2024

Draft Document

DELIVERABLE 4.4

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

D4.4: CONTRACTUAL CLAUSES LEGAL ASSESSMENT REPORT

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

Title:	Document version:
D4.4 – Contractual Clauses Legal Assessment Report	2.0

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

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type*-Security*:
M15 (March 2024)	M15 (March 2024)	R – PU

*Type: P: Prototype; R: Report; D: Demonstrator; O: Other; ORDP: Open Research Data Pilot; E: Ethics.

**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 Lorenzo Gugliotta Peggy Valcke Viltė Kristina Dessers	KUL	WP4

Authors (organization):
Andrea Palumbo (KUL)
Lorenzo Gugliotta (KUL)

Abstract:
This task analyses the limits of contractual freedom in the context of data sharing agreements (whether or not automated). While contract law is a private institution build on the principle of contractual freedom, this principle is not absolute. The legality of contractual clauses, in particular usage conditions (T2.1 and T2.3), is subject to the respect of rules and principles laid down in statutory law such as the GDPR. The analysis will also, where applicable, consider the requirements applicable for the re-use of protected data held by public sector bodies under the EU proposal for a Data Governance Act as well as the relevant rules under the upcoming EU proposal for a Data Act.

Keywords:
Data sharing agreements, smart contracts, online contracting, data sharing, data sharing platform, contract law, contractual freedom

REVISION HISTORY

Revision:	Date:	Description:	Author (Organization)
V1.0	11.03.2023	Table of content	Lorenzo Gugliotta (KUL)
V2.0	11.03.2024	First draft of the deliverable	Andrea Palumbo (KUL)
V3.0	29.03.2024	Final version of the deliverable	Andrea Palumbo (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

1 INTRODUCTION

1.1 Purpose of the Document

The UPCAST project aims to provide a set of universal, trustworthy, transparent and user-friendly data market plugins for the automation of data sharing and processing agreements between businesses, public administrations and citizens. The plugins would be used to enable, among others, the automatic negotiation and execution of data sharing agreement terms. The negotiation and execution of data sharing agreements by automated means raises a series of legal questions regarding the validity of contracts concluded by electronic means, the legal requirements applicable to smart contracts and the challenges related to the automation of specific contractual clauses. Moreover, while contract law is a private institution built on the principle of contractual freedom, this principle is not absolute but subject to many limitations laid down in EU and national law. Therefore, it is necessary to identify and describe the statutory limitations that may apply to the contractual freedom of the parties constructing data sharing agreements on the basis of the relevant EU legislation. The analysis conducted in this deliverable is based solely on EU legislation, for three main reasons. First, the platform is intended to be used primarily within the European Union, where EU law would apply. Second, it is not yet clear in which specific Member States the technologies in question would operate, or in which third countries outside of the EU, and thus it is not possible to take into account national legislation. Third, the legal framework that would apply to smart contracts and to the sharing of personal and non-personal data is, to a large extent, harmonised at the EU level. Therefore, an analysis based on EU law is expected to cover the main applicable provisions.

The observations put forward in this document are intended to provide guidance also for the performance of tasks 2.1 and 2.3 of the project. As concerns the privacy and usage control module of task 2.1, Chapter 2 of this deliverable guides through the automation of privacy and usage conditions specified in the contractual clauses of data sharing agreements, both at a general level and with more detailed indications in the repository of clauses provided in Section 2.2.3. As clauses on the protection of personal data and the usage conditions of the data exchanged between the parties are commonly inserted in data sharing agreements, they are part of the repository of Section 2.2.3. With regard to pricing and valuation of task 2.3, Chapter 3 describes the main limitations to contractual freedom imposed by EU data legislation in relation to the conditions for making data available, including pricing.

Due to the link between this document and the work to be performed in tasks 2.1 and 2.3 of the project, close cooperation between the partners responsible for WP2 and WP4 shall continue in order to ensure that the input provided by task 4.4 is structured in a way that best provides guidance for tasks 2.1 and 2.3.

1.2 Methodology of the document

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 and evaluative legal research methods have been employed to draft chapters 2 and 3. 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 research. The specific acts of EU law taken into account for the purposes of the research underlying this deliverable are indicated in chapters 2 and 3.

In order to map the challenges related to the automation of contractual clauses and the limitations to contractual freedom in the context of data sharing agreements, this document addresses two separate issues as follows.

Chapter 2 focuses on the automation of data sharing agreements. In order to provide legal guidance that can be used in the course of the project, Chapter 2 explains in which cases contracts concluded by electronic means executed through smart contracts are legally valid, which are the EU legal requirements applicable to smart contracts, and which legal challenges arise from the automation of the most common contractual clauses used in data sharing agreement.

As concerns the analysis of specific contractual clauses in Chapter 2, the following methodology has been followed. First, research has been conducted to gather a database of 72 data sharing agreements used by different types of actors, trying to ensure diversity and account for different types of contractual relationships and industries. The relevant sectors where the selected data sharing agreements have been used include education, healthcare, research and public administration. Moreover, some of the templates used do not relate to a specific sector or use case, but can potentially be used for different scopes. Second, the contractual clauses of the agreements in the database were analysed to select the most commonly used clauses and their alternative formulations in the agreements of the database. These clauses also cover the most essential aspects that must be agreed on in a data sharing agreement, *i.e.* data items to be shared and how they will be shared, legal basis for sharing personal data, data usage conditions, cooperation for enabling the exercise of data subjects' rights, security of the processing, data breach procedures, liability and guarantees of the parties, confidentiality, applicable law, dispute resolution, review, indemnity, notices and complaints, intellectual property rights. Third,

among the most commonly used contractual clauses, those that are most specific to the characteristics of data sharing agreements have been selected. For example, while clauses on dispute resolution, applicable law, notices and complaints are part of most contracts in many jurisdictions, clauses on data usage conditions, security of the processing and data breach are more specific to data sharing agreements. Therefore, those that are not specific to data sharing agreements have been excluded from the scope of this document. Fourth, the contractual clauses thus selected have been grouped based on their subject matter and listed in the table in Section 2.2.3, and an assessment has been carried out in order to identify the challenges that may derive from the automation of their execution through smart contracts (i.e. smart contracts in a broad sense), if any. Comments have been added in the table for each contractual clause in order to explain the challenges related to its automation, following the methodology set out in Section 2.2.3.

Chapter 3 describes the limitations to the contractual freedom of parties stipulating a data sharing agreement that derive from EU legislation. The scope of analysis is thus limited to data sharing agreement, stipulated in any sector and for any purpose, either between professionals or between a professional and a consumer. For the purposes of this document, a consumer is any natural person who is acting for purposes which are outside his trade, business, craft or profession. In order to provide a reader-friendly overview of these limitations and their practical implications, a table has been provided in Section 3.1 describing the legislative source of the limitation, the nature of the legal requirement, and its impact on the content or form of data sharing agreements. The identification of the relevant legal limitations to contractual freedom has been done by looking at provisions with the following features:

i) provisions that prohibit certain clauses or impose conditions for the validity of a contractual clause, for instance that a clause be fair for the party in which it has been unilaterally imposed; and

ii) provisions that require certain matters to be stipulated in the contract or require mandatory contractual clauses, for instance the mandatory information to be provided to consumers in contracts concluded at a distance.

