



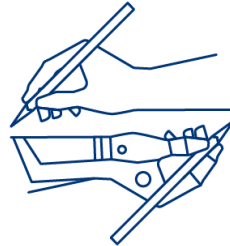
Funded by
the European Union

Project: 101094364 - ITHACA - HORIZON-CL2-2022-DEMOCRA - Ref. Ares(2025)11555022 - 23/12/2025

EUROPEAN RESEARCH EXECUTIVE AGENCY (REA)

REA.C – Future Society

C.1 – Inclusive Society



ITHACA

AI To Enhance Civic Participation

ITHACA

artificial Intelligence To enHance Civic pArticipation

Deliverable D5.6 – Data governance framework for AI civic engagement platforms

Work Package: WP5 – Conformity assessment tools policy recommendations and guidelines

Authors:	SnP (Charikleia-Eleni Nikolaou, Emmanouil Dimogerontakis), KT (Papaioannou, Georgia) MNLT Innovations (Sigalas, Nikolaos)
Status:	Final
Due Date:	31/12/2025
Version:	1.0
Submission Date:	23/12/2025
Dissemination Level:	PU – Public

Disclaimer:

This document is issued within the frame and for the purpose of the ITHACA project. This project has received funding from the European Union’s Horizon Europe Framework Programme under Grant Agreement No. 101094364. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

This document and its content are the property of the ITHACA Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the ITHACA Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the ITHACA Partners. Each ITHACA Partner may use this document in conformity with the ITHACA Consortium Grant Agreement provisions.

(*) Dissemination level. - Public - fully open (automatically posted online)

Sensitive - limited under the conditions of the Grant Agreement

EU classified -RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision 2015/444

ITHACA Project Profile

Grant Agreement No.: 101094364

Acronym:	ITHACA
Title:	artificial Intelligence To enHance Civic pArticipation
URL:	TBA
Start Date:	01/01/2023
Duration:	36 months

Partners

Short Name	Legal Name	Country
KT	KONNEKT ABLE TECHNOLOGIES LIMITED	IE
CERTH	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	EL
UPAT	PANEPISTIMIO PATRON	EL
RtF	RAISING THE FLOOR	BE
SnP	STAMADIANOS KAI SYNETAIROI DIKIGORIKI ETAIREIA	EL
UniGraz	UNIVERSITAET GRAZ	AT
MNLT	MNLT INNOVATIONS IKE	EL
SIMAVI	SOFTWARE IMAGINATION & VISION SRL	RO
PEDAL	PEDAL CONSULTING SRO	SK
BMA	AGENTIA METROPOLITANA PENTRU DEZVOLTARE DURABILA BRASOV ASOCIATIA	RO
MARTIN	MESTO MARTIN	SK



DOCUMENT HISTORY

VERSION	DATE	CHANGES	RESPONSIBLE PARTNER
0.1	30/09/2025	SnP	First Structure/ToC
0.2	10/10/2025	SnP	Sections 1-3
0.3	24/11/2025	MNLT	Section 5.2.3
0.4	30/11/2025	KT	Section 4,5.3,6.4, 7
0.5	12/12/2025	SnP	Rest Sections
0.6	17/12/2025	KT, MNLT, SIMAVI	Internal Review
0.7	22/12/2025	SnP	Final Version and Submission to KT

Table of Contents

- 1. Introduction..... 9**
 - 1.1 What is an AI-enabled Civic Engagement Platform (CEP)?..... 9**
 - 1.2 Typical Data Processed by AI-enabled CEPs 11**
 - 1.2.1 User and account data 11
 - 1.2.2 Participation content..... 12
 - 1.2.3 Process and participation metadata 12
 - 1.2.4 Technical logs and analytics 12
 - 1.2.5 Governance and compliance data..... 12
 - 1.2.6 AI-related data 13
- 2. EU Regulatory Landscape..... 14**
 - 2.1 2.1 General Data Protection Regulation (GDPR) 14**
 - 2.1.1 What is the GDPR?..... 14
 - 2.1.2 How does the GDPR affect AI-enabled CEPs? 14
 - 2.1.3 Which main provisions affect data governance in CEPs? 15
 - 2.2 Artificial Intelligence Act (AI Act) 15**
 - 2.2.1 What is the AI Act?..... 15
 - 2.2.2 How does the AI Act affect AI-enabled CEPs? 15
 - 2.2.3 Which main provisions affect data governance in CEPs? 16
 - 2.3 Digital Services Act (DSA) 16**
 - 2.3.1 What is the DSA? 16
 - 2.3.2 How does the DSA affect CEPs with user-generated content?..... 17
 - 2.3.3 Which main provisions affect data governance in CEPs? 17
 - 2.4 Network and Information Security 2 (NIS2) Directive and Cyber Resilience Act (CRA) 18**
 - 2.4.1 What are the NIS2 and the CRA?..... 18
 - 2.4.2 How do NIS2 and the CRA affect AI-enabled CEPs and their components? 18
 - 2.4.3 Which main provisions affect data governance in CEPs? 19
 - 2.5 Data Governance Act (DGA) and Open Data Directive (ODD) 19**
 - 2.5.1 What are the DGA and the ODD? 19
 - 2.5.2 How do the DGA and ODD affect AI-enabled CEPs? 19
 - 2.5.3 Which main provisions affect data governance in CEPs? 20

2.6	Accessibility Framework: Web Accessibility Directive (WAD) and European Accessibility Act (EAA)	20
2.6.1	What is the WAD and the EAA?.....	20
2.6.2	How do WAD and EAA affect CEPs?	21
2.6.3	Which main provisions affect data governance in CEPs?	21
3.	Key Definitions	22
4.	Data Governance Requirements	23
4.1	Data Governance Rules and Controls for the ITHACA platform and other AI-enabled CEPs	23
4.2	Key results of the Data Protection Impact Assessment for ITHACA platform ...	25
5.	Data Lifecycle Governance	25
5.1	Data Collection	25
5.1.1	Lawful bases for data collection in CEPs	25
5.1.2	Consent as a legal basis.....	26
5.1.3	Data minimisation and transparency notices.....	27
5.1.4	Cookies, local storage and similar technologies (ePrivacy)	27
5.2	Data Classification	28
5.2.1	Purpose of data classification in CEPs.....	28
5.2.2	Core categories	28
5.2.3	Open data and reusable information	29
5.2.4	Applying classification to CEP-related data categories	30
5.3	Data Storage, Retention & Deletion Policies	30
5.3.1	Governance objectives	30
5.3.2	Storage and access control.....	31
5.3.3	Encryption and integrity	31
5.3.4	Retention periods.....	31
5.3.5	Deletion and anonymisation methods	31
5.4	Data Use, sharing & reuse	31
6.	Accountability, Transparency & Human Oversight	33
6.1	Internal Documentation	33
6.1.1	Records of Processing Activities (RoPA) for CEPs	33
6.1.2	AI system registry and transparency logs.....	33
6.2	Audit & Reporting	34
6.2.1	Internal and external audits	34
6.2.2	Risk-register reviews	34

- 6.2.3 DSA transparency reporting 35
- 6.3 Data-Subject Rights Requests and illegal content reporting 35
- 6.4 Security Baseline..... 35
- 6.5 Risk Assessment Methodology..... 36
- 6.6 Platform Governance 36
- 7. Interoperability and Data Standards..... 37
 - 7.1 Metadata Standards and FAIR Principles 37
 - 7.1.1 Minimum metadata requirements..... 37
 - 7.1.2 Findability and accessibility 38
 - 7.1.3 Interoperability and reuse..... 38
 - 7.2 Open Data and Interoperability Obligations 38
 - 7.2.1 Scope of open data 38
 - 7.2.2 APIs and platform interoperability 39
- 8. Conclusion 39
- 9. References 40

LIST OF TABLES

- Table 1: CEPs Functionalities 10
- Table 2: Data Categories of CEPs..... 14

ABBREVIATIONS

AI	Artificial Intelligence
API	Application Programming Interface
CEP	Civic Engagement Platform
CISO	Chief Information Security Officer
CRA	Cyber Resilience Act
CSV	Comma-Separated Values
DGA	Data Governance Act
DOI	Digital Object Identifier
DPIA	Data Protection Impact Assessment

DPO	Data Protection Officer
DSA	Digital Services Act
EAA	European Accessibility Act
GDPR	General Data Protection Regulation
JSON-LD	JavaScript Object Notation for Linked Data
NIS2	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2 Directive)
ODD	Open Data Directive
REA	European Research Executive Agency
SPSS	Statistical Package for the Social Sciences
ToS	Terms of Service
WAD	Web Accessibility Directive
WP	Work Package
XLSX	Excel Open XML Spreadsheet (Microsoft Excel file format)
XML	Extensible Markup Language

EXECUTIVE SUMMARY

This document presents the Data Governance Framework for AI-enabled Civic Engagement Platforms (CEPs), developed on the basis of the legal, ethical and operational insights generated within the ITHACA project. It sets out a holistic and coherent approach to how CEPs should collect, classify, manage, secure, store, share, reuse and delete data, ensuring that all actors involved operate under a common governance baseline. While grounded in the concrete experience of the ITHACA project, the framework is written as a model that can be adopted or adapted by municipalities, platform providers and other initiatives deploying similar participation infrastructures.

The framework first maps the applicable regulatory and normative environment (including data protection, AI, platform governance, security, open data and accessibility requirements) and translates it into clear governance obligations for CEPs. It clarifies what constitutes regulated data in this context and how different categories of data—personal and special categories of personal data, non-personal and open data—should be handled. It also defines the key roles and responsibilities and organizes them through a set of cross-cutting rules and controls. These rules cover lawful bases and conditions for secondary use, consent and preference management, data minimisation, storage and retention, access control and security, internal documentation and logging, handling of data-subject requests and complaints, incident and breach management, audit and reporting, inclusion and accessibility, interoperability and open standards.

Applying these rules across the full data lifecycle, the Data Governance Framework describes how CEPs should govern data from initial collection through storage and internal use, onward sharing and secondary use, management of AI-related data, and final deletion or anonymisation. The framework is explicitly designed to avoid ad hoc decisions: choices about how, why and where regulated data is processed or reused must follow predefined criteria that balance utility and innovation with transparency, security and the protection of fundamental rights.

