



# **D4.6: CONTRACTUAL CLAUSES LEGAL ASSESSMENT REPORT v2**



This project has received funding from the European Union's Horizon Research and Innovation Actions under Grant Agreement N° 101093216.

Title:	Document version:
D4.6 – Contractual Clauses Legal Assessment Report v2	1.0

Project number:	Project Acronym	Project Title
101093216	UPCAST Project	UPCAST Project

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type*Security*:
M30 (June 2025)	M30 (June 2025)	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:
Alexandra Papageorgiou		
Andrea Palumbo		
Vilté Kristina Dessers	KUL	WP4
Jan de Bruyne		
Peggy Valcke		

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

**Abstract:**

With the main focus of task 4.4 being on the limitations of the contractual freedom in the EU, this deliverable focuses on the more particular question of the qualification of UPCAST Negotiation and Contracting Plugin in light of the smart contracts definition provided by the Data Act. It traces contracts' evolution, with a lengthy analysis on Data Act smart contracts. It also contrasts natural versus formal languages and the role of ontologies. It finally provides an assessment of UPCAST'S NCP and concludes that it falls short of fully autonomous smart contracts. It also briefly examines Data Governance Act's constraints on neutrality and users' activity logging.

---

**Keywords:**

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

---

## REVISION HISTORY

Revision:	Date:	Description:	Author (Organisation)
V.1	03.02.2025	Table of contents (ToC)	Alexandra Papageorgiou
V.2	13.06.2025	Deliverable submitted for review	Alexandra Papageorgiou Andrea Palumbo
V.3	24.06.2025	Final version of the deliverable for submission	Alexandra Papageorgiou Andrea Palumbo



This project has received funding from the European Union's Horizon Research and Innovation Actions under Grant Agreement N° 101093216.  
More information available at <https://upcastproject.eu/>

## COPYRIGHT STATEMENT

The work and information provided in this document reflects the opinion of the authors and the UPCAST Project consortium and does not necessarily reflect the views of the European Commission. The European Commission is not responsible for any use that may be made of the information it contains. This document and its content are property of the UPCAST Project Consortium. All rights related to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the UPCAST Project Consortium and are not to be disclosed externally without prior written consent from the UPCAST Project Partners. Each UPCAST Project Partner may use this document in conformity with the UPCAST Project Consortium Grant Agreement provisions.

# INDEX

## INDEX 5

<b>LIST OF FIGURES</b> .....	<b>6</b>
<b>LIST OF TABLES</b> .....	<b>6</b>
<b>1 INTRODUCTION</b> .....	<b>7</b>
1.1 Purpose and Structure of the Document .....	7
1.2 Methodology of the Document.....	8
<b>2 FUNDAMENTALS OF CONTRACTS IN DIGITAL ENVIRONMENTS</b> .....	<b>9</b>
2.1 From Paper to Digital: the Evolution of Contracts.....	9
2.1.1 Timeline of Contract Evolution.....	10
2.1.2 Degrees of Contract Automation .....	11
2.2 Legal Framework Applicable To Electronic Contracts.....	14
2.2.1 Formation and Validity of E-contracts .....	14
2.2.2 Fairness and Transparency Obligations .....	15
2.2.3 Electronic Signatures.....	16
2.3 (Legal) Nature of Smart Contracts.....	16
2.3.1 Definitional Pluralism of Smart Contracts.....	16
2.3.2 Smart 'Contracts'?.....	17
2.3.3 Smart Legal Contracts (SLCs).....	18
2.4 Technologies Supporting Smart Contracts .....	19
2.4.1 Blockchain.....	19
2.4.2 Other Technologies .....	20
2.5 Smart Contracts under the Data Act (DA) .....	21
2.5.1 Definition of Smart Contracts (Article 2(39) DA).....	21
2.5.2 Technological Neutrality of Smart Contracts (Rec. 104 DA) .....	22
2.5.3 Scope of Application.....	22
2.5.4 Legal Nature .....	23
2.5.5 On the Notion of 'Execution' .....	23
2.5.6 Smart Contracts under the Data Act as Technical Protection Measures on the Unauthorised Use or Disclosure of Data .....	25
2.5.7 Data Provision Agreements and Smart Contracts .....	26
2.5.8 Essential Requirements of Smart Contracts (Article 36 DA) .....	26
2.5.9 Addressees of the Obligations of Article 36(1) DA .....	27
<b>3 MACHINE-READABILITY IN SMART CONTRACTS</b> .....	<b>29</b>
3.1 Natural and Formal Language in Smart Contracts .....	29
3.2 The Role of Ontologies in Smart Contracts .....	30
3.2.1 General Elements on Ontologies.....	30
3.2.2 Ontologies in Smart Contracts .....	31
3.2.3 Legal Standing of Ontologies .....	32
<b>4 EVALUATION OF CONTRACTS CONCLUDED THROUGH UPCAST</b> .....	<b>33</b>
4.1 Description Of UPCAST's Negotiation and Contracting Plugin (NCP).....	33
4.1.1 Overview of the Negotiation and Contracting Plugin .....	33
4.1.2 Contract Representation and Standards .....	33
4.1.3 Policy Management and Conflict Handling .....	33
4.1.4 Integration with Consent and Compliance Technologies .....	34
4.1.5 Automated Reasoning and Negotiation Logic .....	34
4.1.6 Structured Negotiation and Contract Finalisation.....	34
4.2 UPCAST Contracts as Smart Contracts or as Electronic Contracts? .....	35
<b>5 MISCELLANEOUS</b> .....	<b>38</b>
5.1 Contractual Implications of the Limitations Imposed by the DGA on Providers of Data Intermediation Services .....	38
5.1.1. The Regime Governing the Provision of Data Intermediation Services (DIS) .....	38

5.1.2.	Operational Constraints on Data Intermediation Services Relevant for Data Sharing Contracts .....	39
5.1.3.	Operational Constraints Affecting Contractual Freedom and Contractual Practices for Data Sharing .....	39
5.2	Logs of Activities of Users on the UPCAST Platform .....	41
<b>6</b>	<b>CONCLUSION .....</b>	<b>42</b>
<b>7</b>	<b>REFERENCES AND ACRONYMS.....</b>	<b>44</b>
7.1	REFERENCES.....	44
7.2	ACRONYMS.....	47

## LIST OF FIGURES

<b>Figure 1</b>	– Phases of a contract's lifecycle .....	10
-----------------	--	----

## LIST OF TABLES

<b>Table 1</b>	– Levels of Contract Automation .....	14
<b>Table 2</b>	– UPCAST Contracts Qualification under Article 2(39) DA.....	36
<b>Table 3</b>	– Acronyms .....	47

# 1 INTRODUCTION

## 1.1 Purpose and Structure of the Document

The rapid growth of data-driven services has transformed how different entities, from organisations, to public bodies and individuals exchange and monetise data. Central to this evolution are data-sharing agreements and the platforms that enable their formation, execution and enforcement. The UPCAST project responds to this challenge by developing a suite of interoperable, user-centric plugins that streamline negotiation, compliance and automated execution of data-sharing contracts. In exploring these innovations, it becomes essential to consider both the legal parameters that shape contractual freedom and the technological means that support these data transactions.

Building on the previous deliverable 4.6, which provided a comprehensive legal analysis of which European Union's ('EU') legislative acts<sup>1</sup> provide limitations for the freedom of parties to negotiate and automate data-sharing agreements and what those limitations are, this deliverable has a narrower focus on smart contracts, **its main objective being to investigate and conclude on whether UPCAST contracts fit within the definition of smart contracts under the Data Act.**<sup>2</sup> In that sense, it aims at clarifying the applicability (or inapplicability) of the above mentioned legislative acts on the UPCAST technology, thereby providing the guidance necessary to create compliant data sharing agreements, which is the final objective of UPCAST's task 4.4. It also briefly discusses some questions that have arisen in the course of the project, mainly related to the legal standing of machine-readability clauses and ontologies, along with some miscellaneous questions in connection to the Data Governance Act.<sup>3</sup>

Thus, the present deliverable is structured as follows: **Section 2** outlines the evolution of contracts from paper-based instruments to digital and smart contracts, detailing the legal and technological foundations. **Section 3** examines the challenges of translating natural-language obligations into formal, machine-readable formats and explores the role of ontologies in ensuring semantic clarity. **Section 4** applies these insights to the UPCAST Negotiation and Contracting Plugin, assessing whether contracts generated by UPCAST qualify as smart contracts under the Data Act or, alternatively, as electronically concluded agreements. **Section 5** addresses two ancillary issues: the impact of the Data Governance Act's neutrality requirements on data-intermediation

<sup>1</sup> 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) 2023 (OJ L, 22/12/2023); 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 152/1, 3/6/2022); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 (OJ L 119/1, 4/5/16).

<sup>2</sup> Data Act.

<sup>3</sup> Data Governance Act.

Commented [HJ1]: I believe that this deliverable objective is to provide actionable tools and guidance for creating compliant data-sharing agreements.

services and logging obligations. Finally, **Section 6** summarises our conclusions and highlights areas for further research.

## **1.2 Methodology of the Document**

This deliverable has been drafted in an identical manner with that of D4.4, i.e. by conducting doctrinal legal research and, where necessary, by integrating computer science-related insights. As part of the doctrinal legal research, descriptive, explanatory and evaluative legal research methods have been employed. 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 considered for the purposes of the research underlying this deliverable are indicated where appropriate.

## 2 FUNDAMENTALS OF CONTRACTS IN DIGITAL ENVIRONMENTS

Contracts have come a long way from ink-and-parchment promises to lines of executable code. This section starts with a short history of contracts in [Sub-section 2.1](#), by situating modern contract law within its philosophical and doctrinal roots – from Plato’s advocacy of written promises and Roman categorisations to the late-20th-century Principles of European Contract Law. This brief consideration of history is necessary in order to comprehend and conceptualise modern forms of contracts. Building upon this narrative, [Sub-section 2.2](#) examines briefly the EU’s legislative framework conferring legal validity and consumer-protection safeguards on e-contracts. [Sub-section 2.3](#) then goes on to interrogate definitional pluralism and doctrinal debates, by distinguishing between mere code-based protocols and fully fledged ‘smart legal contracts’. In [Sub-section 2.4](#) an overview of different technologies that underpin smart contracts is provided. Finally, [Sub-section 2.5](#) assesses the Data Act’s functional definition, scope, and essential requirements with respect to smart contracts.

### 2.1 From Paper to Digital: Contracts’ Evolution

The first discussions on the concept of contracts were already made in ancient times by **Plato**. In his work *Laws*,<sup>4</sup> written in the last years of his life (around 360–347 BCE), Plato explicitly addresses contracts, arguing that written agreements should be legally binding and that disputes over contracts should be resolved through legal means. He distinguishes between voluntary contracts (such as trade agreements and sales) and involuntary interactions (such as fraud or coercion). He also advocates for fairness and ethical dealings, warning against deception in contractual relations. His perspective on contracts is deeply tied to his broader philosophy of law and justice; he sees them not just as legal tools but as instruments for maintaining social harmony and ethical behaviour in the city-state. At the same time, **Roman law** provided already an early division of different types of contracts, with respect to the nature of each transaction.<sup>5</sup>

Contract law has developed and systematised immensely since then. Fast forward to the late 20th century, **the Principles of European Contract Law (PECL)** were developed by the self-styled Commission on European Contract Law, set up by the Lando Commission, in the framework of Resolution of 26 May 1989 on action to bring into line the private law of the Member States.<sup>6</sup> Revised in 1998-1999, PECL are based on the concept of a uniform European contract law system, and contain provisions on the

---

<sup>4</sup> Plato, *Laws*, Book 11, 920d.

