



European
Commission

JRC TECHNICAL REPORT



API strategy essentials for Public Sector Innovation

LEGAL & ORGANISATIONAL
PERSPECTIVE

EUR 31216 EN

interoperable
europe

Joint
Research
Centre

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The contents of this publication do not necessarily reflect the position or opinion of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Contact information

Name: Monica Posada-Sanchez
Address: Joint Research Centre, Via Enrico Fermi, 2749 – 21027 Ispra (VA) Italy
Email: monica.posada@ec.europa.eu

EU Science Hub

<https://joint-research-centre.ec.europa.eu>

JRC129940

EUR 31216 EN

PDF ISBN 978-92-76-56795-0 ISSN 1831-9424 [doi:10.2760/511499](https://doi.org/10.2760/511499) KJ-NA-31-216-EN-N

Luxemburg: Publications Office of the European Union, 2022
© European Union, 2022



The reuse policy of the European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

For any use or reproduction of photos or other material that is not owned by the European Union, permission must be sought directly from the copyright holders.

How to cite: Posada Sanchez, M. and Pogorzelska, K., *API strategy essentials for Public Sector Innovation: Legal and organisational perspective*, Publications Office of the European Union, Luxembourg, 2022, doi:10.2760/511499, JRC129940.

CONTENTS

- ACKNOWLEDGEMENTS 1
- ABSTRACT 2
- EXECUTIVE SUMMARY 3
- 1 Introduction: API strategy legal and organisational essentials 4
 - 1.1 Context 5
 - 1.2 Scope and objectives 5
 - 1.3 Document structure and methodology 5
- 2 API legal considerations 6
 - 2.1 Regulatory background 6
 - 2.2 Conceptualisation of the legal framework for using APIs 9
- 3 API organisational considerations 18
 - 3.1 Roles and responsibilities 18
 - 3.2 Systems and processes 19
 - 3.3 Rights and obligations 20
- 4 Legal and organisational nexus: contractual practices 22
 - 4.1 Contractual nature of API service agreements 22
 - 4.2 Empirical analysis of API ToS from a systemic perspective 23
- 5 Conclusions 28
- List of abbreviations 29
- List of figures 29
- List of tables 29
- References 30
- Annex I: Examples of government API Terms of Service 33
- Annex II: API organisational analysis interviewees 36

ACKNOWLEDGEMENTS

The European Commission funded the research of the API4IPS project through the IPS action (2018.01) of the Interoperability Solutions for Public Administrations Programme (ISA²). Three directorates of the European Commission participated in the making of this project. Namely, the Joint Research Centre (JRC), Informatics (DIGIT), and Communications Networks, Content and Technology (CONNECT).

We want to thank our counterparts in DIGIT and CONNECT for their great support in administering and coordinating the project activities. We also want to thank our DIGIT D3 colleagues for providing insight and expertise that greatly assisted our research. Specifically for their contribution to the overarching API4IPS project: the design of a REST API profile for the [eDelivery CEF building block](#). Letting us actively interact with their activities helped us identify and explore several aspects of the technical essentials of APIs in practice. We sincerely thank our collaborators Hans Graux, Mark Boyd and APIdays for their contributions and fruitful collaboration. A special thanks to all collaborators and participants that contributed to the work with their knowledge and experiences. To name some, from the public administration: Peter Knudsen, Patrick Amarelis, Daniel Sarasa Funes, Roberto Polli, Frank Terpstra, Hanna Niemi-Hugaerts, Kjersti Lunde, Marco Panebianco, Ron Van der Lans, Petteri Kivimaki, Sven Rasmussen, the private sector: Kin Lane, Tyler Singletary, David O'Neill, Alan Glickenhause, Isabel Mauny, Darrel Miller, Erik Wilde, Peter Rabley, Mehdi Medjaoui, Marjukka Niinioja, Jonas Onland,, citizen driven initiatives: Lillith Wittmann, and Academia: Prof. Markos Zachariadis, Francois Xavier CAO.

API4IPS PROJECT REPORTS

The API4IPS project outputs include the following three reports, this document corresponds to report number 2:

1. [*REPORT I: API STRATEGY TECHNICAL ESSENTIALS*](#)

The report analyses essential technical aspects to be considered by government organisations that aim at innovating their processes and leveraging all the potential of their API-driven technological infrastructures. These aspects include API management, discoverability, security and traceability concerns.

2. [*REPORT II: API STRATEGY LEGAL AND ORGANISATIONAL ESSENTIALS*](#)

The report analyses legal and organisational aspects to be considered by government bodies i) to lawfully operate with their API infrastructure and ii) to better coordinate their API-driven digital relationships. These aspects include the analysis of the legal framework applicable to APIs, current organisational practices of digital coordination through APIs, and empirical analysis of the conditions included in 4000 API's Terms of Service documents.

3. [*API STRATEGY ESSENTIALS FOR PUBLIC SECTOR INNOVATION – MAIN FINDINGS & CONCLUSIONS*](#)

This report describes the main findings of the project and draws overarching conclusions about areas to focus when using API infrastructure in public sector innovation processes.

RELATED WORK

- [1] [The role of Application Programming Interfaces \(APIs\) in data governance and digital coordination](#)
- [2] [Application Programming Interfaces in Governments: why, what and how](#)
- [3] [Web Application Programming Interfaces \(APIs\): general-purpose standards, terms and European Commission initiatives](#)
- [4] [An Application Programming Interface \(API\) framework for digital government](#)
- [5] [Unfolding opportunities from the use of APIs in Europe](#)

ABSTRACT

Application Programming Interfaces (APIs) have an enabling role in establishing digital ecosystems and coordinating digital interactions. A robust and performing technical infrastructure is essential but insufficient to ensure a sustainable thriving of digital environments. Both technical and legal stability are necessary to cherish for the mutual benefit of service providers, their users and society at large. This stability is crucial to ensure the robustness and competitiveness of digital value chains and the thriving of the European digital ecosystem.

Against this backdrop, this report explores crucial organisational and legal aspects of managing and coordinating digital interactions through APIs. Specifically, the analysis describes API-related legal obligations and applicable law. The study also analyses the current practices of coordination and negotiation with their digital counterparts in eight different organisations. Finally, the work analyses the clauses and conditions encoded in 4K API's Term of Services documents (ToS) to evaluate if current ToS drafting practices foster or hinder the thriving of fair digital environments.

This work aims to clarify relevant aspects (e.g., API actors' roles and functions, API-related rights and obligations) that should be considered when designing rights and responsibilities flows within digital chains and the ecosystem at large.



Source: © sdecoret, 232770524 / Adobe Stock

EXECUTIVE SUMMARY

APIs have an enabling role in the establishment of digital ecosystems and the coordination of digital interactions. A robust and performing technical infrastructure is essential but insufficient to ensure a sustainable and thriving digital environment. Both technical and legal stability is necessary to secure the mutual benefits for service providers, their users and society at large. This stability is crucial to ensure the robustness and competitiveness of digital value chains and the thriving of the European digital ecosystem.

This report analyses what legal and organisational aspects are essential for managing and coordinating digital interactions from an API viewpoint. The report analyses both from the perspective of an individual organisation as well as of the ecosystem. The objective is to provide information that can help organisations identify critical aspects to establish and manage their API infrastructure and to coordinate, negotiate and properly design responsibility/rights flows within digital value chains and ecosystems at large.

Specifically, the report analyses i) API legal concerns that organisations need to tackle depending on their API-related role and function, ii) organisational and coordination aspects that streamline API-driven digital relationships, and iii) current contractual practises encoded in Terms of Service agreements.

On *API legal concerns*, this report scans the current body of law and identifies regulations that contain rules applicable to API-driven organisations. Then it describes the applicable legal framework and describes the legal implications linked to stakeholder's role and specific API function.

On *API organisational and coordination aspects*, the report identifies new roles and responsibilities that should consider API actions for public sector innovation. Specifically, the work describes the creation of provisory entities that make testing innovative solutions more accessible to the public sector. It also explains how processes and workflows are adapted to ease the digital transition of government while respecting the continuity of its statutory operations. The study also analyses decision-making at different management levels of a public organisation, i.e., the strategic, tactical and operational levels of a public sector organisation.

Finally, this work has conducted an empirical study of *current practices of digital coordination with APIs*. In particular, it evaluates systemic implications of the interactions defined by API contract conditions in 4000 Terms of Service (ToS) documents. In particular, the analysis evaluates the homogeneity in the drafting of ToS contracts, the compliance with currently applicable laws, the encoding of intellectual property rights, whether jurisdiction statements can be perceived as hurdles for digital collaboration. The results show that work still needs to be done to ensure balanced and trustworthy legal and technical stability conditions necessary to guarantee the establishment of a robust, fair, competitive and sustainable digital ecosystem.

1 Introduction: API strategy legal and organisational essentials

The digital transformation of government involves its seamless connection with and integration into the digital ecosystem; i.e., becoming a connected Government. The re-wiring of private-public relationships (business to government, government to business, business to person, government to citizen to government) is evolving quickly. Enabling trust and collaboration through private and public partnerships for the Common Good (World Economic Forum 2019) is vital to balance the potential and risks of this transformation (OECD, 2019). Application programming interfaces (APIs) are enablers of this integration because of their capacity to connect actors and systems and dissolve private-public frontiers.

The management and coordination of API connections are key to steering interactions toward efficient digital service provision. These two processes can support the governance of digital interactions and ultimately help stabilise the conditions necessary for the digital ecosystem to flourish. In particular, these two processes should monitor constraints encoded in APIs that restrict data access and limit the realisation of its full potential either technically or under restrictions in the agreements governing interactions. They also should control API-configurable metrics on the usage (e.g. number of active users, transactions). Additionally, the coordination process should ensure the cooperation of involved stakeholders.

Organisations use API infrastructure to connect to other actors within digital services processes. Figure 1 shows different ways in which APIs can participate in data value chains. The full chain of a digital service can be composed of one or more APIs. Moreover, an API can concurrently belong to different digital service chains. This interconnectedness adds complexity to designing efficient and stable processes and systems. Thus, organisations need to invest in coordination efforts to ensure the interoperability and stability of their digital relationships and processes. This coordination has both legal and organisational components.

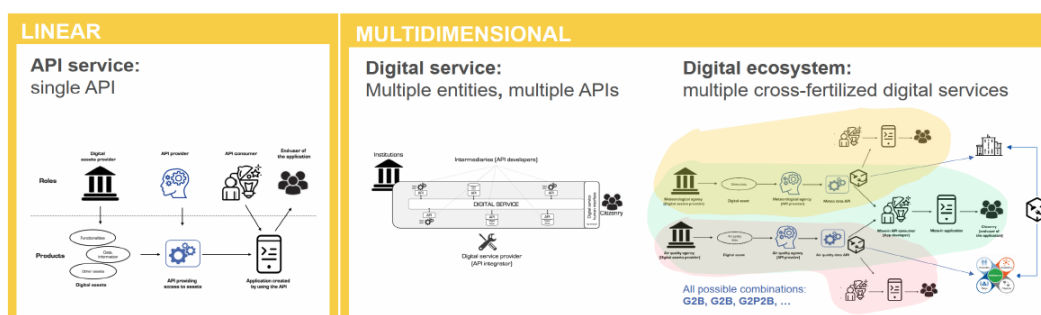


Figure 1: APIs in digital value chains (linear and multidimensional). Source: JRC own elaboration

The legal analysis of APIs is a multifaceted question. On one side, an API is a piece of software that can be subjected to intellectual property rights (IPRs) such as patents, copyrights, trade secrets. The identity of APIs can be also protected by trademarks. On another side, an API is a service that can be ruled by service agreements that coordinate technical and legal aspects. The multi-level nature of such agreements has organisational implications that need to be well understood to ensure the stability of digital solutions and the ecosystem. This report will analyse the most relevant legal and organisational aspects that government organisations should consider when supplying or consuming APIs to ensure an effective connection to the digital ecosystems.

