European
Commission

JRC TECHNICAL REPORT

API strategy essentials for Public Sector Innovation

Joint
Research
Centre

interoperable
europe

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

JRC129923

PDF ISBN 978-92-76-56796-7 doi:10.2760/203781 KJ-09-22-507-EN-N

Luxemburg: Publications Office of the European Union, 2022

How to cite: Posada Sanchez, M., Pogorzelska, K. and Vaccari, L., *API strategy essentials for public sector innovation*, Publications Office of the European Union, Luxembourg, 2022, doi:10.2760/203781, JRC129923.

CONTENTS

ACKNOWLEDGEMENTS 1

ABSTRACT 1

EXECUTIVE SUMMARY 2

POLICY CONTEXT 3

API4IPS PROJECT 3

REPORT I: TECHNICAL ESSENTIAL 4

- API management 4
- API discoverability 4
- API security concerns 5
- API privacy and traceability 5

REPORT II: LEGAL & ORGANISATIONAL ESSENTIALS 6

- API legal concerns 6
- API organisational and coordination aspects 6
- API legal and organisational nexus 6

CONCLUSIONS 8

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 (ISA^2). 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 Glickenhouse, 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.

ABSTRACT

Application Programming Interfaces (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 thriving of digital environments. Both technical and legal stability is 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.

The implications for government organisations are twofold. On one side, the government operative branch - public service provision - must lead by example by setting up API robust infrastructures compliant with the legal framework. On the other side, the government may monitor law compliance and track that its enforcement delivers on the policy goals of the European Strategy.

Within this context, the project 'API for public sector innovation' (API4IPS) investigated API-related crucial aspects that government organisations need to consider when planning and implementing their digital agendas. The project was a collaboration between three directorates of the European Commission: JRC, DIGIT and CONNECT. This report summarises the main findings of the study and draws the overarching conclusions.

EXECUTIVE SUMMARY

The European Commission's Joint Research Centre (JRC), the Directorate-General for Informatics (DIGIT), and the Directorate-General for Communications Networks, Content and Technology (DG CONNECT) launched the APIs for Innovative public Services (API4IPS) study in May 2020. This project belongs to Action 2018.01 ("Innovative Public Services") of the ISA^2 Programme (hereinafter "IPS Action"). The project investigates how APIs can support the development of Innovative Public Services and innovation in the public sector in general. The project was carried out in close collaboration with the eDelivery CEF (Connecting Europe Facility) Building block activities performed by DG DIGIT, Unit D3.

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 technical, organisational and legal aspects is crucial to stabilise the functioning of digital processes and, ultimately, the entire ecosystem in a fair and balanced way.

Within this backdrop, the objective of this project was to identify the API-related technical, organisational and legal essentials to help organisations manage and coordinate digital interactions through APIs.

The API4IPS project outputs include the following three reports:

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.

This document corresponds to report number three, which summarises the analysis of technical, organisational and legal essentials that need to be tackled when using API infrastructure in public sector digitalization processes. Then it draws overarching conclusions identifying focus areas that can support the coordination of digital interactions from an API viewpoint.

Source: ©sdecoret, 232770524/ Adobe Stock

APIs are the connecting nodes of digital ecosystems. These interfaces define technically and contractually the digital relationships among actors and systems. This information is key to steer and monitor fair, strong and sustainable digital interactions

POLICY CONTEXT

The digital transformation has accelerated at a dizzying pace over the last two decades. Digital ecosystems have sprung up through the interconnection of actors and systems. Nowadays, digital connections mostly happen through operative application programming interface (API) services. The current hyperconnectivity situation has increased the complexity of the governance of digital environments.

Ensuring the fairness, robustness and thriving of European digital ecosystems requires both technical and legal stability. This stability is essential for creating the trustworthy relationships needed for the prosperity of the digital single market (DSM). The connecting nature of APIs can facilitate the creation of ecosystems and the monitoring of their stability.

The implications for government organisations are twofold. On the one hand, the government's operative branch – public service provision – must lead by example through setting up robust API infrastructures that are compliant with the legal framework. On the other hand, the government may monitor law compliance and track whether its enforcement delivers on the policy goals of the different strands of European strategies linked with digitalisation.

