2024

Draft Document

DELIVERABLE 1.4

THIS DOCUMENT IS IN DRAFT FORM AND PENDING OFFICIAL APPROVAL. IT IS SUBJECT TO REVIEW AND MAY BE UPDATED.

D1.4: REPORT ON LEGAL FRAMEWORK AND REQUIREMENTS

This project has received funding from the European Union's Horizon Research and Innovation Actions under Grant Agreement № 101093216.

Title: D1.4 – Report on Legal Framework and Requirements	Document version:
	0.3

Project number:	Project Acronym	Project Tittle
101093216	UPCAST Project	UPCAST Project

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type*-Security*:
M18 (June 2024)	M18 (June 2024)	R – PU

*Type: P: Prototype; R: Report; D: Demonstrator; O: Other; ORDP: Open Research Data Pilot; E: Ethics, DEC —Websites, patent filings, videos, etc

**Security Class: PU: Public; PP: Restricted to other program participants (including the Commission); RE: Restricted to a group defined by the consortium (including the Commission); CO: Confidential, only for members of the consortium (including the Commission).

Responsible:	Organization:	Contributing WP:
Andrea Palumbo Peggy Valcke Viltė Kristina Dessers Alexandra Papageorgiou	KUL	WP1

Authors (organization):
Andrea Palumbo (KUL)
Alexandra Papageorgiou (KUL)

Abstract:
This report presents an overview of the law applicable to online platforms for data sharing and the legal implications of automated contracts. It assumes that UPCAST solutions may be used to enable the sharing of both personal and non-personal data, in different settings, and provides an overview of the relevant legal framework, as well as its applicative implications for the project. The report covers the EU data protection framework, legislative acts applicable to online platforms, the Data Act and the Data

Governance Act, relevant sectoral and technology-specific legislation, and provides observations on contract automation and the law relevant to UPCAST.

Keywords:

Data sharing, data sharing platform, artificial intelligence, online contracting, data protection, data processing, trade secrets and intellectual property

REVISION HISTORY

Revision:	Date:	Description:	Author (Organization)
V0.1	22.01.2024	Table of content	Andrea Palumbo (KUL)
V0.2	01.04.2024	First draft	Andrea Palumbo (KUL)
V0.3	31.05.2024	Second draft	Andrea Palumbo (KUL) Alexandra Papageorgiou (KUL)

This project has received funding from the European Union's Horizon Research and Innovation Actions under Grant Agreement Nº 101093216.

More information available at https://upcastproject.eu/

COPYRIGHT STATEMENT

INDEX

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

AEPD	Agencia Española de Protección de Datos (Spanish Data Protection Authority
AI	Artificial Intelligence
AIA	Artificial Intelligence Act
B2B	Business to Business
B2G	Business to Government
Charter	Charter of fundamental rights of the European Union
DA	Data Act

DGA	Data Governance Act
DIS	Data intermediation services
DMA	Digital Markets Act
DSA	Digital Services Act
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
GDPR	General Data Protection Regulation
GPAIMs	General-purpose Artificial Intelligence Models
IoT	Internet of Things
TSD	Trade Secrets Directive

1 Introduction

1.1 Introduction and purpose of the document

Deliverable D1.4, titled ''Report on legal framework and requirements'', aims to provide an overview of the law applicable to data sharing activities involving both personal and non-personal data, to the services enabling such activities, as well as fully automated contracts. This document aims to provide an overview with reference to the state of EU legislation as of the date of the planned deadline for its submission, i.e., 30 June 2024.

Once the relevant pieces of legislation have been identified and analysed, we followed the process of assessing their impact on UPCAST, providing recommendations where appropriate. The impact on UPCAST is assessed taking into account the nature of the technologies under development and their specific intended use in the Pilots of the project. The use of the technologies under development in cases beyond the Pilots was also taken into account, where appropriate, in order to assess the overall legal soundness of the project and its relevance for a potentially wider range of applications.

Deliverable D1.4 should not be considered in isolation, as it complements and draws inspiration from other deliverables.

- First, it partially builds on the observations already provided on the EU legal framework in Chapter 7, titled "Legal framework and requirements'' of deliverable D1.1 titled 'Project concept requirements setup'.
- Second, it complements the analysis carried out in the context of deliverable D4.4, titled 'Contractual clauses legal assessment report v1', which provides an overview of the restrictions to contractual freedom for data sharing agreements stemming from EU law.
- Third, it complements, and will be further complemented by, deliverable D4.6, titled Contractual clauses legal assessment report v2', which will further expand the preliminary considerations provided in Chapter 6 of this deliverable on contract automation and the law.
- Fourth, it complements and supports the work to be carried out in the context of task 4.3 on AI assessment, for which legal input will be provided on the basis of the considerations advanced in this deliverable on the new EU legislation on artificial intelligence. Finally, this deliverable has a central role to play for all the other tasks of the UPCAST project on the development of technical solutions, as it aims to guide partners in ensuring compliance with EU law in the performance of their work under the Grant Agreement.

1.2 Scope and methodology of the document

The scope of this deliverable is limited to the EU legal framework that can apply to the deployment of UPCAST technologies after the completion of the project. National law of the Member States of the EU is thus not under scope, with the sole exception of Chapter 6 on contract automation and the law where the national provisions on contract law of certain EU Member States are summarised in order to provide an overview of the potential differences among national contracts laws at the EU level.

With regard to EU law, this deliverable takes into account all the relevant binding instruments and sources of EU law into force at the date of submission of the deliverable,

with the exception of the proposal on a regulation on artificial intelligence[1], which is addressed in this document despite the fact that it has not yet entered into force.

The instruments under scope include the Treaties, the Charter of fundamental rights of the European Union (hereinafter "Charter")[2], the general principles of EU law, EU directives, regulations and decisions, whether they constitute legislative, delegated or implementing acts, as well as any relevant non-binding instruments, such as recommendations, opinions and communications that may provide interpretive guidance in relation to binding EU law. Moreover, the relevant case-law of the Court of Justice of the European Union (hereinafter the "ECJ") where appropriate to provide interpretive guidance on the provisions of EU law in the scope of this deliverable.

This deliverable has been drafted by conducting doctrinal legal research, integrating where appropriate knowledge and insights provided by scholars from the discipline of computer science. As part of the doctrinal legal research, descriptive, explanatory, evaluative and recommendatory legal research methods have been employed to draft. The relevant EU legal framework has been the object of descriptive and explanatory research, and it has been relied on as the assessment framework for evaluative and recommendatory research.

The first version of the table of contents for this document contained a chapter on contract automation and the law, where several legal aspects related to the status of automated and smart contracts in EU law as well as their impact on UPCAST, would have been analysed. For reasons of efficiency, and by taking into consideration that the matter is partially addressed in D4.4 and will be exhaustively addressed *in toto* in deliverable D4.6., this chapter was retained only to provide exclusively high-level observations relevant to UPCAST.

[1] Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final of 21.4.2021.
[2] Charter of Fundamental Rights of the European Union (OJ C 202, 7.6.2016, pp. 389–405).

2 The EU Legal Ecosystem on Data

2.1 The strategy of the European Commission on data and data sharing

In the span of the last 10 years, there has been a sharp increase in political and policy attention, on the part of the European Commission, towards the **regulation of data processing activities**, the **digital single market**, and **emerging technologies** in general. Many legislative proposals have been proposed and adopted on these matters, leading to the creation of a complex legal framework governing the use of technologies as those under development in UPCAST. The adoption of *ad hoc* rules for the data economy has been part of the agenda of the European Commission since **2014**, when it published a **Communication**[3] pledging the creation of a single market for big data and cloud computing. In this context, the European Commission affirmed that data is at the centre of the future knowledge economy and society and 'open data' (i.e. data made freely available for re-use to everyone for both commercial and non-commercial purposes) in particular will play a significant role in data-driven innovation[4].

The European Commission continued to pursue its objective to create a legal framework for the data economy in the following years, setting out a more articulate policy agenda in its subsequent **Communication of 2017**[5].

In **2018**, the European Commission elaborated its **agenda for the data economy**, and data sharing activities in particular. In its Communication on common European data spaces[6], the European Commission outlined the objective to foster the development of "*a seamless digital area with the scale that will enable the development of new products and services based on data*". Besides announcing the review of the Directive on the re-use of public sector information, this Communication was accompanied by another document titled "**Guidance on sharing private sector data**"[7]. The Guidance recognises the importance of access to, and re-use of, private sector data as a cornerstone of common European data spaces, and sets out key principles that should guide contractual arrangements for business-to-business (hereinafter "B2B") and business-to-government (hereinafter "B2G") data sharing.

As concerns **B2B data sharing**, the European Commission set out the following principles:

- Transparency on the actors, the types of data and the purposes of using the data;
- Recognition of shared value creation where several parties have contributed to creating the data;

[3] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Towards a thriving data-driven economy', 2 July 2014, COM (2014) 442 final.
[4] Ibid.
[5] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Building a European Data Economy', 10 January 2017, COM (2017) 9 final.
[6] Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Towards a common European data space', 25 April 2018, COM (2018) 232 final.
[7] Commission, 'Staff Working Document – Guidance on sharing private sector data in the European data economy – Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Towards a common European data space', 25 April 2018, COM (2018) 125 final.

- Respect for the protection of commercial interests and secrets of data holders and data users;
- Ensure that competition is not distorted when exchanging commercially sensitive data;
- Minimise data lock-in, by enabling data portability as much as possible.

With regard to **B2G data sharing**, the Guidance outlines the following principles:

- Ensuring that the proportionality principle is respected when governments request private sector data (e.g. the request should be adequate and relevant to the intended public interest purpose);
- Purpose limitation;
- Respect for the protection of trade secrets and other commercially sensitive information;
- Collaboration agreements should be mutually beneficial while acknowledging the public interest goal by giving the public sector body preferential treatment over other customers;
- Companies supplying the data should offer support to help assess the quality of the data for the intended purposes;
- Transparency about the parties to the agreement and their objectives.

Finally, the European Commission published in **2020** its Communication on a European strategy for data[8], presenting its vision for the creation of a single European data space, a single market for data, where personal as well as non-personal data are created, processed and shared within the EU, boosting growth and creating value.

In order to achieve this objective, the European Commission announced the introduction of new rules which would foster data flows within the EU and across sectors, fully respecting the EU rules and values, and would put in place fair, practical and clear rules for access to, and use of, data, with trustworthy data governance mechanisms.

This Communication is of fundamental importance for the purposes of this deliverable, as it constitutes the policy basis of some of the pieces of legislation that will be analysed below. The strategy presented in the Communication rests on four pillars:

1. A cross-sectoral governance framework for data access and use;
2. Investments in data and strengthening Europe's capabilities and infrastructures for hosting, processing and using data, interoperability;
3. Competences: empowering individuals, investing in skills and in SMEs;
4. Common European data spaces in strategic sectors and domains of public interest.

2.2 Building blocks of the EU legal framework relevant to the deployment of technologies enabling data sharing

The EU legal framework currently in force that is of relevance to data sharing activities, be it personal or non-personal data, can be described as composed of building blocks, i.e. as grouped in different categories based on the types of provisions and underlying rationale. This deliverable addresses each of these building blocks separately, in order to provide an organic overview of the relevant EU legal framework.

First, there are the provisions on **data protection**. These apply only to activities involving the processing of personal data, subject to the exclusions set out therein. It is important

[8] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European Strategy for data', 19 February 2020, COM (2020) 66 final.

to note that most data protection provisions also apply to mixed datasets, i.e. datasets containing both personal and non-personal data, as is explained below. Chapter 3 is dedicated to EU data protection law.

Second, there are pieces of legislation that apply to **platforms**, i.e. providers of services that have an intermediation role in digital settings, such as those that intermediate in the transmission and storage of information. These are addressed in Chapter 4, in the sections dedicated to the Digital Services Act and the Digital Markets Act.

Third, there are provisions that apply specifically to **data sharing activities**, and set out rules on several aspects, including the re-use of data and the provision of services that enable data sharing between a data provider and a data recipient. These are addressed in Chapter 4, in the sections dedicated to the Data Governance Act and the Data Act, and in Chapter 5 in the section on the Open Data Directive.

Fourth, there is one technology-specific piece of legislation, the upcoming Regulation on artificial intelligence, which regulates the **development and deployment of artificial intelligence systems and models**. There is a section dedicated to this Regulation in Chapter 5.

Fifth, there are pieces of legislation that do not regulate data processing per se, but **protect certain interests in the data**, be it intellectual property rights or commercial interests in the form of trade secrets and are thus relevant for data sharing activities. These are discussed in Chapter 5.

Finally, insofar as data sharing takes place through contractual arrangements, national and EU provisions setting out restrictions and conditions on **contract formation and execution** are also relevant. This is addressed in Chapter 6 of the deliverable.

3 EU Data Protection Law

3.1 The main sources of EU data protection law

3.1.1 Fundamental rights to privacy and data protection

At the apex of the sources on the right to data protection, there is the Charter. The Charter is a primary source in the EU legal order, at the same level of the Treaties, and shall thus function as interpretive guidance for the application of EU secondary law and other lower sources of EU law. The Charter enshrines the fundamental **right to data protection** in its Article 8, where it states that everyone has the right to the protection of personal data concerning him or her.

While the great majority of the provisions governing the conditions for the processing of personal data are set out in the **Regulation (EU) 2016/679** (commonly known as the General Data Protection Regulation, hereinafter "**GDPR**"[9]), Article 8 of the Charter already specifies that personal data must be: i) processed fairly, ii) for specified purposes, iii) based on the consent of the person concerned or on another legitimate basis laid down in the law. These three conditions are equally laid down in the GDPR, where they are further specified and complemented with more detailed rules. Moreover, Article 8 of the Charter states that everyone can access the data that has been collected concerning him or her, and the right to have it rectified, thus laying down the foundations of the data subjects' rights that are better outlined in the GDPR.

Further to the right to data protection, which is the milestone of EU data protection law, the Charter enshrines another right of relevance to data protection: the **right to respect for private and family life, home and communications**. The right to privacy has overlaps with the right to data protection, as they both aim to protect the autonomy of individuals as independent beings, protecting their private physical and psychological sphere. Information privacy, as protected by the right to data protection, contributes also to the protection of the privacy of individuals. However, the two rights are both overlapping and distinct, as they have both distinct and common elements and objectives[10]. Consequently, on the one hand, there may be interferences with the right to privacy that do not restrict the enjoyment of the right to data protection, as is the case for interferences with the privacy of the home and correspondence that do not entail the processing of personal data[11]. On the other hand, there may be violations of the right to data protection that do not interfere with the right to privacy, which would be the case when one's personal data are being processed on one's request[12].

3.1.2 EU horizontal secondary law on data protection: the GDPR

The GDPR is the most important EU secondary legislation on data protection, due to its:

[9] 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) (Text with EEA relevance).
[10] M. Hildebrandt, 'Privacy and Data Protection', Law for Computer Scientists and Other Folk (2020) Oxford Academic.
[11] Ibid, p. 131.
[12] Ibid, p. 131.

i) horizontal applicability of the regulation which applies to almost all processing activities of personal data, irrespective of the sector and the nature of the activity that processing applies to, with only a few exceptions[13],

ii) comprehensiveness and far-reaching impact, which sets out detailed requirements for the processing of personal data.

The GDPR has a clear connection with the fundamental right to data protection, as made explicit in Article 1 where it is stated that the Regulation protects the fundamental rights and freedom of natural persons, and in particular their right to the protection of personal data[14]. Therefore, the GDPR can be seen as the piece of secondary legislation that **particularises the application of the right to the protection of personal data in the Charter**, by specifying how it should be respected in practice and how it should be balanced against other protected interests, such as the freedom to conduct a business, freedom of expression and public interests. The GDPR contributes also to the respect of the fundamental right to privacy enshrined in the Charter, by protecting the informational privacy of natural persons.

The GDPR provides the main framework governing data subjects' rights and obligations for entities processing personal data. It contains **harmonised rules on data protection**, although certain substantive and procedural matters are still within the competences of national data protection law. It applies to **all processing operations of personal data** carried out **wholly or partially by automated means**, as well as to the processing operations conducted by **non-automated means** which form part of a filing system or are intended to form part of a filing system[15].

3.1.3 EU vertical secondary law on data protection: the ePrivacy Directive

The Directive 2002/58/EC on privacy and electronic communications (commonly known as the "ePrivacy Directive")[16] is an EU legal act that complements and particularises the data protection requirements laid down by the GDPR (and previously the Data Protection Directive 1995/46/EC) for the electronic communications sector[17]. Contrary to the GDPR, the ePrivacy Directive **does not have a general scope of application** to all the processing activities involving personal data. In particular, the ePrivacy Directive applies **only to the processing of personal data in the electronic communication sector**[18], i.e. when personal data is processed by providers of publicly available electronic communications services in public communications networks in the EU[19]. According to case-law, a service must be considered publicly available when any part of the public

[13] Exceptions to the scope of application of the GDPR are described in Article 4 (2) and (3,) of the GDPR.
[14] See Article 1(2) of the GDPR.
[15] See Article 2(1) of the GDPR.
[16] 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 OJ L 201, 31.7.2002.
[17] Article 1(1)-(2) of the ePrivacy Directive, to be read in light of article 94(2) GDPR.
[18] Article 1(1) of the ePrivacy Directive reads as follows: "*This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.*"
[19] Article 3(1) of the ePrivacy Directive reads as follows: *"This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community"*.

may choose to make use of the service offered[20]. Even if a service is made available only to the subscribers of a particular undertaking, it is considered to be publicly available where there is no limit placed on the number of potential subscribers and any part of the public may, de facto, make use of the service by becoming a subscriber.

The ePrivacy Directive contains high-level provisions on several aspects, from security and confidentiality of communications to the processing of location data and other traffic data, to the storage of information in the terminal equipment of a subscriber or user and unsolicited communications. For the purposes of this document, only certain provisions of the ePrivacy Directive are to be considered as relevant.

First, the security obligation in **Article 4** of the ePrivacy Directive is to be considered due to its relevance for technologies that enable data-sharing which must ensure that the requisite level of security is provided. Article 4 of the ePrivacy Directive requires providers of publicly available electronic communications services to take appropriate technical and organisational measures to safeguard the security of their services, if necessary, in conjunction with the provider of the public communications network with respect to network security.

Second, **Articles 6 and 7** of the ePrivacy Directive are relevant because they lay down conditions for the processing of certain categories of personal data. According to Article 6, traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. In relation to location data other than traffic data, Article 7 of the ePrivacy Directive states that, when it relates to users or subscribers of public communications networks or publicly available electronic communications services, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service[21].

As mentioned above, **the GDPR and the ePrivacy Directive are legislative texts with an evident overlap in scope of application**. On the one hand, the GDPR lays down rules for the protection of data subjects' fundamental rights in relation to the processing of their personal data, with a broad scope of application that covers almost every processing operation of personal data. On the other hand, the ePrivacy Directive particularises personal data protection rules for the specific context of the processing of personal data in publicly available electronic communications networks.

In principle, both the GDPR and the ePrivacy Directive apply to the processing of personal data in connection with the provision of publicly available electronic communications services. This leads to an overlap in the material scope of the two legislations, as explicitly recognised by the EDPB[22]. In some cases, the ePrivacy Directive and the GDPR converge towards the imposition of essentially the same requirements, whereas in other cases the ePrivacy Directive supersedes the GDPR by virtue of the principle *lex specialis derogate legi generali*.

[20] Case E-6/16 of the EFTA Court Fjarskipti and Icelandic Post and Telecom Administration [2016], para. 56.

[21] Article 2(1)(g) of the ePrivacy Directive defines a value-added service as any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof.

[22] European Data Protection Board (EDB), Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, 2019.

For the purposes of this document, it must be noted that processing operations in publicly available electronic networks are subject to the security requirements of both the GDPR and the ePrivacy Directive, and that these requirements substantially coincide under the two legislative texts. Article 32 of the GDPR and Article 4 of the ePrivacy Directive formulate the security obligation in a similar manner, as they both require to take ''appropriate technical and organizational measures'' that must be determined based on the state of the art and the cost of their implementation, and to ensure a level of security appropriate to the risks presented. There is a difference lying in the fact that Article 4 of the ePrivacy Directive specifies a minimum standard of security that must in any case be ensured, by listing a series of measures that shall always be adopted. However, this difference is likely not to persist in practice, as the level of protection reflected in these measures is very basic and should certainly be respected by controllers and processors under the GDPR as well, irrespective of the circumstances of the case.

Overall, it can be said that the combined framework of the GDPR and the ePrivacy Directive prescribes security requirements that are either equivalent or coincide to some extent.

3.2 Key Data Protection Requirements Relevant to UPCAST

3.2.1 Introductory considerations

The EU data protection framework is of primary relevance to UPCAST, as the UPCAST architecture would most likely entail the processing of personal data, especially in the context of the Pilots. This especially the case for the Pilots on digital marketing data and resources, on biomedical and genomic data sharing, and on health and fitness data trading, where sensitive data is to be processed that falls under one of the special categories of personal data of Article 9 of the GDPR.