<sup>5</sup> Barry Nicholas, *An Introduction to Roman Law* (Oxford : Clarendon Press 1962).

<sup>6</sup> European Parliament, Committee on Legal Affairs, ‘Resolution on Action to Bring into Line the Private Law of the Member States’ (1989) OJ C 158.

formation, validity, interpretation, and performance of contracts.

A contract is concluded if:

- a) the parties intend to be legally bound, and
- b) they reach a sufficient agreement without any further requirement.

In order to ensure a common understanding of the elements to which reference will be made in other points of the present deliverable, the **phases of a contract's lifecycle** can be resumed as follows:



**Figure 1** – Phases of a contract's lifecycle

### 2.1.1 Timeline of Contract Evolution

For the purposes of the present deliverable, the focus will be placed upon the transitory phase of contracts from paper to electronic format, up until the appearance of smart contracts. Alma and Piatti (2024) divide this period in **three (3) distinct phases**:<sup>7</sup>

1. **Instrumental**: The first phase of computerisation of legal tools started taking place in the mid-1990s, with the vast expansion of computer usage. During that phase, the drafting of contracts takes place through the use of electronic tools and then contracts are printed out and signed with a handwritten signature. Electronic contracts produced during that phase enjoy a very limited degree of autonomy and self-sufficiency, given the decisive role that the human presence and interaction plays in the formation of the contractual relationship.
2. **Telematica**: brought by the breakthrough offered by the **Directive 1999/93/EC on electronic signatures**<sup>8</sup>– with its practical implementation following only a decade later – this second phase marks the beginning of the slow emancipation from the pure paper-based conception of contracts towards the creation of new contractual arrangements which are essentially paperless. The possibility for contracting parties to fix electronic signatures on electronic documents opens the door to the simplification and increase of speed of all transaction activities. Examples include more complex operations such as the opening of a bank account to simpler ones,

<sup>7</sup> Roberto Alma and Lorenzo Piatti, 'Smart Contract: The Contract Automation Climax: Back-End and Front-End Legal Implications', *Blockchain and Smart-Contract Technologies for Innovative Applications* (Springer, Cham 2024).

<sup>8</sup> Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures 2000 (L 13/12) 269.

such as online purchases, where the checking of a box with a tick suffices for the conclusion of a commercial contract to be complete. Nonetheless, it is still the case during this second phase that the level of autonomy of the contract remains limited: anything occurring following the execution of the contract (e.g. withdrawal, modification, etc.) is still entirely dependent on the human factor.

3. **Automata**: the third – and current – phase of this natural evolution constitutes the product of the merging of the two contractual moments that were still separate during the *Telematica* phase: contract formation and execution. The paradigm shift brought about this combination of elements is twofold: On the one hand, a **content shift**, where the language used in the contract is no longer (only) human readable but also becomes machine readable. And on the other hand, this first shift results in rendering the execution of the contract immediately enforceable. The innovativeness of this shift, inasmuch as it brings enormous possibilities for the development of contract law as we know it, results, at the same time, in the creation of numerous questions of legal nature that need to be tackled with in order to ensure legal certainty. Legal scholars and lawyers are called upon to understand, and evidently have been already grappling with, the specific implications that this automation and digital transformation of contractual obligations, which are being expressed in machine-readable forms, brings about.<sup>9</sup> In the epicentre of this phase is found nothing else but the **smart contract (SC)** itself, the inevitable outcome of this transformation.

### 2.1.2 Degrees of Contract Automation

In a similar, but in a more granular manner, *Wilkinson and Guiffre* represent the evolution of contract automation by referring to different levels of automation:

- ❖ **Level 0 (paper contract)**: this type of contract is drafted digitally, negotiated digitally by exchanging marked-up changes, and then in its final form, it's printed out to then be signed by the parties to provide a complete original record of the executed contract (paper contract). In case the signed paper contract is afterwards scanned, this level extends to include also the digital file created by simply scanning the original paper contract, but only if this happens without applying a technology that digitised the text (e.g. OCR).
- ❖ **Level 1 (digitally accessible)**: the primary record of the contract is stored in a digitally accessible form (digital contract). This may happen either by adding digital capability to a paper contract by applying OCR to a scanned contract (OCR digital contract), or by executing the contract electronically without printing a copy in any number of ways (electronically signed contract / digitally signed contract). The substantial difference between contracts included in this level from the ones

---

<sup>9</sup> Susannah Wilkinson and Jacques Guiffre, 'Six Levels of Contract Automation: The Evolution of "Smart Legal Contracts"' in Jason Grant Allen and Peter Hunn (eds), *Smart Legal Contracts* (Oxford University Press 2022).

included in the previous one, is the additional digital capability of providing the machine-readability of the text itself (though not its meaning, i.e. not semantic machine processing)

- ❖ **Level 2 (meaning can be processed)**: exactly as it was the case on Level 1, the primary record of the contract exists in a digitalised form, meaning that **both Level 1 & 2 contracts will include basic semantic data** which provide some Level 2 functionality, **but Level 2 functionality can be available only where a digital contract includes more detailed, structured contractual data** (and thus, an OCR contract alone cannot meet the requirements of Level 2). In Level 2, semantic information is added via encodement into the digital contract in two possible ways:
  - ✓ either by a human, using a specialist digital contract authoring software that includes the ability to encode structured data at the outset, such as denoting contractual elements as specific data types or tagging them with information about the element,
  - ✓ or by a machine, by machine learning or other advanced analysis techniques that can be applied to digital contract texts once created in order to automatically encode semantic information.

Commented [LI2]: comma, to avoid pausing before "once"

In both of the abovementioned cases, useful structured data about the contract (such as terms, clauses, and headings) are available, and they can be tagged with logic structures. Moreover, key elements of the contract text can be identified as specific data types, and digital data templates (customisable by the parties) and internal requirements are considered.

- ❖ **Level 3 (specialised digital platform)**: building upon what was previously said for Level 1 and 2 contracts, the primary record of the contract is a digital one. Nevertheless, Level 3 contracts must be **stored on a specialised digital platform** that provides a synchronous shared view of a digital instance of the contract, and most importantly, allows for amendments and variations to the contract to remain synchronised and mutual as a record of the contract. With respect to the specialised digital platform and what this pertains to, use of simple shared drives (e.g. Dropbox or Google Drive) would furthermore necessitate agreeing on any changes after execution on an off-platform level, and the consequent update on-platform to be done manually. As such, these shared drives do not fall under the term of specialised digital platforms.

It should be furthermore noted that Level 3 contracts' view is read-only; in other words, it is not possible for the contract to be directly updated in real time by automated provisions that modify the contract in a direct manner. The same applies for the addition of semantic information as described for Level 2; however, the fully mutual and synchronous view of Level 3 document offers both parties to be assured that the data they are integrating into their systems directly from the contract is the same structured, semantic data that the other party has agreed to; as a result, a

certain amount of uncertainty is removed as far as that data is concerned.

- ❖ **Level 4 (automated performance)**: once a shared view of the digital contract on a specialist platform is available, functionality can be added to allow for coded provisions of the contract agreed by the parties to provide a contractually endorsed automation of performance of certain parts of the contract > this platform must provide a method for the parties to indicate their binding agreement to certain code which itself requires the parties to indicate their binding agreement to certain code which itself requires the parties to fully understand the mechanism that will run the code, how it will access and generate data, and ultimately, satisfy obligations and establish rights

Coded provisions can provide for automated performance of certain obligations that can be entirely reduced to algorithms, given the appropriate data sources, or can provide for identified data within the digital contract to be tagged and paired with relevant automation à events contemplated by the contract may be confirmed upon agreed values being reported by IoT sensors ... connecting to third parties through published Application Programming Interfaces (APIs) or publicly available data services can deal with events within those third parties' control, such as confirmation of payments being made and calculation of price adjustments based on published rates.. each of these automated provisions require the ability to update the contract (such as a price list) or other contractually agreed data, such as the immutable record of transactions performed under the contract >> the specialised digital platform that hosts such contracts must then offer read-write functionality, updating these data according to the mutually agreed rules included in the digital contract, interpreted in accordance with the rules of the platform which would be agreed by reference

- ❖ **Level 5 (fully autonomous)**: contracts on this level are fully automated. The provisions contained are automated for all contract tasks and can operate **without human intervention**. This level of automation is, at least for the time being, difficult to implement and thus, hard not envisageable.

**According to the authors, reference to Smart Contracts can only be made from Level 3 onwards.**

Contract Level	Format		Digital accessibility (machine-readability)	Semantic information (incodemen)	Specialised digital platform	Automated performance	Full automation
	Paper	Digital					
Level 0	x						

**Commented [LI3]:** Full stop? Also is the text repetition below intentional? It does make sense but it might need restructuring.

**Commented [LI4]:** typo?

**Commented [LI5]:** Missing word of typo

**Commented [LI6]:** comma?

**Commented [LI7]:** full stop?

**Commented [LI8]:** do not understand this sentence, unless this is some legal jargon, I suggest "out of scope"

**Commented [HJ9]:** I believe we need to ensure that the subjects discussed are closely linked and scoped to our project. For example, from a legal perspective, we could highlight where UPCASt fits within the different degrees of contract automation.

**Commented [LI10]:** encoding?

Contract Level	Format		Digital accessibility (machine-readability)	Semantic information <b>encodemen</b>	Specialised digital platform	Automated performance	Full automation
	Paper	Digital					
Level 1		x	x				
Level 2	x		x	x			
Level 3	x		x	x	x		
Level 4	x		x	x	x	x	
Level 5	x		x	x	x	x	x

Commented [L110]: encoding?

Table 1 – Levels of Contract Automation

Commented [L111]: Format hiccup with those two subsection numbers on the left?

## 2.2 Legal Framework Applicable To Electronic Contracts

Reiterating to an extent what was analysed briefly in the first version of the legal assessment of contractual clauses in D4.4, the legal framework governing electronic contracts in the EU is built upon several key instruments that aim to ensure that **contracts concluded by electronic means are valid, enforceable, and secure**. It should be noted at the outset that the following analysis is not exhaustive (i.e. there are many other legislative acts that are relevant) but merely focuses on several fundamental pieces of legislation in the context of the present deliverable.

### 2.2.1 Formation and Validity of E-contracts

The general principle upheld by EU contract law is that of technological neutrality: contracts can be concluded by any means that can sufficiently demonstrate the parties' agreement. **Directive 2000/31/EC ('e-commerce Directive')**<sup>10</sup> gives a legal basis for electronic commerce in the European Union and sets rules regarding the provision of information society services, including the legal validity of contracts concluded through electronic means. Its **Article 9** specifies that:

*'1. 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*

<sup>10</sup> 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) 2000 (OJ L 178, 17/7/2000) 1.

*legal effectiveness and validity on account of their having been made by electronic means.'*

This validation of electronic contracts happened in a rather minimalistic manner, with the obstacles to be removed by Member States being purely legal and not technical.<sup>11</sup> The EU's legislature objective was merely to achieve a **functional equivalence** of traditional and electronic contracts, leaving, however the question of fulfilment of formal requirements to be examined on a national level.