2 AUTOMATION OF DATA SHARING AGREEMENTS

2.1 Introduction and scope of analysis

This Chapter intends to provide guidance on the automation of data sharing agreements by using smart contracts in the context of the UPCAST architecture. To this end, the following sections provide high-level considerations on the automation of data sharing agreements and a repository of the most common contractual clauses used in data sharing agreements, with comments on opportunities and challenges for their automation through smart contracts.

The scope of analysis of this Chapter is limited to the automation of data sharing agreements through smart contracts. For the purposes of this document, a data sharing agreement is any legally binding contract stipulated between a party that transfers or makes available data, named ''provider'', and a party that received the data, named ''recipient''.

As concerns the meaning of smart contract, for the purposes of this document this term corresponds to the legal definition adopted by the Data Act in Article 2, point 39). According to this definition, a smart contract is a ''*computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering*''. While the legal definition refers solely to the use of automated tools for the execution of the contract, this Chapter will also take into account contracts that are concluded by electronic means, in line with the architecture of the UPCAST platform.

The three sections below aim to provide a comprehensive overview of the legal implications associated with concluding by electronic means, and automating, data sharing agreements. Section 2.2.1. addresses the legal validity of contracts concluded by electronic means and of smart contract. Section 2.2.2. sets out the general legal requirements applicable to smart contracts, and the specific issues associated with the automation of the clauses of data sharing agreements. Finally, Section 2.2.3. provides a list of contractual clauses that are most commonly used in data sharing agreements, with the aim to offer more detailed and practical guidance on whether, and how, specific clauses may be executed through smart contracts.

2.2 Considerations on the automation of data sharing agreements

2.2.1. Legal validity of contracts concluded by electronic means and of smart contracts

When contracts are concluded and executed by electronic means, in the absence of an underlying natural language contract in the real world, the traditional concepts of national contract law need to be applied to the digital world. As discussed above, in the EU the requirements for the validity of contract are mainly laid down in national legislation, with the consequence that there may be different considerations on the validity of contracts concluded and executed by automated 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, the e-Commerce Directive[1] requires Member States to give electronic contracts a legal status equivalent to the one recognised for paper contracts under national law. In particular, Article 9(1) 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. It follows that 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 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 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

[1] 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.
[2] See Recitals 34 and 35 of the e-Commerce Directive.

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[3], 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 apposed 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)[4]. 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

[3] E. Mik, "'From Automation to Autonomy: Some Non-existent Problems in Contract Law'," Journal of Contract Law, 2020.
[4] 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.

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'.

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[5] and a recipient, contract terms and general

[5] 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:

- *(i) 'at a distance' means that the service is provided without the parties being simultaneously present;*
- *(ii) '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;*
- (iii) *'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request."*

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. Further to exchanging copies between the parties, integrity may also be achieved by using the blockchain technology, which can be qualified as tamper-resistant[6] and offers security through the distributive character of the infrastructure[7].

2.2.2. Legal requirements for smart contracts

The EU legislator has decided to lay down *ad hoc* provisions for smart contracts in the recently adopted Data Act, providing a 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 execution of data sharing agreements[8], also with a view to the development of data spaces[9].

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

[6] Which means that it not impossible but rather very difficult to change or delete information that has been recorded on a blockchain.
[7] Which entails that each node (computer) of the network stores an exact and updated copy of the blockchain. Hence, as noted by Primavera De Filippi and Aaron Wright in their book *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018), "[i]f a single computer on a network has a complete copy of a blockchain, that blockchain will remain available for the others to access and use. As long as there is an Internet connection, a blockchain can be replicated, and the network can be rebuilt".
[8] See Recital 104 of the Data Act.
[9] See Recital 106 of the Data Act.

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[10], used to make data available.

Article 36(1) of the Data Act lays down five essential requirements that smart contracts should comply with[11]:

- 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[12]. The person that draws up the EU declaration of conformity is thus responsible for compliance with the essential requirements of Article 36[13]. Article 36 establishes a mechanism to facilitate the verification of compliance with the essential requirements 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

[10] See Article 2(39,) of the Data Act.
[11] See Article 36(1) of the Data Act.
[12] See Article 36(2) of the Data Act.
[13] See Article 36(3) of the Data Act.

circumstances, the Commission may directly draft common specifications covering any or all of the essential requirements[14]. 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[15].

2.2.3. List of common contractual clauses in data sharing agreements and challenges of their automation

As smart contracts go beyond the digitalisation of contractual clauses, but are also capable of executing obligations by automated means, the question arises as to which contractual clauses, and legal obligations, are apt to be executed by smart contracts.

In order to execute contractual clauses through code, the natural language of the contract needs to be translated into computer language. This may be an inherently complex task for certain contractual clauses, as computer language is characterised by rigidity and mechanic operation while natural language offers flexibility and room for interpretation. While natural language allows for different interpretations, computer language can only express terms with a unique determined meaning.

The differences between natural and computer language pose the challenge of automating clauses containing ambiguous terms that are common in contractual terminology, such as ''good faith'', ''best efforts'' and ''reasonable''. Many terms commonly used in contracts need to be subjectively interpreted to some degree, and to be adapted to unforeseeable future circumstances. For these terms, automated execution through smart contract seems difficult, as computer language may require unequivocal and non-ambiguous instructions for their execution.

Any execution of data sharing agreements through smart contracts requires consistency between the terms of the contracts and the computer language that executes them. This not only stems from the legally binding force of the agreements, whose implementation requires actions that are in line with the legal basis relied on for their execution, but is now also an explicit legal requirement laid down in Article 36(1)(e) of the Data Act. It remains to be seen how the consistency requirement will be intended in the future, i.e. to what extent a smart contract can be considered consistent with the terms of the data sharing agreement that it executes. As the recitals of the Data Act do not provide

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

guidance on this point, further legal certainty may be provided by future interpretive efforts.

Nonetheless, an analysis of the specific challenges related to the automation of clauses commonly used in data sharing agreements can help to map the challenges related to their execution through smart contracts. In order to provide guidance to the use of smart contracts in the UPCAST architecture, the table below provides a list of the most common contractual clauses used in data sharing agreements and provides comments on the possibility to automate them using smart contracts. The contractual clauses under analysis are broken down in multiple categories based on their purpose and content. For each contractual clause, the table below has columns that provide a description of the topic, the full text of the clause and its alternative formulations in data sharing agreements, and comments on the possibilities and challenges associated with its automation.

