they are coming from (Facebook and YouTube in one case, Forthnet in another one). Considering the set of data that has been used in the WP6 context (CRM and live stream data), and, in particular, the (personal) data gathered from live stream events, specific attention should be paid to four lawful bases: 'contract', 'legal obligation to which the controller is subject', 'controller's legitimate interests', and 'consent'. Due to the fact data are generally gathered from two different sources, might be the case that different legal ground have to be found.

5.1.1.2 Contract

The Safe-DEED initial pilot involves the costumer data whose identifiers have been removed to anonymise the data. The CRM data, in the way they are provided within the initial pilot, fall outside the GDPR scope of application. Nonetheless, other sets of data might be processed without the anonymisation process taking place. Thus, rules related to their management will fall under the GDPR scope of application. In this case, the lawful basis for processing the customer data - as well as the data of employees and/or suppliers - could be found in the contract established between the customers and the data controller. The performance of a contract is one of the six grounds listed in Art. 6(1) GDPR. In the context of contract execution, the data processing must be necessary for the performance of a contract at stake. To comply with the GDPR principles, the contract has to define the amount of personal data that can be lawfully processed, limiting such amount to the strictly necessary amount. The scope of the personal data required must be determined on a case-by-case basis.

5.1.1.3 Legal obligation to which the controller is subject

Art. 7(c) GDPR states that the ground for processing personal data can be found where it '*is necessary for compliance with a legal obligation to which the controller is subject*'. Such law must comply with the data protection law, which means it has to comply with the GDPR principles (i.e. necessity, proportionality, purpose limitation). An example of a legal obligation, given by Article 29 Working Party, the board of National data protection authorities now replaced by the European Data Protection Board (EDPB), concerns the responsibility of the employer to report its employees to social security or tax authorities.

5.1.1.4 Legitimate interests

Another lawful ground for processing personal data in the WP6 use case context can be found in the legitimate interest of the data controller. To rely on legitimate interests as legal basis, a data controller has to ensure that the fundamental rights of the data subject are not overriding.

The GDPR and Article 29 Working Party provide clarifying examples of what should be considered legitimate interests. In the Safe-DEED context, the processing of personal data for direct marketing purposes and other forms of marketing or advertisement, which is the purpose pursued by Forthnet, is listed among the activities that legitimate the data controller in processing personal data. An additional example that can justify the processing of personal data for the legitimate interest of the data controller is the prevention of fraud, employees' monitoring for safety or management purposes and data processing for physical security, IT and network security.

When the legitimate interest of the data controller is used as a lawful basis for data processing, Forthnet must demonstrate that the processing activity is necessary to achieve the desirable interests.

In addition, it has to prove that there are no less intrusive activities to pursue its scope. A so-called balancing test between where conflicting interests of the data subject and the data controller must be performed in order to assess whether the legitimate interest of data controller can be used as legal basis for processing personal data.

Key elements that have to be taken into account by the data controller when carrying out such test are:

- The relationship between the data controller (i.e. Forthnet) and the individual/ data subject;
- The individual expectation of the data subject that the data controller will use his/her data according to what has been reported to him by the controller when fulfilling his/her transparency obligations;
- In a company-customer relationship, such as the one characterising WP6 use-case, a Forthnet's costumer could reasonably expect that the company may analyse and use his or her personal data for marketing purposes;
- The nature of the personal data processed and whether it is particularly sensitive or private;
- The possible impact on individuals/ data subjects;
- Whether safeguards can be put in place to minimise the data processing impact.

5.1.1.5 Consent

In the safe-DEED context, the datasets, including Forthnet's customer personal data, have been collected and processed after having received the consent of the data subject to conduct these actions. Art. 4 GDPR states that in order to be valid, the consent of the data subject must be freely given; be specific; be informed; be unambiguous; be given by a statement or by explicit affirmative action.

5.1.2 Purpose limitation principle

The purpose limitation is the second core principle mentioned in Art. 5 GDPR.[11] The purpose limitation principle requires that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[12] Such principle, which has been substantiated by Art. 29 Working Party Opinion 03/2013 on purpose limitation,[13] can be split in two modules, each of them requiring careful attention.

In particular, Art. 5(1)(b) requires that data subjects' personal data have to be collected for a purpose that justifies their collection. In particular, such purpose should be sufficiently defined to ensure the implementation of any necessary safeguard measures and to delimit the scope of the processing operations. The purpose has to be explicit, avoid any possible ambiguity, and match the legitimate expectations of data subjects.