The GDPR presents a complex legal framework, which cannot be exhaustively addressed in this chapter. Sections 3.2.2. to 3.2.5. provide an overview of the most relevant provisions of GDPR, while Section 3.2.6. explains how these requirements would apply, and thus how would they need to be respected, in the context of the UPCAST project.

3.2.2 Notion of 'personal data'

3.2.2.1 Legislative definition

Since the material scope of application of the GDPR is limited to the processing of personal data, the identification of personal data is a fundamental step to be carried out to assess the applicability of the GDPR for a given processing operation.

Article 4(1) GDPR defines personal data as follows:

> "*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*".

The definition of GDPR must be complemented with the Opinion 04/2007 on the concept of personal data provided by the Article 29 Working Party (the 'A29WP')[23], that has been endorsed by the European Data Protection Board (the 'EDPB'). EDPB provided a

[23] Article 29 Working Party (A29WP), Opinion 04/2007 on the concept of personal data, WP 136, 2007.

breakdown and description for the four elements that compose the definition of personal data: 'any information'; 'relating to'; 'an identified or identifiable'; 'natural person'. The blocks are described as follows:

a) '**any information**': must be interpreted broadly
   - Regarding the nature of the information: the concept of personal data includes any sort of statements about a person. It covers "objective" information, such as the presence of a certain substance in one's blood. It also includes "subjective" information, opinions or assessments;
   - Regarding the content of the information: the concept of personal data includes data providing any sort of information. It covers sensitive data but also information touching the individual's private and family life "*stricto sensu*", but also information regarding whatever types of activity is undertaken by the individual;
   - Regarding the format of the information: personal data can take any form, be it alphabetical or numerical data, as well as information stored on videos and pictures.

b) '**relating to**': important to precisely find out which are the relations and/or links that matter and how to distinguish them. Personal data is information that is, by reason of its content, purpose of effect, linked to a particular person.
   - Regarding the content of information: information "relates" to a person when it is "about" that person;
   - Regarding the purpose of information: the data are used or are likely to be used, taking into account all the circumstances surrounding the precise case, with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual;
   - Regarding the result (effect) of information: data can be considered to "relate" to an individual because their use is likely to have an impact on this individual's rights and interests, taking into account all the circumstances surrounding the precise case.

- '**an identified or identifiable natural person**':
   - Identified: a natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group;
   - Identifiable: a natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it. 'identifiability' is in practice the threshold condition determining whether information is within the scope of the third element 'an identified or identifiable [natural person]'.
- '**natural person**': the GDPR does not apply to legal persons or deceased natural persons.[24]

3.2.2.2 The distinction between personal data, pseudonymous personal data and anonymous data

This section is focused on the distinction between personal data, pseudonymous personal data, and anonymous non-personal data.

[24] However, the ECJ has clarified in its decision on the cases, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, that "*Legal persons can thus claim the protection of Articles 7 and 8 of the Charter only in so far as the official title of the legal person identifies one or more natural persons. That is the case where the official title of a partnership directly identifies natural persons who are its partners.*" Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen [2010] ECLI:EU:C:2010:662, pt. 51.

3.2.2.2.1 Pseudonymous data

Pseudonymous data is a legal concept described in the GDPR, on which guidance has been provided by both WP29 and EDPB guidelines, and in the case law of the ECJ. Anonymous data is not a legal concept defined in the GDPR, but it is referred to in the recitals of the GDPR and guidance on it has been provided by WP29, the EDPB, the EDPS and the case-law of the ECJ.

Pseudonymous data is personal data within the meaning of the GDPR that has been subject to pseudonymisation. Pseudonymisation is defined by Article 4, point 5) of the GDPR as:

> *'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.*

Therefore, pseudonymous data remains personal data due to the fact that the data subject it refers to remains identifiable with the use of additional information.

There are **multiple techniques** that can be used to achieve pseudonymisation of a dataset[25]. Encryption is a classic example of pseudonymisation techniques, as it leads to the transformation of the personal data in plaintext into a ciphertext that acts as pseudonym. Encrypted data is pseudonymous data because, once the data in plaintext has been encrypted, the link to an identity can be re-established by combining the ciphertext (i.e. the encrypted data) and a decryption key. The ciphertext as such may not enable the identification of the data subjects that it refers to, but with the use of a decryption key it is possible to reverse the pseudonymisation process and turn the ciphertext into the original plaintext again, thus allowing whoever has the encryption key to re-identify the data subject(s).

A condition of the legislative definition of pseudonymous data is that the additional information needed to re-identify the data subject is kept separately and protected by means of technical and organisational measures. If this information is attached to the ciphertext, the data cannot qualify as pseudonymous because identification of the data subjects is as easy as it would be with the plaintext.

Therefore, it can be said that pseudonymous data differs from personal data with regard to at least two elements: i) the de-identification of the data subjects that the personal data refers to, ii) the fact that any additional information needed to re-identify the data subjects is not readily available to whoever has access to the data.

3.2.2.2.2 Anonymous data

Anonymous data is, by its very nature, **non-personal data** within the meaning of the GDPR. While there is no legislative definition of anonymous data, the concept of anonymous data can be inferred *a contrario* from the definition of personal data, as anonymous data is any data that is not personal. In this regard, Recital 26 of the GDPR provides a conceptual definition of anonymous data as *''information which does not relate to an identified or identifiable natural person"* or as originally personal data that was *'rendered anonymous in such a manner that the data subject is not or no longer*

[25] These include indicatively techniques such as the counter, random number generator (RNG), cryptographic hash function, message authentication code (MAC), encryption. European Union Agency for Cybersecurity (ENISA), Pseudonymisation techniques and best practices – Recommendations on shaping technology according to data protection and privacy provisions. November 2019.

identifiable'[26]. Therefore, the criteria on identifiability of natural persons laid down in the GDPR, and in the relevant guidance by the ECJ and the EDPB, should be used to determine whether a given piece of information enables or not the identification of data subjects, and if it can thus be considered personal or anonymous data. The most important guidance provided by the GDPR on the concept of identifiability of natural persons can be found in Recital 26, there it is stated that

> "*to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly*. *To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*.

This entails that, as also endorsed by WP29 in its Opinion on the concept of personal data, the mere hypothetical possibility to single out a person is not sufficient to qualify that person as identifiable, but it must be proved that the identification is practically possible in the circumstances of the case, taking into account the means that the controller or another person can be reasonably expected to use.

The **"means reasonably likely to be used" test** is thus central for the determination of whether information is anonymous under the GDPR. The ECJ interpreted this test in its famous Breyer case[27], by clarifying that, in the context of dynamic IP addresses, it is not necessary that all the information enabling identification is in the hands of the same person, but it may suffice that a single person has the means to access all the information needed to identify the data subjects. The Court concluded that **dynamic IP addresses** were deemed to be personal data from the perspective of online media service providers, who could rely on legal means to obtain the required additional information held by internet service providers to identify the natural person to whom a dynamic IP address relates[28].

Important clarifications, both conceptual and practical, on anonymous data have been provided by the Spanish Data Protection Authority (hereinafter, the ''AEPD'') and the European Data Protection Supervisor (hereinafter, the "EDPS") in their joint paper on 10 misunderstandings related to anonymisation.[29]

The first clarification of fundamental practical importance is that **for data to be anonymous the risks of re-identification do not need to be zero**. The EDPS and the AEPD stated that a residual risk of re-identification is possible and does not prevent the data to qualify as anonymous. An anonymisation process aims to reduce the re-identification risks below a certain threshold, and this threshold will depend on multiple factors such as: i) existing mitigation controls, ii) the impact on individuals' privacy in the event of re-identification, iii) the motives and capacity of an attacker to re-identify the data. This criterion, however, presents the challenge of determining, on a case-by-case basis, which threshold of identifiability close to zero is accepted for data to qualify as anonymous.

The second important clarification is that **data qualifying as anonymous at a given time may not be anonymous in the future**. Anonymisation may not be a permanent status

[26] See Recital 26 and Articles 6(1) and 9(1) of the ePrivacy Directive, which refer to the notions of anonymization and anonymous data in a similar way.
[27] Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779.
[28] Ibid, pt. 48.
[29] Agencia Española de Protección de Datos & European Data Protection Supervisor, "10 misunderstandings related to anonymisation", 27 April 2021.

and can be subject to changes over time. For instance, technological advancements could increase the risks of re-identification. For this reason, the data controller shall adequately monitor technological or other developments that could affect the risks of re-identification of a data subject from a dataset.

In light of the above, it can be noted that the **distinction between anonymous and personal data is a very factual assessment** that needs to take account of the means available to the data controller or another person to identify the natural persons based on the data.

The qualification of data as personal or anonymous is, as seen above, dependent on the identifiability of a data subject from the data itself, using the 'means reasonably likely to be used' criterion. The assessment on identifiability is evidently highly factual and its outcome would largely depend on the actor from whose perspective the availability of means reasonably likely to be used is assessed. The practical application of the test outlined in Recital 26 is not straightforward and raises questions that have occupied the ECJ in the last years. An important question regarding the concept of personal data, and thus of pseudonymous and anonymous data, concerns the point of view that must be taken to qualify certain information as personal data. In particular, the question is whether the criteria to consider data as personal, personal pseudonymous or anonymous must be applied solely from the perspective of the controller or also from the perspective of other third parties.

The answer to this question has considerable consequences for the application of the GDPR in practice. For instance, if only the perspective of the controller is relevant, it follows that data pseudonymized by a controller and shared with another controller in pseudonymized form, without providing the second controller with the information necessary to re-identify the data subjects concerned, may be anonymous data from the perspective of the second controller. As a matter of fact, the second controller may not be in possession of means reasonably likely to be used to re-identify data subjects, if it cannot acquire those from the first controller or in other ways. If, on the other hand, the perspective of other persons is also to be taken into account, taking on an absolute rather than relative approach to the qualification of personal data, the data would be pseudonymous for the second controller in the example made above. The question of whether a relative or absolute approach should be taken under the GDPR has not yet received a definitive answer, even though the ECJ has taken a stance on it in the recent judgements on cases *SRB v. EDPS*[30] and *IAB Europe v. Gegevensbeschermingsautoriteit,*31 building on the criteria already outlined in Breyer.

An analysis of the judgements from *Breyer* to date shows that , while the ECJ did quite explicitly adopt the relative approach at some point, it also released judgements where this stance is not as evident, and, on the contrary, that give rise to confusion in the line of reasoning followed. Nonetheless, it can be noted that the objective approach has not been affirmed to date as explicitly as the relative approach was in the cases *Breyer* and SRB v EDPS, with the consequence that the relative approach should be considered as the most convincing interpretive approach based on the case-law developed thus far.

3.2.2.3 Special categories of personal data

Within the larger category of personal data, the GDPR defines an additional, narrower sub-category of data that warrants enhanced protection due to the sensitive information that it can reveal about the data subjects that it refers to. In particular, Article 9 of the

[30] Case T-557/20 Single Resolution Board (SRB) v European Data Protection Supervisor (EDPS) [2023] ECLI:EU:T:2023:219.
[31] Case C-604/22 IAB Europe v Gegevensbeschermingsautoriteit [2024] ECLI:EU:C:2024:214.

GDPR imposes specific conditions for the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The processing of these data is in principle prohibited, but the prohibition is lifted if one of the conditions listed in Article 9(2) GDPR is fulfilled.

Among these conditions there is the explicit consent of the data subject, a range of public interests and compliance with legal obligations.

The special categories of personal data are of central importance in the context of UPCAST. First, the health and fitness data to be shared in Pilot 4 fall under this category. Second, the biomedical and genomic data in Pilot 2 would fall under this category insofar as it reveals genetic and health information about natural persons. Third, there might sensitive data also in the other Pilots, especially in Pilot 1 on digital marketing data where such data reveals sensitive personal opinions and habits. Further considerations on compliance with Article 9 in the context of the Pilots are provided below.

3.2.3 Data protection principles

3.2.3.1 Introduction

Article 5 of the GDPR sets out the principles governing the processing of personal data. These are:

- Data processing must be lawful, fair and transparent (**lawfulness, fairness and transparency**);
- Data must be collected for specified, explicit and legitimate purposes and not further processed for purposes other than specified (**purpose limitation**);
- Data must be adequate, relevant and limited to what is necessary in relation to the specified purposes for processing (**data minimization**);
- Personal data must be "accurate and, where necessary, kept up to date" (**accuracy**);
- Personal data must be stored only as long as it is necessary for the purpose of data processing (**storage limitation**);
- The security of personal data must be ensured "against unauthorised or unlawful processing and against accidental loss, destruction or damage" (**integrity and confidentiality**);
- The controller shall be responsible for, and be able to demonstrate compliance with, all the data processing principles (**accountability**).

3.2.3.2 Lawful grounds for personal data processing

According to Articles 5(1)(a) and 6 of the GDPR, the processing of personal data is lawful only if there is a legal ground that allows such processing. Article 6 of the GDPR exhaustively lists the legal grounds that can be relied on for the processing of personal data, and data controllers must be able to demonstrate that any processing of personal data takes place in accordance with one of these lawful grounds.

The notion of lawful ground refers to a legal basis that is needed to authorise the processing operation or set of operations envisaged by the data controller. Article 6 GDPR provides six lawful grounds:

1. Consent given by the data subject;
2. Necessity of processing for the performance of a contract;

3. Necessity of processing for compliance with a legal obligation;
4. Necessity of processing to protect vital interests;
5. Necessity of processing for the performance of a public interest task;
6. Necessity of processing for a legitimate interest.

There is no hierarchy among the lawful grounds of the GDPR, as they are in principle equally valid grounds for the processing of personal data. The applicability and convenience of a specific lawful ground depends on the specific circumstances of the processing.

Consent is the only legal basis that does not require a necessity assessment. All other legal bases require the controller to ascertain whether the intended processing is necessary to the aim at hand. Stricter conditions apply, as explained above, for the processing of special categories of personal data (so-called sensitive data) in accordance with Article 9 of the GDPR.

For the purposes of this report, the most relevant lawful grounds for the processing of personal data are consent and necessity of the processing for a legitimate interest. These grounds are of a more generalised application, as they can be relied on in a wide variety of cases, whereas the other grounds apply to more specific circumstances. Given the different contexts where UPCAST plugins may be used, they are potentially relevant for all contexts where deployment might take place.

When consent is collected in the context of the provision of a service, it is typically gathered from a user by requiring to accept the service's terms and conditions of the privacy policy.

Consent must be collected for each processing operation involving personal data. Even if the controller and the data subject are the same for multiple processing operations, consent must be given for each operation. In order to be correctly gathered, consent must be given in accordance with four conditions [32]. In particular, it must be:

a) freely given,

b) specific,

c) informed, and an

d) unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

When consent is collected in the context of the provision of a service, it is typically gathered from a user by requiring to accept the service's terms and conditions of the privacy policy.

Under the **principle of accountability**, the controller is responsible for ensuring that consent has been validly obtained, and has the duty to properly inform the data subject before collecting his or her consent. The data subject must be informed about the specific, explicit and legitimate purpose for the intended processing activity, so that the consent given is specific to the purpose of processing. The provision of information before collecting consent is essential to enable data subjects to make informed decisions and exercise their rights under the GDPR. Should the controller fail to properly inform data subjects, consent cannot be relied on as a valid basis for the processing[33]. The EDPB guidelines on consent clarify that the controller must provide at least the

[32] See Article 4(11) of the GDPR.

[33] European Data Protection Board (EDPB), Guidelines 05/2020 on consent under Regulation 2016/679', 4 May 2020, para 62.

following information to data subjects: i) the controller's identity, ii) the purpose of each of the processing operations for which consent is sought, iii) what (type of) data will be collected and used and iv) the existence of the right to withdraw consent[34].

Article 7(3) of the GDPR confers the data subject the right to withdraw his or her consent at any time. The data subject must be able to withdraw consent in a way that is as easy as providing consent was.

Regarding the ground of legitimate interests pursued, the existence itself must be carefully assessed in each specific case.[35] In its Opinion 06/2014, A29WP notes that, in case the controller of data claims the existence of legitimate interest for the processing of data, then a balancing exercise must be conducted between those interests and the interests or fundamental rights of the data subject.[36] The notions of accountability and transparency, as well the data subject's right to object to the processing of their personal data, play an especially crucial role, in this case[37]. In view of those considerations, whenever personal data is being processed under the "legitimate interests" ground, the individual has the right to object at any time to the processing, for one of the reasons mentioned in Article 21 GDPR.

3.2.3.3 Fairness and transparency

Fairness and transparency are two data processing principles that are **closely intertwined**, despite still being distinct principles, laid down in Article 5(1)(a) GDPR. First, according to the fairness requirement, personal data have to be processed in a manner that would be expected by data subjects.

The connection with the transparency requirement derives from the fact that data subjects must be properly informed about the envisaged processing operations, and information must be presented to them in a clear and unambiguous manner, in order to ensure that the actual processing is line with their expectations. Under no circumstance should processing operations be performed in secret; it should be also ensured that data subjects are aware of the risks that may arise.[38] For example, manipulative practices that aim at 'tricking' the data subject into providing consent for the processing of their personal data, e.g. by employing so-called 'dark patterns', would be contrary to the principle of fairness. Dark patterns can induce data subjects to mistakenly consent to processing operations whose implications they have not fully understood.

Transparency is an important building block of European data protection law. It grounds data controllers' transparency duties under Articles 13 and 14 GDPR, and is a necessary precondition for data subjects to exercise their rights under the GDPR. The EDPB has provided guidance on how to comply with fairness and transparency by design and by default[39].

3.2.3.4 Purpose limitation

The purpose limitation principle is enshrined in Article 5(1)(b) GDPR. This principle requires that personal data is collected for specified, explicit and legitimate purposes

[34] Ibid, paras 64-65.
[35] See Recital 47 of the GDPR.
[36] Article 29 Working Party (A29WP), 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', 2014.
[37] Ibid.
[38] European Union Agency for fundamental rights, European Court of Human Rights, Council of Europe & European Data Protection Supervisor, 'Handbook on European data protection law', 2018, p. 118.
[39] European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default'', 2019, pp. 15-19.

and not further processed in a manner that is incompatible with those purposes. The rationale of purpose limitation is to prevent a processing of personal data for purposes that the data subjects would find unexpected, inappropriate or objectionable. For example, where data subjects consent to the processing of their personal data for a specified purpose, purpose limitation ensures that such processing takes place in a way that is expected and compatible to the purpose for which consent was given.

The purpose limitation principle is made of two components: **purpose specification** and **compatible use**. Purpose specification requires that personal data is processed only for specified, explicit and legitimate purposes, whereas compatible use prevents to further process personal data in a manner that is incompatible with the original purpose(s) for which it was initially collected. In the latter case, Article 5(1)(b) has to be read conjointly with the provision of Article 6(4) GDPR. Every new purpose for the processing of data which is not compatible with the initial one, has to have its own legal basis. Article 6(4) GDPR stipulates that if the processing for the new purpose is not based on the data subject's consent, or an EU or Member State law, which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives under Article 23(1), the data controller must conduct a compatibility assessment. The factors that need to be taken account include, but are not limited to:

- any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
- the possible consequences of the intended further processing for data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

The EDPB has provided guidance on how to comply with purpose limitation by design and by default[40].

3.2.3.5 Accuracy

The accuracy principle is provided for in Article 5(1)(d) of the GDPR. It requires that "*personal data be accurate and, where necessary, kept up to date*". It also mandates that every reasonable step 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. The accuracy principle is connected to multiple data subjects rights that enable its respect in practice. These are the right of access, the right to rectification and the right to restriction of processing, while there are more feeble connections also with other data subjects rights.

The EDPB has provided guidance on how to comply with the accuracy principle by design and by default.[41]

3.2.3.6 Integrity and confidentiality

One of the general principles governing personal data processing is integrity and confidentiality, of Article 5(1)(f) GDPR, which require that "*appropriate security of personal data is ensured during the processing, including against unauthorised or unlawful*

[40] Ibid, pp. 19-20.
[41] Ibid, pp. 23-25.

processing and against accidental loss, destruction or damage". Those two requirements constitute jointly the data security principle[42].

This data processing principle is connected with Article 32 GDPR, which lays down security requirements for the processing of personal data and therefore better clarifies how compliance with integrity and confidentiality can be ensured in practice. Both provisions require the implementation of appropriate technical and organisational measures to ensure security of the personal data, with the objective of preventing adverse effects for the data subject. The only difference lies in the fact that Article 32 extends the security requirements also to processors, whereas Article 5(1)(f) only applies to controllers. Article 32 is often regarded as a more practical specification of what the principle in Article 5(1)(f) entails, and the two provisions can be intended as imposing the same requirements.

The security obligations of the GDPR impose controllers and processors to, first, gauge the level of risks posed by the processing operation for data subjects and, taking into account the circumstances of the case (including, besides the risks, the state of the art, the characteristics of the processing and the costs of implementation), appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In this regard, it is important to note that this is an obligation of means, and not of results, with the consequence that, as long as risks have been assessed and appropriate measures have been implemented, there will be no infringement of Article 32, even when there is a data breach[43].