1.1 Context

The European Commission's Joint Research Centre (JRC), the Directorate-General (DG) for Informatics and the Directorate-General for Communications Networks, Content and Technology (DG Connect) launched the API for innovative public services study in May 2020. This project belongs to action 2018.01 (innovative public services) of the second interoperability solutions for European public administrations programme (ISA²). The project investigates how APIs can support the development of innovative public services and the innovation of the public sector in general. The project was carried out in close collaboration with the Connecting Europe Facility eDelivery building block activities, performed by DG Informatics, Unit D3– Trans-European Services

1.2 Scope and objectives

The connections among actors in digital ecosystems mostly happen through APIs. Any organisation that embraces digitalisation needs to invest in appropriate API infrastructures. Building up a robust API technical infrastructure is essential, but it is not enough. The coordination and management of legal and organisational aspects is crucial to stabilise the functioning of digital processes and, ultimately, the entire ecosystem in a fair and balanced way.

Against this background, the objective of this report is to help organisations identify the main organisational and legal aspects of managing and coordinating their digital interactions through APIs. Specifically, the analysis describes API-related legal obligations and applicable law. Additionally, the analysis aims to help organisations coordinate and negotiate with their digital counterparts more effectively. This could be useful when designing rights and responsibility flows within digital chains, and the ecosystem at large.

1.3 Document structure and methodology

In this report, we first tackle legal issues related to the provision and use of APIs and conceptualise the applicable legal framework. We then go on to explore the state of the art on practices around organisational aspects of using APIs. To this end we interviewed a range of stakeholders from public and private sectors. Finally, we analysed the contractual relations between stakeholders engaged in the use of APIs by analysing a list of over 4000 Terms of Services (ToS) to explore how ToS drafting enables digital ecosystems to be developed and to thrive.

2 API legal considerations

When an organisation procures, provides, or consumes APIs, it must abide by the applicable regulatory framework. This framework will depend on the distinct roles that the organisation can play and the API functions it exploits. This section will analyse the existing legal framework from an API viewpoint, and then identify legal concerns that an organisation has to tackle depending on their API-related role and the API function they use.

Governments must monitor the implementation of policies, and data governance policies are no exception. APIs can support these duties by computing metrics of API usage and other details of digital transactions when needed. Therefore, public entities should be aware and technically ready for regulatory reporting (ideally, also through API infrastructure).

2.1 Regulatory background

APIs are technical means for sharing and controlling access to data. These characteristics were considered when exploring API-relevant data sharing and the data governance legal framework. In this context, Europe is a pioneer in regulatory initiatives for data governance, and there is already a relevant body of applicable law (see Table 1). Nonetheless, the landscape is changing by the day under the European Data Strategy (European Commission, 2020a), and new policy instruments that are currently being designed, such as the Digital Governance Act [DGA] (European Commission, 2020b); the Digital Markets Act [DMA] (European Commission, 2020c); and the Data Act [DA].

Beyond the European strategy for data, the connective power of APIs facilitate cross-fertilisation among sectors and industries by enabling data exchanges. Therefore, the legal framework linked with APIs expands through other policy initiatives under the European priority of “A Europe fit for the digital age”, namely, the industrial (European Commission, 2020d) (European Commission, 2020e) and artificial intelligence strategies (European Commission, 2020f).

There is literature that evaluates the current legal framework applicable to data sharing (European Commission. DG-CONNECT, 2020) and developing work that analyses it from the API viewpoint. (European Commission Joint Research Centre, 2021), (Vaccari et al., 2021), (Vaccari et al., 2020). Building on these studies, Table 1 presents legal instruments that should be observed when dealing with APIs. The current instruments include obligations that are applicable to all sectors, along with some that are specific to areas such as finance and banking, utilities, telecommunications, mobility, and geospatial data.

In addition to the European legal framework, other government levels (national, regional, and local) may have defined other legal regulatory obligations. Government organisations need to make their API infrastructure compliant with those applicable norms too.

Table 1: European body of law applicable to data sharing Q2-2022

INSTRUMENT	DESCRIPTION	LINK	SCOPE
COMPETITION LAW – TFEU	Competition rules	Articles 101-109 TFEU	Horizontal
E-COMMERCE DIRECTIVE (AMENDED BY DSA)	Rules on information society services, in particular electronic commerce	DIRECTIVE 2000/31/EC	Horizontal
GENERAL DATA PROTECTION REGULATION (GDPR)	Rules on protection of personal data	REGULATION (EU) 2016/679	Horizontal
OPEN DATA DIRECTIVE (REVISED)	Rules on open data and the re-use of public sector information	DIRECTIVE (EU) 2019/1024	Horizontal
REGULATION ON FREE FLOW OF DATA	Framework for the free flow of non-personal data in the European Union	REGULATION (EU) 2018/1807	Horizontal
DATABASE DIRECTIVE (AMENDED BY DATA ACT)	Sui generis protection of data basis	DIRECTIVE 96/9/EC	Horizontal
COPYRIGHT DSM DIRECTIVE	Horizontal rules on copyrights in EU DSM	DIRECTIVE (EU) 2019/790	Horizontal
THE COMPUTER PROGRAM	Copyright protection of computer programs	DIRECTIVE 2009/24/EC	Horizontal
TRADE SECRETS DIRECTIVE	Trade secret protection	DIRECTIVE (EU) 2016/943	Horizontal
EUROPEAN PATENT CONVENTION	Patent protection	EPC, 17th Edition, 2020	Horizontal
THE PORTABILITY REGULATION	Cross-border portability of online content services	REGULATION (EU) 2017/1128	Horizontal
THE DIGITAL CONTENT DIRECTIVE	Rules on contracts for the supply of digital content and digital services	DIRECTIVE (EU) 2019/770	Horizontal
PLATFORM TO BUSINESS REGULATION (P2B)	Promotes fairness and transparency for business users of online intermediation svcs	REGULATION (EU) 2019/1150	Horizontal
CYBERSECURITY ACT	Establishes a cybersecurity certification framework for products and services	REGULATION (EU) 2019/881	Horizontal
SECOND NETWORK AND INFORMATION SECURITY (NIS2) (PROPOSAL)	Establishes measures for a high common level of cybersecurity	COM(2020) 823 final	Horizontal
DATA GOVERNANCE ACT – DGA	Data governance framework, sharing of sensitive data held by public sector	REGULATION (EU) 2022/868	Horizontal
DATA ACT (PROPOSAL)	Data sharing architecture: rules on fair access to and use of data	COM(2022) 68 final	Horizontal
DATA MARKETS ACT –DMA – (PROPOSAL)	Fair markets and competition in digital sector	COM(2020) 842	Horizontal
DIGITAL SERVICES ACT – DSA – (PROPOSAL)	Digital services in DSM, content liability	COM(2020) 825 final	Horizontal
ARTIFICIAL INTELLIGENCE ACT – AI ACT-(PROPOSAL)	Rules on use of AI systems	COM(2021) 206 final	Horizontal
INTEROPERABILITY ACT – IA ACT – (IMPACT ASSESSMENT)	Setting up interoperability framework for public sector data flows and services	Upcoming	Horizontal
THE SECOND PAYMENT SERVICES DIRECTIVE (PSD2)	Banking	DIRECTIVE (EU) 2015/2366	Sectoral
MIFID FRAMEWORK: MIFID II DIRECTIVE	Financial	DIRECTIVE 2014/65/EU	Sectoral
MIFID FRAMEWORK: MIFIR REGULATION	Financial	REGULATION (EU) No 600/2014	Sectoral
E-PRIVACY DIRECTIVE & EU ELECTRONIC COM CODE	Telecommunications	DIRECTIVE 2002/58/EC	Sectoral
INSPIRE DIRECTIVE	Spatial information	DIRECTIVE 2007/2/EC	Sectoral
REGULATION ON ROAD SAFETY	Mobility	REGULATION (EU) 886/2013	Sectoral
REGULATION ON VEHICLE REPAIR AND MAINTENANCE INFO	Mobility-vehicles	REGULATION (EU)886/2013	Sectoral
REACH	Chemicals	REGULATION (EC) No 1907/2006	Sectoral
ELECTRICITY DIRECTIVE	Electricity	Directive 2009/72/EC	Sectoral
GAS DIRECTIVE	Gas	DIRECTIVE 2009/73/EC	Sectoral
THE CLINICAL TRIAL REGULATION	Health	REGULATION (EU) 536/2014	Sectoral

2.1.1 API-based data sharing in the digital single market

APIs play a key role in stabilising digital ecosystems in the digital single market (DSM). While the body of law on data sharing rarely mentions APIs explicitly, the following recent instruments do mention APIs concerning both data supply (sharing) and demand (access):

1. The open data directive (European Union, 2019a). This directive obliges governments to make High Value Data sets (HVD) available through APIs. The goal is to unlock the value of public sector data by exposing them to multiple actors and enabling their re-use. APIs can enable this as they can be concurrently accessed by many actors and systems, scale at near-zero marginal costs, and allow monitoring and control of their use.
2. The Digital Markets Act (DMA) foresees the role for APIs in effective real-time data portability for business and other users to facilitate switching to different service providers (Recital 54) or facilitating compliance under GDPR regulation and ePrivacy Directive.
3. The Data Act (DA) clearly positions APIs as technical means to access data. Article 28(1)(c) states that “the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously or in real-time in a machine-readable format.” The DA positions APIs as a technical means of assuring effective data access rights. It strengthens the user side versus a more potent service provider who has the power to enforce contractual conditions on the service users unilaterally, often totally excluding their liability or without any guarantees on the quality of service (see section 4.2).

In contrast to the open data directive, which sets *obligations for data sharing* with APIs, the DMA and DA introduce APIs in the context of the setting of *data access rights*. Such positioning of APIs highlights their importance in ensuring competition and fostering innovation. We can observe the shift in the regulator’s perspective from a one-dimensional data sharing approach to one that aims to develop and stabilise digital ecosystems. APIs are considered a key technical means to enable such processes.

2.1.2 API-based data sharing for legal enforcement

The role of APIs in digital governance goes beyond the facilitation of sharing data in the DSM. Legal enforcement and compliance monitoring processes can greatly benefit from the deployment of the API infrastructure in public service. Governments must monitor the implementation of policies, and data governance polices are no exception. APIs can support these duties by computing metrics of API usage and other details of digital transactions when needed. Therefore, public entities should be aware and technically ready for regulatory reporting (ideally, also through API infrastructure).

There are many examples of APIs being used as an underpinning tool in the enforcement of regulations. One is the GDPR (European Union, 2016). APIs are a technical enabler of implementing Articles 6 and 20 (data

portability). They could also support monitoring and reporting mechanisms. However, in this case, use of APIs in the technical implementation of the regulation is still uneven and yet not fully operative.