There are four types of comments provided as to the possibility to automate contractual clauses:

- No specific challenges with automation, where it is rather straightforward which actions should be implemented to comply with a legal obligation;
- Automation may be possible with caveats, where automation is possible but there may be some challenges due to the need to perform legal reasoning and value judgements;
- Automation may be difficult, where automation is not impossible but there are signification challenges due to the need to perform legal reasoning and value judgements;
- Liability/guarantee provision that may not require automation, where the clause concerns guarantees provided by the parties, their liability regime, and more in general obligations imposed on a single party that cannot be executed through smart contracts, but only by the obliged party directly or within its organisation.

The following three scenarios of contractual relationship between the parties of a data sharing agreement are considered: i) a scenario where the parties act as separate controllers of any data personal data that may be exchanged, ii) a scenario where the parties act as joint controllers of any personal data that may be exchanged, iii) a scenario where the provider of the data acts as the controller, and the recipient as the processor, of any personal data that may be exchanged. These specific scenarios are addressed due to their complexity as they involve personal data.

The contractual clauses under analysis have been selected from a database of 72 different data sharing agreements, the majority of which have been used in the EU or in the UK in recent years.

TOPIC Article 6 GDPR.	**CLAUSE**	**COMMENTS ON AUTOMATED EXECUTION**
Transfer of the data between the parties (items to be shared and sharing methods)		
Data to be shared under the agreement *(unless the agreement covers any transfer of data between the parties in a given period and the data to be transferred is not predetermined)*	The following data will be provided under this agreement: (…)	No specific challenges with automation, there may be tools aimed at verifying that the correct data is provided.
Methods of transfer and	Data shall be provided by PROVIDER in the following manner:	No specific challenges with automation. Since this clause concerns the data transfer covered by the contract, the requisite transfer and security features can be directly embedded in the technical means executing the contract

access to the data	(…) ***ALTERNATIVE*** Data will be provided to RECIPIENT by PROVIDER in a sufficiently secure manner and in a format to be agreed upon by RECIPIENT and PROVIDER. ***ALTERNATIVE*** Data will be transmitted in (…, detail format e.g. cvs) ***ALTERNATIVE*** PROVIDER shall ensure that the data is transferred to the receiving party using the following measures: (…) RECIPIENT shall implement and maintain the following measures for receiving the data: (…)	

Exclusive use of agreed sharing mechanisms	PROVIDER shall disclose the data to RECIPIENT solely via the agreed sharing mechanisms, and each Recipient shall receive such disclosures solely via the agreed sharing mechanisms.	No specific challenges with automation. It can be arranged that automated tools executing the transfer coincide with the agreed sharing mechanisms.
Provider's right to transfer or make available the data	PROVIDER shall ensure that it possesses all the necessary rights and authorizations to transfer/make the data available for the use by RECIPIENT	Automation may be possible with caveats. If deemed appropriate, technical solutions can be put in place to make sure that RECIPIENT, a third party or a computer programme can verify documents given by PROVIDER that prove right to transfer/make the data available. If the verification is carried out by a computer programme, potential challenges may stem from the fact that this assessment might involve some degree of legal reasoning and value judgements.
Security measures	RECIPIENT and any processor relied on by RECIPIENT to process the data shall implement appropriate data security standards, technical and organisational measures to protect the data from (i) accidental or unlawful destruction, (ii) accidental loss, alteration, unauthorised disclosure or	Liability/guarantee provision that may not require automation.

	access, and (iii) any other breach of security ***ALTERNATIVE:*** The Parties undertake to have in place throughout the term of the Agreement appropriate technical and organisational security measures to ensure a level of security appropriate to: a) prevent: i) unauthorized or unlawful processing of the data; ii) the accidental loss or destruction of, or damage to, the data. b) Ensure a level of security appropriate to: i) the harm that might result from unauthorized or unlawful processing or accidental less, destruction or damage, ii) the nature of the data to be protected.	
Legal basis and purposes of data processing		

Processing in accordance with the agreed purposes	RECIPIENT shall process the data strictly in accordance with the purposes mentioned in this Agreement, except where otherwise required by any EU or national law applicable to RECIPIENT. ***ALTERNATIVE*** PROVIDER and RECIPIENT agree that RECIPIENT shall only use the data for the scientific research purposes described in the RECIPIENT's research plan, and shall not be used for any other purposes, including commercial purposes. ***ALTERNATIVE*** The shared data shall be used for the following agreed purposes: (…)	Automation may be possible with caveats. Compliance with this clause may be automated through technical solutions that enable or facilitate purpose limitation by design and by default, for example by using sticky policies. Verification of compliance of the processing with a predefined purpose may however require value judgements.

Verification of legal ground for processing	PROVIDER declares that it has verified that there is an appropriate legal ground for the provision of the data to RECIPIENT in accordance with ***WHERE APPLICABLE*:** PROVIDER declares that it has verified that there is a valid exception to the prohibition to process (insert relevant category of sensitive data, e.g. personal health data, under Article 9 GDPR). PROVIDER declares that it has obtained approval from the relevant ethics committee and/or national authority to the extent required.	Liability/guarantee provision that may not require automation. Obligation on the PROVIDER that cannot be automated by the smart contract. The PROVIDER must carry out a potentially complex legal assessment as to the existence of an appropriate legal ground for the processing under the GDPR.
Warranties/guarantees and liability		
Warranty/guarantees on utility of data	PROVIDER does not guarantee that the data will be accurate,	Liability/guarantee provision that may not require automated execution.

	merchantable or useful to any particular purposes. ***ALTERNATIVE*** PROVIDER undertakes to guarantee that the data will be sufficiently accurate and useful to enable RECIPIENT to (…) ***ALTERNATIVE*** PROVIDER shall ensure that the shared data is: (…) e.g. complete, true and accurate, not amended or manipulated	
Liability of the parties	PROVIDER cannot and shall not be held liable for any claims or damages by RECIPIENT or any third party, in connection with or as a result of the use of the data by RECIPIENT.	Liability/guarantee provision that may not require automated execution.
Liability of the parties	With regard to the data and personal data breaches, PROVIDER/RECIPIENT shall be responsible and liable for any damages,	Liability/guarantee provision that may not require automated execution.

	losses and fines resulting from its own actions or failures to adhere to the terms of this Agreement and applicable data protection law.	
Data processing		
Restricted data processing operations	RECIPIENT shall not carry out any procedures with the data, such as linking, comparison, processing, with which the identity of data subjects could be derived. ***ALTERNATIVE*** RECIPIENT may not process the data for: (…)	Automation may be possible with caveats. Compliance with this clause may be automated through technical solutions that enable compliant data processing by design and by default, for example by using sticky policies. However, automation may be more or less difficult depending on how the restricted operations are described. For instance, whether the re-identification of a data subject occurs may require legal reasoning and value judgements.
Involvement of third parties	RECIPIENT shall not allow third parties that are not expressly mentioned in this Agreement to access or otherwise process the data without prior written approval of PROVIDER.	No specific challenges with automation. Compliance with this clause may be automated through technical solutions that enable compliant data processing by design and by default, for example by using sticky policies.