Article 32 of the GDPR provides a non-exhaustive list of measures that could be considered appropriate to ensure a level of security proportionate to the risks. These measures are:

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

To ensure compliance with the security obligations, the controller and the processor shall implement the appropriate measures by design and by default. In this regard, Recital 78 of the GDPR states that such measures could consist of "*enabling the controller to create and improve security features*".

The EDPB has provided guidance on how to comply with the security requirements in its Guidelines on Data Protection by Design and by Default[44].

3.2.3.7 Accountability

According to Article 5(2) of the GDPR, the "*controller shall be responsible for, and be able to demonstrate compliance with, the data processing principles of Article 5(1) of the GDPR*." Article 5(2) introduces the accountability principle, which is a cornerstone principle of the GDPR that vests in the controller the accountability for all the processing

[42] European Union Agency for fundamental rights, European Court of Human Rights, Council of Europe & European Data Protection Supervisor (n 40), p. 131.
[43] B. Van Alsenoy, ''Liability under EU Data Protection Law From Directive 95/46 to the General Data Protection Regulation'', JIPITEC, p. 284.
[44] European Data Protection Board (n 35), pp. 26-28.

operations under its control. This entails that, even when the processing is in practice carried out by a processor, the controller remains accountable for such processing insofar as it takes place under its instructions.

Moreover, another corollary of the accountability principle lies in the fact that the controller must be able to demonstrate compliance with the GDPR in relation to its processing operations, and is thus obliged to keep record of the evidence needed to this end. The record-keeping obligation is formalised in Article 30 of the GDPR, according to which each controller shall maintain a record of processing activities under its responsibility.

The EDPB has provided guidance on how to comply with the accountability principle by design and by default.[45]

3.2.4 Roles and responsibilities for personal data processing

3.2.4.1 Controllers, joint controllers and data processors

The assignment of roles and responsibilities in relation to the processing of personal data revolves around the concepts of ''controller'' and ''processor''. Controllers and processors are two categories of persons involved in the processing of personal data that, due to their different roles, are subject to different obligations and responsibilities under the GDPR. Therefore, it is essential to precisely determine which parties participating in data processing activities are acting as controllers and which parties as processors, in order to understand which obligations they are subject and how the respective roles and responsibilities should be arranged, including their contractual relationships. In complex data-sharing environments, such as the architecture of the UPCAST project, identifying controllers and processors is an essential starting point to understand how the GDPR should be complied with.

The first, and central, concept is that of the **controller**. The GDPR defines the controller in its Article 4(7) as

> *''any natural or legal person, public authority agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designed by national or Community law''*.

Based on the legislative definition, the controller can be described, in simple words, as the person or entity having control over the processing of the personal data, and which is also responsible for ensuring that such processing takes place in compliance with the GDPR.

This definition outlines the key criteria to identify the controller. In particular, the controller is the person or entity who determines the: i) purposes and, ii) the means of the processing of the personal data[46]. Based on these criteria, the assessment of controllership is expected to be a very factual assessment that looks at the substance of the relationships between the persons and entities involved in the processing of personal data.[47] Formal agreements in place between the relevant persons and entities

[45] Ibid, p. 28.

[46] European Data Protection Board, 'Guidelines 7/2020 on the concepts of controller and processor in the GDPR', 2 September 2020, section 2.1.4, p. 13

[47] In this case-by-case analysis, ECJ considers a broad definition of the notion of controller, in order to ensure an "effective and complete protection of the data subjects". Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [2014] ECLI:EU:C:2014:317.

are not a decisive factor if the factual situation reveals that the actual roles differ from what is formally agreed.

Regarding the application of the two criteria to assess controllership, two clarifications must be made. The first is that determining the means shall not be intended as determining any means for the processing of personal data, such as any technical means. The determination of the means should cover essential decisions on how the data should be processed. The EDPB guidelines make a distinction between essential and non-essential means[48]. Essential means, which are closely linked to the purpose and scope of the processing, is a decision to be taken by the controller, and relates to aspects such as the type of personal data to be processed, the duration of the processing, the categories of recipients and data subjects[49]. Non-essential means relate to more practical aspects of implementation, such as organisational and technical measures, and they should be regarded as choices to be made by the processor. Examples include the choice for a particular type of hard- or software or the detailed security measures to be implemented[50].

Joint controllership is an additional concept defined in Article 26 of the GDPR. It refers to the situation where two or more controllers jointly determine the purposes and means of processing. In this case, they are joint controllers. Joint controllership is assessed in relation to each processing operation, taking into account the factual situation, as is the case for the controllership assessment[51]. Importantly, there is joint controllership when both the purposes and the means of the processing are jointly determined, whereas the joint determination of only one of the two does not qualify as joint controllership[52].

Joint participation in determining the purposes and means of the processing entails taking a common decision or having converging decisions[53]. In the latter case, while there is no common intention, there are separate decisions complementing each other and leading to a situation where the contributions by each party in the processing are inextricably linked, and are each necessary for the processing to take place[54].

As clarified by the ECJ in cases *Fashion ID*[55] and *Wirtschaftsakademie*[56], it is not necessary that the controllers have exactly the same purpose for the processing, it suffices that the purposes are closely linked or complementary. Similarly, joint determination of the means does not require that all the parties determine all the means jointly, as it suffices that the different controllers decide on different means to be used in different stages, complementing each other[57]. There is also joint controllership where one party provides the means of the processing and makes it available for personal data processing activities by other entities[58].

Regarding the legal regime applicable to joint controllers, the GDPR requires that they agree on their respective responsibilities on how to comply with the obligations under

[48] Ibid.
[49] Ibid, para. 38.
[50] Ibid.
[51] Ibid, para. 49.
[52] Ibid, para. 50.
[53] Ibid, para. 51.
[54] Ibid, para. 53.
[55] Case C-40/17, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV. [2019], ECLI:EU:C:2019:629.
[56] Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH [2018], ECLI:EU:C:2018:388.
[57] European Data Protection Board (EDPB), 'Guidelines 7/2020 on the concepts of controller and processor in the GDPR', 2 September 2020, paras. 61-63.
[58] Ibid.

the GDPR, namely concerning the exercise of data subjects' rights and the duties to provide information[59]. There is no requirement that such arrangement be formalised in a written contract, even though it may be desirable to increase legal certainty. The main aspects of the arrangement made must be made available to data subjects so that they know which of the controllers is responsible for what, and joint controllers can designate in the arrangement a contact point for handling data subjects' requests[60]. Nonetheless, data subjects are not bound by this and remain free to contact either of the joint controllers to exercise their rights under the GDPR[61].

Finally, the GDPR describes the role of processors as the third main category of parties involved in the processing of personal data. The processor is a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller[62]. Two characteristics define who can qualify as a processor: i) being a separate entity in relation to the controller, and ii) processing personal data on the controller's behalf.

The GDPR requires that processing by a processor be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller[63]. While most of the obligations under the GDPR are imposed on controllers, there are some provisions that apply also to processors, such as those on security of the processing[64] and record-keeping[65].

3.2.4.2 Preliminary considerations on the UPCAST platform

As the UPCAST plugins can be used in different contexts and for different purposes, the qualification of the relevant actors as controller and processors is contextual. The fact that a person or entity deploys the UPCAST plugins does not allow to draw definitive conclusions on the role played by that person or entity. This person or entity may qualify as a separate controller for the data processing operations taking place, or as joint controller for all or some of these operations, or as a mere processor insofar as the plugins act as technical infrastructure for enabling the processing.

With the disclaimer that an assessment on the role played in relation to data processing must be carried out in the specific circumstances where the plugins are deployed, an assessment is carried out in Section 3.2.7.2. in relation to each of the Pilots. This assessment should guide the partners in ensuring compliance with the GDPR during the Pilots, as well as provide practical examples of how controllership is to be assessed in practical cases where the plugins are deployed.

3.3 Data subject rights

Data subjects are conferred multiple rights under the GDPR, whose enjoyment is functional to the effective protection of their right to data protection. Data subject rights are provided for in Articles 15 to 22 of the GDPR. The controller is under an explicit obligation to facilitate the exercise of data subject rights, as provided in Article 12(2) of the GDPR. This obligation entails that the controller needs to put in place mechanisms that enable the exercise of data subjects rights, as well as to ensure that the technical

[59] See Article 26(1) of the GDPR.
[60] See Article 26(2) of the GDPR.
[61] European Data Protection Board (EDPB), (n 57), paras. 184-187.
[62] See Article 4(8) of the GDPR.
[63] See Article 28(3) of the GDPR.
[64] See Article 32 of the GDPR.
[65] See Article 30(2) of the GDPR.

and organisational measures in place do not hinder the exercise of such rights. When data is processed by automated means, this would entail to ensure that the technical and organisational solutions in place effectively enable certain operations needed for the exercise of data subjects rights. For instance, the right to erasure would require the technical feasibility of erasing data whenever the necessity arises. Whether data subjects' rights can be exercised in practice must be assessed on a case-by-case basis, taking into account the circumstances of each data processing operation.

More specifically, the controller must facilitate the exercise by data subjects of their rights of access, to rectification, to erasure, to restriction of processing, to data portability, to object and not to be subject to automated individual decision-making.

The content of the rights conferred by the GDPR on data subjects can be summarised as follows:

- **Right of access**: the right of access of Article 15 grants the data subject a right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and to information on the purposes of the processing and the categories of personal data processed[66];
- **Right to rectification**: the right to rectification of Article 16 confers data subjects the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her[67];
- **Right to erasure**: according to Article 17, the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the grounds listed in Article 17(1) applies[68];
- **Right to restriction of processing and to object**: Articles 18[69] and 21[70] provide, respectively, for the right of the data subject to demand the restriction of processing and to object to the processing at the conditions specified in the Articles;
- **Right to data portability**: According to Article 20, the data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, at the conditions specified in the Article[71];
- **Right not to be subject to automated individual decision-making**: According to Article 22, the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her[72].

Table 1 lists legal requirements relating to the various rights of data subjects.

Table 1. Requirements relating to data subject rights

Requirement	Observations

[66] See Article 15(1) of the GDPR.
[67] See Article 16 of the GDPR.
[68] See Article 17(1) of the GDPR.
[69] See Article 18(1) of the GDPR.
[70] See Article 21(1) of the GDPR.
[71] See Article 20(1) of the GDPR.
[72] See Article 22(1) of the GDPR.

Data subjects shall always be provided with the identity and contact details of the data controller and, where applicable, the Data Protection Officer (DPO).	This information shall be clearly mentioned in the terms & conditions and in the privacy policies of data controllers.
Data subjects shall always be informed about the purposes and lawful ground of the processing.	Same as above.
Data subjects shall always be informed about the categories of personal data processed.	Same as above.
Data subjects shall be informed if the controller intends to transfer personal data to a recipient in a third country.	Same as above. Particularly relevant to Pilot 4 (led by NIS) insofar as it envisages the transfer of health-related data to third countries for processing. The privacy policy shall be internally coherent and make sure to ask for the data subjects' consent to carry out such transfers. The data protection conditions of the countries where data may be transferred shall be laid down for data subjects to exercise an informed choice.
Data subjects shall always be informed about the period for which their data will be stored.	Same as above.
Data subjects shall always be informed of their right to access, rectification, erasure, restriction and objection.	Same as above.
Data subjects shall always be informed of their right to withdraw consent, when consent is the lawful ground for processing.	Same as above.
Data subjects shall always be informed of their right to lodge a complaint with a supervisory authority.	Same as above.
Data subjects shall always be informed about the source of the personal data processed.	Same as above.
Data subjects shall always be informed if their data are going to be subject to automated decision-making and, if so, about the logic of the automation and the consequences for data subjects.	Same as above.

Data subjects shall always be informed if the controller intends to further process the personal data for a new purpose.	The new purpose needs however to be compatible with the initial one. A controller cannot simply avoid this obligation by informing the data subject.
The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.	Same as above.
The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.	Same as above.
The data subject has the right to request the erasure of his/her data under the conditions of Article 17(1) GDPR.	Same as above. This right cannot be excluded for the original data provided by the data subject.
The right to erasure shall not apply when the processing is, inter alia, necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as that right is likely to render impossible or seriously impair the achievement of the objectives of that processing.	This is particularly relevant to UPCAST's Pilot 2 (led by NHRF) insofar as data subjects who initially gave consent to the processing of their genomic data may withdraw their consent. Insofar as NHRF processes data for scientific research purposes, it may oppose the data subject's wish to withdraw consent and have the data erased, but only if it demonstrates that such erasure would seriously impair the research conducted by them.
The data subject shall have the right to obtain from the controller the restriction of processing under the conditions of Article 19(1) GDPR.	Same as above.
Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.	Same as above.

3.4 Data protection by design and by default

Article 25 of the GDPR requires the controller to implement data protection principles by design and by default for its processing operations. This is a central principle of the GDPR for the design of data processing technologies and procedures, as it mandates the implementation of data protection principles by design and by default in such technologies and procedures.

Data protection by design requires controller to adopt technical and organisational measures designed in a way that implements data protection principles in an effective manner and that integrates the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects[73]. Data protection by design must be implemented by controllers having regard to the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing. In essence, data protection by design requires controllers to embed in their processing technologies and procedures the measures that, in light of the circumstances of the processing, are most appropriate and proportionate to implement data protection principles.

Data protection by default requires controllers to put in place technical and organisational measures which ensure that, by default, only the personal data necessary for each specific purpose of the processing are processed[74]. In substance, data protection by default requires controllers to ensure that the technologies and procedures used for data processing implement data protection principles by default, without the need for a specific ''opt-in'' action. EDPS has provided further guidance in its Necessity Toolkit[75].

3.5 Application to UPCAST

3.5.1. Application of the GDPR in relation to mixed datasets

It is expected that the UPCAST plugins will be used for the processing of mixed datasets, i.e. datasets that contain both personal and non-personal data. Where such datasets are being processed, the GDPR would fully apply to the whole mixed dataset on one condition: the non-personal data part and the personal data parts must be 'inextricably linked'. The GDPR would apply in such cases also where the personal data represent only a small part of the dataset[76].

This interpretation is in line with the right to personal data protection guaranteed by the Charter of Fundamental Rights of the European Union and with Recital 8 of the Free Flow of Non-Personal Data Regulation. Recital 8 thereof provides that "*the legal framework on the protection of natural persons with regard to the processing of personal data…, in particular [the General Data Protection Regulation] and Directives (EU) 2016/680 and 2002/58/EC… are not affected by this Regulation.*"

The concept of the notion '**inextricably linked**' is **not defined by either of the two Regulations**. For practical purposes, it can refer to a situation whereby a dataset contains personal data as well as non-personal data and separating the two would either be impossible or considered by the controller to be economically inefficient or not technically feasible.

[73] See Article 25(1) of the GDPR.
[74] See Article 25(2) of the GDPR.
[75] European Data Protection Supervisor (EDPS), Necessity Toolkit, Brussels, 11 April 2017.
[76] Commission, 'Communication from the Commission to the European Parliament and the Council - Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union', 29 May 2019, COM/2019/250 final, p. 9.

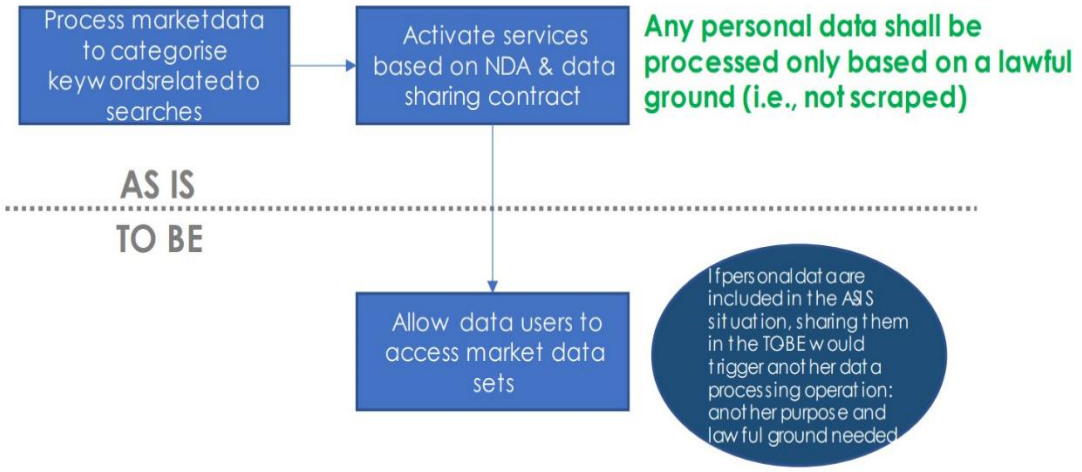
3.5.2. Application of the GDPR to UPCAST pilots

This section zooms in on the five UPCAST Pilots and provides some considerations and requirements tailored to the specific workflows. The analysis is supported by figures that compare the 'as-is' scenario to the 'to-be' scenario.

Pilot 1: Digital Marketing Data and Resources (JOT & CACTUS)

This section describes legal requirements for the digital marketing Pilot of JOT and CACTUS. Figure 1 highlights the main legally relevant workflows relating to the Pilot.

Figure 1. Digital Marketing Data and Resources Pilot



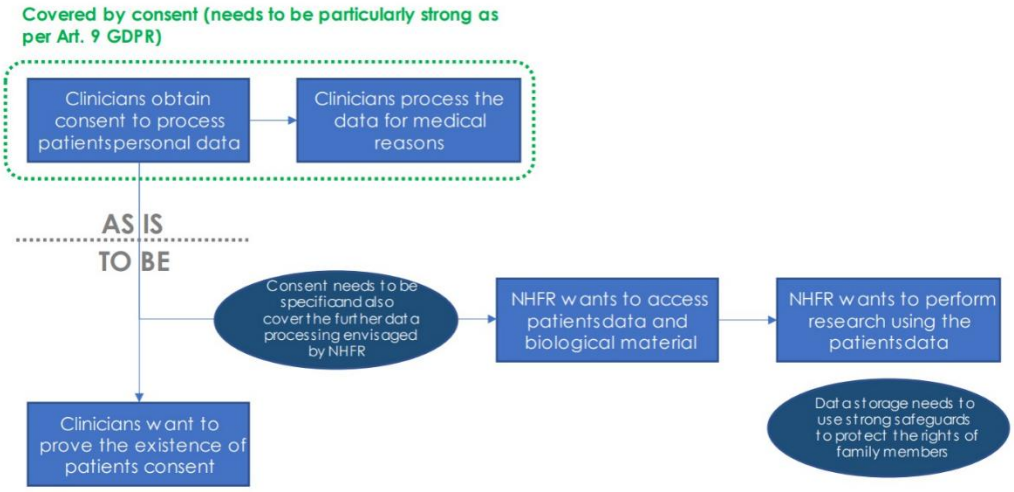
The main considerations on GDPR compliance in the context of this pilot are the following:

- Regarding the role and responsibilities of the entities involved in the personal data processing operations, insofar as the datasets used contain personal data, **JOT and CACTUS would likely qualify as** controllers, and in particular **joint controllers**, when using plugins to offer their services. Users of the service would qualify as separate controllers for the processing of the marketing data that they receive;
- To the extent that the data sets used by JOT and CACTUS in the AS-IS situation contain personal data (e.g., customer accounts passwords, email addresses, IP addresses, etc.), they **shall be processed based on a lawful ground** (Article 6 GDPR). Such data cannot be scraped from the Internet despite being publicly available. The legitimate interest lawful ground cannot be used if the purpose is linked to monetisation/commercialisation, and thus in this case consent may be the most appropriate lawful ground to rely on;
- The legal requirements mentioned in the previous point shall be met also when continuing the same activity in the TO-BE scenario;
- To the extent that in the TO-BE situation JOT and CACTUS intend to **provide data users access to data sets containing personal data**, they shall either a) anonymise that data prior to the sharing; or b) only allow access if the processing operation can be based on a lawful ground pursuant to Article 6 GDPR;
- In the latter case, JOT and CACTUS shall ask data users to sign a contract setting out data protection policies and requirements for the usage of the personal data included in the data sets, making sure that the data users agree to not use those data for other purposes than those specified in the contract and that are linked to the lawful ground for processing.

Pilot 2: Biomedical and Genomic Data Sharing (NHRF)

Figure 2 highlights the main legally relevant workflows relating to this Pilot.