### 2.2.2 Fairness and Transparency Obligations

For contracts concluded electronically, [Article 10 of the e-commerce Directive](#) imposes pre-contractual information duties. In other words, service providers ought to give to the service recipient in a clear, comprehensible and unambiguous manner a specific set of information *prior to the conclusion of the contract*. That information includes, at least:

- (a) *the different technical steps to follow to conclude the contract;*
- (b) *whether or not the concluded contract will be filed by the service provider and whether it will be accessible;*
- (c) *the technical means for identifying and correcting input errors prior to the placing of the order;*
- (d) *the languages offered for the conclusion of the contract.*

Another piece of legislation that touches upon electronic contracts is [Regulation \(EU\) 2019/1150 on promoting fairness and transparency for business users of online intermediation services \(P2B Regulation\)](#)<sup>12</sup> which governs the contractual relationship between online platforms and business users. In the context of data marketplaces, as the case at present, this relationship is typically governed via electronic contracts. More specifically, its Article 3 foresees that Terms and Conditions (T&C) must, *inter alia*, be clear, easily available, and drafted in plain language, and its Article 8 includes provisions which aim at ensuring that electronic contracts do not unfairly restrict or suspend a business user without proper reasoning and due process. Overall, the P2B Regulation makes sure that contractual relationships of online intermediation services (data marketplaces, in the case at present) and business users are not one-sided, and that business users (data providers, in the case of data marketplaces) are protected against unfairness.

Commented [HJ12]: do not unfairly restrict or suspend

Similarly, [Directive 2011/83/EU on consumer rights \(CRD\)](#)<sup>13</sup> applies only with respect

<sup>11</sup> Yuseph Farah, 'Electronic Contracts and Information Society Services Under the E-Commerce Directive' (2009) 12 Journal of Internet Law 3.

<sup>12</sup> Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services 2019 (OJ L 186/57, 11/7/19).

<sup>13</sup> Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer

to consumers (i.e. in B2C contractual relationships), and imposes contract obligations to traders (amongst which, online marketplace providers are explicitly mentioned) imposing general obligations of pre-contractual information of consumers (Article 6) and as well as specific information requirements for contracts concluded on online marketplaces (Article 6a).

### 2.2.3 Electronic Signatures

Regulation (EU) 910/2014<sup>14</sup> on electronic identification and trust services for electronic transactions in the internal market (eIDAS) defines a legal framework for electronic identification/authentication means and trusted services for electronic transactions in the EU. It sets conditions and requirements for the issuance of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, and qualified certificates for website authentication. While each EU Member State defines the legal value and governing laws for these trust services, eIDAS allows Member States to introduce additional services to the framework. This ensures trust service providers can market their products within a legally safeguarded ecosystem, thus providing greater security. At the same time, it also imposes legal responsibility on providers to maintain the quality and reliability of their services.

**It should be clarified that eIDAS does not aim at creating a unified EU identity for users but instead focuses on interoperability among Member States' identity systems.** Given the variations in privacy and security standards across Member States, a Level of Assurance (LoA) system was developed. The LoA includes three tiers – low, substantial, and high – that represent the confidence level in verifying a user's identity.

The main point of relevance for the purposes of the present deliverable is that eIDAS confirms that **electronic signatures are legally valid and enforceable, also on a cross-border level.**

## 2.3 (Legal) Nature of Smart Contracts

### 2.3.1 Definitional Pluralism of Smart Contracts

There is an abundance of definitions of what a smart contract are in literature, which **serve as proof that there are diverse approaches to a concept that is still developing and shaping itself.** The first to coin the term of smart contracts already in 1996, Szabo in his work of reference '*Smart Contracts: Building Blocks for Digital Markets*' defined a smart contract as a set of promises, specified in digital form, including protocols within

---

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 (OJ L 304, 25/10/2011) 64.

<sup>14</sup> 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 2014 (OJ L L 257/73, 28/8/14).

Commented [HJ13]: I believe there is formatting issue as we have 2.3 then 2.2.

Commented [LI14]: empty 2.2 subsection?

which the parties perform on these promises.<sup>15</sup>

According to *Clack et al.*, a smart contract is an '**automatable and enforceable agreement**', whereby automatability is provided by a computer (even though certain parts may necessitate a certain level of human input and control) and enforceability is ensured either by legal enforcement of rights and obligations or via a tamper-proof execution of computer code.<sup>16</sup>

Drawing from those two definitions, *Allen* defines a 'smart contract' as a 'recording of a legal agreement between parties that is written in a language that is both human intelligible and machine-readable, whose text incorporates an algorithm which automates some or all performance of the agreements'.<sup>17</sup> As such, both the performance and the execution of smart contracts relies less on the parties' further actions or the presence of an intermediary, third party, such as a lawyer or a court.

*Alma and Piatti* define smart contracts as '*a set of strings of code that given a certain input, process it following certain instructions to return an output*'.<sup>18</sup>

### 2.3.2 Smart 'Contracts'?

There has been undoubtedly a lot of enthusiasm around the idea of smart contracts, given their potential to encode and automate complex agreements. Nevertheless, there has been doubts casted upon the qualification of smart contracts as contracts, mainly based on the claim that, smart contracts are simply computer programs; as a result, they are not to be called proper contracts at all. Despite the possibility of code indeed covering several of the issues and functions of contracts, **they are not self-standing** and cannot be seen as if in a **legal vacuum**.<sup>19</sup> In other words, those doubts deny the possibility of a code to ever substantially merge with a legal contract. With respect to that latter argument, *Allen* claims that essentially no legal relationship can ever exist in a vacuum, meaning that a technological instrument could never serve as a replacement to a whole, pre-existing legal system, and more specifically that of contract law in case at hand.

In the same line of thought, *Lim et al.*<sup>20</sup> have identified the **limitations of smart contracts, by comparing them to traditional, 'dumb' contracts:**

<sup>15</sup> Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets' (1996) 16 *Entropy* <<https://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf>>.

<sup>16</sup> Christopher D Clack, Vikram A Bakshi and Lee Braine, 'Smart Contract Templates: Foundations, Design Landscape and Research Directions' (arXiv, 15 March 2017).

<sup>17</sup> Jason Grant Allen, 'Wrapped and Stacked: "Smart Contracts" and the Interaction of Natural and Formal Language' (2018) 14 *European Review of Contract Law* 307.

<sup>18</sup> *Alma and Piatti* (n 7).

<sup>19</sup> Cheng Lim, T J Saw and Calum Sargeant, 'Smart Contracts: Bridging the Gap Between Expectation and Reality | Oxford Law Blogs' (11 July 2016) <<https://blogs.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality>> accessed 14 February 2025.

<sup>20</sup> *ibid.*

Commented [HJ15]: redundancy =>automate ...in automatic manner

Commented [L116]: In the computer context, it's programs

- ⇒ Negotiation of terms that are not capable of being assessed deterministically by a computer program (that is, not capable of Boolean expression and an algorithmic determination, but instead requiring human judgement);
- ⇒ Importing of indeterminate concepts of reasonableness or appropriateness by obligations, that again are not suited to algorithmic determination, in order to be sufficiently expressive;
- ⇒ Inaccurate reflection of the expression of an obligation in code to the agreement between the parties (e.g. due to an error or omission);
- ⇒ Inclusion in the contract itself of a further agreement to agree, or a mechanism for amending the contract which is not in itself algorithmically deterministic.

**Other, more fundamental questions**, which do not pertain specifically to smart contracts, but have been **expressed priorly with respect to 'dumb' contracts** – and are by extension applicable, and most certainly magnified, in the context of smart contracts – touch upon issues such as:

- ⇒ Absence of reflection of the true understanding reached between the parties in the code (e.g. due to a mistake of law or fact)
- ⇒ Different representation of the effect of the code to what it actually was meant to represent (i.e. misrepresentation)
- ⇒ Legal incapacity to enter a smart contract (e.g. person under of age, mental impairment).

What they conclude with is that smart contracts fit better the definition of 'an execution mechanism for a set of deterministic obligations' and should not be seen as contracts. They conceive smart contract as simply a part of the 'contractual matrix' between the parties, merely guaranteeing the execution of certain obligations.

Adopting a more moderate position, *Alma and Piatti*<sup>21</sup> argue that, by recognising that a script, although it can certainly retain its autonomy and independence as a piece of code, **does not necessarily need to become a legal contract**. This observation is based on what was previously presented with respect to the *Telematica* phase of contracts, whereby a set of instructions (i.e. a piece of code) can simply serve as an accompaniment to a legal transaction (i.e. a legal contract) but nevertheless remain external to the substantial contractual conditions that characterise the latter.<sup>22</sup>

### 2.3.3 Smart Legal Contracts (SLCs)

Taking the debate a bit further, *Wilkinson and Giuffre* ponder upon the question of **smart legal contracts (SLCs)**, in an attempt to provide sufficient grounds to differentiate from '**a-legal**' smart contracts.<sup>23</sup> They argue that in order for a smart

<sup>21</sup> Alma and Piatti (n 7).

<sup>22</sup> *ibid.*

<sup>23</sup> Wilkinson and Giuffre (n 9).

Commented [L117]: obligations?

Commented [HJ18]: You mean mediocre or moderate position?

contract to qualify as a SLC, it has to necessary include the record of an agreement that fulfils both of the following conditions:

- a) the **integrity of a legally enforceable contract** (according to the laws of the jurisdiction in which the contract is concluded) *and*
- b) the **expression of some (or all) of its terms and implementation in computational logic** (machine-readable code).

Similarly, and by building upon the metaphor of a 'contract stack' proposed by *Allen*,<sup>24</sup> *Blycha and Garside* have constructed a model which sets out **the components that a smart contract must possess in order for it to be considered a SLC**:<sup>25</sup>

- (1) **Status**: legally binding in that an SLC must conform to the established rules of contract law in the relevant jurisdiction;
- (2) **Form**: the contract must be in a machine-readable or digital state;
- (3) **Contents**: the contract must contain a combination of a) natural language, being any of the typical contracting and business language used in the jurisdiction of the contract, as in any traditional contract; and b) computer code, or other forms of machine-executable or algorithmic instructions intended to run digitally;
- (4) **Active Function**: the parties to the contract should reach an agreement on certain elements, namely on how, when, and why the digital components of an SLC are triggered or affected by data or events generated from external or internal data sources, including the results of previously executed algorithms; and
- (5) **Digital Execution Mechanism**: the digital hosting or domain of the SLC and how the digital hosting domain integrates with the Active Function.

An indispensable extension of the conversation on SLCs pertains to considerations relating to the **translation of specific legal obligations to formal language**. This aspect is discussed in more detail under [Section 3.1](#).

## 2.4 Technologies Supporting Smart Contracts

### 2.4.1 Blockchain

#### Public blockchains

According to some authors, smart contracts are exclusively blockchain-based applications that enable businesses to become more efficient through the automation of business processes.<sup>26</sup> It is also claimed that the real breakthrough for smart

<sup>24</sup> Allen (n 17).

<sup>25</sup> Natasha Blycha and Ariane Garside, 'Smart Legal Contracts: A Model for the Integration of Machine Capabilities Into Contracts' [2020] SSRN Electronic Journal <<https://www.ssrn.com/abstract=3743932>> accessed 10 February 2025.

<sup>26</sup> Orlenys López-Pintado and others, 'CATERPILLAR: A Business Process Execution Engine on the Ethereum Blockchain' (arXiv, 22 April 2019) <<http://arxiv.org/abs/1808.03517>> accessed 22 April 2025.

Commented [HJ19]: Linked to my previous comment, this section could be moved to the annex section. From my understanding, it is out of scope. Neither of the pilot plugins uses this technology

Commented [LI20R19]: At this point is kind of the state of the art, so I think blockchains are not out of place.

contracts was the invention itself of the blockchain technology.<sup>27</sup> Its three main data properties are (a) **immutability**, (b) **distributability**, and (c) **decentralisation**.<sup>28</sup> These same properties constitute also the reasons why blockchain is the most widely used and secure technology for smart contracts (as discussed in the present deliverable): thanks to decentralisation, there is no single point of control or failure and immutability renders the code and data unalterable once deployed. Public blockchains are also **transparent**, meaning that anyone can verify contract logic and the results produced. Another major advantage of blockchain-enabled smart contracts is that they are **not externally influenced**, i.e. they do not interact with external data, but are exclusively reliant upon data which are provided by the blockchain system.<sup>29</sup>

Some examples of smart contract platforms are notably Ethereum, as well as Solana, Cardano and Polkadot.