A central feature of the framework is the integration of the results of the Data Protection Impact Assessment (DPIA) carried out for the ITHACA platform. The DPIA's identification of high-risk processing activities, such as large-scale processing of participant's data that may reveal political opinions, is reflected in strengthened safeguards throughout the governance rules. These include stricter handling of special-category personal data, clearly defined human oversight over AI systems, enhanced transparency and logging requirements, a common security and incident-response baseline, and mechanisms for ongoing monitoring of risk exposure and continuous improvement. In this way, this document consolidates the ITHACA's project experience into a practical governance blueprint for CEPs that is both compliant with evolving regulatory requirements and responsive to democratic and ethical concerns.

1. Introduction

The ITHACA project (“artificial Intelligence To enHance Civic pArticipation”) develops and tests a human-centric, AI-enabled CEP to strengthen participation in local governance while safeguarding human rights and democratic values. Pilots in real municipal contexts provide practical experience on how AI-assisted tools affect inclusion, trust and participation, including for vulnerable groups. Work Package 5 addresses the normative, governance and policy dimensions of this work, so that the ITHACA platform is not only technically sound, but also legally and democratically robust.

The present document sets out the Data Governance Framework for CEPs, based on the results and experience of the ITHACA project. It defines how data in CEPs should be collected, classified, accessed, used, shared, secured and retained, and clarifies who is responsible for which decisions. In this way, it provides a set of rules and processes that guide day-to-day data processing activities, avoid ad hoc choices, and ensure that all pilots and partners work within the same governance baseline.

Within Work Package 5, Deliverable 5.6 connects earlier analytical and policy work with the practical data-management rules of the project. Along with the White Paper with Policy Recommendations (Deliverable 5.5), it offers a transferable governance blueprint for AI-enabled CEPs, while the Data Management Plan (Deliverable 7.2) details how these governance rules are implemented in concrete datasets, repositories, formats and access conditions.

1.1 What is an AI-enabled Civic Engagement Platform (CEP)?

Within the ITHACA project, a CEP is understood as a digital, institutionally anchored participation infrastructure. It is not simply a website or a generic social network: it is a socio-technical system operated by, or on behalf of, public authorities to support structured citizen participation in public decision-making. In line with international practice on digital participation tools, CEPs provide an online environment where residents, civil-society organisations and other stakeholders can access information, contribute ideas, deliberate with others and see how their input influences public policies over time (Farina, 2014; Nelimarkka, 2014; OECD, 2022c, 2025d; Tsarchopoulos et al., 2018).

From the perspective of the ITHACA project, as already mentioned in the Deliverable 5.5, the CEP is conceived as part of the regular democratic infrastructure of a municipality rather than a one-off consultation tool. It is intended to complement, and be embedded within, existing institutional processes (e.g. consultations, strategic planning, participatory budgeting, local ordinances), creating durable channels through which citizens can interact with public authorities on an ongoing basis. In this sense, the platform is a mediating layer between citizens and institutions: it structures when, how and on what terms people can participate, and how institutional actors receive, process and respond to contributions (ITHACA Consortium, 2025; OECD, 2022c).

Across different implementations studied in the literature, CEPs typically offer a core set of participation functions. First, they provide access to information about ongoing or upcoming participation processes, including background materials, explanatory content and procedural details (timelines, participation rules, eligibility). Second, they enable users to submit proposals, ideas or problem reports, usually tied to specific themes or processes (e.g. “urban mobility plan”, “climate action strategy”). Third, they support deliberation and feedback, allowing participants to comment on, discuss and refine proposals submitted by others. Fourth, they often include mechanisms for expressing support or preference, such as endorsements, rankings, or votes, sometimes in the context of binding or advisory participatory budgeting and referenda (Farina, 2014; Nelimarkka, 2014; Shin, 2024; Tsarchopoulos et al., 2018). Finally, mature CEPs provide follow-up features, such

as status updates on proposals, institutional responses, implementation tracking dashboards and feedback on how citizen input has been used (OECD, 2022c, 2022e, 2025d).

The ITHACA project focuses specifically on AI-enabled CEPs, i.e. CEPs into which selected AI functionalities are integrated. Internationally, AI is increasingly used in public-sector engagement to help process large volumes of contributions, personalise information, or improve accessibility and language support (Berryhill et al., 2019; OECD, 2019a, 2019b, 2025b, 2025d). Common examples include:

- Search and recommendation tools that help users discover relevant proposals, topics or past debates, and help public officials surface clusters of similar contributions and emerging themes. (OECD, 2025d; OECD.AI, 2024).
- Natural language processing (NLP) and summarisation, which can group and summarise large numbers of free-text inputs submitted during consultations, producing overviews that support both citizens and officials in understanding the “big picture” of a debate (OECD, 2025d; Shin, 2024).
- Assistive moderation tools, such as automated flagging of potentially abusive content or spam to support human moderators; and inclusion tools, such as automatic translation, text-to-speech, or simplified-language interfaces, which can lower participation barriers for people with language or accessibility needs (Berryhill et al., 2019; OECD, 2019a, 2022c, 2025b, 2025d).

In line with emerging guidance on trustworthy AI in the public sector, AI tools in a CEP are conceived as assistive components that enhance, but do not replace, human judgement and institutional responsibility (OECD, 2019/ 2023). They are used to support tasks such as information retrieval, summarisation, translation and pre-classification of content; final decisions on participation processes, policy outcomes or content moderation remain the responsibility of designated institutional actors. This “human-in-command” approach is particularly important in civic participation, where the platform shapes who can speak, how contributions are interpreted, and how they are translated into public decisions (Cortés-Cediel et al., 2019; Farina, 2014; OECD, 2025d).

CEPs Functionalities	Description
Information provision	Publishing clear, accessible information about participation opportunities (process goals, timelines, rules, background documents, contact points) so that citizens understand what the process is about and how to take part.
Submission of proposals and ideas	Allowing users to submit proposals, ideas, questions or problem reports linked to specific themes, territories or participation processes (e.g. mobility plan, neighbourhood improvements, climate actions).
Comments and deliberation	Enabling users to comment on, discuss and refine proposals and ideas from others through threaded discussions and other deliberation features.
Endorsements, votes and preference expression	Providing mechanisms for expressing support or preferences, such as endorsements, rankings, scoring or votes, including in participatory budgeting or advisory polls.

Surveys and structured consultations	Hosting questionnaires, polls and other structured input forms that collect more targeted feedback on specific policy options, scenarios or priorities.
Follow-up and institutional feedback	Showing status updates and institutional responses (e.g. “under review”, “accepted”, “rejected”, “implemented”), and providing explanations on how input was used in decisions, including implementation tracking where relevant.
AI-based search and recommendation	Using AI to surface relevant proposals, topics or past debates, detect similarities and clusters, and help both citizens and officials navigate large volumes of content.
AI-based summarisation and sense-making	Applying natural language processing to group and summarise large numbers of contributions, generate overviews of debates and highlight key themes and arguments.
Assistive moderation support	Using AI tools to pre-flag potentially abusive, illegal or spam content for review by human moderators, helping them prioritise workload without automating final decisions.
Inclusion and accessibility support	Providing translation, text-to-speech, simplified-language and other assistive tools (often powered by AI) to lower linguistic, cognitive and accessibility barriers to participation.
Institutional control and accountability	Configuring roles, workflows and dashboards that allow public authorities to manage processes, review input, document decisions and ensure that human officials retain responsibility for outcomes.

Table 1: CEPs Functionalities

1.2 Typical Data Processed by AI-enabled CEPs

AI-enabled CEPs process a diverse set of data categories that reflect both their role as digital public spaces and their integration into institutional decision-making. Understanding these categories is essential for designing appropriate governance rules, allocating responsibilities, and assessing risks. Building on empirical studies of digital participation tools and civic-tech platforms (Shin, 2024; Tsarchopoulos et al., 2018), on international guidance on citizen participation and AI in government (OECD, 2019a, 2019b, 2022b, 2022c, 2025b, 2025d), and on the specific types of data identified for the ITHACA Platform in the Data Protection Impact Assessment and the Privacy by Design and by Default report, this Framework distinguishes six main data categories that are typically in scope.

1.2.1 User and account data

User and account data comprise the information needed to create, manage and secure user accounts and roles on the CEP. Typical elements include identifiers (such as usernames and internal user IDs), contact details (e.g. email address, telephone number), and authentication data (passwords, credential hashes, multi-factor authentication tokens). In some deployments, additional profile attributes may be collected where justified—for example, municipal area of residence, language preferences or basic demographic attributes in aggregated form—to enable targeted communication, equity analysis, or inclusive participation design (OECD, 2022a, 2022c, 2022d, 2025b, 2025d; Shin, 2024). Role and permission data (e.g. ordinary participant, moderator, administrator, institutional

representative) are also part of this data category, as they determine what actions each user can perform on the platform.

1.2.2 Participation content

Participation content consists of the substantive contributions that users make to civic processes through the CEP. This includes proposals, ideas, reports and position statements; comments and replies in discussion threads, endorsements, ratings or votes attached to proposals or options, and responses to surveys, questionnaires and polls. It also includes documents, images or other files that users upload in support of their contributions, to the extent permitted by platform rules (Farina, 2014; Nelimarkka, 2014; OECD, 2022c). In practice, this is often where sensitive information can appear, such as political views, criticisms of public authorities, or descriptions of personal circumstances that motivate participation.

1.2.3 Process and participation metadata

Beyond user-generated content, CEPs generate process and participation metadata that describe when, where and how participation takes place. Such metadata typically include timestamps for submissions, edits and other actions; identifiers linking each contribution to specific participation processes (e.g. “participatory budgeting 2026”, “consultation on mobility plan”); status flags for proposals (e.g. “submitted”, “under review”, “accepted”, “rejected”, “implemented”); and simple counters or indicators (number of comments, endorsements, views) (OECD, 2022a, 2022c, 2025b, 2025d; Shin, 2024).

1.2.4 Technical logs and analytics

Technical logs and analytics cover the data generated by the technical operation of the platform itself. This includes connection and security logs (e.g. IP address, browser or device information, login attempts, error logs), session identifiers and cookie identifiers, and navigation logs indicating which pages or features are accessed. These logs are essential for ensuring availability, debugging technical issues, monitoring performance and detecting potential security incidents or abusive behaviour (OECD, 2019a, 2019b; Berryhill et al., 2019). In many cases, platforms also produce aggregated analytics on usage patterns (e.g. number of visitors, most viewed pages, time spent on certain sections), which can inform user-experience improvements and outreach strategies.