Secondly, personal data that are collected for a specific and identified purposes should not be further processed in a manner which is incompatible with those purposes. The notion 'further processing' refers to any processing operation occurring after the initial collection. To comply with the purpose limitation requirement, an assessment has been carried out taking into account specific criteria listed in Rec. 50 GDPR.[14]

---

11 Art. 5(1)(b) GDPR : (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, scientific or historical research purposes or statistical purposes shall, in accordance with Art. 89(1), not be considered to be incompatible with the initial purposes'.

12 Art. 5(1)(b) GDPR.

13 Art. 29 Working Party, Opinion 03/2013 on purpose limitation, WP 203, adopted on 2 April 2013.

14 Rec. 50 GDPR list the criteria that should be taken into account when assessing the compatibility between the initial processing purpose and the further ones: (1) the relationship between the purposes for which the data have been collected and the purposes of further processing, (2) the context in which the data have been collected and the reasonable expectations of the data subjects as to their further use, (3) the nature of the personal data and the impact of the further

In the Safe-DEED context, the partners, processing personal data through participatory platforms, must, therefore, clearly indicate the purpose(s) for which the data are collected. By indicating the specific purpose, they will ensure compliance not only with the purpose limitation principle but also with the transparency one. The table below (Table 1) provides concrete example of the purpose limitation principle in relation to a list of different processing activities.

Table 1 Clarification on the purpose limitation principle

Processing Operation	Personal Data	Controller	Legal basis	Purpose
Collection (initial processing)	Postal address	Online sale undertaking	Performance of a contract	Proceed with the delivery
Storage (further processing)	Postal address	Online sale undertaking	/	Storage to proceed with the delivery (compatible)
Use (further processing)	Postal address	Online sale undertaking	/	Print voucher to proceed with the delivery (compatible)
Use (further processing)	Postal address	Online sale undertaking	/	Send personalised offers (incompatible)
New purpose				
Use (further processing)	Postal address	Online sale undertaking	Legitimate interests[15]	Send personalised offers
Use (further processing)	Postal address	Online sale undertaking	/	Send monthly newsletter (compatible)
Use (further processing)	Postal address	Online sale undertaking	/	Transfer to third party advertiser (incompatible)
New purpose				
Use (further	Postal address	Online sale	Consent[16]	Transfer to third party

processing on the data subjects and (4) the safeguards applied by the controller to ensure the fair processing and to prevent any undue impact on the data subjects.

15 According to the guidelines on consent, any change in the lawful basis for processing must be notified to data subject in accordance with the information requirement of Art. 13 and 14 GDPR: Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (WP259) 22.

processing)		undertaking		advertisers

5.1.3 Data Minimisation

The data minimisation principle requires controllers to ensure that personal data are '*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*'.[17] The data minimisation principle aims to ensure that the amount of personal data collected and processed is reasonable and tailored to the identified purpose.

In the Safe-DEED context and, in particular, in the WP6 use-case, the data have to be processed and retained to achieve a specific purpose: data analytics. Consequently, when it comes to personal data, such as the live stream event ones, they have to be processed and retained only to accomplish such purpose.

5.1.4 Accuracy

The data accuracy principle states that personal data shall be '*accurate and, where necessary, kept up to date*'.[18] To comply with the accuracy principle, data controllers must make every reasonable step to ensure that any inaccuracy has been promptly rectified or deleted. In particular, the data controllers need to put appropriate processes in place to check the accuracy of their datasets. An exception to the general rule is foreseen when the processing is carried out for the public interest, scientific or historical research purposes or statistical purposes. Nonetheless, in those exceptional cases, the implementation of appropriate technical and organisational safeguard measures is required.

The level of accuracy depends on the purpose for which such personal data are processed, collected and retained. For the Safe-DEED and, in particular, the WP6 initial trial phase, the process of data aims at maximising Forthnet's datasets value. Thus, it is not necessary to take perplex measures to ensure the accuracy of the collected data.

On the one hand, the GDPR does not establish a standard data retention period. On the other hand, the Data Retention Directive, which provided clarifications on data retention, had been invalidated by the Court of Justice of the European Union (CJEU). The European Commission has not published a new Directive (to replace the invalidated Data Retention one) yet and Member States have started developing legislative initiatives in this field to fill the gap created by the CJEU decision.[19] Thus, considering the current legislative uncertainty it is advised to store the data only for the (limited) amount of time necessary to achieve the specified purpose of the process. The time of data storage, in any case, should not exceed the one specified in the relevant national legislation.