A more developed example is the implementation of the second payment services directive (PSD2) in the banking sector (European Union, 2015). API services underpin the implementation of this directive. Open Banking API-powered standardising initiatives have gathered entrepreneurs, investors, and innovators. This cooperation has enabled the rapid development of a vast and powerful Fintech ecosystem that positively benefits citizens. An example of this cooperation is the Berlin Group NextGenPSD2 (The Berlin Group, 2021). This techno-legal sectorial coordination model could be explored in the context of interoperability of public digital service provisioning in Europe currently being designed under the Interoperable Europe Act.

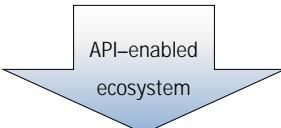
2.2 Conceptualisation of the legal framework for using APIs

When an organisation procures, provides, or consumes APIs, it must abide by the applicable regulatory framework. This framework will depend on the distinct roles that the organisation can play and the API functions it exploits. For a specific organisation the scope of the applicable legal framework will depend on who uses APIs, how, and for what purpose. To help clarify this, we combine an API function with the corresponding stakeholder's role to get a legal perspective linked to the use of an APIs. The resulting four perspectives are not mutually exclusive, i.e. an organisation can consider more than one perspective in order to establish its scope of activity and subsequently determine the applicable legal framework.

For example, a public organisation that considers using APIs for data sharing will need to combine the roles of a data holder, API developer and API service provider in the design/planning phase. Later, those roles – as well as relevant legal obligations and responsibilities – can be distributed among different collaborating organisations or outsourced to the organisations that developed expertise in the specific field (for example standardisation bodies, IT developers, platforms, etc.). As APIs come with the characteristic of enabling development of digital ecosystems, this public organisation will integrate into the digital ecosystem or even become the ecosystem's orchestrator.

As API functions range from product-like software to service provision, API-driven business models also differ. An ownership business model closely linked to the API as a product function is complemented and often replaced by a licensing model, where permission to use APIs is granted without ownership transfer. With the rise of APIs used as a service function one can observe that the subscription model prevails. There are subscription-based licences as well as subscription-based services. In this last version of business model, the licences are often executed on the technical level, whereas the subscription model is executed on the service level. Each one of these models has different legal implications, and adds complexity to the picture. They can even coexist at the level of one single API. Table 2 presents legal obligations/issues and laws applicable to different stakeholder roles depending on the exploited API function. The table also includes legal issues relating to the stabilisation of the API-enabled digital ecosystem from a systemic perspective.

Table 2: Conceptualization of the legal framework applicable to the use of APIs

API FUNCTION	STAKEHOLDER ROLE	PRIMARY LEGAL OBLIGATIONS/ISSUES	APPLICABLE RULES AND LAWS/ SOURCES OF OBLIGATIONS
API as technical means to share data	Data holder	<p>Making sure that data sharing is lawful and secure:</p> <ol style="list-style-type: none"> Incorporation of legal constraints on data into APIs: <ul style="list-style-type: none"> - drafting agreements facing an API developer (APIs developed externally), or - adequate internal control (APIs developed internally) Propagation of data legal constrains across value chain: drafting data licences <p>Making sure that the issue of API ownership is settled when APIs are developed externally</p>	Laws relating to data: focus on what data can be shared and under what conditions: GDPR, open data, Data flows, sectoral regulations, DA, DGA, DMA
API as software	API developer	<p>Lawful API design Design must consider the constrains of the exposed data</p> <p>Legal protection of APIs under IPRs and licencing</p>	<p>Industry standards Agreement between API developer and data holder if API not developed by data holder</p> <p>Protection under IPRs (copyrights, patents, trade secrets)</p>
API as a service	API service provider	<p>Lawful operation of services</p> <p>Drafting and compliance with user-facing agreements (ToS, SLA, individual contracts). Disclosure of relevant licences in the agreements</p> <p>Provision of service in accordance with relevant licences on data and APIs</p>	<p>Laws relating to the information society services, DSA</p> <p>Contract law, laws relating to transparency, data protection, consumer protection laws, competition laws</p> <p>Licences linked to the data behind APIs, and the use of APIs</p>
	API service user: business, public and consumers	Compliance with ToS, SLA, individual agreements	Agreement
			
API as technical enabler of digital ecosystem(s)	Ecosystem orchestrator	<p>Using law as tool to build ecosystem (drafting fair, balanced and transparent agreements to build trust, foster collaboration and allow for competition) Distribution of roles responsibilities and rights among participants – reflected in API itself Setting API standards and developing agile guidelines for API infrastructures to enable interoperability Ensuring API infrastructure security + Observing working examples Allowing room for regulatory sandboxing to innovate</p>	<p>Governance frameworks for the ecosystem: P2B regulation, DGA, DA, DSA, DMA Interoperability frameworks European standardisation regulation Infrastructure security: Cybersecurity Act, NIS2 directive</p>

Source: JRC, 2022

2.2.1 Data holder role

From the perspective of a data holder, APIs are technical means to share data. The general obligation of any data holder when it comes to data sharing is to do it lawfully and securely. A data holder must ensure that the responsibilities relating to the data they hold are propagated and rightly reflected in any API interface that provides access to it.

APIs, while technically enabling data sharing, also provide for technical means to embed legal considerations into a technical process. An API allows for defining “what”, “how”, “with whom” and “under which conditions” of the data sharing process. APIs define what data can be shared and in what form. For example, as APIs allow for data anonymisation they can share valuable information drawn from personal data in an anonymised form, in compliance with GDPR. APIs also allow for the control of how data are shared. In other words they establish the technical conditions of data sharing that can control for legal limitations and contractual conditions such as, for example, warranties for the quality of data or availability of the service. API can also define who has access to use the service and it may execute different consequences if the terms of access are breached by the users. Finally, APIs can define under which conditions they operate, e.g. for what purposes they can be used, under which conditions the shared data can be used (technical execution of data licence), or what security conditions must be executed before data are shared.

Data holders, including public institutions, need to make sure that all legal constraints relating to data are already reflected in APIs at the stage of API development. To this end drafting contracts that procure API developers services (if APIs are developed externally) or adequate internal guidelines should be put in place if APIs are developed internally.

Another data holder’s obligation would be the propagation of data legal constraints across a value chain. In principle, this would require the inclusion of relevant contractual conditions on the limitations on data use, protection, and security. API and data licences can be used to this end. Propagation of legal constraints of the digital assets of an API’s backend may have technical implications because the organisation will need to deploy mechanisms that ensure there are no breaches of those constraints.

2.2.2 API developer role

Developing APIs implies looking at an API from a software product perspective. This perspective impacts on the scope of the applicable legal framework and will usually need to be considered by API developers. The development of an API product must follow relevant technical standards and respect the more general standards and laws related to the sector of operation. As with every digital product, APIs need to comply with the cybersecurity rules applicable to the specific industry.

From the developer firm perspective, APIs are digital assets in the form of code or software products. As such, they could be protected by intellectual property rights (IPRs) such as patents, trade secrets or copyrights (Hoffmann and Gonzalez Otero, 2020).

The issue of API protection under IPRs is far from straightforward, and the scope and type of protection under the United States and EU laws have changed over the years. Most of the recent discussion on IPRs protection evolves around *copyrightability* of APIs. In the EU, copyright protection of APIs has drawn criticism for decades and the general position of the EU Courts is rather against the *copyrightability* of APIs. The Computer Programs Directive makes clear that ideas and principles underlying any element of a computer program, including those which underlie its interfaces, are not protected by copyright. The Directive also excludes from the copyright protection uses of a decompiled code when such is indispensable to achieve interoperability. As APIs are regarded a technical means to achieve interoperability function, they are widely regarded functional, therefore not protected by copyrights. There is, however, a possibility that the expression of API specifications and API implementations could qualify for protection as independent works subject to the originality threshold.¹ Nevertheless, this exception is difficult to apply due to the interoperability function of APIs that technically favours similarity rather than originality.

Another IPR to consider in relation to APIs are patents. Under the European Patent Convention, computer programs “as such” are excluded from patent protection. However, the case law of the European Patent Office (EPO) make it clear that this exclusion does not apply when the computer program has a technical character (Hoffmann and Gonzalez Otero, 2020). This limitation to the exclusion is a potential way for protection of APIs with patents. Nevertheless, the possibility is a narrow and the additional requirements of novelty and inventive step as well as disclosure of the code are often prohibitive in patenting APIs.

The legal situation of APIs protection under IPRs in the US is more dynamic. This should be kept in mind for both a potential conflict of law and future developments when operating outside EU borders. In 2008, Samuelson traced the evolution of the law in the US in relation to the protection of software interfaces (Samuelson, 2008). At first, they were not treated as intellectual property at all. Firms published APIs so that others would make programs to run on their computing systems. As firms recognised that they could license interface information to generate revenues APIs started being protected as trade secrets. In the mid-to-late 1980s, it was argued that copyright law was actually more appropriate to protect the “structure, sequence, and organization” (SSO) of APIs. By the early 1990s, however, courts decided that being functional elements of programs, they were more suited to patent than to copyright protection (*Sega v. Accolade*, 1992; *Lotus Development Corp. v. Borland Intern*, 1995).² Firms therefore began patenting interface designs, as well as continuing to license them as trade secrets.

¹ *Bezpečnostní softwarová asociace – Svaz softwarové ochrany v. Ministerstvo kultury* [2010] ECLI:EU:C:2010:816 para 41 – 43; Case C-406/10, *SAS Institute Inc. v. World Programming Ltd* [2012] ECLI:EU:C:2012:259 para 35 and 39.

² *Sega Enter. Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992); *Lotus Dev. Corp. v. Borland Int'l, Inc.*, 516 U.S. 233 (1996).

The patentability of APIs was negatively impacted in 2014 when the US Supreme Court confirmed that an abstract idea could not be patented just because it is implemented on a computer. The court also introduced a new legal test for the “abstract idea” in the *Alice* decision (2014).³ The decision has had a profound effect on the validity of so-called software patents and business-method patents, including APIs. Since then, many patents relating to APIs have been revoked.⁴

As the patent protection for APIs become less accessible, more stress has been put on using copyright to protect APIs. The decade long legal dispute between *Google v. Oracle* (US Supreme Court, 2021) the Java API code and copyright law was very much expected to bring more clarity into the picture. On April 2021, the US Supreme Court held in favour of *Google* on the basis of “fair use” of the code but did not clearly pronounce about the “copyrightability” of the API. Justice Stephen Breyer wrote in his majority opinion: “Given the rapidly changing technological, economic, and business-related circumstances, we believe we should not answer more than is necessary to resolve the parties’ dispute. We shall assume, but purely for argument’s sake that the entire Sun Java API falls within the definition of that which can be copyrighted.” Even if the eligibility of APIs for copyright protection is assumed, *Google’s* use of more than 11,500 lines of Java code has been ruled “fair use” and thus not considered copyright infringement. Such a large extent of *Google’s* non-infringing fair use means that relying on copyright to protect an API remains highly uncertain. The whole case revealed that “copyrightability” is very much case-dependant and wide systemic reliance on copyrights is risky, as the meticulous screening process for eligibility will be applied in the event of litigation.

Since patents and copyright seem less and less reliable in the context of APIs, trade secret protection has gained more ground. The legal instrument to be observed in case of trade secrets is European Trade Secret Directive (2016). The protection of APIs specifications and implementations as trade secrets is now the least controversial option for IPRs protection in the EU.