### Permissioned/Private blockchains

These blockchains can only be accessed by approved participants and are widely used in business and enterprise environments. They offer more control over participants and privacy but are not truly decentralised. Hyperledger Fabric<sup>30</sup> and R3 Corda<sup>31</sup> are examples of such blockchains.

#### 2.4.2 Other Technologies

Beginning from the starting point of a smart contract being a self-executing code that automatically enforces rules and agreements when certain conditions are met, **blockchain indeed popularised this concept by adding the elements of decentralisation and immutability**; however those elements are not strictly necessary for something to be considered as a smart contract. Other technologies that can support smart contracts include, but are not limited to:

### Distributed databases

These smart contracts run on distributed databases instead of a blockchain. Through the use of database triggers, stored procedures and smart workflows, contracts can self-execute based on predefined conditions. Banks and enterprises use databases to automate contract execution in leasing agreements, finance, and other domains. Even

Commented [HJ21]: I am afraid the statement that "blockchain is the most widely used and secure technology for smart contracts" ignores the fact that many secure and automated agreements are implemented outside of blockchain (through traditional software and database solutions), likely far more than those using blockchain smart contracts.

Commented [HJ22]: I think it should be 2.4.2.1

Commented [HJ23]: I believe this subsection should be included in the blockchain section, since it cannot be categorized as other technologies.

Commented [HJ24]: Including other technologies used in data agreements could be beneficial.

Commented [HJ25]: I think it should be 2.4.2.2

<sup>27</sup> Max Raskin, 'The Law and Legality of Smart Contracts' (2017) 1 Georgetown Law Technology Review 305.

<sup>28</sup> Luca Olivieri and Luca Pasetto, 'Towards Compliance of Smart Contracts with the European Union Data Act', *CEUR Workshop Proceedings* (CEUR-WS 2023) <<https://orbilu.uni.lu/handle/10993/60658>> accessed 10 February 2025.

<sup>29</sup> Vimal Dwivedi and others, 'Evaluation of a Legally Binding Smart-Contract Language for Blockchain Applications' (2023) 29 JUCS - Journal of Universal Computer Science 691.

<sup>30</sup> Nova Novriansyah, 'Understanding Hyperledger Fabric: A Private and Permissioned Blockchain Solution' (*Medium*, 7 May 2024) <<https://medium.com/novai-hyperledger-fabric-101/understanding-hyperledger-fabric-a-private-and-permissioned-blockchain-solution-1c5b037fc9f9>>.

<sup>31</sup> 'Corda Smart Contracts - Corda 4 Tools' (*R3 Documentation*, 30 September 2021) <<https://docs.r3.com/en/tools/cdl/smart-contract-view/corda-smart-contracts.html>> accessed 24 June 2025.

though the transactions made happen generally faster, without requiring any blockchain fees, trust in the data base operator is essential. Examples of such databases include the Oracle Database, PostgreSQL, etc.

### Trusted Execution Environments (TEE)

Contract code in such Trusted Executed Environments (TEE) executes securely and privately, without the need for a blockchain.<sup>32</sup> Use cases of such contracts include medical data contracts as well as private auctions. Nonetheless, specialised hardware is required for the execution of smart contracts in TEE, such as Intel SGX.<sup>33</sup> A secure enclave is created inside the CPU, with code and data inside the TEE being encrypted and protected from the rest of the system. However, TEEs lack the immutability, public verifiability, decentralisation and consensus that the blockchain offers. Some projects like `Secret Network` and `Oasis Network` are combining TEEs with blockchain, in order to achieve private, high-speed complex logic, and public, immutable recordkeeping and consensus.<sup>34</sup>

Commented [LI26]: references?

## 2.5 Smart Contracts under the Data Act (DA)

### 2.5.1 Definition of Smart Contracts (Article 2(39) DA)

In consideration of the elements presented above, [Article 2\(39\) of Regulation \(EU\) 2023/2854 on harmonised rules on fair access to and use of data \('Data Act'\)](#)<sup>35</sup>, provides the following definition with respect to smart contracts:

*'smart contract' means 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 [...]*

This definition highlights key elements that the EU legislator attaches to smart contract for the purposes of the Data Act, which can be summarised as follows:

- (1) **Computer program:** Smart contracts are implemented as software code rather than as traditional legal contracts.
- (2) **Automated execution:** The smart contract automatically carries out the terms of an agreement without needing manual intervention.
- (3) **Electronic data records:** Smart contracts process and rely on structured digital

<sup>32</sup> Rujia Li and others, 'SoK: TEE-Assisted Confidential Smart Contract' (2022) 2022 Proceedings on Privacy Enhancing Technologies 711.

<sup>33</sup> Gérald Doussot, 'Smart Contracts Inside SGX Enclaves: Common Security Enclaves: Common Security Bug Patterns' (*FoxIT*, 24 March 2020) <<https://www.fox-it.com/be/research-blog/smart-contracts-inside-sgx-enclaves-common-security-bug-patterns/>>.

<sup>34</sup> 'How Oasis Protects Privacy Despite TEE Vulnerabilities' (*OASIS*, 29 November 2022) <<https://oasis.net/blog/how-oasis-protects-privacy-despite-tee-vulnerabilities>> accessed 24 June 2025; Guy Zyskind, Oz Nathan and Alex Pentland, 'Enigma: Decentralized Computation Platform with Guaranteed Privacy'; Guy Zyskind, Oz Nathan and Alex Pentland, 'Enigma: Decentralized Computation Platform with Guaranteed Privacy' (arXiv, 10 June 2015) <<http://arxiv.org/abs/1506.03471>>.

<sup>35</sup> Data Act.

information.

- (4) **Integrity and ordering:** Smart contracts ensure that the recorded transactions are secure, tamper-proof, and chronologically accurate.

As far as the benefits brought by smart contracts, **Recital 47** explicitly refers to the reduction of costs which occur in the context of regular or repetitive transactions in business relationships.

### 2.5.2 Technological Neutrality of Smart Contracts (Rec. 104 DA)

A crucial addition for the eventual assessment and evaluation of any smart contract, in view of the obligations that are incumbent on the professionals which either create smart contracts for others or integrate in applications that support the implementation of agreements for data sharing, **Recital 104** provides further clarifications on the underlying technology supporting smart contracts. More specifically, **it clarifies that the notion of 'smart contract' in the DA is technologically neutral**. It further exemplifies 'electronic ledgers' as a technology to which smart contracts can be based upon. Reiterating what was presented above under **Sub-Section 2.4**, even if the prototype of such a fully automated smart contract can ideally be programmed on a blockchain, the concept of smart contracts in general does not necessarily have anything to do with blockchain technology.<sup>36</sup> This is reflected also in the final version of **Article 36 DA**, which also no longer assumes this.<sup>37</sup>

The implications of such a clarification is that the Data Act does not favour or require a specific technology, programming language, or implementation method for smart contracts. Instead, **it applies broadly to any system that meets the functional criteria of a smart contract**, regardless of the underlying technology used to create it. By being technologically neutral, the Regulation ensures flexibility, allowing for innovation and adaptation as technology evolves. It avoids limiting smart contracts to specific blockchain platforms or coding standards, making the rules applicable to a wide range of use cases.

### 2.5.3 Scope of Application

Apart from the element of technological neutrality, **the definition provided by Article 2(39) DA on smart contracts appears to be quite broad**. To this end, *Berberich* highlights the need to narrow it down, either by means of other elements or on the basis of a teleological interpretation of the notion, contextualised by other objectives provided for under Chapter VIII.<sup>38</sup> If not, then there is a high risk exists of **Article 36 DA**

<sup>36</sup> Matthias Berberich, "Intelligente Verträge" Bzw. „Smart Contracts“ in Heinrich Amadeus Wolff and Stefan Brink (eds), *BeckOK Datenschutzrecht*, vol 50 (2024).

<sup>37</sup> Indicatively, smart contracts were defined in the proposal for the Data Act as a 'computer program stored in an electronic ledger system wherein the outcome of the execution of the program is recorded on the electronic ledger'. Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act) 2022 (COM(2022) 68 final, 2022/0047 (COD)), Article 2(16) .

<sup>38</sup> Berberich (n 36).

extending to a large number of IT systems and programs, which is neither intended nor proportionate, as it would create far-reaching obligations for conformity assessments for providers of programs falling under this definition, as mandated by [Article 36\(2\) DA](#).

There is also a view according to which DA's regulation on smart contracts applies only with regard to **smart contracts which are employed for the execution of a data provision agreement**.<sup>39</sup> Consequently, the scope of application to the use of such contracts is limited to those contracts that have as their object automated data exchange, data access or data use within the meaning of the DA. Such an interpretation follows from the meaning and purpose of Article 36 DA, as well as from the requirement of proportionality to prevent an excessive application of Article 36 DA, in consistency with the issues explained in the previous paragraph. From the wording of the Article 36(1) DA the reference 'to make data available' can be understood as including both alternatives, i.e. use of smart contracts for third parties, and to the offering of applications.<sup>40</sup>

#### 2.5.4 Legal Nature

With respect to the nature of smart contracts under the Data Act, and in continuation of the analysis on the legal nature of smart contracts under [Sub-Section 2.2](#), the DA clarifies that **smart contracts are not contracts in the legal sense, but a mere technical execution mechanism**.<sup>41</sup> Whether the computer program must be an independent application or not, is not specified in the text of the DA, or any related documents. In line with the general understanding, **there is a case for considering 'computerised protocols' to be smart contracts**.<sup>42</sup> On the other hand, in view of the far-reaching obligations and consequences of the declaration and assessment of conformity foreseen by [Article 36\(2\) DA](#), it will be necessary to require that the connecting factor at the level of the obligated provider is at least an application in the sense of a marketable and economically definable software product, the main component of which are the smart contracts regulated in [Article 36 DA](#), as otherwise [Article 36 DA](#) would be limitless and no longer practically manageable.<sup>43</sup>

#### 2.5.5 On the Notion of 'Execution'

In response to the need for further precision of the notion of smart contracts under the DA, the notion of execution offers a great opportunity to do so. The following analysis

**Commented [HJ27]:** I draw your attention that the explanation of "execution" is stated multiple time in slight different way==> paragraph 2, 4 and 6 . Same for agreemt/contract

<sup>39</sup> Matthias Berberich, 'Zur Ausführung Einer Datenbereitstellungsvereinbarung' in Heinrich Amadeus Wolff and Stefan Brink (eds), *BeckOK Datenschutzrecht*, vol 50 (2024).

<sup>40</sup> *ibid.*

<sup>41</sup> Rec. 104 DA.

<sup>42</sup> Josef Drexler and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (Social Science Research Network, 25 May 2022) <<https://papers.ssrn.com/abstract=4136484>> accessed 20 March 2025.

<sup>43</sup> Berberich (n 36).

was inspired by the contracts concluded in UPCAST<sup>44</sup>, and is merely recommending an interpretative approach of the term.