Forthnet, which leads WP6 use case initial trial, collects the data in its premises in Greece. Thus, the partner should take into account the retention period (for the specific type of data they are processing) established by Greek legal provisions. While Greek Act 3917/2011[20] sets general retention rules, there are also sector-specific legislations that establish specific retention regimes.[21]

5.1.4.1 Integrity and confidentiality

Integrity and confidentiality are two principles strictly related to the security of data processing, further developed in Art. 32-34 GDPR. On the one hand, the integrity principle requires controllers to

16 Same applies when migrating from legitimate interests to consent of the data subject.

17 Art 5(1)(c) GDPR.

18 Art 5(1)(d) GDPR.

19 Greece implemented the Data Retention Directive with the Act 3917/2011. After the CJEU decision the Act has been updated on 29 November 2017.

20 Greek Act 3917/2011, available at https://docs.google.com/viewer?url=https%3A%2F%2Fwww.ohchr.org%2FDocuments%2FIssues%2FPrivacy%2FGreece.doc, accessed on 14 October 2019.

21 Law 4308/2014 on Greek Accounting Standards.

ensure appropriate security when processing personal data, protecting them against unlawful processing, accidental loss, destruction or damage.[22] On the other hand, confidentiality requires that personal data are not available to everyone within an organisation, but only to those who need them for the processing activities.[23] These two principles, which intend to reinforce data subject security, have been expanded in the ePD and the European Electronic Communication Code (EECC) in the context of electronic communications.

In the Safe-DEED context, the entire architecture of the platform and the communication channels established between the platform peer have to take into account the measures suggested in Art. 32-34 (i.e. encryption) to ensure compliance with these two principles, also taking into account the EECC and the ePD. In the table below (Table 2) the concrete examples of organisational measures are provide that can be taken into account to ensure security and integrity of personal data.

Table 2 Concrete Security measures

Suggested organisational measures for security
➢ Personal data must not be exposed to third parties. Staff must be cautious and avoid unattended electronic screens and unattended paper documents in public areas.
➢ Both paper documents and electronic files must be stored securely on a 24/7 basis. Secure storage entails the use of lockers or restricted access rooms.
➢ Electronic documents or media such as USB sticks, CDs, hard disks etc. containing personal data must not be discarded without guaranteeing their destruction.
➢ Personal data must not be transferred to third parties, and staff should pay attention not to disclose such data.
➢ The confidentiality duties transcend the employment relationship. Employees remain bound by these duties even after their employment contract ends.
➢ Employees are informed about the procedure to handle requests from data subjects to exercise their rights.[24]

5.1.5 Accountability

Accountability represents one of the most important novelties introduced by the GDPR. It is a two-fold principle that obliges data controllers not only to ensure compliance with the GDPR provisions but also to be able to prove it.[25] Chapter IV of the GDPR specifically lists the obligations that data controllers and the processor have to fulfil to prove their compliance with the GDPR provisions.

In the Safe-DEED context such technical and organisation measures have to be taken into account by each partner of the project, and especially by those setting the platform and the ones involved in the management of personal data. Such technical and organisational requirements include, for example, measures to ensure privacy by design and by default; to record processing activities involving personal data such as live stream ones; to conduct a Data Protection Impact Assessment and where necessary to appoint a Data Protection Officer (DPO).

22 Art. 5(1)(f) GDPR.

23 White & Case, Unlocking the EU General Data Protection Regulation – Chapter 6: Data Protection Principles, accessed on 30 October 2019

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

25 P. Voigt and A. von dem Bussche, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International 2017

5.2 Directive 2002/58 on privacy and electronic communications (e-Privacy Directive)

5.2.1 Rules on Tracking Technologies

The Safe-DEED project intends to engage on its platform more than 100 small and medium enterprises (SMEs) to empower their access to data markets. Most of these SMEs are small technological start-ups and entrepreneurs which, similarly to Forthnet, offer online services or interact with their customers using websites or mobile apps. Thus, Forthnet and those private entities have to comply not only with the GDPR requirements mentioned above but also with ad hoc legal requirements established in the ePD for the electronic communication sector.

Rec. 30 GDPR states that cookies should be considered personal data when they make it possible to identify an individual.[26] In this case, the GDPR obligations, rights and principles will apply. Similarly to the GDPR, Art. 5(3) of the e-Privacy Directive requires the data subject's consent for the storage of or access to certain types of cookies.[27] When defining the term "consent" the ePD states that it '*should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC (Data Protection Directive)*'. Now that the GDPR has replaced the former Data Protection Directive the concept of consent has to be interpreted in the light of the GDPR provision: the consent has to be freely given, specific, informed, unambiguous and based on affirmative action.