Given the lack of clarity around the protection of APIs under IPRs, it is important that software developers adopt robust process management for dealing with legal uncertainties and license developing.

2.2.3 API as a service (provider and user role)

The legal considerations of API as a service need to be assessed from the perspective of both service provider and a service user.. API service providers need to comply with general requirements for the provision of information services. API service users need to be aware of their rights and comply with the conditions defined in the contractual terms or other related agreements.

³ *Alice Corp. Pty. Ltd. v. CLS Bank Int'l et al.*, 134 S. Ct. 2347 (2014).

⁴ Hundreds of patents have been invalidated under §101 of the US patent laws in Federal District Courts. Applying *Alice*, district court judges have found many of these claims to be patent-ineligible abstract ideas (<https://www.ndtexblog.com/2015/05/01/alice-the-death-of-software-related-patents/>).

On the provision service side, organisations must lawfully draft ToS and/or Service Level Agreements (SLAs) compliant with contract law (rules on fair contractual terms); laws relating to transparency in platform to business (P2B) relations; and consumer protection laws – just to mention the main horizontal rules. The typical conditions of contracts such as liability, jurisdiction, indemnification and warranties must be thoroughly examined and included. It is argued here that well drafted, balanced, and fair ToS are a cornerstone of the sustainable digital ecosystem building, including the API-centred ecosystem. This line of argument is well in line with the European regulator. Service providers should also comply and communicate to the user relevant licences behind the assets revealed by APIs. The licences should be disclosed to the API users and potential end users of services based on those APIs. In principle they should be propagated down the value chain as part of the ToS and reflected in the API technical implementation itself.

The other side of the coin is the use of a service. The primary obligations for a user will stem directly from the contract, usually the ToS, which are legal offers imposed unilaterally by the service users. Users must comply with the ToS so that their use of services is considered lawful. As ToS become contracts upon adhesion and without the possibility to negotiate, it might be tempting for the service providers to abuse their privileged legal position. The position of consumer has traditionally been protected by the body of law on consumer protection. Those rules will directly apply, even wrongly (or not at all) invoked in the ToS.

The need to strengthen the contractual position of small or medium-sized enterprises (SMEs) vis-à-vis large players (business to business) has also been recognised. The P2B regulation imposes some transparency measures on drafting ToS. The recent DA proposal further strengthens the legal position of SMEs. Chapter IV addresses unfairness of contractual terms in data sharing contracts between businesses in situations where a contractual term is unilaterally imposed by one party on a micro-enterprise or SME. The DA seeks to guarantee that contractual agreements on data access and use do not take advantage of imbalances in negotiating power between the contractual parties.

2.2.4 Ecosystem orchestrator role

This perspective relates to the role of an ecosystem orchestrator. As APIs come with the “built-in” feature to connect, they naturally foster the construction of the digital ecosystem. An organisation that embarks on the deployment of API infrastructure may soon discover countless possibilities of connecting different stakeholders to enable the realisation of policy or business goals.

We observe that recent proposals for European Commission’s regulatory acts relating to the data sharing in the DSM (Digital Single Market) focus on the multidimensional feature of the ecosystem. The European Regulator mentions the term “ecosystem” in different semantic configurations. Box 1 below lists mentions of the term “ecosystem” in formal legal and policy instruments. This gives us an idea of what is considered important for ecosystem development, even if there are no clear definition of the term. It also paints a regulatory background for the ecosystem orchestrator.

Box 1: RECALLING OF THE TERM “ECOSYSTEM” IN THE RECENT REGULATORY LEGAL ACTS AND PROPOSALS:

- Data strategy: “ecosystem of companies, civil society and individuals who can create new products and services based on more accessible data”, “data-driven ecosystems”, “digital ecosystems”, “European data ecosystems”, “ecosystem for a data- and cloud-based supply industry in Europe across the value chain”, “data-sharing ecosystems” and “innovative data-driven ecosystem based on fair contractual relations”,
- DA: “data ecosystem” and “sectoral data ecosystem”,
- DMA: “platform ecosystem”,
- DGA: “data-driven ecosystem independent from any players with a significant degree of market power”,
- DSA: “entire digital ecosystem” and “complex online ecosystem”
- Cybersecurity Act and NIS2: “cybersecurity ecosystem” and “ecosystem”
- Shaping Europe’s digital future communication: “ecosystem of excellence and trust”
- Digital decade declaration: “digital transformation that strengthens the human dimension of the digital ecosystem with the DSM as its core”

One of the messages of the “Data Strategy” and the following DA regulatory proposal imply that legal instruments such as contractual agreements can be used as a tool to build ecosystems. Trust has often been recognised as a cornerstone of relationship-building based on the ecosystem. As we observed in our project, initial ecosystem-building tends to happen without firm legal structures that might hinder innovation. In this initial phase, relationships often develop based on personal trust. However, the process of scaling-up gradually removes the trust based on personal relationships. As the need for trust remains, the introduction of a more formal approach in place of personal trust must occur.

The current legal proposals that enforce the use of legal tools in a way that foster ecosystem-building promote systemic building of trust. To this end the DA imposes rules for drafting fair, balanced and transparent agreements, including those governing relations based on APIs. Article 28(1) of the DA states that “the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously or in real-time in a machine-readable format.” This article proposes a shift from ToS that are often service-provider protective and unbalanced towards ToS that are more akin to an SLA. It is a strong signal that data holders providing API services should embrace more responsibility towards the quality and continuity of service to stabilise building of a data-driven ecosystems. Accessing data via an API service to some extent also alleviates legal liabilities linked to those of a data holder, such as those linked to sharing and securing personal data, or other sensitive data. This makes APIs legally attractive for a business, as it is the

data holder that must ensure lawful and secure data sharing by means of drafting adequate agreements, while a service user must simply follow an agreement (e.g. ToS). Moreover, the use of APIs allows the coupling of legal and economic attractiveness. Using APIs from a third-party developer or data holder is less onerous in terms of time and expertise. This frees business's resources because a company does not need to constantly reinvest in changing its core skills and infrastructure: it can simply use an API and build upon the value it provides. APIs potentially present great incentives for their users. This of course implies more commitments and serious planning for the data holder if it assumes a role of an ecosystem orchestrator. While the DA does not impose on public sector bodies any general obligations to share data via APIs (only high-value datasets are to be shared via APIs), it sets out a way towards developing a sustainable digital ecosystem.

The ecosystem orchestrator must also consider the question of how to navigate the governance of data sharing in a fair and non-discriminatory way which enables collaboration without hindering competition. DMA, DSA and DGA provide for guidelines in this respect, from the perspective of competition in markets and responsibility for content and data sharing governance, respectively. The more recent shift of narrative from the obligation to share towards the right to access is a meaningful one, as it encourages participation. This means that a variety of relations need to be considered at the stage of API development. As APIs allow for execution of many contractual aspects relating to data access, they must be technical reflections of responsibilities and rights that govern an ecosystem. Still, considering the ecosystem perspective, it is not enough to design legal processes for each individual API or even every single digital chain. Organisations need to invest effort in achieving a cohesive coordination of all intertwined connections ensuring a robust and prosperous environment.

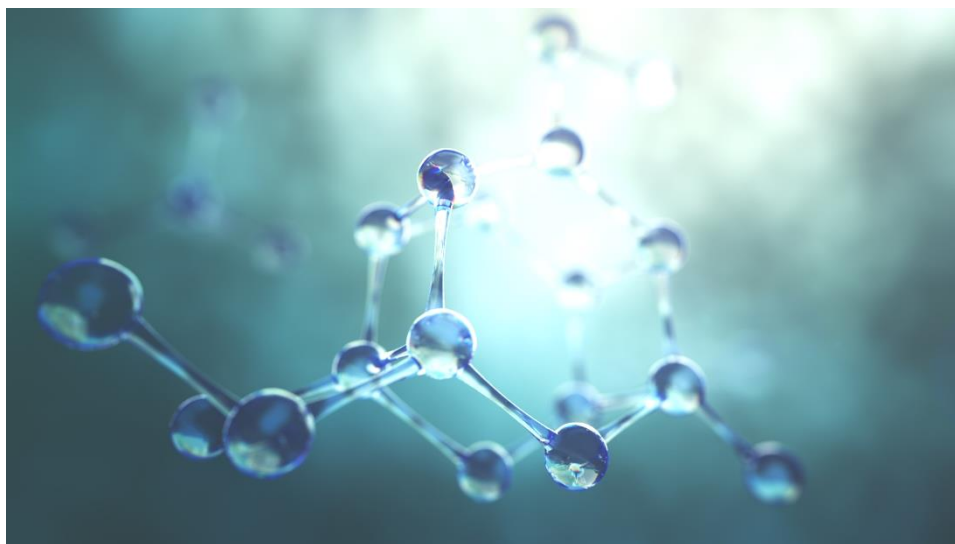
Another issue for the ecosystem orchestrator to consider is interoperability. APIs technically facilitate interoperability among members of the ecosystem. The scope of interoperability has already been subject to interpretation by the courts. While this may allow some manoeuvre for balanced decision-making, it may not guarantee the ambition of efficient re-usability of data (Hoffmann and Gonzalez Otero, 2020). To foster interoperability, the European regulator launched the legislative proposal "Interoperability Act". While this initiative is still at an early stage, APIs have already proven their value for boosting the re-use of data through enabling operability. Development of API-related standards plays a key role with this respect. The DA clearly frames API as technical means ensuring interoperability (recital 86)⁵ and makes standardisation and semantic interoperability applicable to it (Recital 79). It also highlights that it is necessary to provide for a presumption of conformity for interoperability that meets more general harmonised standards in accordance with the regulation on European standardisation. Standardisation of APIs is therefore another legal issue the ecosystem orchestrator should consider.

⁵ Recital (86) of the DA: "In order to ensure uniform conditions for the implementation of this regulation, implementing powers should be conferred on the Commission in respect of supplementing this regulation to adopt common specifications to ensure the interoperability of common European data spaces and data sharing, the switching between data processing services, the interoperability of smart contracts as well as for technical means, such as application programming interfaces, for enabling transmission of data between parties including continuous or real-time and for core vocabularies of semantic interoperability, and to adopt common specifications for."

The Cybersecurity Act introduces the term “cybersecurity ecosystem”. It acknowledges that ecosystems add yet another layer challenging cybersecurity. To tackle this issue the proposal for the second network and information security (NIS2) directive establishes a general framework for a high common level of cybersecurity. Recital (45) of the NIS2 directive mandates that entities should address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem. API are integral part of these interactions and must therefore be robust enough to not create a vulnerability in the whole cybersecurity infrastructure.

Apart from binding rules, an ecosystem orchestrator can benefit from observing soft standards, guidelines, and examples. This is of no less importance as it empowers organisations to work toward deployment of innovative solutions.

API services are enablers of the integration of government organisations into digital ecosystems. The interconnectedness adds complexity to the harmonisation of the functioning and stability of the ecosystem. Strong coordination efforts are needed to ensure legal and technical stability. This stability is crucial to ensure a sustainable flourishing of interactions and transactions in the ecosystem.



Source: @artegorov3@gmail, 126036009 / Adobe Stock

3 API organisational considerations

To be connected and fully integrated into digital ecosystems, governments need to invest in coordination efforts to make their digital interactions practical, robust, and aligned to their principles and objectives. Moreover, from a systemic perspective, legal and technical coordination is essential to ensure the robustness and sustainability of the entire digital scene. This coordination, when put into operation systemically, is known as governance, and it is highly relevant for the stability and prosperity of the DSM.