	ALTERNATIVE RECIPIENT shall not allow third parties that are not expressly mentioned in the Annexes to access or otherwise process the data without prior written approval of PROVIDER, except parties that qualify as data processors and that are relied upon in the context of RECIPIENT's standard business operations.	
Transfers & third party purposes	In no event shall RECIPIENT process the data for its own purposes or those of any third party.	Automation may be possible with caveats. Compliance with this clause may be automated through technical solutions that enable or facilitate purpose limitation by design and by default, for example by using sticky policies. Verification of compliance of the processing with a predefined purpose may however require value judgements.
Liability for data breaches	With regard to the data and personal data breaches, RECIPIENT shall be responsible and liable for any damages, losses and fines resulting from its own actions or failures to adhere to the terms of this Agreement and applicable	Liability/guarantee provision that may not require automation.

	data protection law.	
Notification of data breaches	If RECIPIENT becomes aware of a personal data breach, RECIPIENT shall promptly notify PROVIDER. In such a case the Parties will fully cooperate with each other to remedy the personal data breach, fulfill the statutory notification obligations timely and cure any damages. The term 'personal data breach' refers to articles 33 and 34 of GDPR.	Automation may be possible with caveats. It may not be straightforward to determine which actions are appropriate to fulfil the obligations to cooperate and remedy any damages in any given case, as imposed by the GDPR.
Retention period	The shared data shall be retained for: (…) ***ALTERNATIVE*** Each party will retain the data according to their own retention policy and in line with the GDPR 'purpose limitation' principle.	No specific challenges with automation, insofar as the retention periods are clearly indicated.

	The trigger point for the retention schedule is: (…)	
Method of deletion	Deletion of data in both digital and hard copy shall be secure and auditable. Any third parties engaged to perform deletion will do so under the terms of a formal contract. ***ALTERNATIVE*** Data shall be deleted through the following measures: (…)	No specific challenges with automation.
Data subject rights		
Right to withdraw consent	In the event that the data subject withdraws his/her permission for the use thereof, PROVIDER shall supply RECIPIENT with sufficient information and RECIPIENT shall immediately cease all use of the relevant DATA and shall delete all copies of	Automation may be possible with caveats, there is one interpretive challenge related to the meaning of the term ''sufficient''.

	the relevant DATA. Upon request from PROVIDER, RECIPIENT shall confirm in writing the complete deletion of such DATA	
Information to data subjects	Each party, in relation to their processing of personal data in connection with this agreement, shall provide notice to data subjects about its collection and use of their personal data, including through its privacy notice as required by data protection laws.	Automation may be possible with caveats, as compliance with the transparency requirements under the GDPR requires some degree of legal reasoning.
Assistance to comply with requests from data subjects	The parties each agree to provide such assistance as is reasonably required to enable the other party to comply with requests from data subjects to exercise their rights under the data protection legislation within the time limits imposed by the data protection legislation	Automation may be difficult, as the party that must provide assistance shall understand which actions are required to comply with data subjects requests to the other party, which involves legal reasoning, and assess what assistance would qualify as ‘‘reasonable’’ in a given case.
Remuneration		

Fees	PROVIDER shall provide the data at no cost or with an optional transmittal fee solely to reimburse PROVIDER for the collection and/or preparation of the data.	No specific challenges with automation.
Data protection responsibilities		
Controllership	Pursuant to Article 26 GDPR, RECIPIENT shall be considered as a separate data controller from PROVIDER for the purposes of processing the data. ***ALTERNATIVE*** The Parties acknowledge that the factual arrangement between them dictates the classification of each Party in respect of the Data Protection Legislation. Notwithstanding the foregoing, the Parties anticipate that each Party	Liability/guarantee provision that may not require automation.

	shall act as a separate controller in its own right.	
Related obligations	RECIPIENT shall implement appropriate technical and organisational measures to meet the requirements for data controllers under applicable data protection law.	Liability/guarantee provision that may not require automation.
Subsequent international data transfers		
Geographical scope	The data can only be shared with RECIPIENT established within the EU/EEA or in a country that has been made subject to an adequacy decision by the European Commission.	Automation may be possible with caveats. To be checked if it is feasible to implement sticky policies, conditions for usage and access or any technical solution that allows to block transfers that are not compliant with the relevant contractual and legal provisions.
Conditions for transferring outside of the geographical scope (if allowed)	*(only where the restrictions on the geographical scope listed above are not included in the contract)* RECIPIENT shall not transfer the data (nor permit the data to be transferred) outside of the	Automation may be possible with caveats. To be checked if it is feasible to implement sticky policies, conditions for usage and access or any technical solution that allows to block transfers that are not compliant with the relevant contractual and legal provisions.

	European Economic Area ("EEA"), or a country that has been made subject to an adequacy decision by the European Commission, unless (i) it h (ii) it takes such measures as are necessary to ensure the transfer is in compliance with applicable data protection laws.	
Confidentiality		

Duty of confidentiality	RECIPIENT shall ensure that any person that it authorises to process the data (including RECIPIENT's staff, agents and subcontractors) (an "Authorised Person") is subject to a strict duty of confidentiality RECIPIENT shall not permit any person to process the data who is not under such a duty of confidentiality. The data can only be shared with RECIPIENT established within the EU/EEA. The obligation of confidentiality shall not apply to any disclosure required by law, provided that RECIPIENT notifies PROVIDER of any disclosure required by law in sufficient time so that PROVIDER may express an opposite opinion, if PROVIDER so chooses	Automation may be possible with caveats. To be checked if it is feasible to implement sticky policies, conditions for usage and access or any technical solution that allows to block transfers that are not compliant with the relevant confidentiality obligations.

	ALTERNATIVE (Data sharing for research purposes) The Researcher shall treat any and all information shared by PROVIDER with the Researcher as strictly confidential and shall not disclose it to any third party without the prior written and express consent of PROVIDER as first obtained PROVIDER's prior written consent; and	

Time extension of confidentiality	RECIPIENT shall treat all confidential information as confidential for the duration of this Agreement including any extension thereof and thereafter for a period of [YY] years following termination or expiry of this Agreement.	Automation may be possible with caveats. To be checked if it is feasible to implement sticky policies, conditions for usage and access or any technical solution that allows to block transfers that are not compliant with the relevant confidentiality obligations.
Compliance with the contract and consequences of non-compliance		
Obligation of compliance with the contract and applicable legislation	Each party shall comply with all the obligations resulting from this agreement and from the legislation applicable to the activities to be performed under the contract (the ''applicable legislation'')	Liability/guarantee provision that may not require automation.
Consequences of non-compliance	Any material breach of the agreement or of the applicable legislation by one party shall, if not remedied within x days of written notice from the other party, give grounds to the other party to terminate this agreement	Liability/guarantee provision that may not require automation.

	with immediate effect and to suspend all or part of the sharing activity under this agreement ***ALTERNATIVE*** Where a Party has the right to terminate this Agreement, that Party shall be entitled to terminate the Agreement or suspend all or part of the sharing activity under this Agreement.	