Art. 5(3) of the ePD also highlights the need to provide '*clear and comprehensive information*' about the use of cookies when requesting users' consent. Digital MEnts, thus, have to prepare and publish on their websites a cookie policy allowing users to understand the purpose for which cookies and other tracking mechanisms are used. This information is necessary to enable users to take an informed decision on whether or not to consent to those cookies.

Websites, such as the one of Safe-DEED, need to provide clear, understandable and visible information regarding the use of cookies, giving the possibility to users to access all necessary information. The notice provided should include information on the purpose for which the cookies are used, the possible use and access of the collected data by third parties, and the type of cookies.[28]

26 Rec. 30 GDPR.

27 Art. 5(3) e-Privacy Directive.

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

6 Specification of the Legal Requirements

6.1 Overview of the Legal Requirements

The requirements listed in the *second part* of D3.2 (section 5) develop the legal analysis provided in the first part (section 4) of D3.2 to offer an easily and unambiguously interpretable overview of legal requirements. Differently from technical specifications, legal and ethical requirements reported in this section are subject to variation and implementation. In particular, the national implementation of existing EU legislative initiatives, such as the one of the Digital Content Directive (DCD), or new EU legislative initiatives, such as the one for an ePrivacy Regulation, might require to amend the reported legal requirements.

The full description of the legal frameworks on which the legal and ethical requirements are based was already provided in D3.1 and is not repeated in this section. Nonetheless, both deliverables should be consulted when analysing the EU Privacy and data protection and framework the D3.1 and D3.2.

As for the legal requirements, a differentiation needs to be made between general requirements, that should apply and be taken into account by each partner of the Safe-DEED project, and those that are relevant only to the partners involved in the development of WP6 use case.[29]

6.2 Privacy and Data Protection Law Requirements for the Safe-DEED Platform

In light of the Safe-DEED platform deployment, which intends to address multi-parties requests and inputs, concrete specification of privacy and data protection requirements for the platform itself is considered necessary. Therefore, a clear overview of current and upcoming actors involved in the platform's activities, and in particular in processing personal data, is offered.

In the tables below (Tables 3-8), tasks that have to be taken into account are listed.

Table 3 Definition of roles

TASK	TO DO	WHY	LEGAL BASIS
Definition of role	Define the platform controller	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	• Art. 4(7) GDPR • Art. 24(1) GDPR • Art.82 GDPR • Art. 5(2) GDPR
The GDPR defines Controller as the '*natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*'.			
In Safe-DEED, the appointed data controller should be considered the one in charge of deciding the purpose and the means related to the processing of personal data in the Safe-DEED platform context. The platform controller should not be confused with the one in charge of the pilots or use			

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

case activities.

Table 4 Controller and Processor relation

TASK	TO DO	WHY	LEGAL BASIS
Controller and Processor relation	Draft a controller/processor agreement	To define role and task according to the respective roles	• Art. 28(3) GDPR
According to the GDPR the relationship between a controller and a processor should be determine by a contract (or other legal act). In particular, Art. 28(3) GDPR defines in detail all the elements that such contract should contain.			
In Safe-DEED some partners will act as controllers (also jointly when the platform will be fully implemented) while others will be merely processors. Other partners might not be involved in these activities at all. The appointment of a processor is not necessary, but when the controller delegates part of its processing activities to another entity acting on his behalf, that entity is qualified as a processor. This contract should not be confused with the one that must be drafted for WP6 use case.			

Table 5 Fairness principle

TASK	TO DO	WHY	LEGAL BASIS
Provide all necessary information to the data subject	Draft Privacy policy	In compliance with the transparency principle and in order to provide the data subject with all necessary information regarding the processing activity of his/her personal data for exercising its rights	• Art. 13 • Art.14 GDPR
The GDPR establishes that '*when personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all information listed in Art.13 and 14*'. Art.13 GDPR states that such privacy policy should include: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) the categories of personal data concerned; (e) the recipients or categories of recipients of the personal data, etc.			
The Safe-DEED platform's controller must draft a privacy policy under the transparency principle and give the data subject the possibility/opportunity to exercise his/her rights concerning the processing activity of his/her personal data. Privacy policy requirement should not be confused the one that must be drafted for WP6 use case.			

Table 6 Information to be provided to Data Subjects

TASK	TO DO	WHY	LEGAL BASIS
Provide all necessary information to the data subject	Provide a form for data subjects to exercise their rights	Give the possibility to the data subjects to exercise his/her rights	Art. 15-22 GDPR
Arts. 15-22 GDPR list a series of information that should be provided upon request from the data subject about the processing of his/her data. In particular, the right of access, right to rectification, right to erasure (right to be forgotten), right to restriction of processing, right to data portability, right to object.			
Safe-DEED platform's controller should provide data subjects whose data will be processed within the Safe-DEED platform with all necessary information regarding the processing activities to offer them the possibility to exercise their right.			