**The wording in Article 2(39) of the Data Act** – ‘automated execution of an agreement or part thereof’ - **can easily be confusing due to the fact that the terms ‘execution’ as a legal term meaning ‘signing’ and ‘performance’ as the act of fulfilling contractual obligations, respectively** (see above under [Sub-section 2.1](#)). In fact, here ‘execution’ seems to be borrowed from the computer-science environment, rather than the legal sense. The legislator uses ‘agreement’ instead of ‘contract’ to capture any set of legally binding commitments - whether formalised by signature, embedded in standard terms of service, or even only partly codified in software.

To untangle this, first note that the ‘agreement’ referred to in Article 2(39) lives on the legal side: it is the set of rights, duties, and remedies that the contracting parties have decided upon. That agreement may be a traditional paper or e-signed contract, a click-through license, or simply a mutual understanding recorded in some document or system. Often, a smart contract automates only part of that overall arrangement—for example, triggering an escrow release when certain conditions are met—while other terms (warranties, dispute resolution, liability clauses) remain outside the code. By speaking of “agreement ... or part thereof,” the Data Act makes clear that the software need not embody the entire legal instrument but merely the slice of obligations that has been translated into programmatic logic.

On the technical side, a ‘smart contract’ in the Data Act is simply a computer program that monitors a sequence of electronic data records and, once it sees the right inputs in the correct chronological order, automatically ‘executes’ (i.e., runs) the coded instructions. Whereby the legislator speaks of the ‘execution of an agreement’, they mean ‘the code executes those clauses automatically’ rather than ‘the parties sign the agreement’. In other words, what would legally be called ‘performance’ (i.e., carrying out an obligation) is here referred to as ‘execution’, because it is the act of the program running.

**The choice of the term ‘agreement’ instead of ‘contract’ was probably made in order to avoid importing formalities from national contract law – such as signature requirements, capacity doctrines, or notarial certifications – that are irrelevant to a piece of software.** The Data Act explicitly states (Recitals 2 and 9) that it does not affect how contracts are formed, validated, or enforced under domestic private-law rules. By using the broader word ‘agreement’, the text remains agnostic about whether the underlying commitments were memorialised by a formal contract, by click-through terms, or by some other digital arrangement. This keeps the focus on functionality - namely, that certain obligations are triggered automatically when the programmed conditions appear in the sequential data records – without muddying the picture with

Commented [LI28]: Would we need to define an UPCAST Contract beforehand? Or perhaps reference from D4.4?

Commented [LI29R28]: I see you go over this on section 4.1 of this document, so perhaps a forward reference is all what it takes.

Commented [LI30]: made

<sup>44</sup> A more detailed analysis is provided under 4.1 of the present deliverable.

questions about legal formalities.

**Because 'execution' in most legal systems means 'signing' and 'performance' means 'fulfilling', it appears natural to read Article 2(39) through a legal-theory lens and wonder whether the Data Act is conflating these distinct concepts.** In reality, it is not conflating them but simply using 'execution' in its programmatic sense. Whenever the Data Act speaks of a smart contract 'executing' an agreement, it probably intends to convey that the software is running to perform those coded obligations automatically. The actual legal 'performance' of contract duties now happens in two layers: the smart contract code carries out those obligations automatically, and the parties remain bound by any other terms of the agreement that lie outside the code's scope.

In summary, the Data Act's phrasing – 'execution of an agreement' – combines (1) the legal layer ('agreement' as the set of binding commitments) with (2) the technical layer ('execution' as running the program). Although this wording can initially seem confusing, it ensures that any automated performance of part or all of a data-sharing arrangement is captured without dragging in formal contract-law requirements. **When reading Article 2(39) DA, 'execution' should be simply interpreted as 'running the smart-contract code to perform the coded duties' and 'agreement' should be understood as referring to the broader legal commitments that the code helps to automate.**

#### 2.5.6 Smart Contracts under the Data Act as Technical Protection Measures on the Unauthorised Use or Disclosure of Data

It is essential to note that smart contracts under the DA align with the general aspiration of the EU to 'contractualise' the EU data economy. One of the main goals of the DA is to 'realise important economic benefits of data, including by way of sharing on the basis of *voluntary agreements* and the development of data-driven value creation by Union enterprises' (own emphasis added).<sup>45</sup> Supporting this view, **Article 11(1) DA** lists **smart contracts as a technical protection measure against unauthorised use or disclosure of data**, along encryption (these elements however not being exclusive) in order to ensure compliance with Articles 4, 5, 6, 8 and 9 of the DA, as well as with the agreed contractual terms for making data available. The four (4) requirements that these measures – and as such, smart contracts – need to abide with are the following:

- (a) *Appropriateness*: a term vaguely used also in other contexts<sup>46</sup> needs further specification on the basis of a case-by-case assessment, depending on the type

<sup>45</sup> Data Act, Rec. 6.

<sup>46</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Commented [HJ31]: I would like to point out that there is no connection between the paragraph explaining the measurement and the terms "unauthorized use or disclosure of data."

Commented [HJ32R31]: It can be interesting to explain: How do the measures cover unauthorised use or disclosure of data? Do they cover all aspects?

Commented [HJ33]: three or 4 (a,b,c,d)??

and extent of the data provision.<sup>47</sup>

- (b) *Non-discrimination*: the measures shall not discriminate between data recipients.
- (c) *Rendering difficult or impossible the exercise of a user's right to obtain a copy of, retrieve, use or access data, to provide data to third parties pursuant to Article 5 or any right of a third party*: the point in time at which such exercise is hindered is not however clear, nor the level of security that is considered to be obstructive.<sup>48</sup>
- (d) *Alteration or removal of technical protection measures with agreement with the data holder*: such technical measures cannot be circumvented or compromised by users and/or third parties without full agreement of the data holder.

Paragraphs (2) and (3) further elicit the consequences in very particular challenging data sharing circumstances.

### 2.5.7 Data Provision Agreements and Smart Contracts

Contrary to the non-legal character of smart contracts, **data provision agreements constitute contracts in the legal sense**. This is not to be equated with the smart contract, which executes the contract. However, it will not be necessary to require that such a data provision agreement has already been concluded with legal effect in the individual case, because **Article 36 DA** already starts with the offer of smart contracts on the market, which as a technical instrument typically enables the execution of such agreements according to their intended purpose. However, at this point in time of the offer, it is still unclear in which later context and for which specific data provision agreement (possibly concluded with other parties) the use will take place.

### 2.5.8 Essential Requirements of Smart Contracts (Article 36 DA)

The definitional contours provided in **Article 2(39) DA** are complemented by the provisions of one sole article in the DA, which is that of **Article 36 DA**. The latter sets out specific technical obligations, more specifically foreseeing that:

***‘1. 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 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:***

(a) ***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;

(b) ***safe termination and interruption***, to ensure that a mechanism exists to

<sup>47</sup> Moritz Hennemann and others, *Data Act: An Introduction* (Nomos Verlagsgesellschaft mbH & Co KG 2024) <<https://www.nomos-elibrary.de/index.php?doi=10.5771/9783748918691>>.

<sup>48</sup> *ibid.*

*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;*

*(c) **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);*

*(d) **access control**, to ensure that a smart contract is protected through rigorous access control mechanisms at the governance and smart contract layers; and*

*(e) **consistency**, to ensure consistency with the terms of the data sharing agreement that the smart contract executes.'*

#### 2.5.9 Addressees of the Obligations of Article 36(1) DA

Necessary for a more holistic understanding of the abovementioned obligations, a brief look should be given to the actors by which these obligations are borne, which are on two levels:

##### 1) Vendor of an application using smart contracts (primary addressee)

Following a grammatical interpretation of this category's denomination, it is reasonable to claim that the provider of the smart contract application is **putting the application on the market**. As such, purely internal use in a company or group of companies does not suffice.<sup>49</sup> In the same line of thought, actors who merely develop software are not automatically also considered as distributors. However, it is questionable to what extent the concept of vendor covers constellations of contract developments in which specific individual software is developed in an exclusive manner for the actors carrying these obligations under [Article 36 DA](#).

It has been argued that the contractual form in which smart contracts are distributed on the market, i.e. whether software is provided on a permanent or temporary basis and whether this is done free of charge or for a fee, bears no relevance. In any case, the term 'vendor' does not indicate a restriction to a purchase-like transfer due to the purpose of the DA but means any type of placing on the market.<sup>50</sup> Nonetheless, this position, at least with respect to the term employed in the English version of the DA, is debateable: the term '**vendor**' means exactly the person who is **disposing of something by sale**.

**It is also unclear to what extent Article 36 DA covers open source software.** In view of the deliberate privileging of open source in a large number of legal acts, it cannot (or should not) be assumed that the EU legislator wanted to include them, and thus subject

---

<sup>49</sup> *ibid*, Rec. 104.

<sup>50</sup> Georg Borges, 'Smart Contracts für Datentransaktionen und der Data Act – Potential und Herausforderungen der automatisierten Bereitstellung von Daten' (2024) 40 *Computer und Recht* 425.

them to the obligations of [Article 36 DA](#).<sup>51</sup>

- 2) The person whose trade, business or profession involves the deployment of smart contracts for others (secondary addressee)

**Only in the case of ‘absence’ of a vendor**, the obligations arising from Article 36 DA are carried by the party whose commercial, business or professional activity is involving the use of smart contracts for third parties for the purposes of [Article 36 DA](#). It has been also very correctly argued that whether the vendor as the primary addressee of the obligation fulfils such obligation or fails to do so bears no relevance.<sup>52</sup> Put differently, Article 36 DA’s provision requires the sole existence of the primary addressee and does not place any supplementary burden on the shoulders of the second addressee to control whether the former is abiding by their obligations or not.

As far as the term ‘**deployment**’ is concerned, there are no clarifications provided by Article 36 DA, or any other article or recital of the DA. In the context of blockchain technology, deployment would simply mean an implementation and release of the smart contract for independent execution. Nonetheless, since smart contracts under the DA are technologically neutral – as it was discussed above under [2.5.2](#) – deployment should be generally interpreted as a service that is involving more than a support service or purely technical service, as for example specific control over the content and process of the smart contract.<sup>53</sup>

Commented [LI34]: Section 3 seems to be starting below

---

<sup>51</sup> Matthias Berberich, Heinrich Amadeus Wolff and Stefan Brink, ‘Anbieter oder Einsetzender’, *BeckOK Datenschutzrecht*, vol 50 (2024).

<sup>52</sup> *ibid.*

<sup>53</sup> *ibid.*

### 3 MACHINE-READABILITY IN SMART CONTRACTS

This section examines how smart contracts become machine-readable. Sub-section 3.1 contrasts natural (human) languages, rich in path-dependent syntax, ambiguous semantics, and context-driven pragmatics, with formal (computer) languages. Sub-section 3.2 then shows how ontologies provide a shared vocabulary to generate, audit, and monitor smart contracts, even if they lack standalone legal enforceability.