1.2.5 Governance and compliance data

Governance and compliance data are generated as part of the governance layer surrounding the CEP. Typical examples include records of acceptance of terms of service; records of participation in specific processes (e.g. eligibility checks, confirmations of submission), logs of information and assistance provided to users, records of user requests regarding their data and how these were handled, and logs related to moderation and platform governance, such as notices submitted by users, assessments carried out by moderators, decisions to keep, edit or remove content, and statements of reasons where these are provided to users (OECD, 2022a, 2022c, 2025b, 2025d). Where the platform allows for account-level measures (e.g. temporary suspension due to repeated violations), records of these measures and any subsequent appeals are also part of this data category. These data are central for enabling internal oversight, external audits and public transparency about how the CEP is governed.

1.2.6 AI-related data

Finally, AI-related data encompass those data used to develop, deploy and monitor the AI functionalities integrated into the CEP. This category includes datasets used for training, fine-tuning or evaluating AI models (for example, corpora of past proposals and comments used to train summarisation or classification tools), where such use is justified and consistent with participation expectations, logs of inputs and outputs from AI components, where logging is necessary for debugging, quality assurance or accountability, user feedback on AI outputs (e.g. “helpful/not helpful” ratings, flags indicating perceived bias or error), and derived scores or flags produced by AI tools, such as predicted topic labels, relevance scores, toxicity or spam scores, or accessibility indicators (OECD, 2019a, 2019b, 2019/2024, 2025b). In line with emerging good practice, these data should be handled in ways that make AI behavior traceable and contestable while avoiding unnecessary retention or secondary use.

These six data categories define the scope of the Data Governance Framework. The subsequent chapters will specify, for each data category, how data are to be collected, classified, stored, accessed, shared and deleted, how responsibilities are allocated among actors, and how risks, particularly for fundamental rights and democratic participation, are to be identified and mitigated over time.

Data Category	Short Description	Typical data items
User and account data	Information needed to create, manage and secure user accounts, and to assign roles and permissions.	Username, internal user ID, email address, optional phone number, hashed passwords/credentials, language and municipality, role (participant, moderator, administrator, institutional representative).
Participation content	Contributions made by users in the context of participation processes.	Proposals and ideas, free-text comments and replies, survey and poll responses, endorsements and votes, uploaded documents, images or other files related to public issues.
Process and participation metadata	Structured information describing how, when and in which process participation occurs.	Timestamps for submissions and edits, identifiers of participation processes, proposal status labels (“submitted”, “under review”, “accepted”, etc.), counters (views, comments, endorsements), high-level participation metrics.
Technical logs and analytics	Data generated by the technical operation, security and performance monitoring of the platform.	IP addresses, browser/device information, session and cookie identifiers, login attempts, error logs, navigation paths, aggregated usage statistics (visits, page views, time on page).

Governance and compliance data	Records documenting platform rules, user information and governance actions around participation and moderation.	Records of acceptance of terms of service, evidence of eligibility checks, logs of user help and information, records of user requests about their data and responses, notices submitted by users, moderation assessments and decisions, statements of reasons, account measures and appeals.
AI-related data	Data used to develop, operate and monitor AI components integrated into the CEP.	Training and evaluation datasets, logs of inputs and outputs from AI tools where necessary, user feedback on AI outputs (“helpful”, “biased”, “incorrect”), derived scores or flags (topic labels, relevance scores, toxicity or spam scores).

Table 2: Data Categories of CEPs

2. EU Regulatory Landscape

2.1 2.1 General Data Protection Regulation (GDPR)

2.1.1 What is the GDPR?

The GDPR is the EU’s core framework for the protection of personal data, formally Regulation (EU) 2016/679, applicable since 25 May 2018 in all Member States (European Parliament & Council of the European Union, 2016a). It sets out when and how organisations may process personal data, defines the main actors involved (controllers, joint controllers and processors), and establishes a catalogue of principles-lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability-that must guide all processing operations (European Parliament & Council of the European Union, 2016). It also grants individuals rights such as access, rectification, erasure, restriction, objection and data portability, and requires controllers to demonstrate compliance (“accountability”) through measures like records of processing, data protection by design and by default, and data protection impact assessments (DPIAs), as further clarified in guidance by the European Data Protection Board.

2.1.2 How does the GDPR affect AI-enabled CEPs?

For AI-enabled CEPs, the GDPR affects at least three key aspects of how a CEP operates (EDPB, 2017, 2019, 2020; European Parliament & Council of the European Union, 2016a; ITHACA Consortium, 2025).

- Multiple personal-data streams in one platform

A CEP processes several types of personal data at once: user and account data, participation content, process metadata and technical logs (see Section 1.3). All of these are within the scope of the GDPR whenever they relate to identifiable individuals in the EU, which means that a CEP must be GDPR-compliant.

- Sensitive participation content and chilling effects

Participation content may directly or indirectly reveal political opinions and other special categories of data, triggering the application of Article 9 GDPR and stricter safeguards (European Commission, 2024; European Parliament & Council of the European Union, 2016a). The way a CEP collects, displays, archives and potentially reuses such content has implications not only for compliance but also for people’s willingness to participate - a risk that D5.5 highlighted (ITHACA Consortium, 2025).

- Shared responsibilities and risk-intensive processing

CEPs are implemented through collaborations between municipalities, research partners and technology providers. In such settings, GDPR role allocation—who is (joint) controller, who is processor, and for which processing activities -- is important. This allocation determines who is responsible for informing users, who handles data subject requests and who is responsible for conducting DPIAs (EDPB, 2020). At the same time, processing activities such as large-scale processing of sensitive contributions, systematic monitoring of participation patterns or the use of AI tools that may affect rights are likely to qualify as “high-risk” processing, for which GDPR requires or strongly encourages DPIAs as a structured risk-assessment tool (EDPB, 2017).

2.1.3 Which main provisions affect data governance in CEPs?

For the purposes of this Data Governance Framework, the GDPR mainly shapes three strands of data governance in AI-enabled CEPs (EDPB, 2017, 2019, 2020; European Parliament & Council of the European Union, 2016a; ITHACA Consortium, 2025).

- Data protection principles and lawful bases

The GDPR principles-lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability-provide the baseline against which all CEPs data practices must be tested. This includes selecting appropriate lawful bases for each data category (user accounts, participation content, logs, research datasets), with particular safeguards where special categories such as political opinions are involved.

- Data-subject rights and records of processing

Rights to access, rectification, erasure, restriction, objection and data portability must be translated into clear CEP procedures, timelines and allocation of responsibilities. At the same time, the platform must maintain coherent privacy notices and record of processing activities so that users can understand how their data are used and exercise their rights effectively, while also preserving the integrity and traceability of public deliberation records.

- Data protection by design, DPIAs and accountability

Article 25 GDPR and related EDPB guidance require privacy and data protection principles to be embedded from the earliest stages of a CEP, rather than retrofitted (EDPB, 2019). DPIAs function as structured risk assessments for high-risk processing operations-such as large-scale processing of sensitive participation data or systematic monitoring-linking identified risks to concrete technical and organisational measures (EDPB, 2017). Together, these instruments make accountability an organising principle of CEP data governance, not just a reporting requirement.

2.2 Artificial Intelligence Act (AI Act)

2.2.1 What is the AI Act?

The AI Act is the EU’s horizontal framework for the development, placing on the market and use of AI systems, formally Regulation (EU) 2024/1689 of 13 June 2024 (European Parliament & Council of the European Union, 2024). It introduces a broad legal definition of AI, classifies systems according to their risk level, and allocates obligations to different actors in the AI value chain (providers, deployers, importers, distributors), with the aim of ensuring that AI placed on the Union market is safe, respects fundamental rights and upholds Union values.

2.2.2 How does the AI Act affect AI-enabled CEPs?

For AI-enabled CEPs, the AI Act affects at least three key aspects of how AI is integrated into participation processes (European Parliament & Council of the European Union, 2024a; OECD, 2019, 2025a, 2025b; ITHACA Consortium, 2025).

- Multiple AI functions embedded in participation workflows

In a CEP, AI is typically embedded in specific features rather than in the platform as a whole. This includes search and recommendation tools that help users and officials navigate proposals, summarisation tools (often based on general-purpose language models) that condense large volumes of input, assistive moderation tools that pre-flag potentially abusive or spam content, and inclusion-support tools such as translation or automatic text simplification (OECD, 2019, 2025). These functions directly affect how citizens interact with such a platform and how institutions process contributions.

- Risk for participation equality and perceived legitimacy

Even when CEP-related AI systems are not classified as “high-risk” under Annex III, they can influence whose contributions are seen, how issues are framed and which inputs receive institutional attention. Skewed training data or poorly designed recommendation and moderation tools may amplify existing inequalities or systematically disadvantage certain groups, undermining the fairness and perceived legitimacy of participation processes (OECD, 2019, 2025a, 2025b, 2025d; 2025e, ITHACA Consortium, 2025).

2.2.3 Which main provisions affect data governance in CEPs?

For the purposes of this Data Governance Framework, the AI Act mainly informs three aspects of data governance in AI-enabled civic participation (European Parliament & Council of the European Union, 2024a; OECD, 2019, 2025a, 2025b, 2025d; ITHACA Consortium, 2025).

- Data quality and representativeness

Training, validation and testing datasets for CEP-related AI systems should be relevant and sufficiently representative, so that historical biases in participation data or moderation logs are not simply reproduced in recommendations, summaries or flags. This involves focusing on under-represented groups and examining how participation and moderation data are sampled and pre-processed.

- Basic documentation and transparency about AI functionalities

For each AI functionality integrated into a CEP, there should be concise internal documentation-covering the system’s purpose, main data sources, key limitations and known risks-sufficient to support internal oversight and, where appropriate, simple user-facing explanations of how AI supports platform operations (OECD, 2019, 2022a, 2025a, 2025b, 2025d).

- Human oversight

AI tools in a CEP must remain assistive: human officials must be accountable for participation design, moderation decisions and institutional responses, and there should be light-weight monitoring to detect adverse effects such as systematic exclusion or distortions of deliberation. This aligns a CEP with the AI Act’s emphasis on meaningful human oversight and ongoing monitoring of AI systems with potential impact on fundamental rights.