Table 7 Data Accuracy principle

TASK	TO DO	WHY	LEGAL BASIS
Ensure Accuracy	Data accuracy	Ensure data accuracy principle	Art. 5(1) d/f
Art. 5(1)(d) GDPR requires 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'*.			
In the Safe-DEED context, the accuracy of the data stored on the platform should be verified by the controller both at the time of their collection and at the time of their processing. The processing purpose of each partner should determine the degree of the steps that should be implemented to ensure the accuracy of data processed.			

Table 8 Monitoring activities

TASK	TO DO	WHY	LEGAL BASIS
Monitoring	Verify specific national requirements transposing EU legislations	Ensure compliance with national implementation measures	National legislation implementing EU legislations
According to the different entities involved, the monitoring activity should be carried out about the national transposing acts of the ePD. Member States have the discretion to adopt exceptions and derogations to the general regimes described in D3.1 (GDPR, ePD, and the one developed after the CJEU decision on Data Retention Directive).			
In the Safe-DEED context, we expect that different partners involved in the platform activities are located in the different Member States. Therefore, each one of the platform participants should pay attention to the various national regime.			

6.3 Privacy and Data Protection Law Requirements for the WP6 use case

The actors involved in the development of WP6 must comply with **two types of requirements**, namely: the requirements related to transparency and accountability principles and the requirements surrounding the actual processing of personal data. Tables 9-15 specify the list of tasks that need to be performed in order to comply with the transparency and accuracy principles. Tables 16-25 summarise the requirements that have to be taken into account for processing personal data.

Table 9 Transparency and Accuracy principles

TASK	TO DO	WHY	LEGAL BASIS
Transparency and Accuracy Principle	Draft a privacy policy for the users whose data have been used for the development of WP6 use case	In compliance with the transparency principle and in order to provide data subject all necessary information regarding the processing activity of his/her personal data for exercising its rights	• Art. 13 GDPR • Art. 14 GDPR
According to GDPR, the following information is to be provided: the identity and contact details of the controller, the identity and contact details of the controller's representative (if any), purposes of the processing (in our case marketing and data analytics), legal basis for data processing (contract, legitimate interest of the controller or consent), recipients, the existence of transfers outside EU, the retention period, the existence of data subject's rights, the right to lodge a complaint, the presence of automated decision-making processes, etc.			
For the WP6 use case and, in particular, for those users whose data have not been fully anonymised (live stream events data) all necessary information listed in Arts. 13-14 GDPR have to be provided in a clear and understandable privacy policy.			

Table 10 Transparency and Accuracy principles (2)

TASK	TO DO	WHY	LEGAL BASIS
Transparency and Accuracy Principle	Keep a record of processing activities	To fulfil data controller obligations and complying with transparency and accountability principle	Art. 30 GDPR
In compliance with GDPR provision, information related to data processing activities should include the name and contact details of the controller, purposes of the processing, the description of the categories of data subjects and personal data, recipients, the existence of transfers outside EU, the technical and organisational measures, etc.			
In the Safe-DEED, the data controller in charge of any processing activities involving personal data			

should keep a record of such activities.

Table 11 Security and confidentiality

TASK	TO DO	WHY	LEGAL BASIS
Transparency and Accuracy principle	Security	Ensure security and confidentiality of communications	Art. 32 GDPR
Implementation of security measures tailored to the risks posed by the processing activities to data subjects' rights and freedoms is necessary to comply with confidentiality and security requirements established in the GDPR and ePD.			
Safe-DEED partners will have to consider as security measures, *inter alia*, pseudonymisation, encryption, the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems, the ability to restore the availability and access to personal data in the event of a physical or technical incident, and a process for testing and evaluating the effectiveness of those measures.			

Table 12 Security and confidentiality (2)

TASK	TO DO	WHY	LEGAL BASIS
Transparency and Accuracy principle	Develop ad hoc procedure to manage data breaches	Ensure security and confidentiality of communication	Art. 33 GDPR Art. 34 GDPR
The GDPR describes in detail the modalities surrounding the obligation for a controller to notify the National Data protection Authority (DPA) and data subjects themselves about a data breach.			
The controller (Forthnet), appointed for the WP6 use case, must implement a procedure for managing personal data breaches and notifying the DPA and the data subjects in cases where such notification is mandatory.			