APIs are enablers of data governance (Posada et al., 2022) and a keystone in coordination processes. They are the boundaries that define the interactions among actors: what data can be accessed, how, by whom and under which conditions. This information can be vital in determining appropriate responsibility flows in digital chains.

In recent work, Verhulst outlined approaches for appropriately assigning data responsibility flows in the current data sharing context (Verhulst, 2021). The proposed approaches are clustered in three pillars: roles and responsibilities; systems and processes; and rights and obligations. With this backdrop, this section summarises data sharing coordination approaches observed in practice from an API viewpoint. It does so specifically by performing a structured analysis of eight case studies, which covered cases from the public and private sectors at different administrative levels: local, regional, national, and multinational (see Annex II).

3.1 Roles and responsibilities

From an API perspective, relevant aspects of data governance and digital coordination such as decision-making models, awareness of the legal framework and new profiles were observed:

- Decision making about strategic and tactical data governance issues typically happen in a centralised top-down fashion. However, in design and testing phases, initiatives are often proposed bottom up and involving external actors from private sector and civil communities. This was reported as a useful way to design human-centric digital designs that solve ‘real’ problems.
- Actors are aware of their legal obligations with respect to the legal framework applicable to them. Currently, they are most concerned about data privacy and applicable sectoral regulation (e.g., INSPIRE directive in the geospatial domain).
- Governments establish specific roles and entities to manage and coordinate data-driven actions and relationships with external actors. For example:
 - the Chief Technology Officer of the city of Amsterdam appointed a “programme manager of strategic partnerships” to coordinate the digital interactions of the city of Amsterdam, including big technological players such as Google, Airbnb and Mastercard.
 - the city of Amsterdam established NWD, a satellite, non-profit private entity to test prototypes that integrate data from big tech players into current government processes for specific uses. After proving its efficiency, the city plans to integrate this entity into the public administration in the coming two years.

- the city council of Zaragoza established a non-profit entity the Zaragoza City Knowledge Foundation⁶ to channel and coordinate data requests from actors outside the government: (academia, private sector and civic communities), and to test prototypes.
- New roles and entities are not fully incorporated in government at first. Instead, they are satellite private-public partnerships used as testing platforms in a safe and more flexible legal environment. These capacities are also used for defining roadmaps to integrate successful solutions into government processes and operations.

3.2 Systems and processes

During the interviews we explored the legal infrastructure and coordination models related to current systems and processes. Formal and informal relationship agreements were reported during the interviews. These ranged from less formal practices such as the use of non-disclosure agreements (NDA), to lawful interactions such as contracts, or even the definition of regulations at various levels of government (regional, national, and international).

The relevant related findings can be summarised as follows:

- The management of government APIs for data sharing already tackles aspects of responsibility and accountability in the conditions defined through agreements (e.g. ToS) and encoded as technical constraints. However, no conclusive evidence of comprehensive responsibility and accountability schemes for digital service level ⁷ was found. An API is just one component of the entire data value chain which needs to be integrated into larger ICT solutions to reach the final consumer. An API can concurrently be part of different value chains, and responsibility and accountability schemes could differ depending on their use and role within these different value chains. Nonetheless, there is awareness of this fragmentation issue. Some interviewees said they have already started or have planned multi-stakeholder discussions to begin orchestrating such aspects.
- Interviewees at the local administration level are more inclined to adopt agile methods to innovate their processes through data-driven actions and interactions. They engage in safe-environment testing initiatives involving a wide variety of stakeholders (e.g. from academia, the private sector, citizen initiatives, and in some cases, even artists). This was reported as a useful approach to creatively solve “real” problems in the local context. They embrace trial-error-learning approaches. The testing phase will determine whether there will be a roll-out into the current operational processes. Some of the interviewees stressed the need to evaluate feasibility of solutions at scale all along the creation process.
- Regional and national actors use more formal procedures in their coordination attempts. They tend to oversee the defining and steering of high-level digital interactions and coordination models of government with internal and external stakeholders. Different approaches were observed, ranging

⁶ <https://www.fundacionzcc.org/>

⁷ Digital service level is defined as a composite ensemble of digital components that create a unique data value chain. It can include one or several of these actors: data collector, data holder, data processor, data supplier, intermediate consumer, digital service consumer.

from fully based on technical governance actions such as mandating standards and guiding principles (e.g. Geonovum in the Netherlands); fully based on stakeholder management through procedural processes such as contracts and formal agreements (e.g. Regione Lombardia, Italy); centrally managed through technical platforms (e.g. France); and hybrids of these (e.g. Denmark).

- At the international level, we observed collaborations among countries that share cultural closeness (Nordic Smart Government and Business). This collaboration also includes the private sector (SMEs) and takes place within the framework of a governmental agreement. Even though the agreement is non-binding, its long practice and institutional nature mean that it is perceived as law, possibly causing some de facto rules to evolve as hard law.
- As regards the interaction with private actors, relationships with big technological players appeared to happen in testing mode, building upon personal trust relationships and seemingly unfolding on “win to win” cases. Relationships with smaller actors (e.g. SMEs) were reported to be less complex, based on ad hoc needs and often in the context of trials, but with no initial assurance of long-term sustainability or scalability.

3.3 Rights and obligations

Government entities are aware of their rights and obligations, as their processes and operations are often linked with statutory requirements. Private actors are concerned about their obligations regarding data privacy compliance, data retention policies, enforcement of their ToS, monitoring inappropriate use, and ensuring their own attribution or the one of third parties when necessary. Nevertheless, while the coordination of rights and obligations seem to be well defined in data value chains of the big private players, this does not seem to be the case for other actors. The legal uncertainty that engaging with actors entails weakens their position when they are in competition with other actors. In concluding remarks, Box 2 summarises the analysis of the case studies from the perspective of strategic, tactical and operational decision-making horizons in organisations.



Source: © metamorworks, 178170050 / Adobe Stock

Box 2: API ORGANISATIONAL DIGITAL COORDINATION PRACTICES IN PUBLIC SECTOR

Summary of the analysis of API-related techno-legal coordination initiatives at different levels of planning:

STRATEGIC LEVEL

- In the public sector, national and supranational entities typically set the boundary conditions and governance styles of the digital government interactions, (i.e. techno-legal and coordination practices). They are also concerned about ensuring cohesion and avoiding fragmentation of digital interactions within and across government levels (e.g. specifying interoperability mechanisms, and incorporating scalability concerns from public service design).
- The local level, which is closer to operational concerns, tends to be more innovative and invests in agile multi-stakeholder testing bed processes to identify practical solutions to real problems.
- To fully seize their data value potential, API-provision entities need to further develop their vision of the digital ecosystem beyond their own perimeter.

TACTICAL LEVEL

- *Infrastructure*: Governments create supporting entities and new roles to coordinate and manage digital interactions. APIs are central in the workflows of these entities and the duties of the new profiles. New financial models appear, such as co-funding among internal entities or external actors.
- *Skills*: Organisations invest in up-skilling their workforce and instilling a digital ecosystem mindset to facilitate change management in their digitalisation process.
- *Processes*: Organisations invest in updating their processes and operations. In particular, great attention is paid to stakeholder management initiatives, the definition of terms of use, agreements and contracts, and the streamlining of procurement processes (e.g. instalment of flexible procurements for developing ICT solutions defining clear responsibility and accountability schemes in a timely and practical manner).

OPERATIONAL LEVEL

- *Monitoring compliance*: Organisations need to invest in setting up mechanisms to ensure that the terms and agreements of their digital relationships are respected and their obligations are fulfilled.
- Organisations need to put in place technical mechanisms to fulfil their regulatory reporting obligations. APIs will make this process smoother if an organisation has to report to several entities – in this case, APIs can channel data to different end users with no significant additional costs.

4 Legal and organisational nexus: contractual practices

When operating as data sharing services, APIs usually go unnoticed by the consumers of digital products such as mobile, web application or social networks. However, from the perspective of firms who develop their digital services, APIs are fundamental components upon which their digital business is built. As such, APIs tend to be subject to dedicated agreements between the data-sharing subject and the data service user. We will use the current data sharing legal framework to give some legal interpretation to the systemic implications of the coordination of the “contracts by adhesion” that currently rule digital interactions

4.1 Contractual nature of API service agreements

API service agreements can be found online, usually under the names ‘API Terms of Service’ or (ToS), terms of use (ToU), or terms and conditions (T&C). The definition of ToS can be found in Article 2(10) of the P2B regulation. It provides the definition of ToS in relation to intermediation services. When we adapt it to a larger spectrum of services it states that “terms and conditions” means all terms and conditions or specifications, irrespective of their name or form, which govern the contractual relationship between the provider of online [...] services and its business users and are unilaterally determined by the provider of online [...] services [...]. The core feature here is the unilateral formulation of the ToS.

ToS are unilaterally formed offers which describe the conditions of use of the service and its outputs. When a user uses the service these conditions are subsequently accepted, and they become contracts. They are adhesion contracts – in other words, they are “take it or leave it” contracts and include non-negotiable terms.

The validity of the contracts concluded by electronic/digital means was assured twenty years ago by the e-commerce directive (ECD). Article 9 of the ECD facilitated the conclusion of contracts by electronic means by obliging EU Member States to ensure that their domestic legal frameworks neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of having been made by electronic means. The ECD provided for certainty on the legal status of *contracts concluded by digital means*.

In the area of *consumer protection*, ToS must soon follow the rules of the digital content and digital services Directive adopted in 2019, which has been applied by the Member States since January 2022. The directive lays down common rules on certain requirements concerning contracts between traders and consumers for the supply of digital content or digital services, in particular: a) rules on the conformity of digital content or a digital service with the contract; b) remedies in the event of a lack of such conformity or a failure to supply, and the modalities for the exercise of those remedies; and c) the modification of digital content or a digital service. Since the directive applies to digital services horizontally ToS on API as service falls under its scope, thus it has less relevance in case of API ToS, because API services are used by business entities. Nevertheless, if consumers use APIs, the directive strengthens their position vis-à-vis a trader.

Some ToS also need to follow the P2B regulation adopted in 2019 (applied from July 2020). The regulation promotes *fairness and transparency for business users of online intermediation services*. The API services fall under the scope of the regulation as long as they form an integral part of those services. Recital

11 of the regulation explains that with functionalities or interfaces that are directly connected or ancillary to certain online intermediation services, and the relevant providers of online intermediation services should be subject to transparency requirements related to differentiated treatment based on these functionalities and interfaces. API ToS may narrowly slip out from the scope of the regulation. Nevertheless, whenever the service of an API is an integral sine qua non condition to the existence of the service directed to the consumers, it should not be at odds with the regulation, as such a situation will prevent businesses from executing their rights bestowed on them by this regulation. In such a case, API providers should observe the fairness and transparency requirements promoted by the regulation when it comes to the termination, suspension, change and restriction of provision of services.

Many APIs, however, will stay outside of the scope of the regulation. In this case, the P2B regulation provides guidelines on where we should look for the promotion of trustworthiness in digital ecosystems. To ensure the stability of businesses relying on access to APIs, the issues raised in the P2B regulation are of a key importance, even if not binding upon them.

The recently proposed DA sets out important horizontal changes in the context of contractual relations in the digital ecosystem. The proposed rules are to fill the outstanding legal gaps in the context of contractual fairness. The DA proposes that unilaterally imposed unfair contractual terms shall not be binding (Article 13). The Act also concretises the premises of unfairness. When adopted, the DA will be a basic regulatory tool applicable horizontally to contractual relations in digital ecosystems.