Figure 2. Biomedical and Genomic Data Sharing Pilot



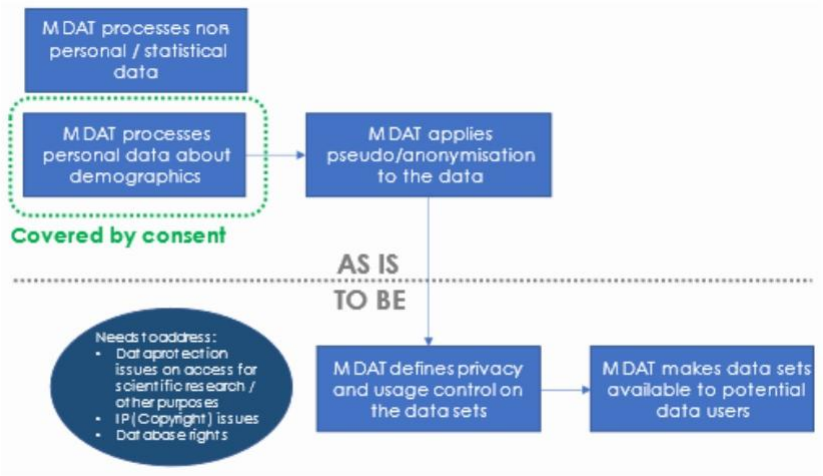
The main considerations relating to this pilot are the following:

- Regarding the role and responsibilities of the entities involved in the personal data processing operations, **NHRF would be acting as controller for the processing operations involving the personal data that it receives**, and the data providers as separate controllers for the personal data that they share. The sharing of personal data is per se a processing operation that requires its own lawful ground under the GDPR. There might be joint controllership between NHRF and the data providers depending on whether a collaboration is in place that fulfils the criteria outlined above;
- Should genetic and health data be shared, NHRF must ensure that any processing operation complies with the lawful grounds of both Article 6 and 9 of the GDPR;
- NHRF must engage with clinicians and ensure that, in order to lawfully process genetic and health-related data for their purposes, the consent forms used by clinicians ask an informed and explicit consent for further processing (by NHRF). The more specific NHRF can be when detailing the purposes and scenarios of the further processing, the better; however, the GDPR scientific research regime allows controllers to provide information only as far as reasonably foreseeable (not every single research purpose can be foreseen when requesting consent);
- Storage of biological material and of health-related data needs to be guaranteed according to the strongest available safeguards in order to protect the data subjects and the family members potentially identifiable via genomic data;
- Unless covered by a thorough consent from data subjects or properly anonymised, the genomic data at hand cannot be traded for monetisation purposes on another legal basis. The scientific research exemption would cease to apply in such a scenario;
- It is recommended that NHRF only considers the synthetic data generated in laboratories as candidates for data trading and monetisation. However, NHRF must ensure that the synthetic data generation process does not allow re-identification of the data subjects. For instance, the resulting synthetic data must not allow a one-to-one matching with the source personal data.

Pilot 3: Sharing Public Administration for Climate (led by OKFGR)

Figure 3 highlights the main legally relevant workflows relating to the Public Administration pilot.

Figure 3. Legally relevant workflows relating to the Public Administration Pilot



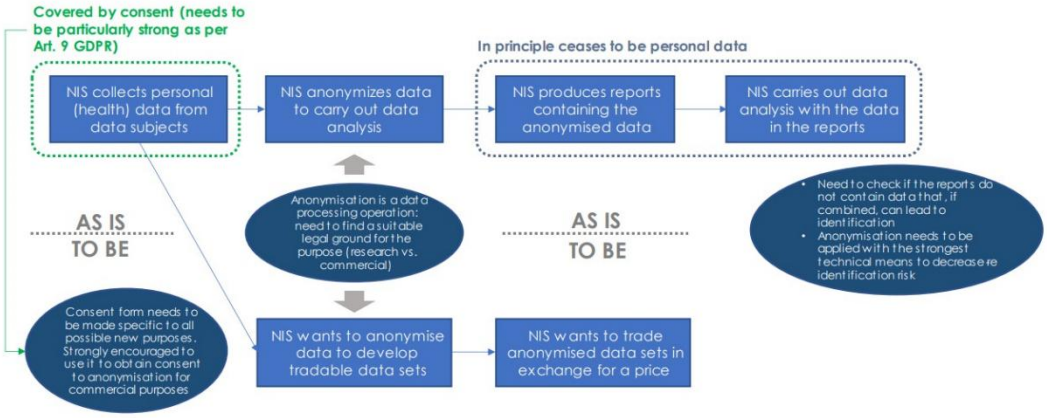
The main considerations relating to this pilot are the following:

- MDAT is controller for the processing operations involving personal data that it carries out, while the data users that make up the environmental data market of the metropolitan area of Thessaloniki act either as separate controllers or as joint controllers, depending on whether there are, or are not, collaborations between the public administrations that lead to a joint determination of the purposes and means of processing operations, in light of the criteria outlined above;
- In order to be able to lawfully share data sets containing demographic data, MDAT needs to continue applying anonymisation to the personal demographic data;
- To the extent that MDAT does not anonymise these personal data, MDAT needs to rely on a lawful ground for further processing those data (i.e., sharing the data with users);
- Any data recipient of the environmental data market needs a separate lawful ground for the processing of any personal data they receive.

Pilot 4: Health and Fitness Data Trading (NIS)

Figure 4 below highlights the main legally relevant workflows relating to the Health and Fitness Data Trading Pilot.

Figure 4. Legally relevant workflows relating to the Health and Fitness Data Trading Pilot



The main considerations relating to this pilot are the following:

- Fitness vendors accessing the data, if the data is not anonymised and thus still personal data, would be separate controllers for the processing operations that they will carry out. NIS would likely qualify as a separate controller for all the processing operations needed to collect, re-elaborate and share personal data. Nonetheless, NIS may also qualify as a simple data processor if it collects, re-elaborates and shares the personal data fully under the instructions of its clients, without making any independent determination on the purposes and means of the processing. Whether this is the case would depend on how the service is structured in practice;
- NIS needs to continue to obtain consent from data subjects for the processing of their sensitive data, making sure that the consent complies with the requirements of Articles 6 and Article 9 GDPR;
- As for the 'to-be' scenario, NIS intends to process these sensitive data for profit. As a result, NIS must thoroughly inform data subjects of this intent. The consent forms need to be exhaustive as regards a) NIS' intent to make profit from the processing and trading of the data; and b) NIS' intent to remunerate data subjects for their contribution to NIS' business model;
- On top of this, as NIS intends to anonymise data before trading them, it is strongly encouraged that the consent forms also ask data subjects to provide their consent to the use of anonymisation techniques on their sensitive data;
- NIS needs to make sure that the envisaged anonymisation techniques conform to the state of the art and that, taking into account reasonable re-identification efforts, do not in principle allow an external attacker to re-identify the data subjects;
- When producing reports based on anonymised data, NIS needs to make sure that the information contained in the reports does not, in isolation or in combination, allow reidentifying the data subjects.

4 EU Law Applicable to UPCAST Data Sharing Activities

4.1 Introduction

This chapter describes the legal requirements laid down in EU law that may apply to data sharing activities as such, irrespective of whether personal data is being processed, and with a general applicability. These requirements may apply either because the sharing of data falls under a specific category of data intermediation activity, as is the case for intermediary service providers, providers of data intermediation services or providers of core platform services, or because the data that is being shared is obtained from a connected product or related services, as is explained below.

Therefore, contrary to the GDPR, the requirements outlined in this chapter do not apply, mostly, because of the nature of the data that is being shared, e.g. whether it is personal or non-personal data, but based on how the data sharing activity is structured and on the provenance of the data. As a consequence, in order to assess the applicability of the relevant EU legal framework, consideration must be given to how the UPCAST plugins are to be used in the pilots, and in particular which is the provenance of the data to be shared, how is the overall activity structured and with which intended purpose.

The relevant pieces of legislation are analysed below. First, a description of the relevant legislation is provided and, second, its applicability to UPCAST is assessed.

4.2 The Digital Markets Act

4.2.1 Introduction and relevance to UPCAST

Regulation (EU) 2022/1925[77] (also known as the Digital Markets Act, hereinafter the "**DMA**") aims to regulate the proper functioning of the internal market by laying down harmonised rules **ensuring for all businesses contestable and fair markets in the digital sector across the EU where gatekeepers are present**, to the benefit of all business users and end users[78].

This piece of legislation regulates large technology platforms which are designated as "gatekeepers"[79]. Regulated entities are subject to several obligations and prohibitions.

The DMA applies to core platform services provided or offered by gatekeepers to business users established in the Union or end users established or located in the Union, irrespective of the place of establishment or residence of the gatekeepers and irrespective of the law otherwise applicable to the provision of service[80]. The DMA provides rules defining and prohibiting perceived unfair business practices by such large online platforms between European businesses and consumers, which apply in parallel with other national and EU competition rules.

The key concept delimiting the scope of application of the DMA is that of "core platform service", which is defined by Art. 2(2) of the DMA as covering the following services:

[77] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265 of 12.10.2022.
[78] See Art. 1(1) of the DMA.
[79] According to Article 2(1) of the DMA, "gatekeeper" means "an undertaking providing core platform services, designated pursuant to Article 3 of the DMA".
[80] See Art. 1(2) of the DMA.

a) online intermediation services;
b) online search engines;
c) online social networking services;
d) video-sharing platform services;
e) number-independent interpersonal communications services;
f) operating systems;
g) web browsers;
h) virtual assistants;
i) cloud computing services;
j) online advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by an undertaking that provides any of the core platform services listed in points (a) to (i);

In the context of UPCAST, it can be concluded that **the DMA would not apply to the data intermediation activities enabled by the UPCAST platform**, in light of two considerations.

First, it appears that **the type of service provided through the plugins would rarely qualify as a core platform service**, because it would rarely fall into one of the service categories, in which this concept consists. The only type of service that could be provided in the context of UPCAST is that of online intermediation pursuant to Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services[81], depending on how the plugins are deployed and in the context of each activity concerned. According to its Article 2(2), ''online intermediations services'' means *''services which meet all of the following requirements:*

a) they constitute information society services within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (12);
b) they allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded;
c) they are provided to business users on the basis of contractual relationships between the provider of those services and business users which offer goods or services to consumers.''

Second, even if there were a provision of a core platform service, **any entity providing core platform services through the UPCAST platform would unlikely qualify as a gatekeeper under Article 3 of the DMA**, at least during the duration of the project. In order to qualify as a gatekeeper, a provider would need to:

a) have a significant impact on the internal market;
b) provide a core platform service which is an important gateway for business users to reach end users; and
c) enjoy an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future.

Based on the envisaged nature and scope of the activities to be carried out in the context of the project, these conditions would certainly not be fulfilled, at least for the duration of the project.

[81] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ L 186 of 11.7.2019.

Based on the above, it can be concluded that the DMA is not of relevance to the UPCAST project, and its provisions and impact are therefore not analysed in this deliverable.

4.3 The Digital Services Act

4.3.1 Introduction and overview of the main provisions

Regulation (EU) 2022/2065[82] (also known as the Digital Services Act, hereinafter the "**DSA**") sets out harmonised rules for a **safe, predictable and trusted online environment by laying down provisions applicable to intermediary service providers**. In particular, the DSA establishes the following[83]:

a) *a framework for the conditional exemption from liability of providers of intermediary services;*
b) *rules on specific due diligence obligations tailored to certain specific categories of providers of intermediary services;*
c) *rules on the implementation and enforcement of this Regulation, including as regards the cooperation of and coordination between the competent authorities.*

Article 3(g) defines the notion of "intermediary service" as one of the following information society services:

a) *a **'mere conduit' service**, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;*
b) *a **'caching' service**, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request;*
c) *a **'hosting' service**, consisting of the storage of information provided by, and at the request of, a recipient of the service.*

The DSA lays down provisions applicable to all providers of intermediary services. Articles 11 to 15 contain obligations applicable to all providers of intermediary services, which relate to the designation of points of contact and of legal representatives, to requirements that must be respected by the terms and conditions used for the provision of the service to recipients, and to the obligation to make publicly available reports on content moderation activities, at least once a year.

Further to the basic requirements applicable to all providers of intermediary services, there are provisions that apply to specific subcategories of providers of intermediary services.

First, Articles 16 to 18 set out rules that apply to providers of hosting service providers only, which lay down obligations to put in place mechanisms for the notification of illegal content, to provide clear and specific statements of reasons to any recipient affected by certain restrictions to their content deemed as illegal or incompatible with the terms and conditions of the service, and to notify suspicions of criminal offences to national authorities.

Second, Articles 19 to 32 are applicable to providers of online platforms only. Article 3(i) defines an online platform as

[82] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277 of 27.10.2022.
[83] See Art. 1(2) of the DSA.

''a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation''.

In turn, ''dissemination to the public'' is defined by Article 3(k) of the DSA as ''*making information available, at the request of the recipient of the service who provided the information, to a potentially unlimited number of third parties*''.

These Articles lay down obligations on internal complaint-handling systems, out-of-court dispute settlement, trusted flaggers, misuse, transparency reporting, online interface design and organisation, advertising, recommender systems, protection of minors, and provisions applicable only to online platforms that allow consumers to conclude distance contracts with traders.

Third, there are provisions specifically applicable to providers of very large online platforms and search engines, which are providers of online platforms and online search engines[84] who meet the dimensional criteria set out in Article 33 of the DSA and are designated as such by the European Commission. These providers are subject to additional obligations on systemic risk assessment and mitigation, putting in place crisis response mechanisms, recommender systems, online advertising transparency, data access and scrutiny, transparency reporting, as well as on setting up a compliance function and being regularly subject to independent audits.

4.3.2 Relevance to UPCAST

In order to assess the impact of the DSA on UPCAST, it is essential to first ascertain **whether the activities carried out in the context of UPCAST could qualify as the provision of an intermediary service**, because only in that case the DSA would apply.

At the outset, it must be noted that the existence of an intermediary service would depend on how the plugins are used, and in the context of which activity, and thus on based on a **case-by-case assessment**. In theory, plugins could be used for the provision of an intermediary service. For instance, plugins could be used for the functioning of the data sharing platform where the service consists of making a platform available to clients, data providers and data consumers, who use it to exchange data. In this case, the platform provided as a service would constitute a hosting service, because the service provider would store data at the request of data providers, in order to subsequently transmit it to data recipients. This qualification, however, would also depend on whether storage of the data is part of the service, and there may not be provision of a hosting service if the platform is only acting as a matchmaker between parties that do not store the data in the platform but directly exchange the data between themselves.

Based on the disclaimer made above, regarding the need to carry out a case-by-case assessment, it is possible to provide some observations about the existence of an intermediary service in the context of the project pilots. To provide more context of the type of activities that could qualify as intermediary services, **Recital 29** of the DSA gives

[84] According to Article 3(j) of the DSA, an online search engine is a ''*hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation*''.

examples of services that would fall under each of the three categories of intermediary services. Mere conduit services include generic categories of services, such as internet exchange points, wireless access points, virtual private networks, DNS services and resolvers, top-level domain name registries, registrars, certificate authorities that issue digital certificates, voice over IP and other interpersonal communication services. Caching services include the sole provision of content delivery networks, reverse proxies or content adaptation proxies. Finally, hosting services include cloud computing, web hosting, paid referencing services or services enabling sharing information and content online, including file storage and sharing. Whether a specific service constitutes a 'mere conduit', 'caching' or 'hosting' service depends solely on its technical functionalities, and thus whether they are in line in the definition provided for each of these services by the DSA.

- In **Pilot 1**, JOT and CACTUS provide a service that does not consist of storing or transmitting data at the request of the recipients of the service, but rather they gather data themselves to subsequently share it with recipients of the service. Therefore, the service cannot qualify as a mere conduit, caching or hosting service.
- In **Pilot 2**, NHRF is exploring the datasets in order to gather data and subsequently process it for scientific purposes. Based on the description of the pilot, it can be concluded that none of the entities involved is using the UPCAST plugins to provide a mere conduit, caching or hosting service.
- In **Pilot 3**, while MDAT acts as an intermediary between data sources and data consumers, its activity does not seem to be structured in the form of a service rendered to recipients consisting of transmission of data in a communication network or storage of data. The service rendered is rather that of providing data to interested parties, based on a selection made by MDAT at its own discretion. Therefore, there does not seem to be the provision of an intermediary service in this.
- Finally, in **Pilot 4** Nissatech cannot be considered as providing a hosting service, since it does not store data at the request of data producers, but rather elaborates data derived from activities of the recipients of the service. It also cannot be considered as a provider of a mere conduit or caching service, since the service does not consist in the transmission of information.

Based on the above, an analysis of the pilots leads to the conclusion that the **DSA would not apply in the context of UPCAST**. Nonetheless, this conclusion is not definitive and the activities concretely carried out in the context of the pilots will be monitored throughout the project in order to assess whether they could qualify as the provision of an intermediary service.

4.4 Data Governance Act

4.4.1 Introduction and overview of the main provisions

Regulation (EU) 2022/868 (commonly known as ''Data Governance Act'', hereinafter the ''**DGA**'')[85] is a composite piece of legislation with provisions dedicated to four different areas: a) conditions for the **re-use**, within the Union**, of certain categories of data held by public sector bodies**; b) a **notification and supervisory framework for the provision of data intermediation services**; c) a framework for **voluntary registration of entities**

[85] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), OJ L 152 of 3.6.2022.

which collect and process data made available for altruistic purposes; and d) a framework for the establishment of a **European Data Innovation Board**[86].

The DGA complements the DA and seeks to facilitate the "voluntary sharing of data by individuals and businesses and harmonises conditions for the use of certain public sector data without altering material rights on the data or established data access and usage rights". The DGA also complements the Open Data Directive.

Some of the requirements set out in the DGA are summarised in Table 2, below, with brief observations on their relevance to UPCAST.

Table 2. Requirements from the Data Governance Act and observations on how they relate to UPCAST

Legal provision/requirements	Observations
Chapter II: Re-use of certain categories of protected data held by public sector bodies	
(Art. 3(1)) Categories of data: This Chapter applies to data held by public sector bodies which are protected on grounds of: (a) commercial confidentiality, including business, professional and company secrets; (b) statistical confidentiality; (c) the protection of intellectual property rights of third parties; or (d) the protection of personal data, insofar as such data fall outside the scope of Directive (EU) 2019/1024.	Under UPCAST and in the context of exchange of data held by public sector bodies, such entities could be subject to the obligations set in this chapter.
(Art. 4(1)) Prohibition of exclusive arrangements + exceptions Agreements or other practices pertaining to the re-use of data held by public sector bodies containing categories of data referred to in Article 3(1) which grant exclusive rights or which have as their objective or effect to grant such exclusive rights or to restrict the availability of data for re-use by entities other than the parties to such agreements or other practices shall be prohibited.	Same as above.
(Art. 5) Conditions for re-use	Same as above.

[86] See Article 1(1) of the DGA.

The article provides a long list of conditions related to the re-use of data. For instance, competent public sector bodies shall make publicly available the conditions for allowing such re-use and the procedure to request the re-use. Such conditions for re-use shall be non-discriminatory, transparent, proportionate and objectively justified with regard to the categories of data and the purposes of re-use and the nature of the data for which re-use is allowed. Those conditions shall not be used to restrict competition. Public sector bodies shall ensure that the protected nature of data is preserved. They may provide for some requirements (see article for list of proposed requirements). Unless national law provides otherwise, the public sector body shall make the re-use of data conditional on the adherence by the re-user to a confidentiality obligation that prohibits the disclosure of any information that jeopardises the rights and interests of third parties that the re-user may have acquired despite the safeguards put in place. Prohibition for re-users from re-identifying any data subject to whom the data relates + shall take technical and operational measures to prevent re-identification and to notify any data breach resulting in the reidentification of the data subjects. Re-use of data shall be allowed only in compliance with intellectual property rights. Where requested data is confidential, the public sector bodies shall ensure that such data is not disclosed as a result of allowing re-use (unless such re-use is allowed). Other rules are detailed in the Article.	
(Art 6) <u>Fees</u>: public sector bodies which allow re-use of the categories of data referred to in Article 3(1) may charge fees. Any charged fees shall be transparent, non-discriminatory, proportionate and objectively justified and shall not restrict competition.	

(Art 9) <u>Procedure for request for re use</u>: This article details the request procedure for re-use.	
Chapter III: Requirements applicable to data sharing services	
(Art. 10) <u>Data intermediation services</u>: The provision of the following data intermediation services shall comply with Article 12 and subject to a notification procedure: (a) intermediation services between data holders and potential data users, including making available the technical or other means to enable such services; those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint use of data, as well as the establishment of other specific infrastructure for the interconnection of data holders with data users; (b) intermediation services between data subjects that seek to make their personal data available or natural persons that seek to make non-personal data available, and potential data users, including making available the technical or other means to enable such services, and in particular enabling the exercise of the data subjects' rights provided in Regulation (EU) 2016/679; (c) services of data cooperatives.	The data exchange platforms/plugins in UPCAST could qualify as data sharing services that would have to comply with the requirements set in Art. 11 and 12.
(Art. 11) <u>Notification of data sharing service providers:</u> This first requirement obliges data sharing service providers to notify their activities.	
(Art. 12) <u>Conditions for providing data intermediation services.</u> This article provides a long list of conditions. These include, for instance, the following conditions: • the provider shall not use the data other than to put them at the disposal of data users and shall provide data intermediation services through a separate legal person; • the commercial terms, including pricing, for the provision of data	All of the conditions in the Article would have to be respected if UPCAST qualifies.

intermediation services to a data holder or data user shall not be dependent upon whether the data holder or data user uses other services provided by the same data intermediation services provider or by a related entity, and if so to what degree the data holder or data user uses such other services; *the data collected with respect to any activity of a natural or legal person for the purpose of the provision of the data intermediation service (e.g., date, time, geolocation data, duration of activity and connections to other natural or legal persons established by the person who uses the data intermediation service) shall be used only for the development of that data intermediation service (e.g., for the detection of fraud or cybersecurity), and shall be made available to the data holders upon request; • the provider shall facilitate the exchange of the data in the format in which it receives it from a data subject or a data holder, shall convert the data into specific formats only to enhance interoperability within and across sectors or if requested by the data user or where mandated by Union law or to ensure harmonisation with international or European data standards + shall offer an opt-out possibility regarding those conversions to data subjects or data holders, unless the conversion is mandated by Union law; • the data intermediation services provider shall ensure that the procedure for access to its service is fair, transparent and non-discriminatory for data subjects + data holders + data users, (including prices and terms of service);	

• the provider shall put in place adequate technical, legal and organisational measures in order to prevent the transfer of or access to non-personal data; *the provider shall take necessary measures to ensure an appropriate level of security for the storage, processing and transmission of non-personal data, and shall further ensure the highest level of security for the storage and transmission of competitively sensitive information. The full list of conditions can be found in the Article.	