2.3 Digital Services Act (DSA)

2.3.1 What is the DSA?

The DSA is the EU’s framework for the governance of intermediary services and online platforms, formally Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (European Parliament & Council of the European Union, 2022). It updates and complements the e-Commerce Directive by setting out due-diligence obligations for providers of hosting services and online platforms, including rules on notice-and-action mechanisms, transparency of terms and conditions, statements of reasons for content decisions, and risk management obligations for very large online platforms and search engines (European Commission, 2025; Fasel & Weerts, 2024). Although the ITHACA platform is public-interest, non-commercial, it still functions as a hosting

service for user-generated content. Therefore, the DSA provides an important regulatory and design reference for how participation spaces handle content, moderation and transparency.

2.3.2 How does the DSA affect CEPs with user-generated content?

For CEPs that host user-generated content, the DSA affects at least three main aspects of how participation spaces are structured and governed (European Parliament & Council of the European Union, 2022; European Commission, 2025; Fasel & Weerts, 2024; Fabbri, 2025).

- Notice-and-action and user reporting mechanisms

The DSA requires hosting services and online platforms to provide “easily accessible and user-friendly” mechanisms for users to notify allegedly illegal content (Article 16) and to process such notices diligently (European Parliament & Council of the European Union, 2022). For a CEP, this means that participants must have clear ways to report content they consider illegal or otherwise problematic, and that the platform must have structured workflows for handling these reports, including record-keeping and feedback to users.

- Statements of reasons and complaints about moderation

Platforms must provide users with statements of reasons whenever they remove content, restrict access, or suspend accounts, explaining the decision in a transparent and comprehensible way (Article 17) and offering internal complaint-handling mechanisms (Articles 20–21). In a CEP context, this aligns closely with democratic accountability: participants whose contributions are removed or restricted should be aware of the reasons for each decision, and must have a channel to contest moderation decisions. Such processes generate governance-related data that must be addressed within this framework.

- Transparency reporting and governance of platform rules

The DSA requires platforms to publish periodic transparency reports on their content moderation activities (Article 15) and to ensure that their terms and conditions clearly communicate policies on content, behaviour and moderation (Article 14) (European Parliament & Council of the European Union, 2022; Ohnesorge, 2025). For CEPs, this reinforces the idea, already present in D5.5, that participation rules, moderation practices and algorithmic interventions should not be opaque: both participants and the wider public need accessible information on how the platform is governed.

2.3.3 Which main provisions affect data governance in CEPs?

For the purposes of this Data Governance Framework, the DSA mainly shapes three strands of data and governance practice in CEPs (European Parliament & Council of the European Union, 2022; Fabbri, 2025; Ohnesorge, 2025).

- Moderation logs and “statements of reasons” as governance data

Implementing Articles 16 and 17 of the DSA in a CEP requires keeping structured records of notices, assessments, decisions (remove/keep/limit) and statements of reasons. These records become a distinct category of governance data that must be governed under this framework, including rules on retention, access, anonymisation and potential publication in aggregated form.

- Design and documentation of user-facing procedures

DSA requirements on user-friendly notice mechanisms, internal complaint handling and clear terms and conditions translate into design and documentation duties for a CEP: processes for reporting content, appealing moderation decisions and understanding platform rules must be documented, logged and periodically reviewed. This creates interfaces between user-experience design, legal compliance and data governance.

- Transparency reporting and accountability for platform rules

Even if the ITHACA platform is unlikely to qualify as a very large online platform, the DSA’s transparency-reporting requirement provides a template for periodic, structured disclosures about participation volumes, moderation actions and use of algorithmic tools (HIIG, 2025). Internal data structures and governance rules must therefore support the generation of reports-at least in an internal or pilot-oriented form-so that public authorities and stakeholders can scrutinise how a CEP is governed over time.

2.4 Network and Information Security 2 (NIS2) Directive and Cyber Resilience Act (CRA)

2.4.1 What are the NIS2 and the CRA?

The NIS2 and the CRA are complementary pillars of the EU’s cybersecurity strategy. The NIS2 Directive [Directive (EU) 2022/2555] aims to achieve a high common level of cybersecurity across the Union by imposing risk-management and incident-reporting obligations on a broad range of “essential” and “important” entities, including many public-sector bodies and digital infrastructure providers (European Parliament & Council of the European Union, 2022b; ENISA, 2025a). It replaces the NIS Directive, expanding its scope and strengthening supervisory and enforcement mechanisms. The CRA (Regulation (EU) 2024/284) introduces horizontal cybersecurity requirements for “products with digital elements”, covering both hardware and software that can be directly or indirectly connected to a network (European Parliament & Council of the European Union, 2024; European Commission, 2025; ENISA, 2025b). Its goal is to ensure that such products are designed, developed and maintained with cybersecurity in mind throughout their lifecycle, including obligations on secure development practices, vulnerability handling and security updates. Together, the NIS2 and the CRA frame both the organisational and the product-level dimensions of cybersecurity that are relevant for the design and operation of AI-enabled CEPs.

2.4.2 How do NIS2 and the CRA affect AI-enabled CEPs and their components?

For an AI-enabled CEP operated by or on behalf of public authorities, NIS2 and the CRA affect at least three main areas of practice (ENISA, 2025a, 2025b; European Parliament & Council of the European Union, 2022b, 2024b).

- Platform operators as essential or important entities

Depending on how Member States transpose NIS2 and classify public administration and digital infrastructure, the authority operating a CEP -and, in some cases, key ICT providers behind it- may fall under the Directive as “essential” or “important” entities. This triggers obligations to adopt cybersecurity risk-management measures (e.g. policies on risk analysis, incident handling, business continuity, supply-chain security) and to report significant incidents to national CSIRTs or competent authorities within strict timelines (European Parliament & Council of the European Union, 2022). In practice, this means a CEP cannot be treated as a low-stakes pilot: it must be integrated into the operator’s formal cybersecurity and incident-response plan.

- Supply-chain security and dependence on external services

Both NIS2 and the CRA emphasise supply-chain and third-party risk management. CEPs typically rely on external hosting services, content-delivery networks, authentication providers, analytics tools and AI APIs. Under NIS2, entities must address supply-chain security as part of their risk management, while the CRA requires that vulnerabilities in components and dependencies be managed in a coordinated way (ENISA, 2025a, 2025b). This affects how the CEP’s architecture is documented, how dependencies are monitored, and how responsibilities are allocated when vulnerabilities are discovered.

2.4.3 Which main provisions affect data governance in CEPs?

From the perspective of this Data Governance Framework, NIS2 and the CRA mainly inform three strands of cybersecurity-related governance that are essential for the protection of CEP data (ENISA, 2025a, 2025b; European Parliament & Council of the European Union, 2022b, 2024b).

- Baseline security measures and incident handling

NIS2 requires covered entities to implement a baseline set of technical and organisational measures, including risk analysis, incident handling, business continuity, crisis management and encryption (Article 21), as well as to notify significant incidents without undue delay (Articles 23–24). For CEPs, these requirements translate into clear rules on access control, logging, backup and recovery, and documented incident-response procedures for both security incidents and personal-data breaches, closely linked to the GDPR obligations described in Chapter 2.1.

- Integration of cybersecurity into procurement and supplier governance

Both NIS2 and the CRA stress that cybersecurity is not only an internal matter but extends to suppliers and service providers. For CEPs, this implies that procurement and contracting must incorporate cybersecurity requirements—for example, by requiring CRA-compliant products where applicable, specifying incident-notification duties for suppliers, and assessing cloud or AI service providers against criteria under NIS2.

2.5 Data Governance Act (DGA) and Open Data Directive (ODD)

2.5.1 What are the DGA and the ODD?

The DGA and the ODD are two complementary EU instruments that structure how public-sector data can be reused and shared. The DGA, Regulation (EU) 2022/868, creates a cross-sector framework to increase trust in data sharing by regulating the reuse of certain categories of protected public-sector data (e.g. data subject to commercial confidentiality, intellectual property or personal-data protection), introducing rules for data intermediation services, and enabling “data altruism” for the common good (European Parliament & Council of the European Union, 2022c; OECD, 2025c, 2025d). The ODD -Directive (EU) 2019/1024-recasts and updates the earlier Public Sector Information (PSI) framework, establishing the principle that public-sector data should be reusable for commercial and non-commercial purposes by default, and introducing obligations on machine-readability, non-discriminatory conditions, limited charging and a special regime for “high-value datasets” (European Parliament & Council of the European Union, 2019a; European Commission, 2024b; OpenAIRE, 2022). Together, they shape the environment in which data generated through CEPs can be made available, shared and reused beyond their original participation context.

2.5.2 How do the DGA and ODD affect AI-enabled CEPs?

For AI-enabled CEPs operated by or on behalf of public authorities, the DGA and ODD affect at least three main areas of practice (European Commission, 2024b; European Parliament & Council of the European Union, 2019a, 2022c; ITHACA Consortium, 2025; OECD, 2019, 2022a, 2025a, 2025d).

- CEPs’ outputs as public-sector information and open data

Many of the outputs generated by a CEP—such as published proposals, institutional responses, and aggregated statistics about participation—qualify as “documents” held by public-sector bodies under the ODD. In principle, these should be reusable by default, under open and non-discriminatory conditions, and, where feasible, provided in machine-readable formats and via APIs. The Implementing Regulation on high-value datasets further illustrates the EU’s expectation that key categories of public-sector data be made available free of charge and with minimal restrictions, using open licences and interoperable formats (European Commission, 2024b; European Parliament &

Council of the European Union, 2019). While civic participation data are not (currently) a dedicated high-value category, the same logic of “open by design” is relevant to how CEPs’ operators treat non-personal and sufficiently anonymised data produced through the platform.

- Institutional roles as data holders, reusers and potential data-altruism actors

Public authorities operating a CEP are, by default, data holders under the ODD and, in some cases, entities responsible for managing reuse of data under the DGA. At the same time, they may themselves act as reusers of data obtained from other public bodies (e.g. demographic or geospatial data) and may wish to encourage data altruism-voluntary sharing of data by individuals or organisations for defined public-interest projects (OECD,2025a).