Table 13 Definition of roles

TASK	TO DO	WHY	LEGAL BASIS
Transparency and Accuracy principle	Draft a controller/processor agreement	To define role and tasks according to the respective roles	Art. 28(3) GDPR
According to the GDPR the relationship between a controller and a processor should be determined by a contract (or other legal act).			
In the Safe-DEED some partners will act as controllers (also jointly when the platform will be fully implemented) while others will be merely processors. Other partners might not be involved in these activities at all. The appointment of a processor is not necessary, but when the controller delegates part of its processing activities to another entity acting on his behalf, that entity is qualified as a processor. This contract should not be confused with the one that must be drafted for the Safe-DEED platform.			

Table 14 Accuracy principle

TASK	TO DO	WHY	LEGAL BASIS
Transparency and Accuracy principle	Ensure that the processors have implemented adequate measures	To ensure that processor activities are in compliance with the GDPR requirements	• Art. 4(8) GDPR • Art. 28(1) GDPR
The GDPR defines a processor as the *'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*'. When the controller delegates part of its processing activities to a processor, the controller has to ensure that the appointed processor provides sufficient guarantees and safeguards in terms of privacy and data protection.			
The WP6 controller has to ensure that the appointed processors provide sufficient guarantees to implement appropriate technical and organisational measures in such manner that processing will meet the requirements established in the GDPR to ensure the protection of the rights of the data subject.			

Table 15 Accountability Principle

TASK	TO DO	WHY	LEGAL BASIS
Transparency and Accuracy principle	Comply with the Accountability principle	Prove that necessary actions have been taken to comply with the EU data protection framework	• Art. 24(1) GDPR • Art. 25(1) GDPR
The GDPR requires the controller to comply with the GDPR requirements and be able to prove it. Compliance with some of the obligations laid down in the GDPR, through a Data Protection Impact Assessment (DPIA) may, *de facto*, lead to proper accountability.			
In the Safe-DEED the controllers must comply with the GDPR provisions and have to be able to demonstrate its compliance activity. The controllers must keep detailed documentation of the essential steps that have been taken while processing the data to achieve the results (within the identified scope of data processing activities).			

Table 16 Identification of a data controller

TASK	TO DO	WHY	LEGAL BASIS
Requirements for the processing of personal data	Define the controller	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	• Art. 4(7) GDPR • Art. 24(1) GDPR • Art.82 GDPR • Art. 5(2) GDPR
The GDPR defines Controller as the '*natural or legal person, public authority, agency or other bodies which, alone or jointly with others, determines the purposes and means of the processing of personal data*'.			
In the Safe-DEED, the controller should be the one in charge of deciding the purpose and the means related to the processing of personal data in the Safe-DEED platform context. The platform controller			

should not be confused with the one in charge of the pilots or use case activities.

Table 17 Appointment of a DPO

TASK	TO DO	WHY	LEGAL BASIS
Requirements for the processing of personal data	Appoint a Data Protection Officer (DPO)	To assist the controller or the processor in monitoring internal compliance with the GDPR requirements	• Art. 37 GDPR • Art. 38 GDPR • Art. 39 GDPR
Art. 37(1)(a) GDPR requires the designation of a DPO when '*the processing is carried out by a public authority or body*'.			
Each partner of the Safe-DEED platform involved in the processing of personal data should designate a DPO.			

Table 18 Purpose specification principle

TASK	TO DO	WHY	LEGAL BASIS
Requirements for the processing of personal data	Purpose specification	To comply with the purpose limitation principle	• Art. 5(1)(b) GDPR
According to the GDPR, personal data have to be collected for a specific purpose. Under the Purpose limitation principle further processing of the same dataset is allowed only if the processing is compatible with the purpose for which they were collected in the first place. To assess the compatibility of the initial purpose with the further ones, a compatibility assessment needs to be carried out. Criteria that should be taken into account are the ones listed in Rec. 50 GDPR. Guidance is provided in the Article 29 Working Party opinion 03/2013 on purpose limitation.			
In the WP6 use case, the process of personal data has to be carried out having a specific purpose. The initial pilot involves datasets collected by third parties (Facebook and YouTube). An assessment of the compatibility of the initial data processing (done by YouTube and Facebook) and the one carried out by Forthnet needs to be done.			