4.4.2 The notion of 'data intermediary'

The DGA lays down requirements for providers of ''data intermediation services'' (hereinafter, ''DIS''), as defined in Article 2(11) of the DGA. Alongside the general definition, **Article 10** of the DGA provides a list of three categories of DIS[87], namely:

a) Intermediation services between data holders and potential data users, including making available the technical or other means to enable such services; those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint use of data, as well as the establishment of other specific infrastructure for the interconnection of data holders with data users;

b) Intermediation services between data subjects that seek to make their personal data available or natural persons that seek to make non-personal data available, and potential data users, including making available the technical or other means to enable such services, and in particular enabling the exercise of the data subjects' rights provided in Regulation (EU) 2016/679116;

c) Services of data cooperatives within the meaning given to this notion by the DGA.

A data intermediation service is defined by Article 2(11) of the DGA as

> *''a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data*''. Recital 28 of the DGA provides examples of data intermediation services, which include *''data marketplaces on which undertakings could make data available to others, orchestrators of data sharing ecosystems that are open to all interested parties, for instance in the context of common European data spaces, as well as data pools established jointly by several legal or natural persons with the intention to license the use of such data pools to all interested parties in a manner*

[87] See Article 10 of the DGA.

that all participants that contribute to the data pools would receive a reward for their contribution''.

Article 2(11) of the DGA explicitly **excludes the following services** from the definition of data intermediation service, with the caveat that this list of exclusions is to be deemed non-exhaustive:

a) services that obtain data from data holders and aggregate, enrich or transform the data for the purpose of adding substantial value to it and license the use of the resulting data to data users, without establishing a commercial relationship between data holders and data users;

b) services that focus on the intermediation of copyright-protected content;

c) services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group, including supplier or customer relationships or collaborations established by contract, in particular those that have as a main objective to ensure the functionalities of objects and devices connected to the Internet of Things;

d) data sharing services offered by public sector bodies that do not aim to establish commercial relationships.

The definition of DIS has raised doubts since the adoption of the DGA, as its interpretation has been subject to debate within academia and beyond. Article 2(11) provides for the general criteria that must be assessed to determine whether a given activity qualifies as a DIS[88].

A DIS is defined as a:

a) Service;

b) Which aims to establish commercial relationships for the purpose of data sharing;

c) Between an undetermined number of data subjects, data holders and data users;

d) Through technical, legal or other means.

It is not clear how the general definition of DIS relates to the three categories listed in Article 10 of the DGA, and in particular whether the three categories in Article 10 are a subset of DIS that alone is subject to the provisions of Articles 11 and 12[89]. While some authors argue that the list in Article 10 should not be understood as creating a subset of

[88] For a detailed analysis of how these criteria may be interpreted and applied, see: T. Bobev, V. K. Dessers, C. Ducuing, M. Fierens, A. Palumbo, B. Peeters, L. Stähler, 'CiTiP White Paper on the Definition of Data Intermediation Services' (2023) accessed on 7 March 2023 at https://ssrn.com/abstract=4589987.

[89] Carovano and Finck suggest that the listing of Article 10 invites speculation as to whether it really creates a subset of DIS (compared to the general definition in Article 2(11)) that are alone subject to Articles 11 and 12, see: G. Carovano, M. Finck, ''Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy'', 50 Computer Science & Law Review 7, 2023.

services that only are subject to Articles 11 and 12[90], other authors do not seem to hold the same view[91].

4.4.3 Requirements relevant to UPCAST – provisions on the re-use of public sector data

In the context of Pilot 3 of UPCAST, public administrations of the Metropolitan area of Thessaloniki will be sharing environmental data between themselves, as well as with private entities. This data could fall under one of the categories of protected data listed in Article 3(1) of the DGA, insofar as it is data protected on grounds of a) commercial confidentiality, b) statistical confidentiality, c) intellectual property rights of third parties, d) personal data protection. When the data held by public sector bodies is going to be shared and re-used by another party, and the data falls under one of the categories listed above, the re-use of this data is subject to the conditions laid down in Chapter II of the DGA. Chapter II would not apply only in the case of one of the exclusions listed in Article 3(2) of the DGA, namely: a) data held by public undertakings, b) data held by public service broadcasters and their subsidiaries, and by other bodies or their subsidiaries for the fulfilment of a public service broadcasting remit, c) data held by cultural establishments and educational establishments, d) data held by public sector bodies which are protected for reasons of public security, defence or national security; or e) data the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules in the Member State concerned, or, in the absence of such rules, as defined in accordance with common administrative practice in that Member State, provided that the scope of the public tasks is transparent and subject to review.

Based on a *prima facie* assessment, the exclusions do not appear to be relevant to Pilot 3, save for the case where the bodies involved qualify as public undertakings under Greek law, or as public sector bodies which are protected for reasons of public security, defence or national security.

As summarised in Table 2 above, the requirements of Chapter 2 relate to the prohibition of exclusive arrangements, to the conditions for re-use, to fees and to the procedure for requesting the re-use of the data.

4.4.4 Requirements relevant to UPCAST – qualification of the platform as a data intermediation service

The characteristics of the UPCAST platform alone do not allow to reach a conclusion about whether it involves the provision of an intermediary service, since this qualification would depend on the **concrete use** that is made of it, in particular in relation to the context where it is deployed and the types of relationships that it helps to establish.

The only context-independent assessment that can be made is with regard to the following factor: the UPCAST platform features technical means that are per se adequate to establish commercial relationships for the purposes of data sharing, and the service rendered would thus qualify as a data intermediation service if, in practice, it

[90] G. Carovano, M. Finck, ''Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy'', Computer Science & Law Review 7, 2023.
[91] H. Richter, ''Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing'', 72 GRUR International 462, 2023; L, von Ditfurth, G. Lienemann, ''The Data Governance Act: – Promoting or Restricting Data Intermediaries?'', Competition and Regulation in Network Industries, 2022.

is aimed at the establishment of commercial relationships between an undetermined number of data subjects and data holders on the one hand and data users on the other.

Another context-independent observation that can be made specific to the UPCAST project regards the question of whether the activities carried out in the context of research projects funded by the European Commission could still qualify as data intermediation services, or if they could be exempted by reason of their research-oriented nature financed through public funds.

The DGA does not explicitly exempt the activities carried out for research purposes from the provisions on data intermediation. Therefore, any service provided in the context of publicly funded research projects that falls under the definition of data intermediation service will be, in principle, subject to the relevant provisions of the DGA. However, besides the absence of a general exemption in the legislative text, such activities could, due to their specific nature, fall out of the scope of the DGA because they do not satisfy the conditions to qualify as data intermediation services[92]. The only condition for which the research and publicly-funded nature of the activity would have some relevance is the one on the qualification as a service since, in this case, it could be argued that the activity does not have an economic finality.

In particular, the research activity may not qualify as a 'service' only in the hypothesis where the participants to the project do not gain any economic benefit from the project itself, besides the reimbursement of the costs via the public funding, and do not obtain, among others, economic benefits for a later commercialization phase (e.g. marketing), IP rights or a remuneration from the recipients of the service[93]. Another situation in which there might not be a 'service' is the case where participants are paid with a remuneration that does not cover all the costs, and there are no other economic benefits gained by the service provider. However, it is difficult to foresee how the ECJ will interpret the DGA in such a case, because the relevant case-law precedents on the notion of "service" only relates to public services provided by public bodies, and not to private entities providing services for a remuneration below costs[94].

4.4.5 Use of the UPCAST plugins to provide a data intermediation service – compliance with the conditions in Article 12

Besides their use in the pilots of the project, UPCAST plugins may be used in other contexts, including as technical tools for the provision of a data intermediation service under the DGA.

When UPCAST plugins are used to provide a data intermediation service, the technical functionalities they enable **must comply with the conditions set out in Article 12 of the DGA**. Article 12 lays down the conditions to which the provision of a data intermediation service is subject, and that must thus always be respected. As part of the assessment of the legal viability of the UPCAST technical solutions, it is therefore essential to examine any potential risks of incompatibility that may arise between the operation and the plugins and the conditions of Article 12. In other words, it must be assessed whether the deployment of plugins would lead to a violation of one or more of the conditions in Article 12.

[92] T. Bobev, V. K. Dessers, C. Ducuing, M. Fierens, A. Palumbo, B. Peeters, L. Stähler, 'CiTiP White Paper on the Definition of Data Intermediation Services' (2023) accessed on 7 March 2023 at https://ssrn.com/abstract=4589987.
[93] Ibid, p. 58.
[94] Ibid.

The majority of the conditions listed in Article do not present incompatibilities with the UPCAST plugins. However, **there are some conditions that may be violated by the pricing and valuation module**. The specific risks of violation are described below.

First, the resource analyser may lead to a violation of the condition of Article 12(a) of the DGA. This condition reads as follows:

> ''*the data intermediation services provider shall not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users and shall provide data intermediation services through a separate legal person*''.

This condition seems to preclude any use that is not strictly necessary to the act of putting the data at the disposal of data users. As stated in Recital 33 of the DGA, providers of data intermediation services shall ''*act only as intermediaries in the transactions, and do not use the data exchanged for any other purpose*''.

Interpretive doubts arise as to the scope of this condition, and the recitals of the DGA do not offer clear guidance in this regard. In particular, two alternative interpretations seem viable. Under a first, narrower and more literal, interpretation this condition could require providers not to use the data they offer for purposes that differ from the mere fact of putting them at the disposal of data users as part of the provision of the service. For instance, they may use the data for storing it or enabling their discovery through a search function, as it is strictly correlated with the putting at disposal of the data, but they cannot use it to set the price of the data itself. An analysis of the data aimed at extracting features to be used to set the price for the data itself would not qualify, under this interpretation, as a use for the purpose of putting the data at the disposal of data users. In particular, pricing is an additional and different activity that is not strictly necessary for making the data available to users. Under a second, broader, interpretation this condition could be read as allowing any use instrumental to all activities correlated with the provision of the service, including not only the mere act of making the data available, but also other aspects of the transaction such as pricing. Should this interpretation be followed, any deployment of the resource analyser would not lead to a violation of the condition.

While a definitive answer as to the interpretation of this condition cannot be provided, a more literal interpretation should be preferred, as it adheres more strictly to the text and due to the absence of other interpretive guidance. Therefore, Article 12(a) of the DGA should be interpreted as precluding the envisaged use of the resource analyser in the context of the provision of a data intermediation service.

Second, the pricing and valuation module may lead to a violation of the condition in Article 12(c) of the DGA. This condition reads as follows:

> *'the data collected with respect to any activity of a natural or legal person for the purpose of the provision of the data intermediation service, including the date, time and geolocation data, duration of activity and connections to other natural or legal persons established by the person who uses the data intermediation service, shall be used only for the development of that data intermediation service, which may entail the use of data for the detection of fraud or cybersecurity, and shall be made available to the data holders upon request*'.

This condition requires, in essence, **not to use the data collected on the conduct of natural or legal persons in the context of the provision of the data intermediation service, safe for the development of the service**. The type of data covered by this limitation may include, for instance, the time when a data provider completed a transaction with a data user, the geographical area where the majority of transactions

have taken place, the categories of datasets that have been exchanged most frequently. The interpretation of this condition also gives rise to doubts, in particular on the meaning of the term ''development'' of a data intermediation service. On the one hand, if broadly interpreted, this term may include a wide array of functionalities and features of a service, including fair pricing algorithms. Fair pricing is an important part of the service, and may be seen by data providers and users as a functionality that provides added value to the service, facilitating transactions. On the other hand, development could be intended to cover only the functionalities that are strictly necessary to enable the provision of the service, i.e. the matchmaking between data subject and holders and users and the putting of data at the disposal of data users. Under this interpretation, the condition would only allow the use of data for the development, for instance, of technical functionalities needed to ensure the security of the service and the establishment of relationships between data subjects and data holders, on the one hand, and the users, on the other (e.g. through resource discovery). Pricing of the datasets, as not strictly necessary to the provision of the service, would not fall under the category of functionalities whose development is under the scope of application of the condition.

In the absence of interpretive guidance, **the stricter interpretation should be followed** in order to ensure that UPCAST solutions are not used in breach of the DGA. Therefore, for the purposes of this report the pricing and valuation module shall be considered as potentially incompatible with this condition, and solutions to enable compliance with it should be explored.

Third, the pricing and valuation module may be at odds with the condition of fair and non-discriminatory access to the data intermediation services, laid down in Article 12(f) of the DGA. This condition reads as follows:

> ''*the data intermediation services provider shall ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data subjects and data holders, as well as for data users, including with regard to prices and terms of service*''.

As the condition explicitly requires fairness and non-discrimination in relation, among others, to prices, the question arises as to whether the pricing features of the module create an unfair or discriminatory treatments of service users. The articles and the recitals of the DGA do not clarify what is meant by fair and non-discriminatory, nor there is specific guidance in this sense with regard to pricing. Given the novelty of the DGA, the interpretation of fairness and non-discrimination in accessing a data intermediation service still needs to be fleshed out. Fairness and non-discrimination also play a central role for the licensing of standard essential patents (SEPs). It has been argued that the principles, developed in the case-law of the European Court of Justice[95] and in EU legislative proposals[96], on the licensing of SEPs on fair, reasonable and non-discriminatory (FRAND) terms could be used as an inspiration for cases of data access[97], and in particular to assist the parties in determining the price of access. However, as FRAND conditions have been elaborated in relation to SEPs for antitrust purposes, they are also bound to assume a meaning that is, at least partially, different than the one they could be ascribed in the context of data intermediation. For instance, fairness in SEPs licensing requires terms that are not anti-competitive.

[95] See the judgement of the European Court Justice of 16 July 2015 *Huawei*, C-170/13.

[96] See the recent legislative proposal by the Commission of 27 April 2023 for a Regulation of the European Parliament and of the Council on standard essential patents and amending Regulation (EU) 2017/1001.

[97] Drexl, J. ''Designing Competitive Markets for Industrial Data - Between Propertisation and Access'' [2017] JIPITEC 257, 285.

While defining the meaning of fairness in access to data intermediation services may require more interpretive efforts, non-discrimination gives rise to less interpretive doubts. As concerns pricing, non-discrimination requires an equal treatment of service recipients. Equal treatment does not entail the application of the same price in any case, but different prices applied in the same situation should have an underlying objective justification. As the pricing and valuation module relies on a series of objective factors to determine the price for datasets, it should be possible to argue that the pricing is non-discriminatory.

Based on the considerations set forth above, it can be concluded that **the most evident and tangible risk of violation of the conditions in Article 12 lies in the infringement by the resource analyser of the condition laid down in letter a)**. As concerns the conditions in letter c), doubts regarding its interpretation preclude a clear answer. However, special attention should be paid to this condition in the development of the pricing and valuation module. Finally, the condition in letter f) is not violated by the use of the pricing and valuation module *per se*, insofar as the criteria employed for pricing are based on objective, non-discriminatory factors. Fairness and transparency should be ensured in the way pricing is calculated. In this regard, an analysis of the envisaged operation of the pricing and valuation module does not indicate, *prima facie*, potential risks of unfair and non-transparent pricing.

4.5 Data Act

4.5.1 Introduction and overview of the main provisions

Over the span of the last years, the number of products connected to the internet[98] that are available on the European single market has grown exponentially. These devices, that range from smart household appliances to intelligent industrial machines, together constitute what we know as Internet-of-Things (hereinafter: "IoT") and thus contribute significantly to the volume of data that is available for access, reuse and sharing in the EU. Nevertheless, a series of obstacles have rendered difficult effective data sharing between actors (consumers, businesses and public bodies): uncertainty about rights and obligations that arise from costs related to contracting and implementing of technical interfaces, lack of standards for interoperability and of data sharing practices. In order to overcome these barriers, the Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data[99] (hereinafter: "Data Act" or "DA") aims at enhancing the EU data economy, by making data more available, accessible and usable, as well as encouraging data-driven innovation. Almost two years after the publication of its proposal[100], the Data Act was published in the Official Journal of the EU on 22 December 2022 and entered into force on 11 January 2024. It will be applicable from 12 of September 2025 onwards.

As laid down in its Chapter I, the main objectives of the Data Act are:

[98] Article 1(5) of the Data Act defies connected products as "*means an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user.*"

[99] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data, OJ L, 2023/2854, 22.12.2023.

[100] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data. COM(2022) 68 final-23.2.2022. 2022/0047 (COD).

- the making available of product data[101] and related service data[102] to the user[103] of the connected product[104] or related service[105];
- the making available of data by data holders[106]:
    - **to data recipients**[107];
    - **to public sector bodies**, the Commission, the European Central Bank and Union bodies, where there is an exceptional need for those data for the performance of a specific task carried out in the public interest;
- facilitating **switching** between data processing services[108];
- introducing **safeguards against unlawful third-party access to non-personal data**; and
- the development of **interoperability standards** for data to be accessed, transferred and used.

In accordance with these objectives, the Act is subsequently structured into the following chapters:

a) Business-to-business ("B2B") and business-to-consumer ("B2C") data sharing (Chapter II)
b) Rules on mandatory B2B data sharing (Chapter III)

---

[101] Article 2(15) of the Data Act defines product data as "*data generated by the use of a connected product that the manufacturer designed to be retrievable, via an electronic communications service, physical connection or on-device access, by a user, data holder or a third party, including, where relevant, the manufacture*r".

[102] Article 2(16) of the Data Act defines related service data as "*data representing the digitisation of user actions or of events related to the connected product, recorded intentionally by the user or generated as a by-product of the user's action during the provision of a related service by the provider"*.

[103] Article 2(12) of the Data Act defines a user as "*a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services*".

[104] See Article 2(5) of the Data Act defines a connected product as "*an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user"*

[105] See Article 2(6) of the Data Act defines a related service as "*a digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase, rent or lease in such a way that its absence would prevent the connected product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the connected product*".

[106] Article 2(13) of the Data Act defines a data holder as "*a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service*".

[107] Article 2(14) of the Data Act defines a data recipient as "*a natural or legal person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law*".

[108] Article 2(8) of the Data Act defines a data processing service as "*a digital service that is provided to a customer and that enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or service provider interaction*".

c) Unfair contractual terms (Chapter IV)
d) Business-to-government ("B2G") data sharing (Chapter V)
e) Switching between data processing services (Chapter VI)
f) Unlawful third country government access (Chapter VII)
g) Interoperability (Chapter VIII)
h) Enforcement and overarching provisions (Chapter IX)

More specifically, Chapter II covers the B2B and business-to-consumer (B2C) sharing, and thus enables users of connected products and related services to access the data co-created by the use of such products and services. An example that illustrates such a co-creation is a mobile app (related service) that allows the user to extract environmental-related data from their washing machine or switch on/off their television (connected product).

Chapter III introduces a set of rules that apply to B2B data sharing and according to which, in certain situations, a business is legally obliged to share data with another business.

As far as B2B data sharing agreements are concerned, Chapter IV enumerates cases of unfair contractual terms. It further distinguishes between terms that are always considered to be unfair[109], and others that are presumed to be unfair[110]. Terms that fall under the first category are *de facto* invalid, whereas terms that fall under the second category need to be proven as fair by the entity that imposed them in order to be valid.

With regards to B2B sharing, public sector bodies are, in virtue of the provisions of Chapter V, able to access data held by data held by businesses under the condition that they demonstrate an exceptional need. The situations that are covered under the term "exceptional need" include public emergencies[111] (such as natural disasters, pandemics, etc.) and non-emergency situations[112].

Moreover, the provisions of Chapter VI seek to ensure that consumers in the EU are able to switch between different data processing services smoothly and continuously, without any switching charges. Minimum requirements for the content of cloud contracts are foreseen[113], in an effort to compensate for the existing power imbalance between providers and customers.