Europe is a pioneer in defining digital governance policy mechanisms, and already possesses a significant body of law. However, this governance is still in its early stages. As the digital transition unfolds, data about the effectiveness of these policy mechanisms will become available. When necessary, these data will assist in adjusting or proposing new ways to achieve the vision of a Europe fit for the digital age.When effectively implemented, specified and documented, APIs define which assets are accessible, how, by whom, and under which conditions. The combination of their gated nature and their connecting capability, when set to do so, allows for the monitoring of both supply and demand of digital interactions. The capacity of APIs to enable the establishment of digital ecosystems and to monitor digital interactions calls for decision-making awareness.

API4IPS PROJECT

Within this policy context, the project "***API for public sector innovation***" (API4IPS) was launched in May 2020 as a collaboration between three directorates of the European Commission: the Joint Research Centre (JRC), the Directorate-General (DG) for Informatics and the Directorate-General for Communications Networks, Content and Technology. The project investigates crucial API-related aspects that government organisations need to consider when planning and implementing their digital agendas. The project is funded through the second interoperability solutions for European public administrations (ISA^2) programme, run by DG Informatics, in particular under action 2018.01 'innovative public services'.

The project produced three reports. Specifically, two reports analyse the strategy essentials of API for public sector innovation from two different viewpoints: i) technical and ii) legal and organisational. Then this third report summarises the highlights of the two viewpoints and extract overarching conclusions.

Specifically, the first report analyses the technical essentials to be considered by organisations regarding APIs such as API management, discoverability and security. The second report discusses legal and organisational issues related to the provision and use of APIs. It also includes an analysis of current practises in the field by evaluating contractual relationships exposed in Terms of Service (ToS) documents.

REPORT I: TECHNICAL ESSENTIAL

The *first report* of API4IPS project describes the technical essentials that any organisation dealing with APIs should take into account to: (i) ensure the stability and continuity of digital solutions (management of the lifecycle of the APIs); (ii) foster the use of API solutions (discoverability); (iii) protect the digital infrastructure of the organisation (security); and (iv) incorporate privacy and traceability concerns in their processes.

API management

When an organisation provides APIs, it is essential to manage those resources appropriately and in a coordinated manner. Until recently, API resources in governments were typically managed in an ad-hoc manner, thus missing out on opportunities to increase efficiency, innovate and even reduce costs due to the cross-fertilisation and reutilisation of resources. However, there is evidence that this trend is slowly transitioning to coordination models at tactical levels, e.g., through setting up portals and catalogues that monitor their APIs in a centralised manner.

The section tackles API management from two angles. The first angle is the management of APIs as a software product. This part describes a set of activities that need to be tackled for delivering a high-quality and sustainable software products. These aspects are inspired by traditional software development lifecycle processes, including specifically: strategy definition, design, documentation, development, testing, deployment, security, monitoring, discovery and promotion, and change management. A specific section is dedicated to properly handling *change management* of APIs.

The second angle is the management of the portfolio of APIs in an organisation, addressing aspects such as goals, platforms and governance structures.

API discoverability

API discoverability of an organisation describes the capacity to make its APIs findable and used. This entails making APIs available and understandable, and to promote their use such that it ensures their uptake by potential end-users. The importance of this characteristic of APIs is linked to technical interoperability and ultimately to an effective connection to digital ecosystems.

This section concludes that government API infrastructures are still in their infancy and that a collection of work cultivating best practices is only commencing. Specifically, the research identified 20 discoverability mechanisms (Figure 1), including innovative discoverability practices such as no-code solutions, open iteration and beta releases and the use of machine learning and service discovery tooling.

The analysis identified the following main conclusions regarding API discoverability in governments:

- discoverability processes are emerging to ensure government uptake of APIs and fostering the creation of digital ecosystems;

- API discoverability in government is mostly targeting internal audiences;

- developer portals are the most widely used discoverability mechanism;

- API discoverability is acknowledged as an enabler of organisation interoperability.