3 OVERVIEW OF LIMITATIONS TO CONTRACTUAL FREEDOM FOR DATA SHARING AGREEMENTS

3.1 Introductory considerations

In the European Union, contract law is a private law institution built on the fundamental principle of freedom of contract[16]. The corollary of this principle is that parties are free to enter into a contract and to choose the terms that should govern their contractual relationship. However, the principle of freedom of contract is not absolute, as national and EU legislation lay down requirements for the validity of contracts as a whole and of specific contractual terms. Contract law has been subject to limited harmonisation at the EU level, with the consequence that the majority of such requirements are part of national law, especially with regard to the conditions for lawful contract formation (e.g. consent of the parties, capacity of the parties, lawful purpose of the contract, etc…).

Nonetheless, the EU legislator has introduced many provisions of direct relevance for the formation and content of contracts in areas where harmonisation was deemed necessary to pursue Union policies and for the harmonisation of the single market. Section 3.1.2. describes the EU legal framework regarding the conclusion of contracts by electronic means and the automation of contract execution. This Chapter is concerned with EU provisions that impose requirements and limitations on the content of data sharing agreements, concluded either between a consumer and a professional or between professionals. On the one hand, data sharing agreements may need to have certain clauses that are prescribed as mandatory, or address certain aspects. On the other hand, EU law lays down prohibitions and conditions on which clauses can be inserted, and which commitments can be agreed, in different categories of contracts, with a direct consequence for data sharing agreements. All of these requirements and limitations lead to constraints on the contractual freedom of the parties, and must be taken into account when drafting and automating data sharing agreements.

[16] Jurgen Basedow, 'Freedom of contract in the European Union' (2008) European Review of Private Law. In this article, Basedow distinguishes between the following different aspects of freedom of contract : freedom to enter into a contract; freedom to select a contractual partner; freedom of classification and content; freedom of form; and freedom of modification. These aspects of freedom of contract may be limited by law.

Section 4.2. presents a list of these requirements and limitations as imposed by EU law, broken down by relevant legislation and topic. For each requirement and limitation, the tables below have columns that provide a description of the topic, the impact on contractual freedom, additional considerations on the meaning and interpretation of the legal requirement, and the full text of the relevant legal provision. The pieces of legislation whose provisions are under the scope of analysis in this Chapter are the GDPR, Regulation (EU) 2023/2854 (the ''Data Act'')[17], Regulation (EU) 2022/868 (the ''Data Governance Act'')[18] and Directive 2011/83/EU (the ''Consumer Rights Directive'')[19].

3.2 List of EU legislative limitations to contractual freedom for data sharing agreements

TOPIC	CLAUSE	DESCRIPTION OF THE RELEVANT LEGAL REQUIREMENT	FULL TEXT OF THE PROVISION
GDPR			
Data processing agreement (where the provider is controller and recipient processor	There must a binding contract between the controller and the processor that sets out the subject-matter and duration of the	Article 28(3) of 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	Article 28(3) GDPR: *Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the*

[17] 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 and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L 2023/2854 of 22.12.2023.
[18] 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), OJ L 152 of 3.6.2022.
[19] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance, OJ L 304 of 22.11.2011.

of any shared personal data)	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. This contract does not need to be standalone, and may integrated in a data sharing agreement.	and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (c) takes all measures required pursuant to Article 32; (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor; (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III; (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account	*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. That contract or other legal act shall stipulate, in particular, that the processor:* *(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on*

		the nature of processing and the information available to the processor; (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.	*important grounds of public interest;* *(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;* *(c) takes all measures required pursuant to Article 32;* *(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;* *(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for*

			exercising the data subject's rights laid down in Chapter III; *(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;* *(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;* *(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the*

			controller or another auditor mandated by the controller. *With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.*
Data Act – Unfair contractual terms			
Prohibition of unfair contractual terms in B2B data sharing	The enterprise which unilaterally imposes a contractual term on data sharing, or liability and remedies for the breach or the termination of data related obligations, to another enterprise cannot formulate this term in an unfair manner	Article 13(1) of the DA prescribes that a contractual term, concerning access to and the use of data or liability and remedies for the breach or the termination of data related obligations, which has been unilaterally imposed by an enterprise on another enterprise, shall not be binding on the latter enterprise if it is unfair. Article 13(6) specifies that a term is unfair it has been supplied by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it. Paragraphs 4 and 5 of Article 13 lay down lists of terms that are, respectively, to be considered unfair in any case and to be presumed unfair under a rebutt Prohibition of unilaterally imposed unfair terms in B2B agreements	Article 13(1),(3),(6) DA: *1. A contractual term concerning access to and the use of data or liability and remedies for the breach or the termination of data related obligations, which has been unilaterally imposed by an enterprise on another enterprise, shall not be binding on the latter enterprise if it is unfair.* *3. A contractual term is unfair if it is of such a nature that its use grossly deviates*

		able presumption.	*from good commercial practice in data access and use, contrary to good faith and fair dealing.* *6. A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it. The contracting party that supplied the contractual term bears the burden of proving that that term has not been unilaterally imposed. The contracting party that supplied the contested contractual term may not argue that the term is an unfair contractual term*.

Data Act – Data sharing agreements implementing the obligation to make available product data and related service data			
Trade secrets protection	Contractual agreement between data holder or trade secret holder and user on measures to protect the confidentiality of trade secrets	According to Article 4(6) of the DA, the data holder or the trade secret holder shall agree with the user proportionate technical and organisational measures necessary to preserve the confidentiality of the shared data, in particular in relation to third parties, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.	4(6) DA: *Trade secrets shall be preserved and shall be disclosed only where the data holder and the user take all necessary measures prior to the disclosure to preserve their confidentiality in particular regarding third parties. The data holder or, where they are not the same person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata, and shall agree with the user proportionate technical*

			and organisational measures necessary to preserve the confidentiality of the shared data, in particular in relation to third parties, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.
Trade secrets protection	Contractual agreement between user and third party on measures to protect the confidentiality of trade secrets	According to Article 5(9) of the DA,	
B2B FRAND and transparent terms and conditions	Data must be made available under fair, reasonable and non-discriminatory terms and conditions and in a transparent manner	According to Article 8(1) of the DA, a data holder that is obliged to make data available to a data recipient must make do so under terms and conditions that are fair, reasonable and non-discriminatory, and in a transparent manner	8(1) DA: *Where, in business-to-business relations, a data holder is obliged to make data available to a data recipient under Article 5 or under other applicable Union law or national legislation adopted in accordance*