Chapter VII governs the sharing of non-personal data from providers of data processing services with third country governmental bodies. Such sharing can in certain instances be considered unlawful, due to contradictions with EU or national law. The Data Act does not prohibit per se cross-border data sharing; it limits itself to providing for rules and safeguards to ensure that the level of protection that is afforded in the EU, is as well afforded when EU data are communicated to non-EU governmental bodies[114].

Matters of interoperability are treated under Chapter VIII, in order to ensure that data coming from different sources comply with harmonized standards, which allow them to be used within and among European data spaces.

[109] See Article 13(5) of the Data Act.
[110] See Article 13(6) of the Data Act.
[111] See Article 14(1)(a) of the Data Act.
[112] See Article 14(1)(b) of the Data Act.
[113] See Article 25(2) of the Data Act.
[114] See Article 32 of the Data Act.

Relating to enforcement and dispute resolution, the Data Act in its Chapter IX foresees the designation of competent authorities ("data coordinator")[115] as well as the setting up of certified dispute settlement bodies[116].

The following table provides a comparative overview of the Chapters II-VII of the Data Act, with regard to a series of aspects (i.e. relevant actors, type of data concerned, reason justifying the sharing, eventual compensation asked from the data holder, limitations on the use of data).

Table 3. Comparative overview of Chapters II to VII of the Data Act

	Data sharing		Type of data concerned	Reason	Compensation asked from data holder	Limitations on the use of data
	From (data holder)	To (user/data recipient)				
Chapter II	Businesses	Businesses (**as users**) or Consumers	Personal and non-personal	Fairness in the data economy and consumer empowerment	N/A	- Data obtained cannot be used to create a competing connected product - GDPR compliance - Trade secrets agreements - Security requirements
Chapter III	Businesses	Businesses (**as data recipients**)	Personal and non-personal	Legal (EU or national) obligation of the business	Reasonable	N/A
Chapter IV	Businesses	Businesses	Personal and non-personal	N/A	N/A	N/A
Chapter V	Businesses	Public sector bodies & EU institutions	Personal and non-personal	Exceptional need during execution of a task of public interest	Reasonable or none	N/A
Chapter VII	Providers of data processing services	Non-EU government bodies	Non-personal	N/A	N/A	N/A

4.5.2 The contractual regime of the Data Act

4.5.2.1. General data sharing obligations

The two main obligations that are incumbent on data holders with regards to data sharing with either businesses (acting as users) or consumers, are a) the obligation to manufacture connected products and design related services in a way that makes data

[115] See Article 37 of the Data Act.
[116] See Article 39 of the Data Act.

available 'by design'[117] and, b) in case such direct access is not possible, make data **'readily available'** to the user, without undue delay.[118] However, such obligation can be bent where accessing, using or further sharing of the data can be detrimental to the security requirements of the connected product, which would result in 'serious adverse effect on the health, safety or security of natural persons'[119].

Special attention is given to the preservation and careful disclosure of trade secrets. Article 4(6) of the Data Act stipulates that following the identification of the trade secrets, proportionate technical and organisational measures have to be adopted, in order to ensure that the data sharing takes place under conditions of complete confidentiality.

4.5.2.2. Contractual freedom restrictions

At the outset, it is important to note that, in virtue of the Data Act's provisions, freedom of contract is becoming increasingly restricted, even in the case of B2B agreements. In this regard, there are two main sets of restrictions that are foreseen:

a) Article 8 on FRAND contractual terms

As regards B2B data sharing agreements, Article 8(1) foresees that the data holder shall agree with the data recipient that the making available data take place (1) under terms and conditions that are **fair**, **reasonable** and **non-discriminatory**, and (2) in a **transparent manner**. To that end:

- With regards to the condition of fairness, Article 8(2) specifies further that unfair contractual terms in the sense of Article 13 and terms that exclude the application or derogate from the rights recognized under Chapter II, are not binding;
- With regards to the condition of non-discrimination, Article 8(3) specifies that data holders shall not discriminate between comparable categories of data recipients;
- With regards to the condition of reasonableness, Article 8(5) neither the data holder nor the data recipients shall be required to provide any information beyond what is necessary.

b) Article 13 on unfair contractual terms

A novelty inserted in the EU legal framework is that stipulated under Article 13, concerning unfair unilaterally imposed contractual conditions. Again with regards to B2B data sharing agreements, terms that are, cumulatively:

- imposed by one contracting party without the other contracting's party influence on the content of the term
- unfair

are considered not to be binding (read conjointly with Article 8(2) of the Act).

Article 13(3) provides a general definition of a contractual term deemed unfair, when such term *"is of such nature that its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing*". This term is relatively vague and can be subject to diverse interpretations. In order to provide more precision to general catch-all clause, Article 13(4) and 13(5) introduce two lists of clauses that are either always or presumed to be unfair, as follows:

[117] Article 3(1) of the Data Act.
[118] Article 4(1) of the Data Act.
[119] Article 4(2) of the Data Act.

Unilaterally imposed contractual terms **always considered unfair** (irrebuttable presumption of unfairness)	Unilaterally imposed contractual terms **presumed to be unfair** (rebuttable presumption of unfairness)
a) exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence; b) exclude the remedies available to the party upon whom the term has been unilaterally imposed in the case of non-performance of contractual obligations, or the liability of the party that unilaterally imposed the term in the case of a breach of those obligations; c) give the party that unilaterally imposed the term the exclusive right to determine whether the data supplied are in conformity with the contract or to interpret any contractual term.	a) inappropriately limit remedies in the case of non-performance of contractual obligations or liability in the case of a breach of those obligations, or extend the liability of the enterprise upon whom the term has been unilaterally imposed; b) allow the party that unilaterally imposed the term to access and use the data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party, in particular when such data contain commercially sensitive data or are protected by trade secrets or by intellectual property rights; c) prevent the party upon whom the term has been unilaterally imposed from using the data provided or generated by that party during the period of the contract, or to limit the use of such data to the extent that that party is not entitled to use, capture, access or control such data or exploit the value of such data in an adequate manner; d) prevent the party upon whom the term has been unilaterally imposed from terminating the agreement within a reasonable period; e) prevent the party upon whom the term has been unilaterally imposed from obtaining a copy of the data provided or generated by that party during the period of the contract or within a reasonable period after the termination thereof; f) enable the party that unilaterally imposed the term to terminate the contract at unreasonably short notice, taking into consideration any reasonable possibility of the other contracting party to switch to an alternative and comparable service and the financial detriment caused by such termination, except where there are serious grounds for so doing;

	g) enable the party that unilaterally imposed the term to substantially change the price specified in the contract or any other substantive condition related to the nature, format, quality or quantity of the data to be shared, where no valid reason and no right of the other party to terminate the contract in the case of such a change is specified in the contract.

In order to address the legal uncertainty that arises from these provisions, according to Article 41 of the Act, the Commission is bound, before 12 September 2025, to provide non-binding model contractual terms on data access and use.

4.5.2.3. Obligatory data sharing with public sector bodies

Another data sharing obligation is set out in **Article 14** of the Data Act in the case a public sector body, the Commission, the European Central Bank or other Union body demonstrate an exceptional need for the use of those data. Upon request of any of the mentioned bodies, data holders are obliged to share the data needed, under the condition that the latter are needed from the body to carry out its statutory duties "in the public interest".

The term "exceptional need", however, requires further explanations. In virtue of **Article 15** of the Data Act, this need has to be limited in time and in scope. This need is considered to exist only:

a) where the data requested is necessary to respond to a public emergency and are impossible to be obtained otherwise, in a timely and effective manner;
b) in cases that do not fall under (a) and only insofar as non-personal data is concerned, where:
    a. specific data have been identified, the lack of which prevents the body from fulfilling a specific task carried out in the public interest, that has been explicitly provided for by law, such as the production of official statistics or the mitigation of or recovery from a public emergency; and
    b. all other means to obtain such data have been exhausted, including purchase of non-personal data on the market by offering market rates, or by relying on existing obligations to make data available or the adoption of new legislative measures which could guarantee the timely availability of the data.

Additionally, the public sector body has to respect certain obligations, such as to:

a) abstain from using the data in a manner incompatible with the purpose for which the request was made;
b) implement technical and organisational measures to protect data subjects' rights and freedoms, if personal data must be processed;
c) destroy the data once they are no longer necessary and inform the data holder of the destruction;[120]
d) not use the data or insights about the economic situation, assets and production or operation methods of the data holder to develop or enhance a connected product or related service that competes with the connected product or related

[120] Article 19(1) of the Data Act.

service of the data holder, nor share the data with another third party for any such purposes[121].

4.5.3 Requirements for interoperability of data, data sharing mechanisms and services

4.5.3.1. Introduction

The provisions on data interoperability contained in the Data Act are another step that clarifies the regulatory architecture of European Common Data Spaces. In virtue of **Article 33(1)**, participants in data spaces that offer data or data services to other participants are obliged to provide:

a) machine-readable descriptions of dataset content, use restrictions, licences, data collection methodology, data quality, and uncertainty;
b) publicly available descriptions of data structures, data formats, vocabularies, classification schemes, taxonomies, and code lists;
c) machine-readable (where possible) descriptions of the technical means to access data (e.g. APIs), alongside their terms of use and quality of service;
d) the means to enable interoperability of automation tools for data sharing agreements, such as smart contracts (where applicable).

4.5.3.2. Interoperability of data processing services

According to Article 2(8) of the DA, a "data processing service" is defined as a:

> *"digital service that is provided to a customer and that enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or service provider interaction"*

With regard to the objective of the Data Act to facilitate switching between data processing services, it is necessary for the providers of such services to comply with a set of minimum regulatory obligations in order for pre-commercial, commercial, technical, contractual and organisational obstacles, which would otherwise hamper the effective switching between data processing services, to be eliminated.[122]

To that end, Article 35(1) of the Data Act foresees the objectives that have to be accomplished by open interoperability specifications and harmonised standards for the interoperability of data processing, which are to:

a) achieve of interoperability between different data processing services that cover the same service type (where technically feasible);
b) enhance the portability of digital assets between different data processing services covering the same service type;
c) facilitate functional equivalence between different data processing services referred to in Article 30(1) of the Data Act, covering that cover the same service type (where technically feasible);
d) not have an adverse impact on the security and integrity of data processing services and data;
e) being designed in a way which allows for technical advances and the inclusion of new functions and innovation in data processing services.

[121] Article 19(2) of the Data Act.
[122] See Recital 78 and 79 of the Data Act.

The issues addressed by the same specifications and standards, are also provided for in Article 35(2), which are:

a) the cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioural interoperability and policy interoperability;
b) the cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability;
c) the cloud application aspects of application syntactic portability, application instruction portability, application metadata portability, application behaviour portability and application policy portability.

Articles 35(4) to 35(9) of the Data Act specify which entities are responsible for the drafting of the above: more specifically, common specifications based on open interoperability specifications can be adopted by the Commission by means of implementing acts, and harmonised standards can be requested by the Commission to be drafted by one or more European standardisation organisations. Neither of the two is adopted or drafted to date.

4.5.4. Requirements relevant to UPCAST – contractual freedom restrictions and data sharing obligations

Two of the most essential elements for the evaluation of the UPCAST project with regard to the DA is the **core service provided** (i.e., data market plugins for the automation of data sharing and processing agreements), and the **multiplicity of actors that can be potentially involved** (i.e., businesses, public administrations and citizens).

As B2B data sharing agreements are concerned, for instance in the context of Pilots 1 and 4, Articles 8 and 13 of the DA find application. To the extent that automated data sharing agreements are concerned, the conditions included therein shall be fair, reasonable and non-discriminatory, and ensure that the sharing of data takes place in a transparent manner, as stipulated by Article 8. It shall be furthermore ensured that these predefined conditions included in the automated data sharing agreements by no means include any of the conditions listed as unfair under Article 13(1), and preferably avoid including any of the conditions under Article 13(2) of the DA.

The provisions regarding the mandatory data sharing according to Article 14 do not apply in any of the included Pilots but could be of future use in the context of data sharing with public sector bodies, such as in the case of Pilot 3.

4.5.5. Requirements relevant to UPCAST – requirements for interoperability of data

In consideration of the fact that the UPCAST project is aiming at ensuring the availability of interoperable datasets, the provision of **Article 33(1)** of the DA enumerates the requirements that need to be fulfilled in order to ensure data interoperability. Therefore, UPCAST's standard-compliant plugins shall be compliant with the elements of the said article.

In respect of the requirements for the interoperability of data processing services as set out by **Article 35**, it is crucial to understand if UPCAST's safety and monitored execution plugins offer a data processing service. In the explanation of the plugin's operation, it is mentioned that the relevant modules (MDL 9&10) are ensuring a safe and secure execution of a data processing workflow (DPW). A DPW can be executed on a trusted

centralised cloud provider, such as the Nokia Data Marketplace[123] or the Gaia-X federation services. Moreover, according to the approach followed, UPCAST's plugins will be "built upon" the Nokia Data Marketplace proxy[124], and "supported by" its technology[125]. Data exchange services such as the one provided by data marketplaces fall under the scope of data processing services, as defined in Article 2(8) DA.

However, Article 35 does lay down itself any obligations and/or requirements to be fulfilled by data processing services providers, but merely describes what the content of the open interoperability specifications and harmonised standards for the interoperability of data processing has to be. **Compliance with both open interoperability specifications and harmonised standards will be required once both are drafted and adopted by the Commission** (in the form of an implementing act as regards the specifications) and by the European standardisation body appointed by the Commission (as regards the harmonisation standards) respectively. Consequently, this provision does not, for the time being, require the attention of the Partners, but it shall in the near future.

[123] The Nokia Data Marketplace technology is a "*proven, secure and scalable solution for business-to-business i.e. B2B data exchange (…) [and] facilitate secure, trusted and automated exchange of digital assets in the form of data streams between data buyers and sellers.*" "What is a Data Marketplace?", NOKIA, https://www.nokia.com/networks/bss-oss/data-marketplace/.
[124] See UPCAST Proposal, p. 14.
[125] Ibid, p.35.

5 Sectoral and technology-specific legislation applicable to UPCAST

5.1 Artificial Intelligence Act

5.1.1 Introduction and overview of main provisions

The Regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence, also known as the Artificial Intelligence Act (hereinafter, the ''**AIA**'') is an upcoming regulation that was recently approved by the EU co-legislators. Following the corrigendum procedure, it is awaiting publication in the Official Journal of the European Union. Once published in the official Journal, it will enter into force and start to apply in a phased manner.

Pending publication in the Official Journal, for the purposes of this deliverable the latest version available is used, i.e. the corrigendum of the AIA issued by the European Parliament on 16 April 2024[126]. Therefore, the numbering and text of articles referred to in this deliverable are those resulting for the corrigendum, with the caveat that they might change in the version that will be published in the Official Journal.

As outlined in its Article 1(2), the AIA lays down:

a) harmonised rules for the placing on the market, the putting into service, and the use of AI systems in the Union;
b) prohibitions of certain AI practices;
c) specific requirements for high-risk AI systems and obligations for operators of such systems;
d) harmonised transparency rules for certain AI systems;
e) harmonised rules for the placing on the market of general-purpose AI models;
f) rules on market monitoring, market surveillance, governance and enforcement;
g) measures to support innovation, with a particular focus on SMEs, including startups.

The AIA applies to **different obliged entities**. The main addressees of its obligations are deployers[127] and providers[128] of AI systems[129] or general-purpose AI models[130]

[126] European Parliament. (2024, April 17). Corrigendum to the position of the European Parliament adopted at first reading on 13 March 2024 with a view to the adoption of Regulation (EU) 2024/ ..... of the European Parliament and of the Council laying down harmonised rules on artificial intelligence.https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf.

[127] Article 3(4) of the AIA defines a deployer as ''*a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity*''.

[128] Article 3(3) of the AIA defines a provider as ''*a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge*''.

[129] Article 3(1) of the AIA defines an AI system as ''*a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*''.

[130] Article 3(63) of the AIA defines a GPAIM as ''*an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the*

(hereinafter, ''GPAIMs''), which have their place of establishment or are located in the EU, or place on the EU market AI systems or models, or place on the market GPAIMs, or whose AI systems produce outputs used in the EU. Further to deployers and providers, there are provisions applicable to importers[131] and distributors[132] of AI systems, to product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark, and to authorised representatives[133] of providers that are not established in the Union. Finally, AIA provisions also produce effects for affected persons, that the regulation intends to protect from AI-caused harm.

The AIA establishes a **risk-based framework** that aims to regulate the placing on the market, the putting into service and the use of AI systems and GPAIMs in the EU. The risk-based approach is reflected into the layered approach adopted by the EU legislator in regulating AI systems and models, laying down different obligations depending on the level of risks posed by the AI systems in question. For the purposes of this deliverable, the requirements applicable to providers and deployers of AI systems only should be considered as relevant. An overview of these requirements is provided below.

Article 5 of the AIA prohibits certain AI practices, whose risks are deemed unacceptable. This constitutes, in the risk-based classification of AI-related harm, the highest category.

Chapter III of the AIA, which includes Articles 6 to 49, lays down the provisions applicable to **high-risk AI systems**. Chapter III constitutes a central part of the AIA, and introduces a rather complex system of risk management requirements for AI systems and verification of compliance with such requirements. A system is high risk when: a) it is intended to be used as a safety component of a product or is itself a product covered by (certain) Union harmonisation legislation; and b) the product whose safety component is an AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment prior to is putting into the market or into service. AI systems referred to in Annex III of the proposal are also considered high-risk.

Article 50 of the AIA lays down **transparency obligations** that apply to a list of AI systems described therein, irrespective of whether they qualify as high-risk or non-high-risk systems. These transparency obligations are imposed on account of the specific risks posed by certain AI systems used to interact directly with natural persons, to generate synthetic content, deepfakes, or for emotion recognition or biometric categorization.

Finally, Chapter V lays down general rules applicable to all providers of GPAIMs, mainly relating to transparency, as well as specific rules for providers of GPAIMs with systemic risk. According to Article 51(1) of the AIA, a GPAIM is classified as having systemic risk if it meets any of the following conditions: a) it has high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks; b) based on a decision of the Commission, ex officio or following a

---

way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market''.

[131] Article 3(6) of the AIA defines an importer as ''*a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country*''.

[132] Article 3(7) of the AIA defines a distributor as ''*a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market*''.

[133] Article 3(5) of the AIA defines an authorised representative as ''*a natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation*''.

qualified alert from the scientific panel, it has capabilities or an impact equivalent to those set out in point a) having regard to the criteria set out in Annex XIII.

A general-purpose AI model shall be presumed to have high impact capabilities when the cumulative amount of computation used for its training measured in floating point operations is greater than 10.

Providers of GPAIMs with systemic risk are subject to more stringer requirements, including the obligation to assess and mitigate the systemic risks stemming from the development, the placing on the market, or the use of a general-purpose AI model.

5.1.2 Relevance to UPCAST

5.1.2.1 Introduction, applicability *ratione temporis* and research exemption

In the UPCAST project, AI seems to be employed in connection with the following functionalities:

a) In the context of the smart contracts, AI applications are used for the pricing of the datasets using their meta-data, seemingly without having a safety function;
b) In the context of the environmental impact optimiser, AI applications are used to assess the environmental impact of a data processing workflow.

Further to the direct use of AI applications in UPCAST, partners will develop a methodology for assessing the AI trustworthiness, including aspects such as explainability, transparency, justifiability, social robustness and accountability of the developed tools and frameworks.

Another AI application of UPCAST lies with its task will also deliver a privacy-enhancing federated Machine Learning plugin, which constitutes a solution for private training of ML models on distributed data of individual system participants.

Therefore, the relevance of the AI Act in the context of the UPCAST project **must be examined in relation to the uses mentioned above**, as well as to the self-assessment tool, despite the fact that the latter does not involve the use of an AI system or model *per se*.

At the outset, it must be noted that there at least two reasons for which the AIA would not apply to the use of AI systems and models during the duration of the UPCAST project, but could still be relevant for potential uses following the conclusion of the project.

First, Article 2(6)-(8) provides for a research exemption from the application of the AIA. In particular, the AIA does not apply to AI systems or models specifically developed and put into service for the sole purpose of scientific research and development, and it does not apply to any research, testing or development activity regarding AI systems or AI models prior to their being placed on the market or put into service.

Based on these provisions, the AIA would not apply to research activities, testing and developments for AI systems and models conducted during the UPCAST project, nor for any AI system or model whose intended purposes is limited to scientific research and development. Nonetheless, the ultimate objective of the UPCAST project is to create applications that could be potentially used and commercialised at a later stage, following the conclusion of the project. For this reason, it is necessary to ensure that they are compliant with the AIA, which would apply once the research activity has concluded.

Second, the AIA would not apply, *ratione temporis*, to the activities conducted during the UPCAST project. According to its Article 113, the AIA applies from 24 months from its date of entry into force. Considering that the AIA has not yet been formally adopted, and that it will enter into force on the twentieth day following its publication in the Official

Journal of the EU, it will start to apply after the expected conclusion of the UPCAST project. Nonetheless, since UPCAST solutions are being developed in order to be used after the conclusion of the project, it is essential to assess compliance with the AIA with the aim to ensure that they will be legally-compliant, once put into use.