4.2 Empirical analysis of API ToS from a systemic perspective

With the objective of exploring the current legal stability of digital environments, we have made an exploratory analysis of the legal empirics found in contracts that rule interactions through APIs, i.e. ToS. Specifically, we systematically analysed the contents of a list of 4000 ToS documents self-declared by API providers in the Programmable Web directory (snapshot of 2019). From this list, 2800 documents were downloaded successfully, and their content was extracted and analysed using well established natural language programming techniques (e.g. the use of regular expressions, geo-parsing text entities, n-grams analysis, easiness to read tests, and context extraction).

The analysis of current of techno-legal coordination practices from the contractual perspective was designed to answer the following questions from a systemic viewpoint:

- is there homogeneity in the drafting of API ToS contracts?
- do the ToS comply with current governing laws?
- how do the ToS handle Intellectual Property rights?
- are jurisdiction statements hindering innovation?
- do ToS drafting practices foster/hinder cooperation and/or fair competition?

With regard to the *homogeneity of ToS*, we found structural commonalities across documents. General clauses and statements found are listed in Box 3. However, we also observed that prominent providers (e.g.

Google, Facebook) present a multi-layered ToS structure, for instance having ToS defining terms for horizontal services (e.g. authentication) and ToS specific to the particular functionality they provide (e.g. google maps, ads, etc.).

Box 3: ToS COMMON CLAUSES AND STATEMENTS:

- Contracting parties to the agreement
- Start of the contract
- Termination/suspension/modification/ restriction of service provision
- Payment
- Governing Law
- Liability
- Indemnification
- Warranty
- Privacy
- Severability
- License of the generated content (e.g. IPR)

Another relevant aspect in the ToS documents was that the term “API” was mentioned more than five times in just 25% of them, while the term was not mentioned at all in 36.7% of the documents. When checking this fact, often ToS do not specifically apply to the API service but to the application in which it is being used. This raised the following doubts: do API providers have ecosystem vision? Are they missing opportunities to exploit the full potential of their API infrastructure?

With regard to the encoding of governing laws, of the 2800 ToS analysed, 111 legal documents from various parts of the world were mentioned (see Figure 2). Most of them were more recent than 1980, except for the Federal Arbitration Act which is mentioned in 107 files and was enforced in America in 1926.



Figure 2: Legal documents found in the ToS ordered by year of appearance and enforcement regional area
 NB: Each dot in X-axis represents one legal document and its size, the number of files that mention it.

Governing laws included acts, regulations, directives, ordinances, and decrees. Around 60% of them belong to the Europe, Middle East and Africa (EMEA) region, and in the vast majority to the European body of law. North, Central and South America (AMER) documents generally appear more often than in other regions, except for the GDPR, which is the most mentioned among all legal documents. A possible explanation is that Programmable Web is an American based repository and therefore its directory is skewed towards API products from there. However, the digital operations of APIs are potentially global, so APIs' ToS legal restrictions should be compliant with applicable frameworks in the context of their operations. How and if this is monitored it is not clear to the authors.

A final note concerns the fact that there were also mentions of soft regulatory measurements, i.e. standards, codes of conduct and codes of practice.

Of the governing law documents identified (see Figure 3), almost a quarter relate to privacy regulations. There were also other ICT regulations such as the database directive and the P2B regulation. Intellectual Property Rights were also present in the ToS, along with contracts and consumer protection laws. There were also mentions of sector specific regulations in the context of environment, health, finance, taxes, trade/export, and antifraud legislation.

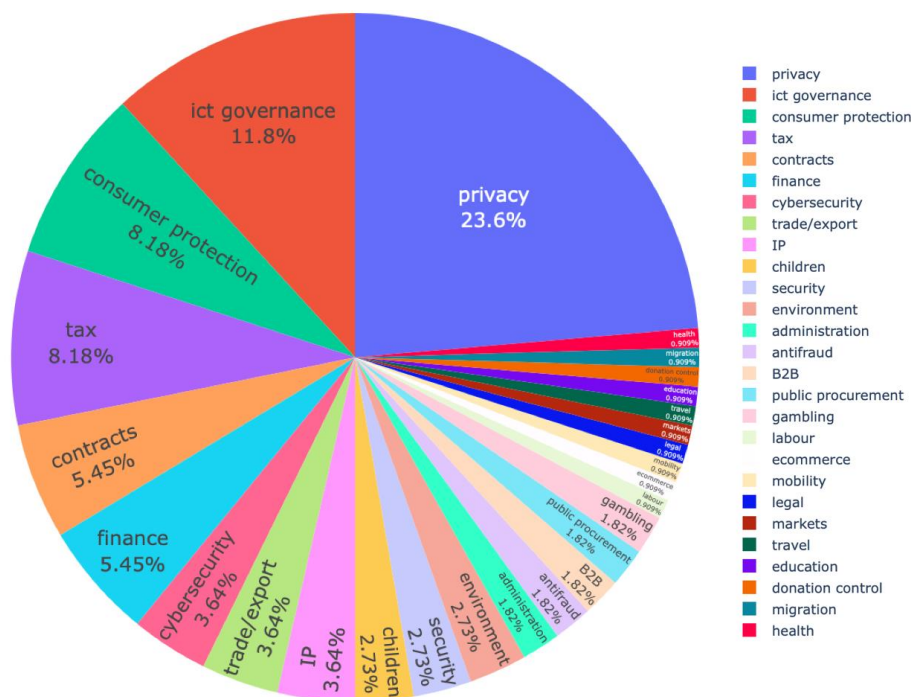


Figure 3: Governing laws categories

Of all the legal instruments mentioned in ToS documents, 25 were privacy related. The instruments were applicable in 13 different geographic areas at regional levels (e.g. California, Gibraltar), national level (Australia, Brazil, Canada, Germany, Ghana, Indonesia, the Netherlands, New Zealand, Russia, Singapore, Spain and

Switzerland) and pluri-national level (the EU). Of all the privacy related laws, the most referenced one was the GDPR with 16.6% of documents mentioning it. The ToS documents specifically referred to the following articles of the GDPR: 4, 5, 6, 8, 9, 13, 15, 16, 17, 18, 20, 21, 22, 28, 30, 32, 33, 37, 45, 46, 77 and 89.

Another aspect explored was the relevance, if any, of *intellectual property rights* (IPR) in ToS documents. We scanned for terms and expressions related to IPR. Figure 4 shows that IPR is indeed a concern for legal teams defining ToS documents linked with API provision.

Patent	29.54%
Trade secret	23.04%
Copyright	63.75%
Intellectual property right	42.29%

Figure 4: Percentage of ToS files with IP terms/expressions

We also analysed explicit mentions of determined *jurisdictions for conflict resolution*. The geographic distance to the court of dispute for settlement implies high costs: the lack of knowledge of legal background on remote place, different language, cultures etc. This can represent a legal barrier to innovation as it may discourage potential digital interactions due to uncertainties derived from the lack of effective conflict resolution when API services are operational in disparate geographical contexts. Figure 5 shows the different courts of dispute declared in the ToS. The analysis was inconclusive as of now, but further exploration will be performed to geo-contextualise the links between the APIs declared jurisdictions and their consumers.

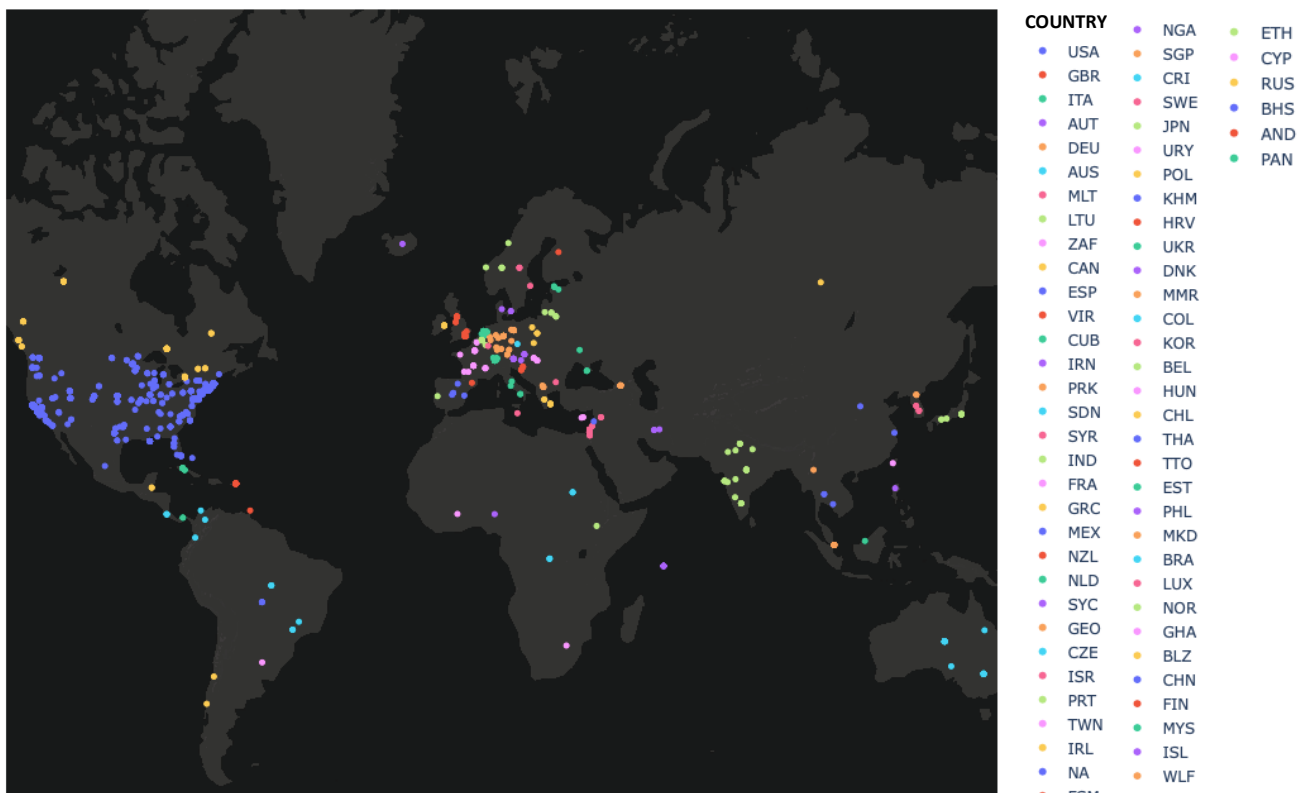


Figure 5: Jurisdiction locations for dispute resolution in ToS documents

We also explored statements regarding “out of court” conflict resolution methods. As courts can be located in remote geographical locations the possibility to settle disputes under out-of-court procedure encourages digital participation. We found mentions of different intermediates (e.g. the ombudsman, mediators, complaints board), and other means such as arbitration, mediation, and even explicit indications of alternative dispute resolution mechanisms (see Figure 6).

ombudsman	12
conciliat	20
complaints board	1
out of court	1
mediat	108
arbitrat	446
alternative dispute resolution	45

Figure 6: number of files containing “out of court” terms/expressions

Finally, we looked at whether current ToS drafting practices will more likely *foster or hinder cooperation and fair competition in the DSM*. Specifically, we analysed transparency, the termination conditions, liability, and warranty clauses. The highlights of the results can be found below:

- We hypothesise that *transparency* is linked to the concept of trust among business partners, which is essential for the flourishing of digital relationships and the fostering of innovation. Our initial attempt to measure contractual transparency was based on the readability of the ToS documents and the inclusion of definitions. Definitions were absent in 80% of the ToS analysed and their readability, assessed through Flesh-Kincaid testing, did not score well. Further analysis is needed to state what is the “easiness to read” baseline for ToS documents.
- On *termination conditions*, we found that 35.7% of the ToS analysed declare unbalanced termination conditions (Figure 7). By this we mean that API providers state that they can decide to discontinue their service at any time without being responsible, liable, or accountable. If statements are directly linked to an operative API, this could create potential discontinuities in all data value chains this API provides for. This risk may create uncertainty on the viability and sustainability of digital services including this API components in their processes, notably discouraging innovation.
- On *liability clauses*, we scanned for the existence of “unfair” liability statements. We found a considerable number of examples where liability was circumvented to a certain extent. These examples ranged from limiting the liability to specific conditions, to fixing a mild financial cap, or even excluding it completely.
- In a similar vein, we scanned *warranty clauses*. We only found evidence of some level of warranty on the quality of service in 11% of the cases. Up to 2% of the cases excluded all warranties to the extent permitted by governing law.