Figure 1 – API discoverability mechanisms

API design	API publication	Ecosystem facilitation	Automated tooling
1. Metadata 2. Standardisation	3. Developer portals 4. Search engine optimisation (SEO) 5. Directory listings 6. APIs on open data platforms 7. Business-focused portals 8. GitHub accounts 9. Postman collections	10. Social media 11. Hackathon/ challenges 12. Developer summits and Information sessions 13. Accelerators 14. Case studies, storytelling 15. Domain-level ecosystem networks and websites 16. Mailing lists	17. Citizen and no-code tools 18. Service discovery tools 19. Predictive analytics 20. Recommendation engines

NB: Discoverability mechanisms grouped by strategy type. Source: JRC own production.

While there are growing examples of best practices across governments, there are some key areas where further progress could be pursued. This report specifically recommends the following:

– Governments should create a single API catalogue for the whole of government. This should not preclude department-level API catalogues and API product catalogue landing pages. However, these should all be connected so that a whole-of-government API catalogue is available as a comprehensive overview of all government APIs. One level of government, such as the EU Member State level, should also be responsible for listing all government APIs across all tiers of government.

– API product managers should be appointed, and they should ensure that API implementation is aligned with the organisation's API practices. A product management approach should also be adopted for API catalogue/development portals to ensure both technical sustainability and organisational outreach.

– APIs should include an OpenAPI Specification (or similar) file that describes the API in a machine-readable format. OpenAPI specification files should be available for download for every API listed in an API catalogue.

– Website accessibility guidelines should be treated as a higher priority, with regular reviews being conducted, and with clearer goals to ensure that government developers with a disability are able to use developer portals without barriers.

API security concerns

The flexibility to connect and re-use digital assets that APIs grant to organisations comes with a risk. APIs are doors through which to enter digital infrastructures, thus, the security and resilience of digital environments will also depend on the robustness of the API infrastructure. This has consequences at both the organisational and at systemic levels. If not properly protected, API infrastructures can lead to serious vulnerability issues (e.g., the disclosure of unentitled private information, the access to infrastructure by malicious systems, or the halting of critical infrastructure).

Governments manage the sensitive information of citizens and companies, thus, cybersecurity must be considered a priority when designing, implementing and deploying digital internal and public services. In this context, it is essential to maintain safe and monitored the access to APIs to avoid malicious cyber-attacks. Some examples of government API breaches are provided, and the consequences described.

This report describes API-specific security risks and mitigation measures. The analysis is based on the annual work performed by the Open Web Application Security Project® (OWASP) foundation that publishes a document with the top 10 most critical security concerns for web application security, namely: Broken Object Level Authorisation, Broken User Authentication, Excessive Data Exposure, Lack of Resources and Rate Limiting, Broken Function Level Authorisation, Mass Assignment, Security Misconfiguration, Injection, Improper Assets Management, and Insufficient Logging and Monitoring.

Security standards are another aspect analysed in this report. Some widely used standards related to API security at the application level include: *OAuth 2.0* for delegated authorisation which is essential for third-party applications to access resources they do not own without the need for the resource owner to share security credentials; *Extensible Access Control Markup Language (XACML)*, which defines an attribute-based access control system but can also be used to implement role-based access control. XACML defines base concepts (policy set, policy and rules) and the language for expressing an access control policy; and *OpenId Connect specification*, which exploits the OAuth 2.0 delegated authorisation mechanism to provide a federated authentication functionality.

Standards related to API security at the transport level include *Transport Layer Security (TLS)*, which provides communication integrity, confidentiality and authentication. It encrypts data and authenticates connections when moving data over the internet via HTTP, an extension of the protocol Hyper Text Transfer Protocol Secure (HTTPS). At the message/payload level, the following standards apply: *JSON Advanced Electronic Signature (JAdES)*, and *JSON Web Signatures (JWS).*

This report also analyses the eIDAS Regulation from an API viewpoint, in particular how APIs can use eIDAS implementation in authentication and authorisation processes within online public services in Europe, and also for tracing purposes, through timestamping of electronic transactions.

API privacy and traceability

Privacy preservation is a right protected under the General Data Protection Regulation (GDPR). GDPR obligations must be considered during API design, implementation and operational phases. Two approaches are adopted to govern API interactions in organisations with distributed systems: API gateways and service meshes. This type of tools can monitor and trace digital interactions. Organisations such as OWASP and MyData suggests best practices for logging, monitoring and managing private data and its processing.