2.5.3 Which main provisions affect data governance in CEPs?

From the perspective of this Data Governance Framework, the DGA and ODD mainly inform three strands of governance for CEP-related data (European Commission, 2024b; European Parliament & Council of the European Union, 2019a, 2022c; OECD, 2019, 2022a, 2025a, 2025d; ITHACA Consortium, 2025).

- “As open as possible, as closed as necessary” for CEP datasets

The ODD’s principle of reuse by default encourages CEP operators to treat non-personal and sufficiently anonymised data, such as aggregated participation statistics, metadata on processes, or non-identifiable institutional outputs-as open data, provided under clear licences and in machine-readable formats where feasible.

- Structured regimes for secondary use and controlled access

The DGA’s rules on reuse of protected public-sector data and secure processing environments offer a template for how CEP operators can enable research and innovation on participation data without releasing raw, identifiable datasets.

2.6 Accessibility Framework: Web Accessibility Directive (WAD) and European Accessibility Act (EAA)

2.6.1 What is the WAD and the EAA?

The WAD and the EAA form the core of the EU’s digital accessibility framework. The Web Accessibility Directive-Directive (EU) 2016/2102-requires Member States to ensure that websites and mobile applications of public sector bodies are accessible to persons with disabilities, on the basis of common accessibility requirements (European Parliament & Council of the European Union, 2016b). It operationalises accessibility through the “perceivable, operable, understandable and robust” principles and relies on harmonised standards, in particular EN 301 549 and the Web Content Accessibility Guidelines (WCAG) 2.1, as technical benchmarks (European Commission, 2024c; ETSI, 2021). Public bodies must publish accessibility statements, provide feedback mechanisms for users to report accessibility issues and be subject to monitoring and enforcement at national level. The EAA -Directive (EU) 2019/882 (European Parliament & Council of the European Union, 2019b)-sets EU-wide accessibility requirements for a range of products and services, mainly in the private sector. The EAA aims to harmonise divergent national rules and strengthen the rights of persons with disabilities and others with functional limitations by requiring that covered products and services meet common accessibility requirements based on functional outcomes rather than specific technical solutions.

2.6.2 How do WAD and EAA affect CEPs?

For CEPs operated by or on behalf of public authorities, the accessibility framework affects at least three main dimensions of platform design and operation (European Commission, 2024c; European Parliament & Council of the European Union, 2016b, 2019b; ETSI, 2021; OECD, 2022c; ITHACA Consortium, 2025).

- Public-sector digital participation as an accessibility-obliged service

A CEP operated by a municipality or other public body falls squarely within the WAD's scope for public sector websites and mobile applications. This implies that core participation functions, information pages, proposal forms, discussion threads, voting interfaces, dashboards, terms and conditions, privacy notices and AI explanations, must be accessible to users with a wide range of disabilities.

- Procurement and lifecycle alignment with accessibility standards

The EAA and associated standardisation efforts, including EN 301 549, influence how public bodies procure and manage ICT products and services, including CEP components and related tools (European Commission, 2024; ETSI, 2021; European Commission, 2025). Even if a specific CEP module is not directly listed as an EAA-covered service, public authorities are increasingly expected to require accessibility compliance across their digital estate. This means that platform architecture, third-party widgets, AI-based interaction components and document formats used in CEPs should be chosen and configured to meet EN 301 549 requirements across the lifecycle—from design and development to updates and decommissioning. Guidelines from national authorities (e.g. service design and accessibility guidelines) further indicate how public websites and services must integrate these standards into practice.

2.6.3 Which main provisions affect data governance in CEPs?

From the perspective of this Data Governance Framework, the WAD and the EAA mainly shape three strands of governance around accessibility, interoperability and inclusion (European Commission, 2024c; European Parliament & Council of the European Union, 2016b, 2019b; ETSI, 2021; OECD, 2022c; ITHACA Consortium, 2025).

- Accessibility of all “governance-related” content and interfaces

Accessibility requirements apply not only to the main participation flows but also to the content and interfaces through which governance and compliance are communicated: privacy notices, terms of service, consent dialogues, statements of reasons for moderation decisions, accessibility statements themselves, feedback and complaint forms.

- Accessibility-related logs, feedback and monitoring as governance data

The WAD requires public bodies to provide accessibility statements and feedback mechanisms so users can signal accessibility problems or request accessible alternatives, and Member States must monitor and report on implementation (European Commission, 2024; European Parliament & Council of the European Union, 2016). In a CEP, this generates a specific class of governance data: logs of accessibility feedback, remediation actions, test results and monitoring outcomes.

- Inclusion, interoperability and openness as design constraints for data formats

Compliance with EN 301 549 and related standards has implications for how data and content are structured: documents and datasets should use machine-readable, semantically rich formats; multimedia content should include captions, transcripts and alternatives; and APIs should support assistive technologies and alternative clients. These choices affect not only user experience but also the reusability and interpretability of data within open-government and research ecosystems.

3. Key Definitions

For the purposes of this document, the following working definitions apply. It must be noted that the definitions are consistent with D5.5 as well as with the regulatory and standards landscape outlined in Chapter 2.

Civic Engagement Platform (CEP)

A Civic Engagement Platform (CEP) is a digital system designed to enable individuals and groups to submit proposals, comments, and endorsements; support deliberation; and route inputs into administrative or decision-making workflows with appropriate logging and public feedback. CEPs are not limited to government use: they may be operated directly by public authorities, on their behalf, or by non-governmental and civil society organizations pursuing public-interest objectives (Farina, 2014; Martínez-Gil et al., 2025).

Data governance

The set of principles, decision rights and accountability arrangements that determine who can decide what about data (e.g. collection, access, sharing, retention, reuse) and under which conditions, across the full data lifecycle (Khatri & Brown, 2010; OECD, 2022a). It is distinct from data management, which focuses on day-to-day implementation.

AI governance

A specialised layer of data governance that focuses on policies, roles and processes for the design, procurement, deployment, monitoring and decommissioning of AI systems, including how AI systems use data and how their impact on rights and democratic processes is assessed (OECD, 2019a; ITHACA Consortium, 2025).

Data lifecycle (in the CEP context)

The sequence of stages of CEP-related data: creation/collection, ingestion, storage, transformation, use, access and sharing (including open-data release), documentation, archival and deletion, for all data categories identified in Section 1.

Personal data

Any information relating to an identified or identifiable natural person, including user/account data, participation content, logs and metadata where individuals can be singled out, directly or indirectly (European Parliament & Council of the European Union, 2016a).

Special categories of personal data (sensitive data)

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for identification, health data or data concerning sex life or sexual orientation. In a CEP, political opinions and related information are particularly salient (European Parliament & Council of the European Union, 2016).

Controller and Processor of personal data

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (European Parliament & Council of the European Union, 2016a; EDPB, 2020).

Provider and deployer of AI systems

Under the AI Act, ‘provider’ means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge; ‘deployer’ means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity;(European Parliament & Council of the European Union, 2024a).

In the CEP context, municipalities or project partners typically act as deployers, while vendors or open-source communities act as providers.

4. Data Governance Requirements

4.1 Data Governance Rules and Controls for the ITHACA platform and other AI-enabled CEPs

Building on the legal analysis in Chapter 2, as well as on the practical experience from the design, deployment and assessment of the ITHACA Platform (including the DPIA and Privacy by Design/Default report), the following data governance rules and controls constitute the binding internal rules for all ITHACA partners. At the same time, these rules form a reusable governance blueprint for AI-enabled CEPs, as well as baseline rules that future AI-enabled CEPs can adopt or adapt as a concrete “result” of the project’s implementation.

Rule 1 – Lawful data processing

All processing of personal data must rely on a lawful basis under Article 6 and/or Article 9 GDPR. Use of this data for other purposes is prohibited unless a new lawful basis or explicit, informed consent is obtained.

Rule 2 – Data minimization

Only data strictly necessary for the stated civic-participation purposes may be collected. Non-essential cookies and analytics tools may operate only after explicit opt-in consent.

Rule 3 – Storage and retention

Retention periods are predefined:

- User registration data - Project duration + 12 months
- Logs - 6 months
- Compliance data and audit files - 5 years.

Deletion must be irreversible and documented in a specific register maintained by each partner.

Rule 4 – Access control

Access to any dataset must be on a strictly need-to-know basis and the relevant logs must be retained.

Each ITHACA partner must keep an access control list reviewed quarterly. Use of personal or non-corporate accounts for project data storage is prohibited.

Rule 5 – Security and encryption

Encryption in transit and at rest (TLS 1.3 / AES-256 or equivalent) is mandatory for all personal or confidential data.

Passwords must comply with ISO 27001 complexity and renewal standards. Non-corporate devices may not locally store the platform’s data.

Rule 6 – Data sharing and transfers

Data sharing to external parties is allowed only with DPO's prior written approval and a valid legal basis.

Cross-border transfers must rely on EU adequacy decisions, SCCs, or DGA-compliant mechanisms. All sharing events must be logged in a specific register.

Rule 7 – Accountability and documentation

Each ITHACA partner must maintain the following living registers:

- Record of Processing Activities (RoPA)
- AI System Registry
- Incident and Breach Log Updates are reported quarterly.
- Dataset templates and the allocation of roles for their completion are provided in D7.2; mandatory registers (RoPA, AI Registry, Incident Log) shall be governed by this Rule 7.

Rule 8 – Data-subject rights

Requests for access, rectification, erasure, restriction, portability, or objection must be acknowledged within 24 hours and fulfilled within 30 days. Refusals require written justification and DPO approval.

Users shall have clear, accessible online channels to exercise their rights.

Rule 9 – Incident and breach management

Suspected breaches must be reported internally within 24 hours.

Notifiable incidents, such as cybersecurity events and breaches of personal data, must be reported to the competent authorities within the time frames specified by applicable national and EU law.

Every incident needs to be recorded, evaluated, and then followed by recorded corrective and preventive measures.

Rule 10 – Audit and compliance enforcement

DPO conducts annual internal audits covering privacy, security, and AI-risk governance. Findings are binding and subject to corrective action within 30 days. Persistent non-compliance may lead to suspension of data access and notification to REA.

Rule 11 – Inclusiveness and accessibility

All platform interfaces, data visualisations, and participation tools shall comply with the WAD, the EAA, as well as with the WCAG 2.1 AA standards.