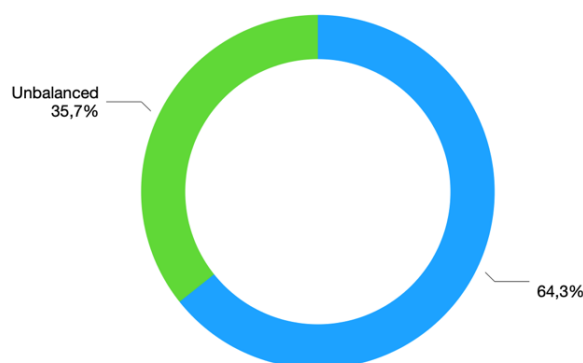


Figure 7: Termination conditions in ToS

5 Conclusions

Nowadays, organisations need to connect to the digital ecosystem and effectively manage digital interactions to thrive. Government organisations are no exception to this need. The interactions among actors in digital ecosystems mostly happen through API services. From a digital ecosystem point of view, APIs are intermediate components that connect actors and systems in digital value chains. Integrating different API components within digital chains has implications on the assignment of responsibilities, accountability, liability, and intellectual property rights.

An API can concurrently belong to different digital chains that have other conditions. This interconnectedness increases the complexity of the governance of the digital environments. Ensuring the robustness of the ecosystem and minimising the risk of systemic failures requires both technical and legal stability. This stability is essential for creating trustworthy relationships needed for the DSM to thrive.

This work explored what legal and organisational aspects are essential to manage and coordinate digital interactions from an API viewpoint. The analysis included the perspective of an individual organisation and the ecosystem. We first analysed the legal framework applicable to the provision and use of APIs. Then, we proposed a [framework](#) to identify API-related legal obligations and applicable laws depending on different possible combinations of API functions and API stakeholder roles.

On the organisational side, we explored the legal infrastructure and organisational coordination models that private and public practitioners use to coordinate their digital interfaces through APIs effectively. We evaluated new roles and responsibilities, organisational infrastructures and the rewiring of systems, processes, and rights and obligations. We then analysed it from the [managerial decision-making perspective](#) of a public sector organisation.

Finally, from a systemic perspective, we carried out an [empirical analysis](#) of current practices of the legal coordination reflected in the interactions defined by an API's ToS. From a list of 4000 ToS documents, 2800 were systematically analysed. The results show that there is still work to improve transparency, fairness and stability in the conditions included in these contractual documents. Creating balanced and trustworthy legal and technical stability conditions is crucial to guarantee the foundation of a robust, fair, competitive, and sustainable digital ecosystem.

In concluding remarks, first, we conclude that Europe is a pioneer in setting policy mechanisms for digital governance. There is a growing body of law governing and shaping our digital future. However, the results of the empirical analysis in current contractual documents showed that digital coordination is still in its early stages. Therefore, there is work to do about setting a legally and technically stable digital environment in the EU. An initial step could be an analysis of the impacts of the implementation of the current policy mechanisms, followed by making the necessary adjustments to fulfil the vision of a Europe fit for the digital age. This work did not study the effect of legal fragmentation on coordination efforts at different levels of governments in Europe.

List of abbreviations

API	application programming interface
CEF	Connecting Europe Facility
DA	Data Act
DGA	Digital Governance Act
DMA	Digital Markets Act
DSA	Digital Services Act
ECD	e-commerce directive
GDPR	general data protection regulation
IPRs	intellectual property rights
ISA ²	second interoperability solutions for European public administrations programme
JRC	Joint Research Centre
MIFID	markets in financial instruments directive
NIS2	second network and information security directive
P2B	platform to business
PSD2	second payment services directive
SLA	service level agreement
ToS	terms of service

List of figures

Figure 1: APIs in digital value chains (linear and multidimensional).....	4
Figure 2: Legal documents found in the ToS ordered by year of appearance and enforcement regional area	24
Figure 3: Governing laws categories	25
Figure 4: Percentage of ToS files with IP terms/expressions.....	26
Figure 5: Jurisdiction locations for dispute resolution in ToS documents	26
Figure 6: number of files containing “out of court” terms/expressions.....	27
Figure 7: Termination conditions in ToS.....	27

List of tables

Table 1: European body of law applicable to data sharing Q2-2022.....	7
Table 2: Conceptualization of the legal framework applicable to the use of APIs.....	10
Table 3: Examples of government API Terms of Service.....	35
Table 4: Legal infrastructure case study description.....	36

References

- European Commission, 'A European strategy for data, COM(2020) 66 final', 2020a (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>) (accessed 23 February 2021).
- European Commission, 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act)', 2020b (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN>) (accessed 22 February 2021).
- European Commission, 'The Digital Markets Act: ensuring fair and open digital markets', 2020c (https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en) (accessed 22 February 2021).
- European Commission, A new industrial strategy for Europe, COM(2020) 102, COM/2020/102, 2020d.
- European Commission, 'SME Strategy for a sustainable and digital Europe, COM(2020) 103 final', 2020e (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0103>) (accessed 2 March 2021).
- European Commission, 'White Paper on Artificial Intelligence: a European approach to excellence and trust, COM(2020) 65', 2020f (https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en) (accessed 23 February 2021).
- European Commission. DG-CONNECT, 'Report on EU law applicable to sharing of non-personal data | Support Centre for Data Sharing', 2020 (<https://eudatasharing.eu/legal-aspects/report-eu-law-applicable-sharing-non-personal-data>) (accessed 17 June 2020).
- European Commission. Joint Research Centre., *Unfolding opportunities from the use of APIs in Europe: the role of API in data governance processes*, Publications Office, 2021 (<https://data.europa.eu/doi/10.2760/074141>) (accessed 5 July 2021).
- European Union, Directive (EU) 2015/2366 on payment services in the internal market, OJ L 337, 2015, p. 35–127.
- European Union, General Data Protection Regulation 2016/679, OJ L 119, 2016.
- Hoffmann, J. and Gonzalez Otero, B., *Demystifying the Role of Data Interoperability in the Access and Sharing Debate*, Social Science Research Network, 2020 (<https://papers.ssrn.com/abstract=3705217>) (accessed 1 July 2021).
- OECD, *OECD Enhancing access to and sharing of data: reconciling risks and benefits for data re-use across societies*, 2019 (<https://www.oecd.org/going-digital/enhancing-access-to-and-sharing-of-data.pdf>) (accessed 30 June 2021).
- Posada, M., Pogorzelska, K. and Vespe, M., *The role of Application Programming Interfaces (APIs) in data governance and digital coordination*, European Commission, 2022 (<https://publications.jrc.ec.europa.eu/repository/handle/JRC128250>) (accessed 1 March 2022).
- The Berlin Group, 'PSD2 Access to Bank Accounts', 2021 (<https://www.berlin-group.org/psd2-access-to-bank-accounts>) (accessed 16 February 2021).
- US Supreme Court 18-956 Google LLC v. Oracle America, Inc. (04/05/2021), 2021.
- Vaccari, L., Posada, M., Boyd, M., Gattwinkel, D., Smith, R., Santoro, M., Nativi, S., Medjaoui, M. and Reusa, I., 'Application Programming Interfaces in Governments: Why, what and how', 2020

(<https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/application-programming-interfaces-governments-why-what-and-how>) (accessed 16 February 2021).

Vaccari, L., Posada, M., Boyd, M. and Santoro, M., 'APIs for EU governments: A landscape analysis on policy instruments, standards, strategies and best practices', *Data*, Vol. 6, No 6, 2021, pp. 59.

Verhulst, S.G., 'Reimagining data responsibility: 10 new approaches toward a culture of trust in re-using data to address critical public needs', *Data & Policy*, Vol. 3, 2021.

Annex I: Examples of government API Terms of Service

API_NAME	TERMS_OF_SERVICE_URL	PROVIDER	REMIT
NYC OPEN DATA	http://www.nyc.gov/html/data/terms.html	--	Local
AUSTRALIAN BUSINESS NUMBER LOOKUP	http://www.abr.business.gov.au/(wxn3jr45ap3vb43jlf1td55)/content.aspx?page=conditionswebservice&Agree=N	--	National, Federal, plurinational
HOME ENERGY SAVER	http://www.lbl.gov/Disclaimers.html	--	National, Federal, plurinational
FCC	http://reboot.fcc.gov/developer/api-terms-of-service	--	National, Federal, plurinational
SOCRATA OPEN DATA	http://www.socrata.com/terms-of-service	--	National, Federal, plurinational
UK STREET LEVEL CRIME	http://www.police.uk/api/docs/licence/	--	National, Federal, plurinational
GOVINFO	https://www.gpo.gov/privacy	U.S. Government Publishing Office	National, Federal, plurinational
NYC BENEFITS SCREENING	https://screeningapidocs.cityofnewyork.us/terms-of-service	City of New York	Local
U.S. GSA JOBS SEARCH	https://search.gov/tos.html	USA.gov	National, Federal, plurinational
MUCKROCK	https://www.muckrock.com/tos/	MuckRock	National, Federal, plurinational
VETERAN AFFAIRS BENEFITS INTAKE	https://developer.va.gov/explore/terms-of-service	U.S. Department of Veterans Affairs	National, Federal, plurinational
VETERAN AFFAIRS BENEFITS APPEALS STATUS	https://developer.va.gov/explore/terms-of-service	U.S. Department of Veterans Affairs	National, Federal, plurinational
CARROLL PUBLISHING GOVSEARCH	http://www.carrollpub.com/Subscribers/copyright_pub.asp	Carroll Publishing	National, Federal, plurinational
COMPANIES HOUSE	https://www.gov.uk/help/terms-conditions	UK Crown	National, Federal, plurinational
UNHCR	http://www.unhcr.org/en-us/terms-and-conditions.html	United Nations	National, Federal, plurinational
CONSUMER FINANCIAL PROTECTION BUREAU HMDA	https://cfpb.github.io/source-code-policy/	Consumer Financial Protection Bureau	National, Federal, plurinational
UK GOVERNMENT GATEWAY HMRC INDIVIDUAL BENEFITS	http://www.hmrc.gov.uk/terms/	UK Crown	National, Federal, plurinational
UK GOVERNMENT GATEWAY HMRC INDIVIDUAL EMPLOYMENT	http://www.hmrc.gov.uk/terms/	UK Crown	National, Federal, plurinational
UK GOVERNMENT GATEWAY HMRC NATIONAL INSURANCE	http://www.hmrc.gov.uk/terms/	UK Crown	National, Federal, plurinational
UK GOVERNMENT GATEWAY HMRC MARRIAGE ALLOWANCE	http://www.hmrc.gov.uk/terms/	UK Crown	National, Federal, plurinational
UK GOVERNMENT GATEWAY HMRC INDIVIDUAL INCOME	http://www.hmrc.gov.uk/terms/	UK Crown	National, Federal, plurinational
PROPUBLICA CONGRESS	https://www.propublica.org/datastore/terms	ProPublica	National, Federal, plurinational
H2OFLINT	http://www.h2oflint.com/terms/	H2OFlint	Local
NASA TECHPORT OPENDATA SUPPORT REST	http://www.nasa.gov/about/highlights/HP_Privacy.html	NASA	National, Federal, plurinational
GOVDELIVERY	https://govdelivery.com/legal-privacy/	GovDelivery	National, Federal, plurinational
DIEREN THEATER	http://opendatacommons.org/licenses/odbl/	--	National, Federal, plurinational
KONINKLIJKE BIBLIOTHEEK DIGITAL PROCEEDINGS OF DUTCH PARLIAMENT	http://kb.nl/banners-apis-en-meer/dataservices-apis/staten-generaal-digitaal	National Library of the Netherlands	National, Federal, plurinational
FIXMYSTREET	http://fixmystreet.org.nz/terms		National, Federal, plurinational