			with Union law, it shall agree with a data recipient the arrangements for making the data available and shall do so under fair, reasonable and non-discriminatory terms and conditions and in a transparent manner in accordance with this Chapter and Chapter IV.
Compensation in B2B data sharing	Non-discriminatory and reasonable compensation that may include a margin	According to Article 9(1) of the DA, data holders and data recipients shall agree a reasonable and non-discriminatory compensation in B2B agreements for making data available. Such compensation may also include a margin, but there is no obligation to this end. Article 9(2) of the DA provides for two factors to account for to determine a reasonable compensation: - costs incurred in making the data available, including, in particular, the costs necessary for the formatting of data, dissemination via electronic means and storage; - investments in the collection and production of data, where applicable, taking into account	9(1),(2) DA: *1. Any compensation agreed upon between a data holder and a data recipient for making data available in business-to-business relations shall be non- discriminatory and reasonable and may include a margin.* *2. When agreeing on any compensation, the data holder and the data recipient shall take into account in particular:*

		whether other parties contributed to obtaining, generating or collecting the data in question.	*(a) costs incurred in making the data available, including, in particular, the costs necessary for the formatting of data, dissemination via electronic means and storage;* *(b) investments in the collection and production of data, where applicable, taking into account whether other parties contributed to obtaining, generating or collecting the data in question.*
Data Act – Requirements for smart contracts executing data sharing agreements			
Consistency of smart contracts with data sharing agreements	Smart contracts should be executed in a way that ensures consistency with the meaning of the data sharing agreements that they execute.	Article 36(1)(e) of the DA requires the vendor of an application using smart contracts or the person whose trade, business or profession of smart contracts to ensure that the smart contract complies with a requirement of consistency, i.e. that there is consistency between the code executing a smart contract and the natural meaning of the terms of the data sharing agreement that is being executed.	Article 36(1) DA: *The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others*

		In essence, this requirement mandates that smart contracts are not just technically sound, but also fit for purpose as their execution is consistent with the meaning of contractual terms.	*in the context of executing an agreement or part of it, to make data available shall ensure that those smart contracts comply with the following essential requirements of:* *(…)* *e) consistency, to ensure consistency with the terms of the data sharing agreement that the smart contract executes.*
Data Act – requirements for participants in data spaces			
Provision of information to facilitate the interoperability in data spaces	Participants in data spaces that offer data or data services to other participants shall provide a series of information to facilitate interoperability. This information may either be included in a	Article 33(1) of the DA imposes the following requirements upon participants in data spaces that offer data or data services to other participants: a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described, where applicable, in a machine-readable format, to allow the recipient to find, access and use the data;	*33(1) DA: Participants in data spaces that offer data or data services to other participants shall comply with the following* involves the deployment *essential requirements to facilitate the interoperability of data, of data sharing mechanisms and services,*

	contract or in a separate medium.	b) the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists, where available, shall be described in a publicly available and consistent manner; c) the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously, in bulk download or in real-time in a machine-readable format where that is technically feasible and does not hamper the good functioning of the connected product; d) where applicable, the means to enable the interoperability of tools for automating the execution of data sharing agreements, such as smart contracts shall be provided.	*as well as of common European data spaces which are purpose- or sector-specific or cross-sectoral interoperable frameworks for common standards and practices to share or jointly process data for, inter alia, the development of new products and services, scientific research or civil society initiatives:* *(a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described, where applicable, in a machine-readable format, to allow the recipient to find, access and use the data;* *(b) the data structures, data formats, vocabularies,*

			classification schemes, taxonomies and code lists, where available, shall be described in a publicly available and consistent manner; *(c) the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously, in bulk download or in real-time in a machine-readable format where that is technically feasible and does not hamper the good functioning of the connected product;* *(d) where applicable, the means to enable the*

			interoperability of tools for automating the execution of data sharing agreements, such as smart contracts shall be provided.
Data Governance Act – Clauses on the re-use of data held by public sector bodies			
Prohibition of clauses granting exclusive rights on data held by public sector bodies	Parties to a data sharing agreement cannot agree on clauses that grant exclusive rights, or which have as their objective or effect to grant such exclusive rights or to restrict the availability, in relation to the re-use of data held by public sector bodies.	Article 4(1) prohibits certain agreements or other practices pertaining to the categories of data held by public sector bodies specified in Article 3(1). In particular, it prohibits arrangements that: • grant exclusive rights; or • 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. Article 4 provides for derogations to the prohibition of exclusive arrangements, when necessary for the provision of a service or the supply of a product in the general interest that would not otherwise be possible, or when an exclusive right is granted through an	<u>4(1)-(3) DA:</u> *1. 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.*

		administrative act or contractual arrangement in accordance with applicable Union or national law.	*2. By way of derogation from paragraph 1, an exclusive right to re-use data referred to in that paragraph may be granted to the extent necessary for the provision of a service or the supply of a product in the general interest that would not otherwise be possible.* *3. An exclusive right as referred to in paragraph 2 shall be granted through an administrative act or contractual arrangement in accordance with applicable Union or national law and in compliance with the principles of transparency, equal treatment and non-discrimination.*
Exception to the prohibition of	An exclusive right to re-use data may be granted, by way of derogation from Article	There is one exemption to the prohibition of exclusive rights on data re-use, for cases where it must be granted to the extent necessary for the provision of a service or the supply of a product in the general	4(2)-(4): *By way of derogation from paragraph 1, an exclusive right to re-use data referred to in that*

exclusive arrangements	4(1), to the extent necessary for the provision of a service or the supply of a product in the general interest that would not otherwise be possible.	interest that would not otherwise be possible. As explained by Recital 13, this may be the case where the exclusive use of the data is the only way to maximise the societal benefits of the data in question. To benefit from the exemption, the exclusive right must be provided in the contract in compliance with the law and the principles of transparency, equal treatment and non-discrimination. The duration of an exclusive right to re-use data shall not exceed 12 months. Where a contract is concluded, the duration of the contract shall be the same as the duration of the exclusive right.	*paragraph may be granted to the extent necessary for the provision of a service or the supply of a product in the general interest that would not otherwise be possible.* 3. *An exclusive right as referred to in paragraph 2 shall be granted through an administrative act or contractual arrangement in accordance with applicable Union or national law and in compliance with the principles of transparency, equal treatment and non-discrimination.* 4. *The duration of an exclusive right to re-use data shall not exceed 12 months. Where a contract is concluded, the duration of the contract shall be the*