Current technological solutions, knowingly active on the protection of privacy data, are explored and described in this report. Namely, 'CaPe', 'Solid', AMdEX and "privacyTracker".

REPORT II: LEGAL & ORGANISATIONAL ESSENTIALS

The *second report* analyses what legal and organisational aspects are essential for managing and coordinating digital interactions from an API viewpoint. The analysis was performed 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 aspect 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.

API legal concerns

Due to its statutory nature, government and public administrations need to tackle diverse legal aspects applicable to API data sharing, API data access and beyond. On one hand, they need to abide by the legal framework of their operations and lead by example. On the other hand, government duties include monitoring law compliance, and they need to set up appropriate infrastructures and processes to do so.

The legal analysis of APIs is a multifaceted problem. On one hand, an API is a piece of software subject to intellectual property rights such as patents, copyrights, trade secrets and trademarks. On the other hand, an API is a service governed by service agreements on both the technical and contractual levels. Moreover, APIs enable the connection into digital ecosystems, and API technical and legal constraints dictate the interactions among actors in these environments.

While there are no specific API laws, API stakeholders do not operate in a legal vacuum. An organisation providing or consuming APIs needs to ensure that it follows specific rules that, although scattered across different regulations, form the legal framework to comply with.

This section describes the applicable legal framework of APIs at length. It also analyses the legal implications linked to the different facets depending on what the role of the stakeholder in the API-driven interactions. Table 1 summarises the latter analysis and aims to help determine the legal framework applicable to the specific use of APIs.

API organisational and coordination aspects

The multifaceted legal nature of APIs adds complexity to digital management and coordination. However, these steps are crucial to ensuring the stability of digital solutions and, ultimately, the entire digital ecosystem.

This section explores the legal infrastructure and organisational coordination models used by private and public practitioners to effectively coordinate their digital interfaces through APIs.

Through an analysis of eight case studies from the public and private sectors, we have studied the current dynamics of the rewiring of systems, processes and rights and obligations.

Specifically, we identified new roles and responsibilities created around public sector innovation. We also observed the creation of provisory entities that make the testing of innovative solutions more accessible to the public sector. Moreover, we observed the adaptation of processes and workflows to ease the digital transition of government while respecting the continuity of their statutory processes, i.e., to ease innovation processes. 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.

API legal and organisational nexus

To add a systemic perspective to the analysis of digital coordination through APIs, the work included an empirical analysis of current practices of legal coordination encoded in the interactions defined by API contract conditions, i.e., the ToS. From a list of 4000 ToS documents, 2800 were successfully decoded and systematically analysed to shed some light on questions such as:

– Is there homogeneity in the drafting of API ToS contracts?

– Do ToS comply with currently applicable laws?

– How do ToS consider intellectual property rights?

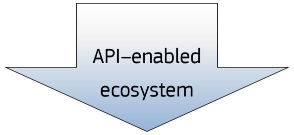
– Are jurisdiction statements hindering innovation?

– Do ToS drafting practises foster/hinder cooperation and/or fair competition?

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.

Source: ©apinan, 74362160 / Adobe stock

API FUNCTION	STAKEHOLDER ROLE	PRIMARY LEGAL OBLIGATIONS/ISSUES	APPLICABLE RULES AND LAWS/ SOURCES OF OBLIGATIONS
API as technical means to share data	Data holder	Making sure that data sharing is lawful and secure: 1. Incorporation of legal constraints on data into APIs: - drafting agreements facing an API developer (APIs developed externally), or - adequate internal control (APIs developed internally) 2. Propagation of data legal constrains across value chain: drafting data licences	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
		Making sure that the issue of API ownership is settled when APIs are developed externally	
API as software	API developer	Lawful API design Design must consider the constrains of the exposed data	Industry standards Agreement between API developer and data holder if API not developed by data holder
		Legal protection of APIs under IPRs and licencing	Protection under IPRs (copyrights, patents, trade secrets)
API as a service	API service provider	Lawful operation of services	Laws relating to the information society services, DSA
		Drafting and compliance with user-facing agreements (ToS, SLA, individual contracts). Disclosure of relevant licences in the agreements	Contract law, laws relating to transparency, data protection, consumer protection laws, competition laws
		Provision of service in accordance with relevant licences on data and APIs	Licences linked to the data behind APIs, and the use of APIs
	API service user: business, public and consumers	Compliance with ToS, SLA, individual agreements	Agreement



API as technical enabler of digital ecosystem(s)	Ecosystem orchestrator	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	Governance frameworks for the ecosystem: P2B regulation, DGA, DA, DSA, DMA Interoperability frameworks European standardisation regulation Infrastructure security: Cybersecurity Act, NIS2 directive

Table 1: Conceptualisation of the legal framework applicable to the use of APIs

CONCLUSIONS

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 preserve 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 a thriving European digital ecosystem.