NATIONAL CRIME VICTIMIZATION SURVEY	http://www.bjs.gov/developer/ncvs/termsofservice.cfm	--	National, Federal, plurinational
U.S. DEPARTMENT OF STATE OFFICE OF THE HISTORIAN EBOOK CATALOG	http://www.state.gov/misc/152386.htm	--	National, Federal, plurinational
IDESCAT ONOMASTICS API	http://www.idescat.cat/api/?lang=en#cdu	--	Regional
IDESCAT EMBED	http://www.idescat.cat/api/?lang=en#cdu	--	Regional
PROPUBLICA FREE THE FILES	https://www.propublica.org/datastore/terms	ProPublica	National, Federal, plurinational
DATAKC	http://www.kingcounty.gov/About/dataTermsOfUse.aspx	--	Regional
OPEN STATES	http://sunlightfoundation.com/legal/terms/	--	National, Federal, plurinational
HELSINKIKANAVA OPEN DATA	http://open.helsinki.fi/tos.html	--	Local
HEALTHDATA.GOV	https://www.hhs.gov/web/policies-and-standards/terms-of-service-agreements/index.html	U.S. Department of Health and Human Services	National, Federal, plurinational
NEPHICS EUROPEAN VAT NUMBER VALIDATION	http://nephics.com/terms.html	--	National, Federal, plurinational
USA.GOV SOCIAL MEDIA REGISTRY	http://www.usa.gov/About/developer-resources/terms-of-service.shtml	--	National, Federal, plurinational
ST. LOUIS FRED	http://api.stlouisfed.org/terms_of_use.html	--	Regional
INSTITUTE OF DEVELOPMENT STUDIES	http://api.ids.ac.uk/about/terms.shtml	--	National, Federal, plurinational
LEGISCAN	http://e-lobbyist.com/terms-of-service	LegiScan	National, Federal, plurinational
EMPIRE 2.0 TECH TALK	http://techtalk.cio.ny.gov/a/panelDetails.do?detailID=82288	--	National, Federal, plurinational
REALSEARCH TIN REVERSE	https://www.realsearch.com/TermsandConditions.asp	--	National, Federal, plurinational
POSTCODE ANYWHERE GOVERNMENT DATA	http://www.postcodeanywhere.co.uk/privacy.aspx	--	National, Federal, plurinational
SUNLIGHT LABS REAL-TIME CONGRESS	http://services.sunlightlabs.com/accounts/register/#tos	--	National, Federal, plurinational
RICHMOND SUNLIGHT	http://www.richmondsunlight.com/about/tos/	--	National, Federal, plurinational
OPEN STATE PROJECT	http://services.sunlightlabs.com/accounts/register/#tos	--	National, Federal, plurinational
IDESCAT MUNICIPALITY IN FIGURES	http://www.idescat.cat/api/?lang=en#cdu	--	Regional
GUARDIAN POLITICS	http://www.guardian.co.uk/open-platform/politics-api/terms-and-conditions	--	National, Federal, plurinational
NEW YORK TIMES NY STATE LEGISLATURE	http://developer.nytimes.com/Api_terms_of_use	--	National, Federal, plurinational
PROJECT VOTE SMART	http://api.votesmart.org/docs/terms.html	--	National, Federal, plurinational
DEA NUMBER	http://deanumber.com/Library/InfoManage/Guide.asp?FolderID=163&SessionID=%7B04DF7CF0-8DB4-45C8-A3A3-8309419CB360%7D&InfoGroup=Main&RLMsg=	--	National, Federal, plurinational
LARIMER COUNTY PUBLIC RECORDS DATABASES	http://www.co.larimer.co.us/legal.htm	--	Regional
NANTES OPEN DATA	http://data.nantes.fr/licence/	--	Local
API.LEIPZIG	http://www.apileipzig.de/wiki/show/Nutzungsbedingungen	--	Local
DATANEST FAIR-PLAY ALLIANCE	http://datanest.fair-play.sk/pages/terms_of_service	--	National, Federal, plurinational
BERLIN OPEN DATA	https://www.berlin.de/wir-ueber-uns/agb/	--	Local

DATA.GOV.SG	http://data.gov.sg/common/terms.aspx	--	National, Federal, plurinational
SAN FRANCISCO OPEN311	http://apps.sfgov.org/Open311API/?page_id=486	--	Local
CITY OF EDMONTON OPEN DATA CATALOGUE	http://www.edmonton.ca/city_government/open_data/open-data-terms-of-use.aspx	--	Local
KENYA OPEN DATA	http://opendata.go.ke/page/terms-of-service	--	National, Federal, plurinational
OPENCOLORADO	http://opencolorado.org/about/	--	National, Federal, plurinational
KING COUNTY OPEN DATA	http://www.kingcounty.gov/About/dataTermsOfUse.aspx	--	Regional
ALAMEDA COUNTY SERVICE PROVIDER	http://opendatacommons.org/licenses/by/summary/	--	Regional
OAKLAND CRIME REPORTS	http://opendatacommons.org/licenses/by/summary/	--	Local
DATA.GOV.AU	http://data.gov.au/about/terms-of-use/	Australia	National, Federal, plurinational
SHROPSHIRE COUNCIL	http://shropshire.gov.uk/websiteinfo.nsf/open/2F5121395E2D0EE5802574C20047E748	--	National, Federal, plurinational
UK BIS	http://data.gov.uk/terms-and-conditions	--	National, Federal, plurinational
UK NATIONAL ARCHIVES DISCOVERY	http://discovery.nationalarchives.gov.uk/SearchUI/API-terms-and-conditions.htm	--	National, Federal, plurinational
UK GOVERNMENT GATEWAY HMRC	http://www.hmrc.gov.uk/terms/	UK Crown	National, Federal, plurinational
OPENDATAPHILLY PHILADELPHIA PUBLIC ART	http://www.opendataphilly.org/terms/	--	Local
USASEARCH	http://search.usa.gov/api/tos	--	National, Federal, plurinational
USASEARCH PRODUCT RECALL DATA	http://search.usa.gov/api/tos?locale=en&m=false	--	National, Federal, plurinational
VULEKAMALI DATASTORE	https://vulekamali.gov.za/terms-and-conditions	South African National Treasury	National, Federal, plurinational
AYUNTAMIENTO DE ZARAGOZA	https://www.zaragoza.es/sede/portal/aviso-legal#condiciones	Zaragoza	Local
SWEDISH API LICENCE	https://apilicens.se/en	Swedish Agency for Innovation Systems	National, Federal, plurinational
SINGAPORE	https://www.mas.gov.sg/terms-of-use/api-terms-of-service	Singapore Monetary Authority	National, Federal, plurinational
CALIFORNIA	http://www.ca.gov/Use	California	National, Federal, plurinational
SEATTLE	https://data.seattle.gov/stories/s/Data-Policy/6ukr-wwup/	City of Seattle	Local
CANADA	https://api.canada.ca/en/terms-and-conditions	Canada	National, Federal, plurinational

Table 3: Examples of government API Terms of Service

Annex II: API organisational analysis interviewees

CASE	CONTEXT	HIGHLIGHTS
I	LOCAL	Focus on testing operational solutions. Highly innovative. Management of operational environments. Problem solving mindset. Connections with BigTech companies. Sandboxing. Scalability concerns and design efforts in cooperation with other European cities. Creation of intermediate entity to operationalise prototypes at scale. If succeeds, the entity will be absorbed in the administration. Soft legal agreements.
II	LOCAL	Focus on creating innovative solutions for problems of the city of Zaragoza. Highly innovative. Management of research and innovation environments. Intermediate body to handle innovative data driven initiatives interfacing academia, private and public sector and civilian communities. Integration of city infrastructure. Soft legal agreements.
III	NATIONAL – SECTORAL	Focus on the coordination of technical solutions in geospatial context. Management of interoperability at semantic and technical levels. Strong coordination and guidance at tactical levels, not legally prescriptive but still binding. Not compliance should be explained.
IV	NATIONAL – GENERAL	Focus on centralising government technical infrastructure and then monitoring and coordinating value-creation opportunities among different actors, including from the private sector. The infrastructure is governed by its own legal framework; and there is a privacy policy that addresses GDPR issues. Responsibilities are also centrally described with no formal agreements. The governance is shared among different stakeholders and orchestrated by an internal Committee in the Agency and several Forums with technical and user side representatives where private sector participate.
V	REGIONAL	Focus on the use and re-use of available solutions in the region. No operational concerns. Coordination at tactical level. Ecosystem mindset. Interoperability efforts at semantic, technical, organisational and legal levels. Legal instruments: contracts, regional mandates.
VI	PRIVATE SECTOR	New role as intermediary: legal controller of the compliance with API's SLA.
VII	PRIVATE SECTOR	No profit organisation. Innovative business model. Data collector without data ownership. Data hold in a Data Trust as club good managed by them. Members of the club can access the data by paying a yearly subscription. Price structure controlled through technical capacities of the API.
VIII	MULTINATIONAL	Multi-country coordination of public services: registries and tax processes. Coordination at strategic level. Steering board under MoU in different bodies in governments of all countries. Advisory board members composed by public, private and SME members. Streamlining data processes to simplify mandatory reporting by re-use of data assets and processes (e.g. book keeping data). Interoperability issues as legal fragmentation across members although, due to the cultural closeness, those are solvable issues.

Table 4: Legal infrastructure case study description

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696,
- via the following form: european-union.europa.eu/contact-eu/write-us_en.

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

Open data from the EU

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.



EU Science Hub
joint-research-centre.ec.europa.eu



@EU_ScienceHub



EU Science Hub - Joint Research Centre



EU Science, Research and Innovation



EU Science Hub



EU Science



Publications Office
of the European Union