Information must be presented in clear, plain language, available in local languages of pilot cities, and usable by persons with disabilities. AI-based functionalities (translation, summarisation, moderation) shall be continuously tested for fairness, inclusivity, and accessibility bias.

Rule 12 – Interoperability and open standards

Data formats, APIs, and metadata shall comply with:

- FAIR Principles (Findable, Accessible, Interoperable, Reusable);
- Interoperable Europe Act (EU) 2024/903;
- ODD.

The ITHACA platform must expose interoperable APIs enabling lawful data reuse for research and policy purposes, subject to ethical review and consent mechanisms.

Rule 13 – Removal of unlawful or non-compliant content

When the ITHACA platform publicly disseminates user content, the following apply under the DSA:

- Notice-and-Action mechanism: Users may flag allegedly illegal or ToS-breaching content through a dedicated form or button.
- Assessment & Removal: Moderators must review notices in good faith, remove or disable access to unlawful content, and document decisions in the transparency log.

- Statement of Reasons: Affected users receive a written notice detailing the decision and available remedies.
- Complaint Handling: Users can appeal moderation decisions via the internal complaints mechanism; persistent disputes may be referred to certified out-of-court bodies.

Rule 14 – Review and update

- The legal and ethics compliance rules set out in this document-covering data protection, AI governance, platform governance, cybersecurity and democratic safeguards-are subject to structured, periodic review. At least once per year, and whenever there is a material change in law (e.g. new EDPB guidance, AI Act implementing acts, DSA secondary legislation, NIS2 national transposition) or in the platform’s use, the CEP’s operator convenes a review along with the DPO, legal counsel, AI governance lead and Ethics Advisory Board. This review assesses whether the existing rules remain accurate, proportionate and effective in light of updated legal requirements, ethical standards, case law and supervisory guidance, and whether any gaps have emerged (e.g. new AI functionalities, new categories of vulnerable users, new cross-border data flows).

4.2 Key results of the Data Protection Impact Assessment for ITHACA platform

The ITHACA partners carried out a Data Protection Impact Assessment (DPIA) for its operation as a CEP in line with Article 35 GDPR and the EDPB relevant Guidelines. The assessment covered the full data lifecycle of the platform - registration, participation, moderation, analytics, - as well as cross-cutting governance processes such as role allocation, logging and security. It combined legal analysis with technical and organisational input from all relevant partners, and explicitly took into account the types of data and risk scenarios already identified in the Privacy by Design and by Default report and in the Records of Processing Activities.

The DPIA identified a set of high-risk areas. First, the large-scale processing and online publication of participation content that can directly or indirectly reveal political opinions and other special categories of data raises heightened risks for rights and freedoms, including chilling effects on participation - if users perceive surveillance or profiling. Second, the use of AI components introduces risks of bias, lack of explainability and over-reliance on automated suggestions, which may affect the visibility and perceived legitimacy of contributions and exacerbate existing inequalities in participation.

On this basis, the DPIA proposes a reinforced package of safeguards for AI-enabled CEPs, which are embedded in the aforementioned Data Governance Rules and Controls, the Data Lifecycle Governance (Chapter 5) and the risk-management framework (Chapter 6). Concretely, these include strict data-minimisation and purpose-limitation rules for all personal data categories, predefined retention periods and deletion procedures, role-based access control, encryption, pseudonymisation/anonymisation for research and testing datasets, and a multi-layered transparency and consent model.

5. Data Lifecycle Governance

5.1 Data Collection

5.1.1 Lawful bases for data collection in CEPs

For CEPs, every element of collecting personal data must be linked to a clearly defined purpose and a corresponding lawful basis under Articles 6 and 9 GDPR (European Parliament & Council of the European Union, 2016a). In practice, it is helpful to work with “processing clusters” (e.g. registration,

public display of content, analytics, AI training, secondary research) and assign a lawful basis to each cluster rather than to individual fields.

For core participation functions-user registration where necessary, publication of proposals and comments, voting/endorsements, institutional feedback, archiving of processes-public authorities will typically rely on:

- Article 6(1)(e) GDPR (task carried out in the public interest / exercise of official authority), when the CEP is used to perform democratic or consultative functions laid down in law or in formal mandates; and/or
- Article 6(1)(c) GDPR (legal obligation), where specific Union or national provisions require certain records to be kept (e.g. public registers, transparency or audit rules).

For optional or add-on features-such as newsletters, certain types of behavioural analytics, or community functions not strictly necessary for the participation process-Article 6(1)(a) (consent) may be appropriate, and in non-public settings sometimes Article 6(1)(f) (legitimate interests), subject to a balancing test.

Because participation content often contains or reveals special categories of personal data, particularly political opinions, controllers must also identify a legal basis under Article 9(2) GDPR. Depending on the national framework, this will usually be either:

- Article 9(2)(g), where Union or Member State law recognises processing as necessary for reasons of substantial public interest (e.g. democratic participation), coupled with specific safeguards; or
- Article 9(2)(a), explicit consent, where participation in a given sensitive process is clearly optional, consent is truly free and withdrawal is always possible.

5.1.2 Consent as a legal basis

Consent is one legal basis among several, but in a democratic participation context it must be treated carefully and sparingly. Under Article 4(11) GDPR and EDPB guidelines, valid consent must be freely given, specific, informed and unambiguous, with a clear affirmative act (EDPB, 2020b). In CEPs this implies:

- No conditional access to core participation on non-essential consent. Users should not be required to consent to extensive tracking or secondary uses just to submit a proposal or vote. If consent relates to optional analytics, reuse for research purposes or newsletters, refusal or subsequent withdrawal must not affect access to the core democratic function.
- Granular consent and purpose limitation. Separate consent options should be provided for clearly distinct purposes (e.g. “statistics/analytics”, “email updates”, “reuse of anonymised content for research”), avoiding bundled “accept everything” mechanisms.
- Clear information and withdrawal of consent. Users must receive clear information, in plain language, about what they are consenting to, and they must be able to withdraw consent at any time through simple, accessible mechanisms. Withdrawal should stop further processing for that purpose, without negative consequences for the main participation process.

At governance level, CEPs’ operators should maintain a central consent-management mechanism that serves as a record of consent status per user and per purpose. This mechanism should:

- log when and how consent was obtained, including the version of the information/consent notice shown at that time;
- expose a simple interface (e.g. “My settings”) where participants can review and change their choices;
- be technically integrated so that services such as analytics tools or AI training pipelines check consent before using data for optional purposes.

This avoids fragmented consent handling across modules and supports accountability under Article 5(2) GDPR.

5.1.3 Data minimisation and transparency notices

Data minimisation (Article 5(1)(c) GDPR) requires CEPs to design data entry points so that data are adequate, relevant and limited to what is necessary for the defined participation purposes (European Parliament & Council of the European Union, 2016a). In practice, this means:

- Account and identity data: collect only what is needed for eligibility and communication (e.g. email, municipality, age bracket where relevant). Avoid routine capture of detailed demographic profiles or political affiliations unless these are essential to the specific process and justified in a DPIA.
- Participation forms: limit mandatory fields to the minimum; structure questions to reduce unnecessary exposure of sensitive data; clearly indicate where content will be public and for how long.
- Logs and technical data: configure logging and analytics at the minimum granularity in order to meet security and evaluation needs.
- AI-related data: retain only the inputs, outputs and feedback necessary to provide and monitor the AI functionality; avoid “function creep” where AI logs are silently reused for unrelated profiling or secondary research without a new lawful basis and updated transparency information.

Alongside data minimisation, transparency under Articles 12–14 GDPR is a central requirement and a condition for trust. A robust CEP data-governance framework should adopt a multi-layered notice model:

- A general privacy notice for the platform explaining controllers/processors, categories of data, main purposes, lawful bases, recipients, retention, international transfers (if any), rights and contact points (including the DPO).
- Just-in-time notices at sensitive points-for example, when an AI feature is used (“This summary is generated by an AI system”) or when a user action will have long-term public visibility (“Your contribution will remain publicly visible after the process ends”).

All notices should be written in clear language, available in relevant languages, and implemented in accessible formats consistent with the WAD and the EN 301 549 (European Parliament & Council of the European Union, 2016b; ETSI, 2021). This ensures that people with disabilities or lower literacy can understand how their data is handled.

5.1.4 Cookies, local storage and similar technologies (ePrivacy)

Collection of data via cookies, local storage, and other identifiers on user devices is governed by Article 5(3) of the e-Privacy Directive, which requires prior informed consent before storing or accessing information on a user’s device, except where the technology is “strictly necessary” to provide a service explicitly requested by the user (European Parliament & Council of the European Union, 2002). The GDPR consent standard applies equally in this context (EDPB, 2020b).

For CEPs, this leads to three core governance requirements:

1. Comprehensive inventory and categorisation

CEP operators should maintain an up-to-date list of all cookies and similar technologies, i.e.:

- Strictly necessary (e.g. session cookies for authentication and security, load balancing, remembering accessibility settings, storing consent choices).
- Preferences (e.g. language or layout settings where not strictly essential).

- Analytics and performance (e.g. tools measuring usage and page views).
- Marketing or cross-site tracking (generally inappropriate for public-interest CEPs and should normally be avoided).

2. Consent for non-essential technologies

For any cookie or tracker that is not strictly necessary, the platform must obtain opt-in consent before activation. In practice this means that:

- non-essential cookies are disabled by default until the user has actively chosen them;
- the consent interface clearly explains purposes and allows granular choices (e.g. “analytics on/off”), with refusal as easy as acceptance; access to core participation functions is not conditioned on accepting analytics or tracking cookies (“no cookie walls” for the main democratic service)

A concise cookie and tracking policy, linked from the banner and the privacy notice, should describe categories, purposes, retention and third-party involvement. Together with the consent-management system, this forms part of the CEP’s accountability for data collection under both GDPR and ePrivacy regime.

5.2 Data Classification

5.2.1 Purpose of data classification in CEPs

Data classification is the bridge between abstract legal requirements and day-to-day handling rules. For CEPs, it determines which data are subject to which regulatory regimes and safeguards and thus guides security levels, access rights, retention, reuse and eligibility for “open data” publication. International guidance treats classification as a cornerstone of data governance: data should be categorised according to sensitivity, regulatory status and intended use so that handling rules are clear and enforceable.