			same as the duration of the exclusive right.
Data Governance Act – Conditions for contracts for the provision of data intermediation services (DISs)			
Commercial terms and pricing	Prohibition to make the commercial terms, including pricing, of DISs to a data holder or user dependent upon whether the data holder or user uses other services provided by the same DIS provider or by a related entity	Article 12(b) of the DGA states that the provision of a DIS is subject, inter alia, to the condition that the commercial terms, including pricing, for the provision of data 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. This condition impacts the contractual freedom of the DIS provider to include certain contractual terms in its contracts with data holders and users, especially as concerns pricing.	12(a): *The provision of data intermediation services referred in Article 10 shall be subject to the following conditions:* *(…)* *b) the commercial terms, including pricing, for the provision of data 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; *(…)*
Conditions for access to the DIS	Obligation for the provider to ensure that prices and terms of service, and any other contractual arrangement in place, enable access to its service under fair, transparent and non-discriminatory conditions	Article 12(b) of the DGA states that the provision of a DIS is subject, inter alia, to the condition that the procedure for access to the 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. This condition impact the contractual freedom of DISs providers to determine the price and other terms for the provision of the service.	12(f): *The provision of data intermediation services referred in Article 10 shall be subject to the following conditions:* *(…)* *f) 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;* *(…)*
Right to withdraw consent –	If a provider of DISs provides tools for	According to Article 12(n) DGA, one of the conditions to respect when providing DISs is the following: where	12(n) DGA: *The provision of data intermediation*

contracts with providers of DISs	obtaining consent from data subjects of permissions to process data made available by data holders, it has obligations that would respectively result in contractual clauses: • Obligation to specify the third-country jurisdiction in which the data use is intended to take place; • Provide tools to data subjects and data holders to withdraw, respectively, their consent and their permissions.	a data intermediation services provider provides tools for obtaining consent from data subjects or permissions to process data made available by data holders, it shall, where relevant, specify the third-country jurisdiction in which the data use is intended to take place and provide data subjects with tools to both give and withdraw consent and data holders with tools to both give and withdraw permissions to p two rocess data.	*services referred in Article 10 shall be subject to the following conditions:* *(…)* *n) where a data intermediation services provider provides tools for obtaining consent from data subjects or permissions to process data made available by data holders, it shall, where relevant, specify the third-country jurisdiction in which the data use is intended to take place and provide data subjects with tools to both give and withdraw consent and data holders with tools to both give and withdraw permissions to process data;* *(…)*

Data Governance Act – Contractual arrangements on international access and transfer			
Unlawful international transfer or governmental access to non-personal data	Natural or legal persons to which a right to re-use has been granted under the DGA, or a provider of DISs, shall put in place all the reasonable contractual arrangements to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State. This could be in the form of a clause prohibiting the data recipient from transferring or allowing access to data in a way that is contrary to Union or national law. Provide tools to data subjects and	According to Article 31(1) of the DGA, the public sector body, the natural or legal person to which the right to re-use data was granted under Chapter II, the data intermediation services provider or the recognised data altruism organisation shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State.	31(1): *The public sector body, the natural or legal person to which the right to re-use data was granted under Chapter II, the data intermediation services provider or the recognised data altruism organisation shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3.*

	data holders to withdraw, respectively, their consent and their permissions.		
Unlawful international transfer or governmental access to non-personal data	On a contractual level, providers of DISs must put in place adequate contractual clauses to prevent the transfer of or access to non-personal data that is unlawful under Union or national law.	According to Article 12(j), providers of DISs put in place adequate technical, legal and organisational measures in order to prevent the transfer of or access to non-personal data that is unlawful under Union law or the national law of the relevant Member State.	12(j) DGA: *The provision of data intermediation services referred in Article 10 shall be subject to the following conditions:* *(…)* *j) the data intermediation services provider shall put in place adequate technical, legal and organisational measures in order to prevent the transfer of or access to non-personal data that is unlawful under Union law or the national law of the relevant Member State;* *(…)*

Consumer Rights Directive (CRD) – Requirements for distance contracts with consumers			
Mandatory information to be provided in a distance contract with a consumer	The trader shall make sure that the following information forms an integral part of the distance contract, and is also provided to the consumer before the latter is bound by the contract: (a) the main characteristics of the goods or services; (b) the identity of the trader, such as his trading name; (c) the geographical address at which the trader is established and the trader's telephone number, fax number and e-mail address;	Article 6 of the CRD requires traders to provide the consumer with a list of information before the consumer is bound by an off-premises or distance contract. Importantly, this Article has an impact on the content of contracts given that its paragraph 5 requires that this information forms an integral part of the distance or off-premises contract, and therefore should be inserted in one or more clauses of the contract. These information requirements apply also to contracts on digital content that is not supplied on a tangible medium pursuant to paragraph 2 of Article 6. For the purposes of the CRD, digital content is defined as ''data which are produced and supplied in digital form''. Based on this definition, data sharing agreements concluded with consumers should fall under the scope of application of the CRD.	<u>6(1), (2), (5):</u> 1. *Before the consumer is bound by a distance or off-premises contract, or any corresponding offer, the trader shall provide the consumer with the following information in a clear and comprehensible manner*: (list as provided in the left column) 2. *Paragraph 1 shall also apply to contracts for the supply of water, gas or electricity, where they are not put up for sale in a limited volume or set quantity, of district heating or of digital content which is not supplied on a tangible medium.*

	(d) if different, the geographical address of the place of business of the trader; (e) the total price of the goods or services inclusive of taxes, or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated, as well as, where applicable, all additional freight, delivery or postal charges and any other costs or, where those charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable.		5. *The information referred to in paragraph 1 shall form an integral part of the distance or off-premises contract and shall not be altered unless the contracting parties expressly agree otherwise.*

	(f) the cost of using the means of distance communication for the conclusion of the contract where that cost is calculated other than at the basic rate; (g) the arrangements for payment, delivery, performance, the time by which the trader undertakes to deliver the goods or to perform the services and, where applicable, the trader's complaint handling policy; (h) where a right of withdrawal exists, the conditions, time limit and procedures for exercising that right in accordance with Article 11(1), as well as the		

	model withdrawal form set out in Annex I(B); (i) where applicable, that the consumer will have to bear the cost of returning the goods in case of withdrawal and, for distance contracts, if the goods, by their nature, cannot normally be returned by post, the cost of returning the goods; (j) that, if the consumer exercises the right of withdrawal after having made a request in accordance with Article 7(3) or Article 8(8), the consumer shall be liable to pay the trader reasonable costs in accordance with Article 14(3);		

	(k) where a right of withdrawal is not provided for in accordance with Article 16, the information that the consumer will not benefit from a right of withdrawal or, where applicable, the circumstances under which the consumer loses his right of withdrawal; (l) a reminder of the existence of a legal guarantee of conformity for goods; (m) where applicable, the existence and the conditions of after sale customer assistance, after-sales services and commercial guarantees;		