#### 3.1 Natural and Formal Language in Smart Contracts

Mainly in connection to the question of SLCs as presented above under Sub-Section 2.3.3 and insofar as contracting languages are concerned, languages that can be read by machines and by humans do not necessarily always coincide. In a more general context, human-readable languages are referenced to as **natural (human) languages**, whereas machine-readable ones are referred to as **formal (computer) languages**. An example of a natural language is English, which allows for humans to communicate with one another. Conversely, an example of a formal language is C++, which allows for programming of deterministic agents. Both languages consist of structured, symbolic content, but are different in many aspects.<sup>54</sup>

The three (3) different aspects of languages allow for these similarities and differences to become apparent:

- ⇒ **Syntax** is a logic that is inherent in devices such as prefixes, infixes and suffixes, articles, and other parts of speech. In that regard, natural and formal languages do not differ that much, since they both are, to a certain level of abstraction, characterised by the same syntactic properties. Natural languages are still, nonetheless, much more syntactically path dependent.
- ⇒ **Semantics** consider the meaning that different words and combinations have. The main considerable – and at the moment, insurmountable in its whole – obstacle is the formalisation of the semantic content of natural languages. Since meanings and ambiguities in natural languages are several, a formal language being able to succeed in rendering them all machine-readable is definitely questionable.
- ⇒ **Pragmatics** consists in the meaning that words uniquely get in the context in which they are used. Similarly to what was said on semantics, context plays a crucial role when constructing and interpreting the meaning of natural languages phrases, especially in much more complex cases (e.g. specific legal terminology)

A considerable part of the discussions with respect to SLCs concerns the possibility and, consequently, the possible limitations of the translation of legal obligations expressed in natural language, into formal language.<sup>55</sup> Such a consideration is inevitably leading to the assumption that automation can only be to the benefit of legal

---

<sup>54</sup> Allen (n 17).

<sup>55</sup> Wilkinson and Giuffre (n 9).

Commented [LI35]: C++

obligations that are fully translatable into formal language, meaning that automation would be limited to such cases. According to *Wilkinson and Giuffre* speak of two categories of two categories in that regard:

- 1) **Unified Method (UM)**: this method adheres to the idea that only natural language obligations that can be completely translated into computational logic can be automated. In that sense, this approach is very limiting.
- 2) **Paired Method (PM)**: this method is more flexible since it considers that the natural language components of a contracts are (a) retained and (b) expanded, either by pairing them or by tagging them to beneficial coded automation or digital connectivity.

Irrespective of the choice of either of these methods, the challenge is to ensure that whatever terms are eventually written in natural language be sufficiently translated into formal language in a way that the meaning and understanding of the terms is identical between the two languages. *Allen (2018)* hints at the creation of a smart contracting language which the parties could then adopt as a 'dictionary', entailing suitable interpretation under national law.<sup>56</sup>

## 3.2 The Role of Ontologies in Smart Contracts

### 3.2.1 General Elements on Ontologies

According to *Studer et al.*, an ontology is a 'formal, explicit specification of a shared conceptualisation'.<sup>57</sup> An ontology essentially constitutes a classification of entities, through the definition of a set of concepts that they can be categorised by.<sup>58</sup> Especially in the context of data science, **ontologies are employed in order to link data and entities and clarify the links between them**. Thanks to ontologies, it is easier to specify classes, relations and restrictions, but in a manner which renders this classification reusable, i.e. these classifications can always be revisited and modified at a later point in time and be adjusted in a way that can allow for the ontology to be further enriched.

**Ontologies typically entail classes and properties.** *Classes* describe concepts or objects that one wishes to represent (e.g. animals). They have their own hierarchy, which means that classes can have subclasses, each of which inherits the properties of the class in which it belongs (e.g. cats, dogs, birds..). *Properties* describe the main characteristics and attributes that this class has, thus they are able to define the values that this class has (e.g. 4-legged, 2-legged..).

**Ontologies can be represented in different formats, but the most widely accepted language is Web Ontology Language (OWL).** It offers a larger vocabulary and better

---

<sup>56</sup> Allen (n 17).

<sup>57</sup> Rudi Studer, V Richard Benjamins and Dieter Fensel, 'Knowledge Engineering: Principles and Methods' (1998) 25 *Data & Knowledge Engineering* 161.

<sup>58</sup> Charles Brecque, 'An Introduction to Ontologies and How to Use Them' (*TextMine*, 22 January 2024) <<https://textmine.com/post/an-introduction-to-ontologies-and-how-to-use-them>> accessed 12 February 2025.

semantic representation than plain XML, RDF, or RDF Schema<sup>2</sup>, and facilitates higher machine interpretation.<sup>59</sup>

Commented [LI36]: Missing footnote?

Ontologies come with significant advantages, as they enable data extension, facilitate the integration and standardisation of diverse formats, and support easier data understanding by explicitly defining the constraints and relationships that govern the data.<sup>60</sup>

### 3.2.2 Ontologies in Smart Contracts

Ontologies also provide a machine-readable representation of agreements,<sup>61</sup> especially in the context of smart contracts,<sup>62</sup> whereby parties can use them to define the responsibilities and authorisations between them.<sup>63</sup>

Ontologies can play a significant role in facilitating consensus among parties through different phases of the contract cycle (see **Figure 1** – Phases of a contract's lifecycle). They can constitute a tool which will be providing a shared understanding of the terms, conditions and semantics, by establishing a common vocabulary and structure for representing the latter.<sup>64</sup>

*Dominiguez et al.* identify the utility of ontologies in the different phases of the smart contract lifecycle as follows:

- Ontologies can constitute the basis on which the use of rules and templates for the generation of smart contracts, as well as smart contract language can be defined
- Ontologies can also be created or used in order to detect any kind of malicious behaviour in smart contracts, before they are executed.
- Ontologies can also be used for monitoring and evaluating smart contracts during their execution.

<sup>59</sup> Olivia Choudhury and others, 'Auto-Generation of Smart Contracts from Domain-Specific Ontologies and Semantic Rules', *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (2018) <<https://ieeexplore.ieee.org/document/8726491/?arnumber=8726491>> accessed 10 February 2025.

<sup>60</sup> Brecque (n 58).

<sup>61</sup> Mario Scrocca and others, 'Modelling Business Agreements in the Multimodal Transportation Domain through Ontological Smart Contracts' (arXiv, 5 September 2022) <<http://arxiv.org/abs/2209.05463>> accessed 20 March 2025.

<sup>62</sup> Adrian Paschke and Martin Bichler, 'Knowledge Representation Concepts for Automated SLA Management' (arXiv, 2008) <<http://arxiv.org/abs/cs/0611122>> accessed 6 May 2025.

<sup>63</sup> Domenico Cantone and others, 'Ontological Smart Contracts in OASIS: Ontology for Agents, Systems, and Integration of Services' in David Camacho and others (eds), *Intelligent Distributed Computing XIV*, vol 1026 (Springer International Publishing 2022) <[https://link.springer.com/10.1007/978-3-030-96627-0\\_22](https://link.springer.com/10.1007/978-3-030-96627-0_22)> accessed 6 May 2025.

<sup>64</sup> Johnny Alvarado Dominguez, Silvio Gonnet and Marcela Vegetti, 'The Role of Ontologies in Smart Contracts: A Systematic Literature Review' (2024) 40 *Journal of Industrial Information Integration* 100630.

### 3.2.3 Legal Standing of Ontologies

**Ontologies are not legally binding by themselves.** Unless they represent agreements between parties themselves, they are not enforceable in court like any other contract would. Instead, **they serve as a reference framework to aid in legal interpretation and automation.** In that sense, they can play a crucial role in:

- Structuring legal knowledge to assist in legal decision-making.
- Enhancing interoperability between legal systems, contracts, and AI-driven legal tools.
- Supporting smart contracts and automated compliance by providing standardised definitions.

## 4 EVALUATION OF CONTRACTS CONCLUDED THROUGH UPCAST

On the basis of the analysis provided in the two previous sections (Sections 2 and 3), this section provides an assessment of the contracts concluded in UPCAST.

### 4.1 Description Of UPCAST's Negotiation and Contracting Plugin (NCP)

A reiteration of what was extensively analysed in **D3.1** is indispensable in order to critically assess UPCAST contracts against the DA's provisions.

Commented [L137]: critique?

#### 4.1.1 Overview of the Negotiation and Contracting Plugin

The Negotiation and Contracting plugin is designed to streamline the often-complex processes of reaching agreements and managing data-sharing contracts. This plugin facilitates clear communication and collaboration between data providers and consumers, offering tools to initiate, monitor, and finalize negotiations within a unified interface.

In addition to negotiation capabilities, the plugin includes comprehensive contract management features. It supports the creation, review, and execution of contracts, while automating routine steps and offering customizable Data Processing Workflows (DPWs). These features collectively enhance the efficiency and compliance of data-sharing practices, particularly under regulatory frameworks like the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, 'GDPR').<sup>65</sup>

#### 4.1.2 Contract Representation and Standards

UPCAST contracts are built using well-established semantic standards to ensure clarity, interoperability, and legal relevance. These contracts extend the usage control specifications defined by the International Data Spaces Association (IDSA), which leverage the Open Digital Rights Language (ODRL) for machine-readable and platform-agnostic contract descriptions. In addition, NCP integrates the Data Privacy Vocabulary (DPV), which enables detailed representation of data processing purposes, legal bases, and obligations – all aligned with privacy legislation, including the GDPR.

#### 4.1.3 Policy Management and Conflict Handling

At the core of UPCAST's negotiation system is its role as a Policy Management Point (PMP). It evaluates machine-readable contracts against input from various other components - including privacy settings, environmental impact considerations, and pricing rules - to determine if an agreement can be reached automatically. **If no**

---

<sup>65</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

**conflicts are detected**, the plugin finalises the agreement, with a prior request for human approval in order to turn the offer/request into an agreement. **If conflicts do arise**, it launches a structured negotiation, allowing data providers and consumers to present and respond with counteroffers. The data provider retains the authority to accept, reject, or further revise offers.

Additionally, the system offers a Policy Administration Point (PAP), complete with an intuitive graphical interface that allows users to define and manage restrictions, data use permissions, and privacy policies with ease.

#### 4.1.4 Integration with Consent and Compliance Technologies

UPCAST leverages and integrates two previously validated technologies to enhance its negotiation capabilities:

- (1) EPCON, developed by the University of Southampton (SOT), which supports the capture and enforcement of personal consent through business rules.
- (2) goodFlows, developed by ICTabovo, enables automated process re-engineering to ensure GDPR compliance, using detailed modeling of regulatory rules.

These tools enhance UPCAST's ability to automate negotiation logic and ensure that resulting contracts align with evolving legal and organizational requirements.

#### 4.1.5 Automated Reasoning and Negotiation Logic

The negotiation plugin processes two key inputs:

- (1) **A set of machine-readable constraints** defined by the data provider via the Privacy plugin.
- (2) **A set of processing intentions** expressed by the data consumer.

With these, UPCAST applies a reasoning engine capable of identifying conflicts, generating counterproposals within configurable ranges, and suggesting possible resolutions. This engine is designed to support negotiation strategies that incorporate rule prevalence schemes such as:

- Most recent rule takes precedence
- Deny overrides
- Stricter rule prevails
- Inclusion–Exclusion logic for comparing constraints
- Evaluation of contextual preconditions and actions

#### 4.1.6 Structured Negotiation and Contract Finalisation<sup>66</sup>

UPCAST's negotiation functionality facilitates structured, rule-driven dialogue between **Resource Providers (RPs)** and **Resource Consumers (RCs)**. Negotiation is triggered based on compatibility of preferences and the definition of negotiation terms, including alternatives and interdependent rules.

<sup>66</sup> Finalisation coincides with the term 'execution' as described above under 2.1.1.

Commented [LI38]: If you got this from D3.1, we are ignorant if Finalisation is a word with legal charge and you probably need to mention that is the alignment.

NPC verifies that the requested DPW aligns with the data provider's constraints, the consumer's intentions, and applicable legal and policy frameworks. It also takes into account economic and environmental parameters as defined in the dataset metadata. If no conflicts are identified, an agreement is finalised automatically. If disagreements occur, the system initiates a guided negotiation process involving an exchange of offers and counteroffers. Through an intuitive interface, both parties can iteratively adjust terms until a consensus is reached. The system respects preconfigured negotiation ranges, allowing controlled flexibility for each term in the resource specification.