In CEPs, classification must work across the data categories of Section 1.3: user and account data; participation and deliberation content; process metadata; technical logs and analytics; governance and compliance data (including moderation); and AI-related data (training, validation and monitoring logs). The same data category may contain several classes at once (e.g. a single log file can include personal identifiers, security-sensitive events and non-personal aggregate metrics).

5.2.2 Core categories

a) Personal data.

For CEPs, this typically includes:

- account and profile data (identifiers, contact details, roles)
- participation records linked to a user (proposals, comments, votes, survey responses, endorsements);
- process metadata tied to individuals (timestamps, process IDs, status changes);
- logs and analytics where user actions can be linked to a device or user account;
- governance data, such as consent records, rights-request logs and moderation decisions referring to specific users.

Even if participation content is made public, it remains personal data as long as individuals are identifiable (e.g. by username, context or content details).

b) Special categories of personal data.

In CEPs, the following dimensions are especially salient:

- explicit political opinions and positions expressed in proposals, comments or survey responses;
- information that indirectly reveals sensitive attributes (e.g. participation in disability-focused consultations).

These data require increased protection, and particularly a separate legal basis under Article 9(2) GDPR.

c) Other regulated data (non-personal)

Not all regulated data are personal. Non-personal data may still be subject to sectoral legislation, confidentiality obligations, intellectual-property or trade-secret protection, cybersecurity requirements or national-security considerations. In CEPs, examples include:

- security and incident logs revealing vulnerabilities or attack patterns;
- algorithm configuration parameters or models protected as trade secrets;
- data falling under specific sectoral regulations (e.g. procurement processes, financial information in budget consultations).

d) Non-personal and anonymised data

Non-personal data include data that are never related to an identifiable person and data that have been irreversibly anonymised so that individuals are no longer identifiable, taking into account all means reasonably likely to be used (Recital 26 GDPR). In CEPs this may cover:

- aggregate participation statistics (number of proposals per district, vote counts per option);
- anonymised datasets where direct and indirect identifiers have been removed or robustly transformed.

5.2.3 Open data and reusable information

For public-sector CEPs, classification must also support decisions on reuse of data and openness. The ODD (European Parliament & Council of the European Union, 2019a; European Commission, 2024b) establishes common rules for making public-sector information reusable and promotes an “open by design and by default” approach, including the notion of “high-value datasets” that should be freely available in machine readable formats via APIs. The DGA (European Parliament & Council of the European Union, 2022a) complements this with mechanisms to increase the availability and trusted sharing of both personal and non-personal data, including public-sector data subject to rights or confidentiality.

Within CEPs, it is useful to distinguish at least three “openness” sub-classes:

- Internal-only data: accessible only to authorised staff (e.g. raw logs with identifiers, internal moderation notes, security events, detailed AI training/validation datasets).
- Restricted-sharing data: may be shared under controlled conditions (e.g. with researchers under agreements; within data spaces governed under the DGA) but not published openly.
- Open data / public data: datasets that can be made publicly available for reuse, typically non-personal or robustly anonymised, or public-domain content where no rights or legitimate interests are infringed (e.g. aggregated statistics, anonymised deliberation datasets,

documentation).

5.2.4 Applying classification to CEP-related data categories

A practical framework for CEPs should apply the above categories consistently across the data categories identified in Section 1.2:

User and account data

Almost always personal data; may include special categories if users voluntarily disclose them (e.g. disability status, political affiliation). Normally internal-only.

Participation and deliberation content

Personal data whenever linked to an identifiable person; frequently contains special-category data (political opinions, sometimes health or union membership). Public visibility on the platform does not change this classification. Any reuse for AI training, evaluation or open data must start from this assumption.

Process and participation metadata

Often personal data (e.g. timestamps linked to user IDs, participation histories); some elements can become non-personal when aggregated.

Technical logs and analytics

Typically contain personal data (IP addresses, device identifiers, session IDs) and security-sensitive regulated data (e.g. failed login attempts, attack patterns). Raw logs should be internal-only; derived aggregates can often be non-personal and, in some cases, candidates for restricted or open publication (e.g. high-level usage statistics).

Governance and compliance data (including content-moderation data)

Data subject requests' records, consent logs, ToS acceptance, statements of reasons, appeals and moderation actions all constitute personal data referring to specific users. Moderation categories may reveal or imply special-category attributes or allegations ("racist content", "health misinformation") and should be treated with particular care. These datasets are generally internal-only or, at most, subject to highly controlled sharing (e.g. for audits or research under agreements).

AI-related data

Datasets used to develop, deploy, evaluate and monitor the AI functionalities integrated into the CEP. AI-related data are generally internal-only, because training sets often contain personal data or may reveal sensitive attributes, participation patterns, or protected characteristics. Under certain conditions, like secure processing environments for vetted researchers, it may be possible to share some data with restrictions when the datasets have been properly anonymized.

5.3 Data Storage, Retention & Deletion Policies

5.3.1 Governance objectives

For CEPs, rules about storage, retention and deletion determine where data is stored, who can access it, for how long it is kept, and how it is securely erased. These rules operationalise GDPR principles (integrity and confidentiality, storage limitation, accountability), cybersecurity obligations under NIS2/CRA, and open-data/archival requirements, where CEPs are part of the public record (European Parliament & Council of the European Union, 2016a, 2019a, 2022a, 2022c, 2024; ENISA, 2023).

5.3.2 Storage and access control

Data should be stored only in approved locations (e.g. defined data centres/regions, approved cloud services) and in line with contracts and data-transfer rules. For each data category (Section 1.2), CEPs' operators should define:

- Authorised repositories (databases, file stores,) including geographic location and backup arrangements.
- Role-based access controls (RBAC): access rights tied to governance roles (Section 3.1) and to the “need-to-know” principle (e.g. moderators can see reported content but not all security logs; AI developers see curated training sets, not full raw logs).
- Strong authentication and session management for administrative interfaces, in line with NIS2/CRA security practices (e.g. MFA for admin roles, strict session timeouts).

Access control configurations and changes should be logged and periodically reviewed by the CISO and DPO.

5.3.3 Encryption and integrity

To protect CEPs' data against unauthorised access and tampering, the framework should require:

- Encryption in transit (TLS for all user and admin traffic, secure protocols for internal services).
- Encryption at rest for databases, file systems and backups that store data, with managed keys and restricted key access.

5.3.4 Retention periods

The storage limitation principle requires that data should be kept “no longer than is necessary” for the purposes for which they were collected (Article 5(1)(e) GDPR). Retention rules for CEPs should be defined per data category and per processing purpose.

5.3.5 Deletion and anonymisation methods

When data reach their retention period, or when users exercise their right to erasure, where applicable, CEPs' operators must ensure effective deletion or anonymisation of the data.

- Deletion methods appropriate to the storage medium (e.g. secure overwrite or cryptographic erasure for disks).
- Anonymisation or aggregation processes where continued use is needed for statistics or research, applying techniques robust enough to meet GDPR's standard for anonymisation (Recital 26) and avoiding small-cell re-identification risks.

CEPs' operators should keep deletion/anonymisation logs for accountability and demonstrate compliance in audits or inspections (EDPB, 2019; ENISA, 2023).

5.4 Data Use, sharing & reuse

An important aspect of any AI-enabled CEP, including the ITHACA platform, is the robust governance of data use, external sharing and secondary reuse. This section sets out general rules and procedures for CEPs, which are implemented concretely in ITHACA but are intended as a reusable blueprint for similar platforms.

All internal data collected and processed within a CEP are primarily used for its operational functions, analytical purposes and documentation of participation processes. This ensures proper functioning and continuous improvement. Access to any internal dataset should be granted strictly on a “need-to-know” basis and monitored through role-based access control and periodic reviews, in line with Rule 4 – “Access Control”.

External sharing of data from a CEP is subject to strict guidelines to protect personal data, source code and other confidential information. Such sharing is permitted only with prior written approval from the competent governance function (e.g. DPO) and must always rely on a valid legal basis (Rule 6 – “Data Sharing and Transfers”) (European Parliament & Council of the European Union, 2016a, 2022a).

In line with the principle “as open as possible, as closed as necessary” (see Section 6.2.1 – Open Data Scope), CEPs’ operators should make selected data and documentation openly available whenever legally and ethically possible, while minimising and clearly justifying any restrictions. Typical examples of data sets suitable for open publication include aggregated participation statistics, engagement metrics and sufficiently anonymised or synthetic datasets derived from citizen interactions.

The secondary use of data for exploitation or research purposes requires careful planning and a clear understanding of which stakeholders will potentially reuse CEP data (e.g. researchers, policymakers, civil-society organisations, other public authorities). In line with Rule 12 – “Interoperability and Open Standards”, and in order to facilitate lawful reuse of data for research and policy purposes, CEP operators should provide external stakeholders with stable, well-documented APIs specifying input/output schemas, authentication mechanisms and usage policies. Any reuse of data via these interoperable APIs remains subject to the applicable lawful bases, ethical review and, where required, consent mechanisms.

Key stakeholder groups across CEPs typically include:

- Municipalities and public authorities: using the platform for consultations, public polls, participatory planning and policy co-creation.
- Polling, market-research and e-governance solution providers: leveraging CEP data and workflows to enrich their citizen-feedback and engagement services.

All stakeholders using CEP data must assume responsibility for the users and processing operations within their scope. Data sharing must be conducted in a way that ensures safety for both data subjects and receiving parties. Comprehensive documentation on platform usage, data-handling protocols and role allocation should be made available to all relevant actors.

A further potential secondary use of CEP data is participation in regulatory sandboxes. These are controlled environments, typically established by regulatory authorities, that allow innovative products, services or business models to be tested under adapted regulatory requirements for a limited period. For an AI-enabled CEP, this may involve using platform data in such sandboxes to test new civic-engagement tools or AI systems, while still respecting this Framework’s governance rules and the underlying legal obligations.

Technical monitoring is also essential. CEP operators should adhere to a common security baseline applicable to all systems and data-processing activities, as detailed in Section 5.4 – Security Baseline. This includes encryption, anonymisation/pseudonymisation where appropriate, robust access control, and continuous monitoring and logging of security-relevant events.