5.1.2.2 Assessment on the applicability to UPCAST

As concerns the direct uses of AI in the context of the project, it can be concluded that **the AI Act would unlikely find application for such uses**, in light of the following observations.

First, the foreseen uses of AI in UPCAST do not fall into any of the categories of prohibited practices listed in Article 5 of the AIA. Therefore, such uses are not forbidden as such.

Second, the AI systems to be used in UPCAST also do not appear to qualify as high-risk AI systems pursuant to Article 6 of the AIA. First, it appears that they are not intended to be used as safety components of a product, nor that they are themselves products covered by the Union harmonisation legislation listed in Annex I of the AIA. Second, based on the intended use of the AI systems to be deployed in UPCAST, they do not seem to fall into any of the categories listed in Annex III of the AIA. Based on this first assessment, if AI systems used in the context of UPCAST indeed do not qualify as high-risk AI systems, the majority of the provisions of the AIA would not apply to their providers and deployers.

Third, the AI applications to be used in UPCAST do not seem to qualify as general-purpose AI models, nor to be systems with embedded general-purpose AI models (hereinafter, "GPAIMs"). Based on the definition of GPAIMs in Article 3(63) of the AIA, it can be concluded that the applications to be used in UPCAST do not display the level of generality and capability to perform different tasks of GPAIMs, as they are designed to perform specific tasks only.

Fourth, once that the qualification of the AI applications and related practices in UPCAST as prohibited and high-risk has been excluded, and ascertained the absence of GPAIMs embedded in the systems deployed in UPCAST, it remains to be seen if they fall into the category of AI systems whose providers and deployers are subject to transparency obligations under Article 50 of the AIA. Based on the description of the AI systems under scope in Article 50(1-4), UPCAST AI applications should not fall under its scope of application on account of the fact that they are not intended to interact directly with natural persons, they do not generate synthetic audio, image, video or text content, nor deep fakes, and they do not perform emotion recognition or biometric categorisation.

Notwithstanding the likely non-applicability of the AIA to the development and use of the UPCAST AI applications, **the AIA is still relevant for the development of a methodology for assessing AI trustworthiness**. Trustworthiness is not a legal concept, but it is mentioned in multiple recitals and articles of the AIA. There are two recitals of the AIA that mention trustworthiness as the ultimate objective, and rationale, of the AIA requirements on high-risk AI systems[134], while Article 1(1) also specifies that the purpose of the regulation is to promote the uptake of trustworthy AI.

However, it is important to stress that trustworthiness *per se* is not a legal requirement, it is rather an objective pursued by different legal provisions. Trustworthiness is a term widely used in AI policy and ethical discourse, and is generally used to describe the quality of an AI system or model that has certain characteristics in line with ethical principles and meets certain requirements for the protection of individuals, groups and

[134] See recitals 64 and 123 of the AIA.

society from AI harm. Importantly, the HLEG laid down the seven principles for trustworthy AI. In EU law, despite the absence of a legal concept of trustworthiness, this term is widely used by legal scholars, practitioners and policy-makers to refer to the quality of an AI system or model that meets a series of legal requirements. For example, and in line with the use of this term in the recitals of the AIA, a high-risk AI systems that meets the requirements of the AIA could be considered trustworthy.

However, it is important to **distinguish between requirements of trustworthiness** that are part of an ethical discourse or are outlined in soft law (such as the HLEG guidelines on trustworthy AI), which are not legally binding, and **the legal requirements that the AIA lays down for AI systems and models**, that will be directly enforceable and applicable across the EU. While respect of ethical and soft law principles might also lead to compliance with certain legal requirements, as the latter have been largely inspired by the former, it is of crucial importance to keep the two distinguished and not to assume compliance with legal requirements when ethical and soft law principles are respected. If the UPCAST self-assessment methodology is aimed at verifying compliance with legal requirements under the AIA, it is essential that such self-assessment starts from the classification of the relevant AI system or model. As explained above, different legal requirements apply depending on the category that an AI system or model belongs to. Once this classification has been made, the relevant legal requirements can be identified and compliance therewith assessed.

Some of the requirements set in the AIA are summarised in Table 4 below, with brief observations on their relevance to UPCAST.

Table 4. Requirements of the AIA of relevance to UPCAST

Legal provision/requirements	Observations
(Article 2(6-8)) Research exemption The AIA does not apply to AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development. The AIA does not apply to any research, testing or development activity regarding AI systems or AI models prior to their being placed on the market or put into service. Such activities shall be conducted in accordance with applicable Union law.	AIA would not apply to the research, testing or development of AI systems or models during the UPCAST project, insofar as these activities are limited to research and there is no placing on the market or putting into service of the AI systems or models.
(Article 5) Prohibited AI practices Article 5 lists the AI practices that are in any case prohibited	Not relevant in the context of UPCAST
Provisions on high-risk AI systems	
(Art. 6) Classification rules for high-risk AI systems	Relevant to understand the applicability of the majority of the AIA requirements for AI systems, useful in particular in the

	context of the self-assessment under task 4.3.
(**Art. 9 – 15**) **<u>Requirements for high-risk AI systems</u>** The Articles lay down several requirements for high-risk AI systems to be respected by providers. These include obligations on the implementation of a risk management system, on data governance, on technical documentation and record-keeping, on transparency and the provision of information to deployers, on human oversight, on accuracy, robustness and cybersecurity.	Potentially relevant to build the self-assessment tool under task 4.3.
(Art. 17) <u>Quality management system</u> Providers of high-risk AI systems shall put a document quality management system in place that ensures compliance with the AIA.	Same as above.
(Art. 26-27) <u>Obligations of deployers of high-risk AI systems and FRIA</u> The two articles set out key obligations for deployers of high-risk AI systems, mainly regarding use of the systems in accordance with the instructions for use, huma oversight, and performance of the fundamental rights impact assessment.	Article 26 is potentially relevant to build the self-assessment tool under task 4.3, as they set out key obligations for deployers of high-risk AI systems. Article 27 is probably not relevant for the purposes of UPCAST, since none of the uses listed in Annex III of the AIA is contemplated in the Pilots.
(Art. 43) <u>Conformity assessment</u> The Article details which are the conformity assessment procedures that can be followed that providers can follow in order to demonstrate compliance of the high-risk AI systems with Art. 8 – 15 of the AIA.	Potentially relevant to build the self-assessment tool under task 4.3.
(Art. 50) <u>Transparency obligations for providers and deployers of certain AI systems</u> Transparency obligations imposed on account of the specific risks posed by certain AI systems.	Same as above.
(Art. 53) <u>Obligations for providers of GPAIMs</u>	Same as above.

Lays down general rules applicable to all providers of GPAIMs, mainly relating to transparency.	
(Art. 55) <u>Obligations for providers of GPAIMs with systemic risk</u> Lays down obligations on model evaluation, systemic risk management, incident reporting and cybersecurity.	Same as above.

5.2 The Open Data Directive

5.2.1 Introduction and overview of main requirements

Directive (EU) 2019/1024 on open data and the re-use of public sector information[135], also known as the Open Data Directive, establishes a set of minimum rules governing the **re-use** and the practical arrangements for facilitating the re-use of:

a) existing documents held by public sector bodies of the Member States;
b) existing documents held by public undertakings that are:
    a. active in the areas defined in Directive 2014/25/EU;
    b. acting as public service operators pursuant to Article 2 of Regulation (EC) No 1370/2007;
    c. acting as air carriers fulfilling public service obligations pursuant to Article 16 of Regulation (EC) No 1008/2008; or
    d. acting as Community shipowners fulfilling public service obligations pursuant to Article 4 of Regulation (EEC) No 3577/92;
c) research data pursuant to the conditions set out in Article 10.

The Directive does not apply, among others, to documents access to which is excluded or restricted by virtue of the access regimes on grounds of protection of personal data, to documents for which third parties hold intellectual property rights, and to documents access to which is excluded on the ground that they constitute sensitive data under national law, e.g. for statistical and commercial confidentiality or for the protection of national security.

The Directive lays down rules on how requests on the re-use of documents held by the public sector should be processed[136], on the conditions for the re-use of data to which access has been granted[137], including provisions on the available format, applicable charges and other conditions[138] and practical arrangements for facilitating the search of publicly held data[139]. Furthermore, the Directive requires that any applicable conditions for the re-use of documents are non-discriminatory and shared under fair conditions[140]. Specific and additional conditions are laid down for datasets qualified as "high value"[141],

[135] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172 of 26.6.2019.
[136] See Article 4 of the Open Data Directive.
[137] See Article 5 of the Open Data Directive.
[138] See Article 6, 7 and 8 of the Open Data Directive.
[139] See Article 9 of the Open Data Directive.
[140] See Articles 11 and 12 of the Open Data Directive.
[141] See Articles 13 and 14 of the Open Data Directive.

complemented by the provisions of the implementing regulation on high-value datasets[142].

It must be noted that the Open Data Directive does not apply directly in the Member States, as it is a directive that needs implementing laws by the Member States. Therefore, looking at the provisions of the Directive is not sufficient to fully understand its applicability in a given Member State, as national laws should also be looked at to understand how the Directive provisions have been formulated therein.

5.2.2 Applicability to UPCAST

The Open Data Directive is relevant to the use of the UPCAST plugins in the context of Pilot 3, on sharing public administration data for climate across Thessaloniki cities.

This Pilot potentially entails the sharing of data held by public sector bodies. It must be noted that the Open Data Directive provides a **broad definition of public sector body**, as including "the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities or one or more such bodies governed by public law"[143]. In turn, a body is governed by public law if:

> "a) they are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character,
>
> b) they have legal personality; and
>
> c) they are financed, for the most part by the State, regional or local authorities, or by other bodies governed by public law; or are subject to management supervision by those authorities or bodies; or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law[144]".

Based on the definition, the public bodies involved in the Pilot, and that will be sharing the data they hold, are likely to fall under the scope of application of the Open Data Directive. Once that the applicability to the concerned bodies has been ascertained, however, it must be assessed whether the type of data to be shared falls under the scope of the Open Data Directive, considering the list of exclusions set out therein. This assessment must be made on a case-by-case basis, and no conclusions can be provided based on the available information since the data to shared have not been described in detail.

If the data to be shared fall under the scope of application of the Open Data Directive, the relevant provisions of the Directive, as transposed in national legislation, would have to be respected in the context of the Pilot.

5.3 Legislation on copyright and database rights

While they do not have a central role in the analysis presented in this document, partners also should be aware of EU and national legislation on copyright and database rights.

The central piece of legislation on EU copyright law is the **Directive 2001/29/EC** on the harmonisation of certain aspects of copyright and related rights in the information

[142] Commission Implementing Regulation (EU) 2023/138 of 21 December 2022 laying down a list of specific high-value datasets and the arrangements for their publication and re-use, OJ L 19 of 20.1.2023.
[143] See Article 2(1) of the Open Data Directive.
[144] See Article 2(2) of the Open Data Directive.

society145, also known as the **InfoSoc Directive**. This Directive harmonises certain aspects of national copyright laws. While harmonisation does not cover every area of national copyright law, and thus there still may substantial differences in national legislation, it constitutes an important and practical starting point to understand how copyrighted works are protected across the EU. Nonetheless, the Directive should only be looked at as the starting point, and complemented with an assessment of national law, since the copyright protection of works eventually derives from national law.

In the context of UPCAST, the data to be shared may be protected under national copyright law. If this is the case, UPCAST partners must ensure that the copyright of any data to be shared is fully respected.

Further to copyright, another important right of relevance to data sharing activities is the **sui generis database right**. At the EU level, the database right is harmonised **by Directive 96/9/EC on the legal protection of databases**[146].The Directive protects databases whose content has been selected and arranged in certain way by the author. As for copyright, national legislation should be read in combination with the Directive to fully understand which provisions are applicable in practice.

The Directive may also be applicable in certain situations since UPCAST relies on datasets. In particular, it is recommended that data providers and the UPCAST platform verify whether any of the datasets made available are covered by sui generis database rights within the meaning of the Directive, and, if so, make sure to comply with relevant requirements.

5.4 The Trade Secrets Directive

5.4.1 Introduction and overview of main requirements

Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure147, also known as the Trade Secrets Directive (hereinafter, the "**TSD**") introduced an harmonization of national substantive trade secret law. The TSD harmonises central aspects of national trade secret legislation, such as the definition of trade secret, the conditions to qualify the acquisition, use and disclosure of trade secrets as lawful or unlawful, and the enforcement of trade secrets protection. As such, the TSD has harmonized trade secrets protection in terms of both substantive and procedural law. The TSD lays down minimum standards of harmonization that the Member States were obliged to transpose in national law.

For the purposes of this document, the most important provision of the TSD is its **Article 2(1)**, which provides a definition of trade secret by setting out three requirements that must be met by a piece of information to qualify as a trade secret. In particular, a trade secret is information that meets all of the following requirements:

a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to

[145] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167 of 22.6.2001.
[146] 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 of 27.3.1996.
[147] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157 of 15.6.2016.

persons within the circles that normally deal with the kind of information in question;
b) it has commercial value because it is secret;
c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

As Article 2 refers to 'information', it can be argued that trade secrets protect the semantic meaning of data, i.e. the meaning understandable in natural language of the information encoded in the data, and it does not protect data on a syntactic level, which concerns the bits and bytes that compose the data[148].

As a consequence, every type of information can, in principle, be protected as trade secrets, with no limitation that applies prima facie. Based on this definition, it can be noted that many types of data can be trade secrets, including subject matter that could be protected by intellectual property rights such as a patent or copyright. Recital 14 of the TSD offers a glimpse of the large scope of the definition, that includes "know-how, business information and technological information where there is both a legitimate interest in keeping them confidential and a legitimate expectation that such confidentiality will be preserved".

Therefore, much of the data to be shared in the data economy may fairly easily qualify as containing trade secrets, if they have commercial value. There are many types of data, including non-personal data, that can have commercial value, as evidenced by the fact that there are well-developed markets for non-personal data. Where a market already exists for a specific type of data, it could be straightforward to prove the existence of commercial value and of trade secrets, but potential commercial value could also be proved for markets that do not yet exist.

5.4.2 Applicability to UPCAST

The TSD is relevant for any activity entailing the sharing of data that may contain trade secrets. The relevance of the TSD derives from the fact that trade secret owners may have an interest in ensuring that data containing trade secrets is shared in a way that preserves its secrecy, and thus its protectability under trade secrets legislation, in line with the requirements laid down in Article 2 of the TSD.

Therefore, in the context of each of the Pilots of UPCAST, the implementation of certain security requirements may also enable an appropriate protection of trade secrets. This is of fundamental importance to ensure trust in UPCAST technological solutions, as information protected as trade secrets may have significant commercial value, and whoever shares data may want to ensure that its confidentiality is properly protected.

To this end, UPCAST technologies should ensure a level of security in data sharing that enables to fulfil the 'reasonable steps' requirement of Article 2(1) of the TSD. This is the requirement that assumes most importance in the context of data sharing and storage, as it pertains, inter alia, to the level of (cyber)security and confidentiality of the data during the transfer. In particular, the data owner who intends to protect trade secrets contained in the data to be shared and stored would need to ensure that the technical security measures adopted in practice qualify as reasonable steps under the TSD.

While the meaning of which measures qualify as reasonable steps differ across the EU Member States, an analysis of the principles affirmed in the case-law of some EU

[148] J. Drexl, 'Data access and control in the era of connected devices', Report for the European Bureau of Consumers' Union (2018), 101.

Member States allows to identify a set of common features that would most likely belong to the meaning of reasonable steps under the TSD. In particular, these features are as follows:

a) A case-specific contextual assessment is always warranted, because the qualification as reasonable of the measures adopted by the trade secret holder can only be judged on the basis of the circumstances. This does not exclude that a low, objective threshold needs to be met irrespective of the circumstances, such as that the storage of data containing trade secrets is accompanied by measures controlling access to that data;
b) The existence of reasonable steps in a given case must be assessed in light of the principle of proportionality, in order to ascertain if, under the circumstances and considering the capacities of the trade secret holder, the steps taken are proportionate to the value of the trade secret. There are two implications stemming from this conclusion:
    a. The adoption of reasonable steps should always start from an analysis of the information protected as trade secrets;
    b. Reasonable steps can be designed on the basis of the characteristics and available resources of the trade secret holder, and of the costs that can be sustained by the latter;
c) The requirement to adopt reasonable steps does not prescribe the attainment of a specific result, and even less so to achieve optimal and extreme security of trade secrets;
d) Both internal and external steps may be needed, combining different types of safeguards. Based on the national case-law developed at the EU level, it can be argued that reasonable steps may be implemented at four levels[149]:
    a. Organisational, e.g. by limiting access to trade secrets through a strict access policy, marking documents as confidential, splitting confidential information;
    b. Physical, e.g. camera surveillance, physical restriction of access, document destruction and physical authentication and identity verification of personnel;
    c. Legal, e.g. non-disclosure agreements with the relevant employees and collaborators;
    d. Technical/IT, e.g. encryption, obfuscation, remote storage, private use restriction and ad hoc cybersecurity measures.

The features identified above may thus be used as high-level guidance for the adoption of reasonable steps, with the disclaimer that any such steps must always be based on the circumstances of the case and that official guidance on the interpretation of Article 2(1)(c) of the TSD is lacking at present. Despite their high-level guidance, the principles set out above can be used to provide practical recommendations on how to facilitate trade secret protection by default, in particular in the design of technological solutions used for data sharing.

[149] M. De Vroey, & M. Allaerts, 'Trade secrets protection: an interim update of Belgian and EU case law' (2021) Journal of Intellectual Property Law & Practice, p. 1394.

6 Contract automation and the law

6.1 Introductory considerations

This chapter provides a summary of the legal consequences of contract automation, whether it takes place through smart contracts or other technical solutions. However, this chapter is only intended to provide basic considerations on contract automation and the law, for the purposes of starting to guide partners as early as possible in their activities, and it is not meant to be exhaustive because more detailed and comprehensive explanations will be provided in Deliverable 4.6 during the project, ''*Contractual clauses Legal Assessment Report v2*'', which is due by month 30.

Deliverable 4.6 will thus further develop and complete the preliminary considerations presented in this Chapter, and will provide concrete recommendations on the automation of data sharing contracts.

6.2 The legal validity of contracts concluded by electronic means in the EU

In the EU legal order, it is expressly recognised that contracts can be concluded by electronic means, even in the absence of an underlying paper contract in the real world.

At the outset, it must be clarified that there is no EU contract law as such, and the provisions on the validity of contracts, whether electronic or not, are mainly laid down in national legislation. As a consequence, there may be different considerations on the validity of contracts concluded by electronic means depending on the national law to which the contract is subject.

Nonetheless, there are some general considerations that can be made to bring clarity on the validity of such contracts at the EU level.

First, it is EU law that explicitly requires to recognise legal effects to contracts concluded by electronic means. The e-Commerce Directive[150] requires Member States to give electronic contracts a legal status equivalent to the one recognised for paper contracts under national law. In particular, of the e-Commerce Directive states that Member States shall

> "*ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means*".

Therefore, the fact that contracts are concluded by electronic means does not *per se* lead to a different legal status under national law compared to paper contracts. Member States had to adapt their legislation where it required form requirements which are likely to constitute an obstacle to the use of contracts by electronic means, allowing for the electronic equivalent, in particular as concerns requirements for secure electronic signatures[2]. The aim of Article 9(1) was thus to allow for the development of full contract automation. Article 9(2) allows Member States to provide that this principle does not apply to certain categories of contracts, such as those relating to real estate and those governed by family law. Data sharing agreements cannot fall under the scope of the

[150] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178 of 17.7.2000.

exceptions in Article 9(2), with the consequence that they are eligible to the same legal effects of paper contracts.

Second, for a contract to be valid, there must be a verifiable declaration of intent by the parties to enter into the same contract. This is a requirement common to all of the national legal orders of the EU, whose application to contracts concluded by electronic means has been subject to discussions. As argued by author Eliza Mik[151], the conclusion of a contract by electronic means shall not raise issues for the recognition of the valid intentions of the parties to mutually enter into the contract. In support of this argument, she notes the following:

- **The operator's prior intention is embodied in the programming of the system and contract law does not require the minds of the parties to meet in perfect simultaneity.** Computers solely execute human decisions according to the parameters contained in their programs, upon the occurrence of specified conditions. In addition, while there is no direct human involvement at the time of contract formation, the operator's intention can be traced back to an earlier moment;
- **In contract law, the decision-making process behind a statement is generally irrelevant.** Thus, the fact that the system cannot be understood or explained by the operator or the addressee is irrelevant. In most cases, the mental origin of our decisions cannot be understood either;
- **Computers must be regarded as tools.** The computer's autonomy does not change the fact that it is programmed, initiated and/or controlled by the operator and have no goals of their own.