Using APIs for data sharing and data access will remove barriers to innovation and ease interoperability among organisations at the technical and legal levels. Technically, this is due to the flexibility of APIs to concurrently interact with different actors and systems. Organisationally, API infrastructure can be used to control and monitor digital interactions between actors and systems. This characteristic makes APIs a relevant object of study when defining data governance processes and digital interactions via contracts or other technical agreements.

Governments defining their digital agenda should consider managing and coordinating their API infrastructure both internally and externally. Internally, to improve their processes and advance in their digital transition. Externally, to successfully integrate into the digital scene and be ready to be the custodians of a robust, fair and competitive Digital Single Market.

DIGITAL MANAGEMENT AND COORDINATION IN ORGANISATIONS (internal perspective)

The appropriate management and coordination of API infrastructure in organisations requires a robust technical infrastructure and its proper coordination. This work describes technical essentials that decision-makers should keep in mind to better profit from their API infrastructure. Specifically, this work dives into API management both at the product and organisational levels, API discoverability and security and its links with digital traceability.

The management of APIs in organisations is a multi-level and multi-stakeholder effort that also requires of a digital ecosystem vision within the organisation. API infrastructure can facilitate the re-use of internal assets, avoid duplication and reduce efforts to improve quality-of-service provision. API infrastructure and its use can be employed to manage and monitor the digital interactions of the organisation and its evolution. Moreover, government organisations can use their API infrastructure as regulatory reporting tools to support their policy implementation duties.

Governments that handle APIs as ad-hoc, isolated information and communications technology projects without any coordination are missing out on opportunities to advance in the digital transition. Among other things, this approach can cause inefficiencies derived from the lack of interoperability due to ad-hoc implementations, duplication of resources, process inefficiencies, issues with scalability and lack of sustainability of APIs. These issues were confirmed by the government entities engaged in our investigation.

DIGITAL GOVERNANCE AND SYSTEMIC COORDINATION (external perspective)

Successful organisations are connected to the digital ecosystem and effectively manage digital interactions. These interactions mostly take place through API-driven services that modulate the conditions of access and use. From a digital ecosystem perspective, 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. These implications need to be coordinated in order to stabilise the digital ecosystem, and governments will have an active role as custodians.

Europe is a pioneer in setting policy mechanisms for digital governance with a systemic approach, and there is a growing body of law governing and shaping digital futures. APIs already feature implicitly and explicitly in the current body of law. Yet, we consider that digital coordination is still in its early stages. Work remains to be done to fulfil the vision of a Europe fit for the digital age. For instance, one aspect that was not tackled in the study was the effect of legal fragmentation on coordination efforts. This may be tackled in further work.

RELATED WORK

[1] Posada Sanchez, M., Pogorzelska, K. and Vespe, M., 'The role of application programming interfaces (APIs) in data governance and digital coordination', European Commission, 2022.

[2] Vaccari, L. et al., *Application Programming Interfaces in Governments: Why, what and how*, Joint Research Centre, Publications Office of the European Union, Luxembourg, 2020.

[3] Santoro, M. et al., *Web Application Programming Interfaces (APIs): General-purpose standards, terms and European Commission initiatives*, Joint Research Centre, Publications Office of the European Union, Luxembourg, 2019.

[4] Boyd, M. et al., *An Application Programming Interface (API) Framework for Digital Government*, Joint Research Centre, Publications Office of the European Union, Luxembourg, 2020.

[5] Posada Sanchez, M., Vaccari, L. and Pogorzelska, K., *Unfolding Opportunities from the Use of APIs in Europe*, Joint Research Centre, Publications Office of the European Union, Luxembourg, 2021.

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