Table 19 Lawfulness principle

TASK	TO DO	WHY	LEGAL BASIS
Requirements for the processing of personal data	Legal basis (social media)	To comply with lawfulness principle	• Art. 5(1)(a) • Art. 6(1)(f)
Art. 5(1)(a) (lawfulness) and Art. 6(1)(f) (legitimate interests) GDPR requires that processing of personal data requires a lawful legal basis. Guidance on the legitimate interests is provided in Article 29 Working Party opinion 06/2014.			
In the WP6 initial pilot, for the personal data obtained through social media, a legitimate basis for processing data should be considered the legitimate interests of the controller.			

Table 20 Lawfulness principle (2)

TASK	TO DO	WHY	LEGAL BASIS
Requirements for the processing of personal data	Identify a suitable legal basis for open, participatory platforms	To comply with lawfulness principle	Art. 4(11) GDPR Art. 5(1)(a) GDPR Art. 6(1)(a) GDPR Art. 7 GDPR
When the controller use as legal basis for processing personal data the user consent, the GDPR specifies that data controller has to fulfil specific requirements. Consent must be freely given; it has to be specific, informed, and unambiguous. Guidance is provided in 29 Working Party guidelines on consent under Regulation 2016/679.			
In light of the exploitation of the Safe-DEED platform, personal data obtained by the partners that will be using the participatory platform, should be processed based on a legal basis. According to the purpose limitation principle whether the further processing activity is incompatible with the initial purpose, another legal basis has to be found.			

Table 21Data Minimisation principle (general)

TASK	TO DO	WHY	LEGAL BASIS
Requirements for the processing of personal data	Data minimisation (general)	Comply with data minimisation principle	• Art. 5(1)(c) GDPR
According to the GDPR, controllers, when processing data, should assess whether these purposes could be achieved with either fewer data or with appropriately anonymised datasets.			
Within the WP6 use case, the collection of data should be restricted to the identified purpose(s), which are limited to the strictly necessary scope, namely, data analytics for marketing purposes. According to the purpose limitation principle, Forthnet should only process personal data that are suitable and reasonable to accomplish the specified goals.			

Table 22 Data minimisation (social media)

TASK	TO DO	WHY	LEGAL BASIS
Requirements for the processing of personal data	Data minimisation (social media)	To comply with data minimisation in a social media context	• Art. 5(1)c GDPR
In compliance with the data minimisation principle established in the GDPR, the data collection should be limited to publicly available profiles, avoiding to collect more data than necessary to achieve the purpose.			
For the purposes of the WP6, collecting a full list of data subjects that have had access to the events provided by Forthnet details might be considered as excessive.			

Table 23 Storage limitation principle

TASK	TO DO	WHY	LEGAL BASIS

Requirements for the processing of personal data	Storage limitation	To comply with the storage limitation principle	Art. 5(1)(e) GDPR
The GDPR establishes that controllers should identify the purposes for which they are processing the data and determine a retention period accordingly to such purposes. Once those purposes have been fulfilled, data must be anonymised or securely deleted, unless there is another legal ground justifying their processing in an identifiable form.			
In WP6, personal data should be erased once the identified purposes have been achieved unless there is another legal ground justifying their processing in an identifiable form. If the same sets of data might be used for another purpose, another legal ground that justifies the new processing activity should be found.			

Table 24 Data subject's rights

TASK	TO DO	WHY	LEGAL BASIS
Requirements for the processing of personal data	Data subject's rights	Provide data subjects necessary ground to exercise their rights	• Art.12 GDPR • Art.15-22 GDPR
Art. 12 GDPR sets out the modalities for the exercise of the rights of data subjects. taking into account transparency and fairness principles, any communication issued by the data controller must be phrased in a concise, transparent, intelligible and easily accessible form, using clear and understandable language. In addition, the data controller should support and facilitate the exercise of data subject rights.			
In WP6, the data controller should implement the necessary measures for data subjects to exercise their prerogatives (access, rectification, erasure, restriction, data portability, object). To comply with such requirement a form that data subjects can use to contact the data controller can be provided.			

Table 25 Data Protection by default

TASK	TO DO	WHY	LEGAL BASIS
Requirements for the processing personal data	Data protection by default	Ensure data protection by design	Art. 25(2) GDPR
The GDPR establishes that *'the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons'.*			
Partners involved in the WP6 use case have to ensure that the less privacy-invasive preferences are selected by default.			

7 Ethical requirements for the processing of Personal Data

The processing of personal data is meant to be a crucial activity within the Safe-DEED Project. Data protection, as a fundamental right, is a central issue for research ethics in Europe, especially under the European Charter of Fundamental Right.[30] Thus, all the activities carried out under Horizon 2020 must comply with ethical principles and relevant national, EU and international legislation. Ethical considerations in the management of personal data have to be used as an interpretative tool for positive law.