	(n) the existence of relevant codes of conduct, as defined in point (f) of Article 2 of Directive 2005/29/EC, and how copies of them can be obtained, where applicable; (o) the duration of the contract, where applicable, or, if the contract is of indeterminate duration or is to be extended automatically, the conditions for terminating the contract; (p) where applicable, the minimum duration of the consumer's obligations under the contract; (q) where applicable, the existence and the		

	conditions of deposits or other financial guarantees to be paid or provided by the consumer at the request of the trader; (r) where applicable, the functionality, including applicable technical protection measures, of digital content; (s) where applicable, any relevant interoperability of digital content with hardware and software that the trader is aware of or can reasonably be expected to have been aware of; (t) where applicable, the possibility of having recourse to an out-of-court complaint and redress mechanism, to which the trader is		

	subject, and the methods for having access to it.		
Formal requirements for distance contracts - transparency	The trader shall give the information provided for in Article 6(1) or make that information available to the consumer in a way appropriate to the means of distance communication used in plain and intelligible language. In so far as that information is provided on a durable medium, it shall be legible.	Article 8(1) of the CRD lays down the formal requirements for distance contracts, requiring an appropriate and intelligible communication based on the means of distance communication used. Since the information in Article 6(1) is an integral part of the contract, and especially if this information is provided through the contract only, the contract shall be made accessible in a way that is intelligible and appropriate to the means of communication used.	8(1): *With respect to distance contracts, the trader shall give the information provided for in Article 6(1) or make that information available to the consumer in a way appropriate to the means of distance communication used in plain and intelligible language. In so far as that information is provided on a durable medium, it shall be legible.*
Formal requirements for distance contracts – obligation to pay in contracts concluded by electronic means	If the consumer assumes an obligation to pay when concluding a distance contract by electronic means, the trader shall:	Article 8(2) of the CRD requires transparency in relation to the obligation to pay that the consumer assumes in contracts concluded by electronic means, i.e. contracts that are not just concluded by distance but concluded electronically, e.g. on the internet. Smart contracts are an example of contracts concluded by electronic means. For the interpretation of the requirement on transparency regarding the	8(2): *If a distance contract to be concluded by electronic means places the consumer under an obligation to pay, the trader shall make the consumer aware in a clear and prominent manner, and*

	a) make the consumer aware in a clear and prominent manner, and directly before the consumer places his order, of the information provided for in points (a), (e), (o) and (p) of Article 6(1) b) ensure that the consumer, when placing his order, explicitly acknowledges that the order implies an obligation to pay. If placing an order entails activating a button or a similar function, the button or similar function shall be labelled in an easily legible manner only with the words 'order with obligation to pay' or a corresponding unambiguous	placement of an order that implies an obligation to pay, the ECJ provided clarifications with its judgement in case	*directly before the consumer places his order, of the information provided for in points (a), (e), (o) and (p) of Article 6(1).* *The trader shall ensure that the consumer, when placing his order, explicitly acknowledges that the order implies an obligation to pay. If placing an order entails activating a button or a similar function, the button or similar function shall be labelled in an easily legible manner only with the words 'order with obligation to pay' or a corresponding unambiguous formulation indicating that placing the order entails an obligation to pay the trader. If the trader has not complied with this subparagraph, the consumer shall not be*

	formulation indicating that placing the order entails an obligation to pay the trader.		*bound by the contract or order.*
Right of withdrawal – need for consumer's prior express consent and acknowledgement of losing right of withdrawal	A clause shall be inserted into the contract where the consumer provides express prior consent to the performance of the supply of digital content on a non-tangible medium and acknowledges that he/she thereby loses the right of withdrawal.	Article 9 of the CRD establishes the right of withdrawal for consumers that conclude distance and off-premises contracts. However, according to Article 16(m) of the CRD, the right of withdrawal does not apply for the supply of digital content which is not supplied on a tangible medium if the performance has begun with the consumer's prior express consent and his acknowledgment that he thereby loses his right of withdrawal. Therefore, for data sharing agreements, in order for the right of withdrawal not to apply it is necessary to draft contractual clauses in a way that there is a verifiable consumer's prior express consent of the performance of the contact and the acknowledgement of losing the right of withdrawal.	16(m): *Member States shall not provide for the right of withdrawal set out in Articles 9 to 15 in respect of distance and off-premises contracts as regards the following:* *(m) the supply of digital content which is not supplied on a tangible medium if the performance has begun with the consumer's prior express consent and his acknowledgment that he thereby loses his right of withdrawal.*

4 CONCLUSIONS AND NEXT STEPS

This deliverable provides an overview of the challenges and possibilities related to the conclusion by electronic means, and execution by smart contracts, of data sharing agreements, and provides an overview of the limitations to the contractual freedom of the parties for these types of contracts. The observations put forward in Chapters 2 and 3 of this deliverable aim to provide guidance for the development of UPCAST plugins for the automation of data sharing agreements between businesses, public administrations and citizens in the context of the UPCAST project.

The main takeaways of this deliverable can be summarised as follows.

First, the conclusion of a contract by electronic means is not prohibited *per se*, nor somehow opposed in EU law. On the contrary, EU law aims to ensure that contracts concluded by electronic means produce the same legal effects of paper contracts, insofar as certain conditions are met.

Second, the EU legislator has recognised the important role that smart contracts have to play in the European data economy, and thus decided to lay down harmonised requirements applicable to smart contracts. The new requirements on smart contracts, provided for in the Data Act, aim to promote the interoperability of tools for the automated execution of data sharing agreements, and ultimately also to foster the development of data spaces. As a consequence, the new requirements are particularly pertinent to the technical solutions to be developed in the UPCAST project, and the rationale behind these requirements is in line with the overall objective of the UPCAST project. For this reason, compliance with the smart contracts provisions of the Data Act is important to show adherence to the vision of the EU legislator on the development of data sharing infrastructures for the European data economy. Article 36 of the Data Act lays down the requirements for smart contracts, which however raise questions in relation to their legal interpretation and technical implementation. This creates some legal uncertainty in which operators will have to navigate at least for the near future.

Third, while the automated negotiation and execution of data sharing agreements presents some challenges, it is not impossible and many contractual clauses have alternative formulations who are all suitable to automation. The table in Section 2.2.3. provides a list of alternative formulations of each contractual clause, which can be relied on to automate negotiation of data sharing agreements, and provides an assessment of the challenges deriving from the automation of their execution. While automation may be possible in some cases, particular attention must be paid to how it is structured in practice, to ensure that any risks related to automation are properly addressed.

Fourth, there are multiple limitations to the contractual freedom of parties in constructing the terms of data sharing agreements. Most of these limitations

stem from the recent Data Act and Data Governance Act, whose interpretation and applicative consequences are still uncertain in some respects. However, it must be noted that these requirements of the Data Act and the Data Governance Act do not apply to all data sharing agreements, but only in specific circumstances as described in the table in Section 3.2.

It must be stressed that this is the first version of the deliverable, and that an updated version will be developed in M30. While developing the second version, close collaboration will be ensured between all the partners responsible for the task, paying particular attention to establishing continuous dialogue between partners with legal expertise and partners with technical expertise. This dialogue is essential to ensure that the final version of the deliverable provides useful guidance to technical partners, including for the work to be performed under tasks 2.1 and 2.3.