Once an agreement is reached, UPGAST generates both:

- **A machine-readable contract for system enforcement and interoperability, and**
- **A natural language contract for legal clarity and human comprehension.**

Consequently, NPC ensures full transparency of the negotiation outcome, empowering both parties to make informed, accountable decisions.

#### **4.2 UPGAST Contracts as Smart Contracts or as Electronic Contracts?**

Theoretical analyses aside, the main goal of this deliverable is to provide an assessment of UPGAST contracts with respect to the provisions of the DA. The following sub-section offers an analysis using elements as exposed in previous sections, along with the respective references to such sections.

Testing UPGAST contracts against the foundational components of smart contracts according to Article 2(39) DA as presented under 2.5.1, the assessment in that respect can be summarised as below:

Criterion	UPCAST NCP	Alignment
Automated Execution	NCP automates negotiation workflows, counter-proposal generation, conflict resolution, and contract generation.	Partial
Computer Program	NCP is implemented as software.	Full
Electronic Data Records	Machine-readable policies and processing intentions (ODRL/DPV-based) are exchanged and tracked systematically.	Full
Integrity & Chronological Order	There is a structured sequence of negotiation states; however, no mention of tamper-proof logs or hash-based sequencing is made.	Partial

**Table 2** – UPCAST Contracts Qualification under Article 2(39) DA

With respect to the element of automated execution, NCP automates aspects of the negotiation and contract formation, facilitating agreements between data providers and consumers. However, this execution is **not fully automated**, keeping the human-in-the-loop during the negotiation process. Also, the UPCAST NCP merely assists in reaching agreements but is not executing the agreements automatically upon predefined conditions.

Although the EU Data Act adopts a technologically neutral definition of smart contracts – focusing on functionality rather than underlying technologies such as blockchain – UPCAST contracts still only partially meet that definition. While UPCAST NCP incorporates automation in contract negotiation and management, it most probably **does not fully qualify as a smart contract** under a strict interpretation of the definition. It is more of a **negotiation and contract management system** rather than an autonomous, self-executing program. And this is because UPCAST’s NCP facilitates the creation of contracts through automated negotiation, reasoning over policy constraints, and generating both machine-readable (ODRL, DPV) and natural language contract versions. These agreements are then accepted by the parties through a user interface. **However, the contracts are not self-executing (in terms of computer code)**, with the DPV and Monitoring Plugin being concerned with checking that the processing intended by the consumer is compliant with the terms of the agreement. **The agreed terms are not automatically enforced, but rather, the execution relies on subsequent actions by the involved parties or systems, outside the plugin itself.**

This process fits well within the common understanding of electronic contracts – that

Commented [LI39]: If you think is useful, you may add the DPV and Monitoring are concerned with checking that the processing intended by the consumer is compliant with the terms of the agreement

is, agreements concluded and stored electronically, expressed digitally, and accepted through electronic means, as explained above. **UPCAST-concluded contracts therefore are best classified as electronic contracts with automated negotiation capabilities, rather than fully autonomous smart contracts.** This distinction ensures legal clarity and accurate understanding of the NCP's role in data governance and compliance.

**Commented [HJ40]:** What are the rules or requirements from the Data Act that apply to electronic contracts with automated negotiation capabilities? If there are rules, I believe we need a table that assesses electronic contracts according to identified rules.  
I draw your attention that there is a section about the Essential Requirements for Smart Contracts but I believe nothing about electronic contracts.

## 5 MISCELLANEOUS

This section is devoted to two separate issues that have arisen in the course of the project, and which are more loosely related to the analysis above. They pertain to two specific provisions of [Article 12 of the Regulation \(EU\) 2022/868 on European Data Governance \(Data Governance Act, 'DGA'\)](#).<sup>67</sup>

### 5.1 Contractual Implications of the Limitations Imposed by the DGA on Providers of Data Intermediation Services

#### 5.1.1. The Regime Governing the Provision of Data Intermediation Services (DIS)

The DGA regulates the provision of data intermediation services. Data intermediation services are defined by the DGA as services which: i) aim to establish commercial relationships for the purposes of data sharing, ii) between an undetermined number of data subjects and data holders on the one hand and data users on the other, iii) through technical, legal or other means. **Some examples of DIS include data marketplaces, orchestrators of data sharing ecosystems, and data pools.**

Data intermediation services (DISs) that meet the definition are subject to structural and operational requirements to carry out their activities. Further to complying with these substantive requirements, providers of DISs must also meet the procedural obligation to submit a notification to the competent authority before commencing their activity.

In addition to the definition provided in [Article 2\(11\) DGA](#) and the related exclusions listed therein, a full understanding of the contours that a DIS can have in practice requires taking into consideration the operational limitations set out in [Article 12 of the DGA](#). This article lays down the conditions to which the provision of a DIS is subject, thus determining the operational structure of the service. Through Article 12 DGA, the EU legislator outlined the model of data intermediation that it intended to promote, and impose, for the EU digital single market. In particular, the operational limitations in virtue of its provisions guide the development of data intermediation towards specific business models, while excluding others. These requirements can be summarised as follows:

**A first requirement for the provision of DISs is neutrality.** [Article 12\(1\)\(a\) DGA](#) requires intermediaries to limit the use of the data for which they provide their service for the purpose of putting them at the disposal of data users. Therefore, such data can only be used for the purposes of matchmaking between providers and users, whilst its use for the provision of additional services and/or for other activities is precluded. Relatedly, [Article 12\(1\)\(b\) DGA](#) prohibits practices that render commercial terms for the provision of a DIS dependent on the use of other services by the data holder or data user, whether offered by the provider or by a related entity. This requirement prevents the bundling of different services that would prejudice the neutrality of data

---

<sup>67</sup> Data Governance Act.

Commented [LI41]: missed the last bit of bold brush

intermediation. Finally, [Article 12\(1\)\(c\) DGA](#) completes the series of neutrality requirements by prescribing that the data collected on the conduct of natural or legal persons in the context of the provision of the DIS can only be used for the development of that DIS. This data includes the date, time and geolocation data, duration of activity and connections to other natural or legal persons established by the person who uses the DIS.

**Second, providers of DISs are restricted in the additional features, functionalities and services that they can provide alongside the data intermediation service.** [Article 12\(1\)\(d\) DGA](#) allows to convert the data into other formats only in limited cases, and providers are constrained in the additional tools and services that they can offer as part of the data intermediation service, according to [Article 12\(1\)\(e\)](#).

**Third, [Article 12\(1\)\(f\) DGA](#) requires access to data intermediation services to be fair, transparent and non-discriminatory,** interoperability between different DIS should be enabled according to [Article 12\(1\)\(i\) DGA](#), and the highest level of security should be ensured for the storage and transmission of competitively sensitive information, pursuant to [Article 12\(1\)\(l\) DGA](#). All of these requirements aim to foster fair competition in data intermediation markets.

**Fourth, while providers of DIS are expected to play a neutral role in intermediating between data providers and users, they are also obliged to take positive steps to ensure that their service meets certain standards.** [Article 12\(1\)\(g\) DGA](#) requires DISPs to prevent fraudulent and abusive practices through appropriate procedures, [Article 12\(1\)\(j\) DGA](#) to prevent the unlawful access to, or transfer of, non-personal data, [Article 12\(1\)\(m\) DGA](#) to act in the data subjects' best interest, and [Article 12\(1\)\(o\) DGA](#) to maintain a record of the data intermediation activity.

#### **5.1.2. Operational Constraints on Data Intermediation Services Relevant for Data Sharing Contracts**

The operational constraints set by the DGA for data intermediation services have the inevitable consequence of shaping the functioning of data-sharing markets, insofar as data intermediation services play a role in such markets. **As a result, contractual practices and relationships can also be influenced by how data intermediation takes place.** The way the DGA can impact data sharing agreements can be multifaceted, complex and difficult to comprehensively map without empirical evidence. For the purposes of this deliverable, we only focus on one specific aspect: the limitations to contractual freedom in data sharing contracts stemming from the operational restraints imposed by the DGA on data intermediation. In this regard, the focus is on the neutrality requirements for DISs, and their consequences for the formation of data-sharing contracts.

#### **5.1.3. Operational Constraints Affecting Contractual Freedom and Contractual Practices for Data Sharing**

Data intermediation services can play a key role in enabling, or facilitating, the formation of data sharing contracts. By reason of their matchmaking purpose, they broker the encounter of demand and offer for data sharing. This intermediation can take in different ways, and solutions have been developed so far to assist data holders and data users in concluding data sharing contracts. These solutions can intervene for instance on the formation of prices for datasets, e.g. based on the preferences of parties and on market dynamics, or through the provision of additional services to enrich data intermediation. However, neutrality requirements significantly limit what can be done to assist matchmaking between data holders and users. **Article 12(1)(a)-(c) DGA** precludes the bundling of services and the use of data and information about the conduct of natural or legal persons during the provision of a DIS for any other purpose than matchmaking per se. The consequence of these limitations is that providers of DISs cannot use information extracted from the datasets or the behaviour of their customers to dynamically or statically set prices for the datasets to be exchanged. For instance, dynamic pricing is a pricing practice that consists of basing products and services' prices on a series of evolving market trends, such as the level of offer and demand at a given time, in order to maximise the expected profits. In the context of data markets, prices may be based on the past transactions of providers and users, the level of demand for certain datasets at a given time, or specific characteristics of the user (e.g., their location), or the data (e.g., value of data for a specific task). **Providers of DISs cannot do dynamic pricing due to the neutrality obligations that restrict the use of the information needed to define prices for any purpose other than matchmaking.**

These obligations are not imposed directly on the parties of data sharing agreements, but only on the providers of data intermediation services. Therefore, it cannot be said that they directly limit the contractual freedom of the parties to data sharing agreements. **However, by limiting the operational freedom of providers of online tools that are used to conclude data sharing agreements, they have significant implications for contractual practices and the form that contracts eventually assume.** These implications concern which actor(s) would in practice define the terms of the contract.

**First, the terms of data sharing agreements would be mainly defined by the parties, rather than drawn up by an intermediary who suggests terms that must be approved by the parties.** A clear example is pricing. If the prices of datasets are not set by intermediaries based e.g. on market dynamics, the parties will have to negotiate the contract between themselves. A literal interpretation of the conditions in **Article 12 DGA** suggests that providers of DISs would hardly be able to even suggest a price for datasets in their matchmaking function, insofar as suggesting this price would require information about the behaviour of customers and the datasets to be exchanged. Similar considerations can be made about other terms of the contract, as providers of DISs are restricted in the additional features, functionalities and services that they can provide alongside the data intermediation service. This would likely preclude the

possibility to provide templates for the conclusion of contracts online, or to suggest specific terms for the contracts. Therefore, the restrictions imposed on providers of DISs affect how parties to data sharing agreements can conclude contracts and the terms of these contracts.

## 5.2 Logs of Activities of Users on the UPGAST Platform

With respect to the data intermediation activity that takes place in the course of the data intermediation service provision, [Article 12\(o\) DGA](#) specifically foresees that 'the intermediation services provider shall maintain a log record of the data intermediation activity'. This provision is thus not only providing the legal ground necessary for the UPGAST platform to maintain such logs of users' activity but essentially imposes an obligation to do so. What is more, the UPGAST Monitoring and Auditing Plugins can further contribute in that regard, in the sense that a DIS installing UPGAST plugins can monitor users' interactions mediated by the plugins, and create that 'Verifiable Credential' in a third party auditor.

**Commented [LI42]:** You may point at the Monitoring and Auditing plugins that help with that.

A Data Intermediation Service that installs UPGAST plugins can monitor users' interactions mediated by the plugins, and create that "Verifiable Credential" in a 3rd party auditor.