The Safe-DEED consortium, aiming at conducting its research on data markets in compliance with the existing EU legal framework, performs all its activities in line with the principle established in such framework. Taking into account the legal and ethical developments that characterise the data market context, the requirements listed below may be subject to amendments.

The table below (Table 26) takes into account the development of the ongoing discussion, led by the European Data Protection Supervisor (EDPS), on the ethical principles that should be taken into account when managing personal data. In particular, the requirements which are aligned with the ones already embedded in the previous sections of the deliverable consider the work developed by the EDPS Advisory group, whose guidelines have been already reported in D3.1.[31] Table 26 lists those EU Data Protection principles that have to be taken into account when processing personal data to address ethical issues coming from the processing of personal data.

Table 26 Ethical issues

Ethical Issue	Required activity
Transparency and information (in general)	• In line with the EU data protection framework, data subjects whose data will be processed in the context of Safe-DEED project will need to be informed about the activities involving their personal data. This should be done mainly by specifying the privacy policy on the Safe-DEED website. • Due to the nature of data collected and processed during the WP6 initial trial phase, informed consent forms have not been developed. • In the deployment phase of the Safe-DEED project, all essential information should be taken into account to fulfil all necessary obligations. Such requirement can be fulfilled through an easy readable format with all necessary information about the processing of personal data to be provided to data subjects.
Data minimisation	• To fulfil their ethical obligation, those appointed as data controllers should, first of all, identify the nature of the different datasets. While the large amount of (personal and non-personal) data are essential for the data evaluation activity, each partner involved in the project activities are suggested to limit their collection to the lowest possible number of different data sources. To achieve such purpose, a variety of different datasets, categorised according to the diverse needs, might be a

30 European Commission, Ethics and data protection, 14 November 2018, p.3, https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf , accessed 28 October 2019.

31 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 28 October 2019.

	feasible solution in order to combine ethical requirements and partners business claims. • For the initial trial stage, the use of so-called "dummy" data is warmly recommended. • Personal data collected and processed within the Safe-DEED project context by partners will solely be used to develop and improve the Platform, which minimises the processing as far as possible.

Purpose specification and use limitation	• The Safe-DEED partner collecting personal data should specify the purpose for which personal data are collected
	  ○ The Safe-DEED project aims to develop a tool for data analytics in compliance with current legal and technical requirements in order to extract additional value from the Safe-DEED partners datasets.
	  ○ At this stage, Safe-DEED partners are committed to not process personal data for other purposes.
	• Personal data collected should be processed and stored until it is necessary to fulfil the collecting purpose or if other reasons will justify their use, the subsequent purpose should be compatible with the initial one
	  ○ If this is not the case, another legal ground for processing should be identified.

Storage limitation	• Personal data processed in the context of the initial research stage will be stored for the time that is necessary for the project purposes to be achieved. • Within the WP6 use case data initially collected for the research phase will be used in order to test the functionality of the Safe-DEED platform. Once the models are trained and validated, it will be possible to delete the datasets. • Due to the fact that the Safe-DEED platform characteristics do not foresee the possibility for the data to be stored in the platform, there is no need to provide guidelines in relation to data storage on the platform. Each partner sharing its dataset will have to comply individually with such requirement.
Data transfers	• Safe-DEED partners have decided to develop their platform which servers are exclusively located in the EU to avoid data transfers to a country where the same level of data protection is not ensured. • At this stage partner involved in the project and sharing their data are all located within the EU.

8 Conclusion

The Deliverable D3.2 lists and analyses essential legal requirements that have been extracted from the EU Data Protection and Privacy framework (GDPR and ePD). The D3.2 also provides a detailed list of actions that have to be carried out by Safe-DEED partners, according to their role, to comply with the identified privacy and data protection principles. Compliance with the legal and ethical challenges coming from the deployment of the second phase demonstrator will be provided, in the form of recommendations, integrating and developing, if necessary, the requirements that have been listed in D3.2.

9 References

9.1 Legislations

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

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

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

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

9.2 Others

Article 29 Working Party, Opinion 03/2013 on purpose limitation, WP 203, adopted on 2 April 2013.

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

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 28 October 2019.

European Commission, Ethics and data protection, 14 November 2018, available at < https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf>, accessed 28 October 2019

Law 4308/2014 on Greek Accounting Standards.

P. Voigt and A. von dem Bussche, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International 2017.

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

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

White & Case, Unlocking the EU General Data Protection Regulation – Chapter 6: Data Protection Principles, available at < https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection>, accessed 28 October 2019.