However, in order to have a valid manifestation of the intention of the parties, it is essential that their signatures are legally valid. The validity of signatures made by electronic means is an issue specific to the conclusion of contracts by electronic means, which however has been address by the EU legislator in Regulation 910/2014 (the "eIDAS Regulation)[152]. According to Article 25(1) of the eIDAS Regulation, an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures. This requirement translates the principle of Article 9(1) of the e-Commerce Directive to electronic signature, with the aim to enable legally valid electronic transactions. Moreover, the eIDAS Regulation distinguishes three types of electronic signature: simple, advanced and qualified. Each of these types of electronic signature is given different legal validity in recognition of its different features.

An electronic signature means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign (Articles 3(10) and 26). This type of signature is used for instance when entering the pin code of a credit card or when ticking a box on an online document. The legal value is limited as it does not allow to identify with certainty the identity of the signatory nor to guarantee that the document has not been altered. It can only be considered as a 'prima facie evidence'.

[151] E. Mik, 'From Automation to Autonomy: Some Non-existent Problems in Contract Law' (2020) Journal of Contract Law.
[152] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257 of 28.8.2014.

An advanced signature is an electronic signature that meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable (Articles 3(12) and 26). This signature allows to ensure the identification of the signatory and the integrity of the signed document, and can thus be used as evidence of these elements.

A qualified signature is an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures (Article 3(13)). This type of signature is the most reliable, both technically and legally. This type of signature requires to use the services of a 'trust service provider' (a certification authority) verifies the signatory's identity. According to the eIDAS Regulation, solely qualified electronic signatures have the equivalent legal effect of a handwritten signature and are thus legally binding (Article 25(2)).

Third, there is the issue of proving the existence of a contract concluded by electronic means. Proving the existence of a contract is essential for its enforcement by the parties. To be admitted as evidence in the same way as a paper version contract, smart contracts must meet the criteria of intelligibility and integrity. Intelligibility means that the contract can be read. This implies that any technical means necessary to read the smart contracts are available. In addition, the criteria of integrity entails that both the information in the contract and the medium of the contract have not been altered which implies a high level of security. EU law contains a requirement on the integrity of the contract, which ensures that a minimum standard of integrity is guaranteed across the EU for contracts concluded by electronic means. Article 10(3) of the e-Commerce Directive prescribes that, when a contract is concluded between a provider of information society services[153] and a recipient, contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them. This obligation ensures that recipients possess a copy of the contract that cannot be unilaterally altered by information society service providers, thus setting a minimum level of integrity.

6.3 Legal requirements for smart contracts

The Data Act lays down *ad hoc* requirements for smart contracts in the recently adopted Data Act. The Data Act provides a long-awaited legal definition of smart contracts, and prescribing the essential requirements that they should comply with.

This *ad hoc* regime is particularly relevant for the purposes of this document, as it is addressed specifically to smart contracts executing data sharing agreements. As stated in the recitals of the Data Act, essential requirements for smart contracts have been set out at the EU level in order to promote the interoperability of tools for the automated

[153] Article 1(b) of Directive (EU) 2015/1535 defines an information society service as follows:
"any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.
For the purposes of this definition:

a) 'at a distance' means that the service is provided without the parties being simultaneously present;
b) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
c) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request."

execution of data sharing agreements[8], also with a view to the development of data spaces[154].

The Data Act addresses smart contracts in its Article 36, which lays down essential requirements regarding smart contracts used for executing data sharing agreements. Article 36 is part of Chapter VIII of the Data Act, which is titled interoperability. While Article 36 of the Data Act has a clear connection with the objective to facilitate interoperability of tools in the European data economy, as stated in the recitals, the requirements that it lays down may have consequences beyond interoperability as they introduce a new level of harmonisation on the technical features that smart contracts should exhibit when they execute data sharing agreements.

With regard to the personal data scope of application of Article 36, its obligations are primarily addressed to the vendors of an application using smart contracts to make data available, i.e. to execute a data sharing agreement. In the absence of a vendor, the obligation would fall upon the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement, or part of it, to make data available. As concerns its material scope, Article 36 applies to smart contracts, as defined in the Data Act[155], used to make data available.

According to Article 36(1), vendors or deployers should ensure that smart contracts comply with the following five essential requirements[156]:

- robustness and access control, to ensure that the smart contract has been designed to offer access control mechanisms and a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;
- safe termination and interruption, to ensure that a mechanism exists to terminate the continued execution of transactions and that the smart contract includes internal functions which can reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions;
- data archiving and continuity, to ensure, in circumstances in which a smart contract must be terminated or deactivated, there is a possibility to archive the transactional data, smart contract logic and code in order to keep the record of operations performed on the data in the past (auditability);
- access control, to ensure that a smart contract is protected through rigorous access control mechanisms at the governance and smart contract layers; and
- consistency, to ensure consistency with the terms of the data sharing agreement that the smart contract executes.

The natural or legal person responsible for ensuring that smart contracts comply with these requirements must perform a conformity assessment to verify if the requirements are met in relation to any smart contract provided or deployed and, should such assessment be positive, issue an EU declaration of conformity[157].

The person that draws up the EU declaration of conformity is thus responsible for compliance with the essential requirements of Article 36[158]. Article 36 establishes a mechanism to facilitate the verification of compliance with the essential requirements

[154] See Recital 106 of the Data Act.
[155] See Article 2(39) of the Data Act.
[156] See Article 36(1) of the Data Act.
[157] See Article 36(2) of the Data Act.
[158] See Article 36(3) of the Data Act.

of smart contracts, providing that the Commission shall request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements and that, in some circumstances, the Commission may directly draft common specifications covering any or all of the essential requirements[159]. Compliance of a smart contract with the harmonized standards drafted by standardization organisations, or with the common specifications adopted by the Commission, leads to a presumption of conformity of the smart contract with the essential requirements[160].

6.4 Impact for UPCAST

As regards smart contracts, a full assessment of whether any of the solutions used in UPCAST qualify as smart contracts will be provided in deliverable 4.6. For the time being, it seems that UPCAST solutions are used for the negotiation, rather than the execution, of contracts, and thus they should not qualify as smart contracts. However, as per grant agreement, smart contracts should be deployed using a CeADAR solution. It must be further investigated what this solution entails, how it is structured and with which role within UPCAST.

Regarding contract negotiation and conclusion, as Section 6.2 shows, contracts concluded by electronic means can have legal validity, and the EU legal framework lays down the foundations for facilitating their use with full legal effects equivalent to those of paper contracts. As a consequence, the conclusion of contracts electronically in UPCAST does not encounter significant legal obstacles.

It must be noted, however, that while electronic contracts are not per se opposed by EU, and national, legislation, different requirements on legal validity are laid down across the EU Member States. To provide an overview of how these could relate to UPCAST, Table 5 below lists the legal status of contracts concluded by electronic means under the law of Belgium, France, Italy and Malta, as per the Grant Agreement.

Table 5. Key national provisions on contract validity

Requirement	Observations
Belgian law	
Pursuant to Article 1108 of the Belgian Civil Code, an electronic contract can qualify as a legal contract when the parties can exercise their independent will as to the subject matter of the agreement and the other contracting parties.	This requirement can be easily satisfied by an electronic contract. Any party can access the technical means for executing their will, including after having negotiated it via UPCAST plugins.
An electronic contract can qualify as a valid legal contract when it respects the applicable formal requirements for its validity. For those contracts that only require the exchange of consents between the parties, automated and electronic contract can qualify as valid	The law prescribes that certain types of contracts are valid or opposable only if accompanied by certain formalities that electronic contract cannot always provide. However, data sharing and data use contracts aren't subject to such formalities.

[159] See Article 36(5) and (6) of the Data Act.
[160] See Article 36(4) and (9) of the Data Act.

legal contracts if they allow the parties to freely exchange their wills.	
Pursuant to Article 5.27 of the Belgian Civil Code, an electronic contract can qualify as a valid legal contract if they have a certain subject matter and a lawful cause.	This requirement can be easily satisfied by both (partially) automated contracts and by electronic contracts.
Pursuant to Article 5.69 of the Belgian Civil Code, contracts have the force of law between the parties who concluded them. An electronic contract can therefore qualify as a valid legal contract if it provides the parties with the possibility to have its terms enforced before a court.	Automated contracts can in principle satisfy this requirement to the extent that their terms can foresee the resort to arbitration or judicial authorities. Their (partially) automated nature would not hinder such possibilities. This may prove difficult in electronic contracts given their immutable and generally non-reversible character.
Pursuant to Article 5.57, the sanction for failure to comply with the contract validity requirements is the nullity of the contract.	This requirement should be fairly easy to comply with for automated contracts. It may however prove difficult in electronic contracts. Nullity implies that the effects of the invalid act (the contract) are assumed as though they never took place. However, the irreversible character of electronic contracts sits at odds with this condition.
French law	
Pursuant to Article 1129 of the French Civil Code, for a contract to be valid, the parties need to a) share their genuine consent; b) have the legal capacity to enter into a contract; and c) base the contract on a certain and lawful subject matter.	Same considerations as above regarding exchange of consents; capacity; and subject matter.
Articles 1174, 1366 and 1367 of the French Civil Code allow contracts that require the written form to have this requirement satisfied if they are concluded in an electronic form.	This can be the legal basis for considering blockchain-based contracts as in principle compliant with the written form requirement in French law.
Pursuant to Article 1178 of the French Civil Code, a contract that doesn't comply with its validity requirements shall be considered null and void.	Same considerations as above regarding the challenges posed by nullity of contracts for electronic contracts.
Pursuant to Article 1193 of the French Civil Code, the parties to a contract need	This requirement should be fairly easy to comply with for automated contracts. It may however prove difficult with

to have the possibility to amend the contract upon their wills.	electronic contracts. When a block in the blockchain is validated by a node, thereby triggering the execution of the contractual terms, that block can no longer be amended.
Italian law	
Unless otherwise specified, pursuant to the Italian Civil Code, the parties have the freedom to determine the form they wish their contract to take.	This implies that electronic contracts can at least be used as the vehicle through which a contract can be concluded and subsequently enforced.
Pursuant to Article 8-ter(2) of Law No. 12/2019, upon the digital identification of the contracting parties, electronic contracts are considered to be legally valid contracts as their registration in the blockchain satisfies the requirement of written form.	This Italian law establishes that the registration of an electronic contract on the blockchain satisfies the 'written form' requirement that applies to certain types of contracts. Provided that the electronic contract satisfies other applicable contract law requirements, it can be considered as a legally valid contract if the parties digitally identify themselves.
Pursuant to Article 1331 of the Italian Civil Code, the parties can agree that the contract is based on an irrevocable proposition by one of the parties.	In this case, the electronic contract, because of its immutable character, may represent one form through which that party can make its proposition irrevocable.
Pursuant to Article 1418 of the Italian Civil Code, those contracts that do not comply with their validity requirements are null and void.	Same considerations as above regarding nullity and electronic contracts.
Maltese law	
For an electronic contract to be legally recognised and binding, the parties need to have legal capacity to enter into a contract.	Same considerations as above regarding exchange of consents; capacity; and subject matter.
For an electronic contract to be legally recognised and binding, all the parties intending to conclude the contract need to provide and demonstrate their free and undistorted consent to the agreement.	Same considerations as above regarding exchange of consents; capacity; and subject matter.
For an electronic contract to be legally recognised and binding, the contract shall have a subject (tangible or intangible) that is lawful.	Same considerations as above regarding exchange of consents; capacity; and subject matter.

For an electronic contract to be legally recognised and binding, the contract shall have a lawful consideration.	Same considerations as above regarding exchange of consents; capacity; and subject matter.

7 Conclusions

Data sharing is an activity that is subject to a potentially complex set of rules. In particular, this is the case where datasets to be shared are heterogeneous and can include different categories of data ranging from personal data to data protected by statistical or commercial confidentiality, data qualifying as trade secrets, data obtained from a connected product, and data protected by intellectual property rights. The heterogeneity of data is reflected also in the legal framework, as different provisions apply to different categories of data. These different requirements can apply at once, when datasets are being shared that contain different categories of data, e.g. personal data and data protected as trade secrets. If such situation arises, the organisational and technical measures in place to enable data sharing need to be designed in a manner that ensures compliance with more legal requirements at once. This approach should be followed also when the categories of data that may be shared is not known *ex ante*, and thus compliance by design and by default for different scenarios must be envisaged.

By describing the different requirements applicable to different categories of data, this report aims to facilitate the implementation of measures enabling compliance with all the relevant provisions. In some cases, provisions from different pieces of legislation may be complied with through the same technical and organisational measures, as would be the case for technical arrangements ensuring security of data sharing that are required both under the GDPR and under the TSD if the confidentiality of trade secrets is to be preserved. Therefore, the overview provided in this report should also guide in connecting different requirements and finding common technical solutions, where appropriate, to comply with them.

While the majority of the provisions in the scope of this report apply to specific categories of data, **there are two exceptions**.

First, the rules on the provision of data intermediation services can apply to the use of data sharing technologies irrespective of the type of data being shared. **Second**, the upcoming AIA applies to the development and deployment of AI systems and its applicability is not dependent on whether the processing of a given type of data is involved. For these pieces of legislation, an analysis of the type of service provided to enable data sharing, and of the technologies developed or deployed, is needed to assess their applicability to the project.

Contract law also plays a key role in the UPCAST project. Some preliminary considerations have been provided in this report. As explained above, a more comprehensive analysis will be provided in another deliverable of the project, D4.6.

Overall, the report finds that many EU legislative acts would potentially apply to the use of UPCAST solutions to enable data sharing. The analysis has been carried out based on the scenarios describes in the Pilots and can thus change for applications to different use cases. An important conclusion presented in this report is that the context where the plugins would be deployed is what matters the most. As a consequence, different conclusions have been reached for the different pilots.

As a general note, it should be noted that this report has been drafted **during a period of important transition for the EU legal framework applicable to data processing and data sharing activities**. The EU legislation on data has significantly developed in the last years, with new legislative acts entering into force. Due to the novelty of some of the legislative acts in the scope of this report, their interpretation and applicative implications are still surrounded by some uncertainty. The European Commission is expected to provide guidance in the next future, which will help to clarify many aspects of relevance to UPCAST.

Table 6. Overview of EU legislative acts applicable to UPCAST Pilots

<table>
<tr><th></th><th>Pilot 1</th><th>Pilot 2</th><th>Pilot 3</th><th>Pilot 4</th><th>Other uses (in cases other than the pilots)</th></tr>
<tr><td rowspan="2">GDPR</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td rowspan="2">No incompatibility per se, depends on circumstances of use</td></tr>
<tr><td>JOT and CACTUS as joint controllers (Art 26)</td><td>NHRF as controller (Art 2(7))

Processing of special categories of data requires special attention</td><td></td><td></td></tr>
<tr><td rowspan="2">DMA</td><td>×</td><td>×</td><td>×</td><td>×</td><td>N/A</td></tr>
<tr><td colspan="4">None of the entities qualify as a gatekeeper (Art. 3).</td><td></td></tr>
<tr><td rowspan="2">DSA</td><td>×</td><td>×</td><td>×</td><td>×</td><td rowspan="2">No incompatibility per se, depends on circumstances of use</td></tr>
<tr><td colspan="4">None of the entities offer mere conduit, caching or hosting services (Art. 4-6). However, activities should be constantly monitored throughout the execution of the project in order to ensure that this assessment remains relevant.</td></tr>
<tr><td rowspan="2">DGA</td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td><td rowspan="2">Likely violation of the conditions in Article 12 DGA if the pricing and valuation module is used for the provision of a data intermediation service</td></tr>
<tr><td colspan="4">A case-by-case analysis of the concrete use of the Pilots is needed in order to establish whether any of the entities provide a data intermediation service.</td></tr>
<tr><td rowspan="3">DA</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td rowspan="3">No incompatibility per se, depends on circumstances of use</td></tr>
<tr><td>Obligation to ensure FRAND contracting terms (Art. 8 & 13)</td><td></td><td>Obligation to ensure FRAND contracting terms (Art. 8 & 13)</td><td></td></tr>
<tr><td colspan="4">Compliance with interoperability obligations required (Art. 33(1))

Compliance with both open interoperability specifications and harmonised standards required once both are drafted and adopted by the Commission (Art. 35)</td></tr>
<tr><td rowspan="2">AIA</td><td>×</td><td>×</td><td>×</td><td>×</td><td rowspan="2">N/A</td></tr>
<tr><td colspan="4">None of the Pilots involve the development of AI products. However, it would be advisable that the AIA be taken into consideration when developing a methodology for AI trustworthiness (Rec. 26).</td></tr>
<tr><td rowspan="2">Open Data Directive</td><td>×</td><td>×</td><td>✓</td><td>×</td><td rowspan="2">No incompatibility per se, depends on circumstances of use</td></tr>
<tr><td></td><td></td><td>Compliance with rules regarding the request for re-use of documents</td><td></td></tr>
</table>

			required (Art. 4-14)		
InfoSoc Directive	N/A	N/A	N/A	N/A	No incompatibility per se, depends on circumstances of use
	A case-by-case analysis of the concrete use of the Pilots is needed in order to establish whether any of the documents include copyrighted works.				
TSD	N/A	N/A	N/A	N/A	No incompatibility per se, depends on circumstances of use
	A case-by-case analysis of the concrete use of the Pilots is needed in order to establish whether any of the documents include trade secrets.				

8 References

8.1 Legislation

Charter of Fundamental Rights of the European Union [2006] OJ C 202

Commission Implementing Regulation (EU) 2023/138 of 21 December 2022 laying down a list of specific high-value datasets and the arrangements for their publication and re-use [2023] OJ L 19.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L 201.

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) [2016] OJ L 119.

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L 186.

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), [2022] OJ L 265.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) [2022] OJ L 152.

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data [2023] OJ L 2023/2854.

8.2. Documents from public bodies

Article 29 Working Party (A29WP), 'Opinion 04/2007 on the concept of personal data', WP 136 [2007].

Article 29 Working Party (A29WP), 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' [2014].

Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Towards a thriving data-driven economy' [2014] COM 442 final.

Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Building a European Data Economy' [2017] COM 9 final.

Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European Strategy for data' [2020] COM 66 final.

Commission, 'Communication from the Commission to the European Parliament and the Council - Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union'' [2019] COM/2019/250 final.

Commission, 'Staff Working Document – Guidance on sharing private sector data in the European data economy – Accompanying the document Communication from the

Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Towards a common European data space' [2018] COM 125 final.

Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Towards a common European data space' [2018] COM 232 final.

Corrigendum to the position of the European Parliament adopted at first reading on 13 March 2024 with a view to the adoption of Regulation (EU) 2024/ of the European Parliament and of the Council laying down harmonised rules on artificial intelligence. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf.

European Union Agency for Cybersecurity (ENISA), 'Pseudonymisation techniques and best practices – Recommendations on shaping technology according to data protection and privacy provisions' [2019].

European Union Agency for fundamental rights, European Court of Human Rights, Council of Europe & European Data Protection Supervisor, 'Handbook on European data protection law' [2018].

European Data Protection Board (EDB), 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' [2019].

European Data Protection Board (EDPB), 'Guidelines 7/2020 on the concepts of controller and processor in the GDPR' [2020].

European Data Protection Supervisor (EDPS), 'Necessity Toolkit' 11 [2017].

8.3 Case-law of the Court of Justice of the European Union and the EFTA Court

Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779.

Case T-557/20 Single Resolution Board (SRB) v European Data Protection Supervisor (EDPS) [2023] ECLI:EU:T:2023:219.

Case C-604/22 IAB Europe v Gegevensbeschermingsautoriteit [2024] ECLI:EU:C:2024:214.

Case C-40/17, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV. [2019] ECLI:EU:C:2019:629.

Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH [2018] ECLI:EU:C:2018:388.

Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González [2014] ECLI:EU:C:2014:317.

Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen [2010] ECLI:EU:C:2010:6.

Case C-170/13 Huawei Technologies Co. Ltd v ZTE Corp., ZTE Deutschland GmbH [2015] ECLI:EU:C:2015:477

Case E-6/16 of the EFTA Court Fjarskipti and Icelandic Post and Telecom Administration [2016]

8.4 Literature

M. De Vroey, & M. Allaerts, ‘Trade secrets protection: an interim update of Belgian and EU case law’ (2021) Journal of Intellectual Property Law & Practice.

J. Drexl, ‘Data access and control in the era of connected devices’, Report for the European Bureau of Consumers’ Union (2018).

J. Drexl ‘Designing Competitive Markets for Industrial Data - Between Propertisation and Access’ [2017] JIPITEC 257.

M. Hildebrandt, 'Privacy and Data Protection', Law for Computer Scientists and Other Folk (2020) Oxford Academic.

E. Mik, ‘From Automation to Autonomy: Some Non-existent Problems in Contract Law’ (2020) Journal of Contract Law.

T. Bobev, V. K. Dessers, C. Ducuing, M. Fierens, A. Palumbo, B. Peeters, L. Stähler, ‘CiTiP White Paper on the Definition of Data Intermediation Services’ (2023) accessed on 7 March 2023 at https://ssrn.com/abstract=4589987.