## 6 CONCLUSION

This deliverable has undertaken a systematic journey, which aimed, through historical, legal, technical, and practical lenses to assess whether UPGAST's data-sharing contracts qualify as 'smart contracts' under the EU Data Act.

**Section 2** laid the groundwork by tracing how contracts evolved from ancient written promises through the instrumental, telematica, and automata phases, culminating in today's smart-contract paradigm. The EU's electronic-contracts framework to establish legal validity, fairness, and signature requirements for e-contracts was also discussed on a high-level, leading to a closer focus to smart contracts' definitional pluralism, and the distinction between mere code-based protocols, smart contracts, and full Smart Legal Contracts (SLCs). Furthermore, the technological foundations of smart contracts were briefly examined, to then narrow the focus of the analysis in the Data Act's technologically neutral, functional definition of smart contracts in Article 2(39)), its Recital 104 clarification, scope, legal nature, execution semantics, and the essential requirements of Article 36.

Building on that foundation, **Section 3** focused on machine-readability of smart contracts, with a high contrast between natural language's path-dependent syntax, rich but ambiguous semantics, and context-driven pragmatics with formal languages' precision and determinism, highlighting the limitations of the "Unified Method" (full translation) versus the more practical "Paired Method" (tagging or pairing natural clauses with code). Ontologies as formal, explicit specifications of shared conceptualizations (in OWL) were discussed in their capacity to support contract template generation, pre-execution vulnerability detection, and runtime monitoring, with the necessary clarification of them not being legally binding on their own, ontologies enhance interoperability, auditability, and automated compliance.

In **Section 4**, these insights were leveraged to assess to the UPGAST Negotiation and Contracting Plugin (NCP). A summary of the NCP's architecture's description was at first provided, to then turn to the evaluation of UPGAST contracts against the Data Act criteria. While NCP fully satisfies the 'computer program' and 'electronic data records' elements and offers substantial automation in negotiation, it retains human oversight and does not itself self-execute contractual obligations; therefore placing contracts produced thereunder, with a strict reading of Art 2(39) DA, in the realm of advanced electronic contracts rather than fully self-executing smart contracts.

**Section 5** addressed two ancillary but crucial regulatory pillars. First, the Data Governance Act's neutrality, non-discrimination, interoperability, and security constraints on Data Intermediation Services (DIS) were analysed, showing how these operational limits shape data-sharing contract practices by restricting bundling, dynamic pricing, and intermediary-driven term suggestions. Second, a short reference to the DGA's logging requirement of Article 12(o) DGA was made, confirming that the latter mandates UPGAST to maintain comprehensive activity logs—both fulfilling legal

obligations and reinforcing auditability for compliance and dispute resolution.

Overall, the present analysis demonstrates that UPCAST's NCP embodies a robust, legally sound, and technologically flexible approach, in the following manners:

- ✓ It leverages formal policy languages and ontologies to ensure semantic clarity, modularity, and machine interpretability.
- ✓ It integrates automated negotiation and contract-generation workflows that materially reduce manual effort while preserving human control.
- ✓ It partially aligns with the DA's functional, technology-neutral smart contract definition and essential requirements.
- ✓ It adheres to the DGA's neutrality and logging mandates, reinforcing transparency and fairness in data-sharing markets.

An outlook to future research would definitely explore how UPCAST might possibly develop to become a technology which supports and enables smart contract creation. It should also investigate empirical impacts of DIS constraints on real-world pricing and negotiation dynamics, and the development of standardised 'smart-contract dictionaries' under national contract-law regimes, as suggested.

In conclusion, while UPCAST contracts do not yet meet the strictest interpretations of 'smart contracts' in terms of full self-execution, they represent a mature, interoperable, and compliance-focused instantiation of advanced electronic contracts, which are well positioned to evolve alongside emerging EU standards and technologies in the future

Commented [HJ43]: How?

## 7 REFERENCES AND ACRONYMS

### 7.1 REFERENCES

Allen JG, 'Wrapped and Stacked: "Smart Contracts" and the Interaction of Natural and Formal Language' (2018) 14 *European Review of Contract Law* 307

Alma R and Piatti L, 'Smart Contract: The Contract Automation Climax: Back-End and Front-End Legal Implications', *Blockchain and Smart-Contract Technologies for Innovative Applications* (Springer, Cham 2024)

Berberich M, '„Intelligente Verträge“ Bzw. „Smart Contracts“' in Heinrich Amadeus Wolff and Stefan Brink (eds), *BeckOK Datenschutzrecht*, vol 50 (2024)

—, 'Zur Ausführung Einer Datenbereitstellungsvereinbarung' in Heinrich Amadeus Wolff and Stefan Brink (eds), *BeckOK Datenschutzrecht*, vol 50 (2024)

Berberich M, Wolff HA and Brink S, 'Anbieter Oder Einsetzender', *BeckOK Datenschutzrecht*, vol 50 (2024)

Blycha N and Garside A, 'Smart Legal Contracts: A Model for the Integration of Machine Capabilities Into Contracts' [2020] SSRN Electronic Journal <<https://www.ssrn.com/abstract=3743932>> accessed 10 February 2025

Borges G, 'Smart Contracts für Datentransaktionen und der Data Act – Potential und Herausforderungen der automatisierten Bereitstellung von Daten' (2024) 40 *Computer und Recht* 425

Brecque C, 'An Introduction to Ontologies and How to Use Them' (*TextMine*, 22 January 2024) <<https://textmine.com/post/an-introduction-to-ontologies-and-how-to-use-them>> accessed 12 February 2025

Cantone D and others, 'Ontological Smart Contracts in OASIS: Ontology for Agents, Systems, and Integration of Services' in David Camacho and others (eds), *Intelligent Distributed Computing XIV*, vol 1026 (Springer International Publishing 2022) <[https://link.springer.com/10.1007/978-3-030-96627-0\\_22](https://link.springer.com/10.1007/978-3-030-96627-0_22)> accessed 6 May 2025

Choudhury O and others, 'Auto-Generation of Smart Contracts from Domain-Specific Ontologies and Semantic Rules', *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (2018) <<https://ieeexplore.ieee.org/document/8726491/?arnumber=8726491>> accessed 10 February 2025

Clack CD, Bakshi VA and Braine L, 'Smart Contract Templates: Foundations, Design Landscape and Research Directions' (arXiv, 15 March 2017)

'Corda Smart Contracts - Corda 4 Tools' (*R3 Documentation*, 30 September 2021) <<https://docs.r3.com/en/tools/cdl/smart-contract-view/corda-smart-contracts.html>> accessed 24 June 2025

Dominguez JA, Gonnet S and Vegetti M, 'The Role of Ontologies in Smart Contracts: A Systematic Literature Review' (2024) 40 *Journal of Industrial Information Integration* 100630

Doussot G, 'Smart Contracts Inside SGX Enclaves: Common Security Enclaves: Common Security Bug Patterns' (*FoxIT*, 24 March 2020) <<https://www.fox-it.com/be/research-blog/smart-contracts-inside-sgx-enclaves-common-security-bug-patterns/>>

Drexl J and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (Social Science Research Network, 25 May 2022) <<https://papers.ssrn.com/abstract=4136484>> accessed 20 March 2025

Dwivedi V and others, 'Evaluation of a Legally Binding Smart-Contract Language for Blockchain Applications' (2023) 29 *JUCS - Journal of Universal Computer Science* 691

European Parliament, Committee on Legal Affairs, 'Resolution on Action to Bring into Line the Private Law of the Member States' (1989) OJ C 158

Farah Y, 'Electronic Contracts and Information Society Services Under the E-Commerce Directive' (2009) 12 *Journal of Internet Law* 3

Hennemann M and others, *Data Act: An Introduction* (Nomos Verlagsgesellschaft mbH & Co KG 2024) <<https://www.nomos-elibrary.de/index.php?doi=10.5771/9783748918691>>

'How Oasis Protects Privacy Despite TEE Vulnerabilities' (*OASIS*, 29 November 2022) <<https://oasis.net/blog/how-oasis-protects-privacy-despite-tee-vulnerabilities>> accessed 24 June 2025

Li R and others, 'SoK: TEE-Assisted Confidential Smart Contract' (2022) 2022 *Proceedings on Privacy Enhancing Technologies* 711

Lim C, Saw T and Sargeant C, 'Smart Contracts: Bridging the Gap Between Expectation and Reality | Oxford Law Blogs' (11 July 2016) <<https://blogs.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality>> accessed 14 February 2025

López-Pintado O and others, 'CATERPILLAR: A Business Process Execution Engine on the Ethereum Blockchain' (arXiv, 22 April 2019) <<http://arxiv.org/abs/1808.03517>> accessed 22 April 2025

Nicholas B, *An Introduction to Roman Law* (Oxford : Clarendon Press 1962)

Novriansyah N, 'Understanding Hyperledger Fabric: A Private and Permissioned Blockchain Solution' (*Medium*, 7 May 2024) <<https://medium.com/novai-hyperledger-fabric-101/understanding-hyperledger-fabric-a-private-and-permissioned-blockchain-solution-1c5b037fc9f9>>

Olivieri L and Pasetto L, 'Towards Compliance of Smart Contracts with the European Union Data Act', *CEUR Workshop Proceedings* (CEUR-WS 2023) <<https://orbilu.uni.lu/handle/10993/60658>> accessed 10 February 2025

Paschke A and Bichler M, 'Knowledge Representation Concepts for Automated SLA Management' (arXiv, 2008) <<http://arxiv.org/abs/cs/0611122>> accessed 6 May 2025

Plato, *Laws, Book 11*

Raskin M, 'The Law and Legality of Smart Contracts' (2017) 1 *Georgetown Law Technology Review* 305

Scrocca M and others, 'Modelling Business Agreements in the Multimodal Transportation Domain through Ontological Smart Contracts' (arXiv, 5 September 2022) <<http://arxiv.org/abs/2209.05463>> accessed 20 March 2025

Studer R, Benjamins VR and Fensel D, 'Knowledge Engineering: Principles and Methods' (1998) 25 *Data & Knowledge Engineering* 161

Szabo N, 'Smart Contracts: Building Blocks for Digital Markets' (1996) 16 *Entropy* <<https://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf>>

Wilkinson S and Giuffre J, 'Six Levels of Contract Automation: The Evolution of "Smart Legal Contracts"' in Jason Grant Allen and Peter Hunn (eds), *Smart Legal Contracts* (Oxford University Press 2022)

Zyskind G, Nathan O and Pentland A, 'Enigma: Decentralized Computation Platform with Guaranteed Privacy'

—, 'Enigma: Decentralized Computation Platform with Guaranteed Privacy' (arXiv, 10 June 2015) <<http://arxiv.org/abs/1506.03471>>

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures 2000 (L 13/12) 269

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) 2000 (OJ L 178, 17/7/2000) 1

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 (OJ L 304, 25/10/2011) 64

Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act) 2022 (COM(2022) 68 final, 2022/0047 (COD))

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 (OJ L 119/1, 4/5/16)

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services 2019 (OJ L 186/57, 11/7/19)

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 152/1, 3/6/2022)

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) 2023 (OJ L, 22/12/2023)

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 2014 (OJ L L 257/73, 28/8/14)

## 7.2 ACRONYMS

Acronyms List	
DA	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)
DGA	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 152/1, 3/6/2022)
EU	European Union
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
NPC	Negotiation and Contracting Plugin
OWL	Web Ontology Language (OWL)

**Commented [LI44]:** Should be NCP. Later in the document you sometimes use NCP and others NPC

**Table 3** – Acronyms