Finally, addressing potential negative implications-such as toxic speech or unlawful content-falls under Rule 13 – “Removal of Unlawful or Non-Compliant Content”. CEPs should implement systems that can automatically flag potentially toxic or unlawful content, trigger a human review process and

support timely action. Moderators are responsible for assessing such notices, removing or disabling access to unlawful or rule-breaking content, and documenting their decisions, with clear procedures for complaint handling and remedies.

This approach to data utilization, external sharing and secondary reuse-combining strict internal controls, carefully framed openness, interoperable APIs, readiness for regulatory sandboxes and a strong security and moderation baseline-is applied in ITHACA and proposed as a transferable governance model for AI-enabled CEPs more generally.

6. Accountability, Transparency & Human Oversight

6.1 Internal Documentation

Internal documentation is the backbone of accountability for CEPs. It makes it possible to show how data and AI systems are governed, not only to supervisory authorities and auditors, but also to institutional owners and the public. Under GDPR, controllers and processors must be able to demonstrate compliance (Articles 5(2), 24, 30). The AI Act adds detailed documentation and monitoring duties for AI systems, and NIS2 requires evidence of cybersecurity and supply-chain risk management (European Parliament & Council of the European Union, 2016a, 2022b, 2024a).

6.1.1 Records of Processing Activities (RoPA) for CEPs

Article 30 GDPR requires controllers and processors to maintain Records of Processing Activities (RoPA) and to present them to supervisory authorities on request. For CEPs, the RoPA should not be a generic corporate template but an organised map of platform-related processing activities, such as:

- user registration and account management;
- publication of proposals, comments and votes;
- survey and poll management;
- analytics and reporting on participation;
- content moderation and complaint handling;
- AI-assisted functionalities (ranking, recommendation, summarisation, assistive moderation);
- secondary uses (research, evaluation, open-data publication).

For each processing activity, the RoPA should at least capture the elements listed in Article 30(1)–(2) GDPR (e.g. purposes, categories of data subjects and data, recipients, transfers, retention periods, security measures),

6.1.2 AI system registry and transparency logs

The AI Act requires providers of high-risk AI systems to maintain technical documentation and a post-market monitoring system that evidences compliance over the AI system lifecycle. Even where CEPs' AI tools are not always classified as high-risk, similar documentation is emerging, as best practice.

For CEPs, this translates into an internal AI system registry that, for each AI component (e.g. recommender, summariser, toxicity detector, spam filter, translation engine), records at least:

- role in AI value chain (provider and deployer), version, deployment context.

- intended purpose and integration point in the CEP;
- main input and output types, including whether personal or data of special categories are involved;
- AI-Act classification (high-risk, limited-risk, GPAI model, etc.);
- links to technical documentation, risk assessments, DPIAs/FRIAs and monitoring reports.

Alongside the AI system registry, CEPs should maintain logs for automated or AI-assisted operations that affect users, in particular:

- content-moderation actions (removals, demotions, labelling, account restrictions);
- automated ranking/recommendation decisions that materially influence visibility;
- AI outputs that are shown to users as “summaries”, “recommendations” or “highlights”.

6.2 Audit & Reporting

For CEPs, audits and structured reporting are the main mechanisms to verify that governance rules are actually applied and to evidence compliance to institutional owners, regulators and the public. They operationalise GDPR’s accountability principle (Articles 5(2), 24, 32), the AI Act’s monitoring duties for AI deployers, NIS2’s requirements on risk management and supervision, and-where applicable-the Digital Services Act’s (DSA) transparency and auditing obligations for online platforms (European Parliament & Council of the European Union, 2016a, 2022a, 2022b, 2024a).

6.2.1 Internal and external audits

A CEP governance framework should provide for both internal and, where proportionate, external audits.

Internal audits review whether data-governance rules are implemented in practice: RoPA completeness; effectiveness of access control and retention rules; AI registry accuracy; execution of DPIAs/FRIAs; handling of data subject rights requests; implementation of cookie and consent policies; and accessibility of notices and interfaces.

External audits or assessments may be commissioned periodically to obtain an independent view on privacy, AI governance, security and accessibility. For entities in scope of NIS2 or for deployers of high-risk AI systems, such independent assurance is increasingly seen as good practice (ENISA, 2023).

6.2.2 Risk-register reviews

Risk management for CEPs should be captured in a central risk register covering:

- privacy and data-protection risks,
- AI-related risks (bias, over-reliance on automated outputs, explainability gaps),
- security/cyber risks (availability, integrity, confidentiality, supply chain),
- democratic-process and fundamental rights risks (exclusion, manipulation, lack of transparency, impact on freedom of expression).

The framework should require regular reviews of this register, updating risk scores, implemented controls, incident learnings, and planned mitigation actions.

6.2.3 DSA transparency reporting

If a CEP qualifies as an “online platform” under the DSA (e.g. it hosts user-generated content and provides dissemination to the public), it may be subject to DSA transparency obligations, including annual transparency reports detailing content-moderation activities (Articles 14–15 DSA).

6.3 Data-Subject Rights Requests and illegal content reporting

For CEPs there are two distinct but interlinked channels that must be clearly governed: data subject rights requests (DSRs) under GDPR and notices about illegal or rule-breaking content (including toxic speech), which fall under content-governance and, where applicable, the DSA (European Parliament & Council of the European Union, 2016a, 2022a).

CEPs should offer a simple, visible DSR entry point (“Your data rights”) explaining rights in plain language and providing an online form plus alternative contact options. Requests are categorised (access, rectification, erasure, restriction, objection, portability), verified with proportionate identity checks and answered within one month (Articles 12–17 GDPR).

In parallel, each content item (proposal, comment, etc.) should have a “Report content” function for illegal content or toxic speech. The form collects only essential data, provides distinct categories (e.g. illegal hate speech, threats, harassment, violation of participation rules), and supports a moderation workflow with documented decisions (European Parliament & Council of the European Union, 2022a).

6.4 Security Baseline

A harmonised security baseline is essential for AI-enabled CEPs to ensure a minimum, consistent level of protection for personal and non-personal data and to support compliance with GDPR, ethics commitments and the technical governance rules defined for each platform. Drawing on the ITHACA project, this section sets out such a baseline, which applies to all partners, systems and data-processing activities within the project and is proposed as a model for AI-enabled CEPs more broadly.

At minimum, all ITHACA partners must implement the following controls:

- i. **Encryption:** State-of-the-art encryption (e.g. TLS for data in transit and appropriate encryption for data at rest), especially for personal, sensitive or operationally critical information.
- ii. **Anonymisation / pseudonymisation:** Use of anonymisation or pseudonymisation for research, analytics, testing or demonstration datasets, in accordance with data-minimisation and purpose-limitation obligations.
- iii. **Access control:** Role-based access control, least-privilege principles, strong authentication and periodic review of user permissions for all systems handling project data.
- iv. **Vendor and supply-chain risk management:** Basic due diligence and contractual safeguards for cloud services, external platforms and third-party tools used in the project, including mandatory security and privacy clauses, vulnerability notification and minimum technical controls.
- v. **Monitoring and logging:** Security-relevant events must be monitored and logged when proportionate, supporting incident detection and compliance verification, while respecting data-protection requirements.
- vi. **Incident response:** All ITHACA partners must maintain incident-response procedures compatible with the project-wide breach-management rules (Section 5.7), ensuring timely containment, investigation and recovery.

Any references in D7.2 or other technical deliverables are summaries only; this section is the authoritative definition of the ITHACA security baseline.

6.5 Risk Assessment Methodology

A structured, repeatable risk-assessment methodology is essential for AI-enabled CEPs in order to identify, evaluate and mitigate data-related and AI-related risks throughout the lifecycle of the platform and its supporting components. Drawing on the ITHACA project, this section describes such a methodology, which integrates GDPR, ethics, secure-by-design and AI transparency/oversight requirements already defined in the project and is proposed as a model for other AI-enabled CEPs.

The methodology includes:

- Risk identification: Systematic identification of risks to individuals' rights and freedoms, data quality, system integrity and democratic processes, including risks stemming from AI components (e.g. bias, lack of explainability, over-reliance on automated outcomes).
- Risk analysis and evaluation: Risks are assessed using a common scale (likelihood × impact), considering the nature and sensitivity of data, the context of processing, the operational role of AI and existing controls.
- Mitigation planning: Appropriate organisational and technical measures are selected and documented, e.g. privacy-by-design controls, security measures (Section 5.4), transparency mechanisms, human-oversight checkpoints, data-quality controls and constraints on AI model deployment or use.
- Documentation and traceability: All significant risks, assessments and mitigation actions are recorded.

6.6 Platform Governance

Where a CEP is public-facing and hosts user-generated content, platform governance must comply with the DSA in addition to data-protection and AI-governance obligations. With respect to the ITHACA platform, the following measures apply and are proposed as a governance template for similar CEPs:

- a) Terms and Conditions: Clarity and Accessibility (DSA Art. 14)

The platform's Terms and Conditions (T&Cs) clearly describe the service, participation rules, content standards, moderation approach (including any use of automated tools or AI) and the rights and obligations of users. T&Cs are written in plain, accessible language, easily accessible from all main user interfaces.

- b) Notice-and-Action Mechanism (DSA Art. 16)

Users and trusted flaggers can report allegedly illegal or rule-breaking content via a dedicated "Report content" function attached to each item. The form is simple, collects only minimal data, allows categorisation of the issue (e.g. illegal hate speech, threats, harassment, violation of platform rules) and supports a structured moderation workflow. Notices are assessed diligently and in a timely manner, with decisions documented in transparency logs.

- c) Statement of Reasons to Affected Users (DSA Art. 17)

When content is removed, restricted, demoted or otherwise moderated-or when an account is suspended or terminated-the affected user receives a "statement of reasons" explaining what decision was taken, whether automated tools were used and what remedies are available.

d) Internal Complaints Handling (DSA Art. 20)

The platform offers an internal complaint mechanism allowing users to contest moderation decisions within a reasonable period. Complaints are handled by human reviewers, not solely automated tools, and outcomes (including reversals or confirmations) are documented. Statistics and recurring patterns identified through complaints feed into ongoing risk monitoring and policy updates.

7. Interoperability and Data Standards

This chapter sets out the core principles and minimum obligations for interoperability, data formats and metadata standards for the ITHACA project and, by extension, for research and innovation (R&I) projects that design, pilot or deploy CEPs. It translates FAIR and open science commitments into practical rules for project partners (Wilkinson et al., 2016; European Commission, 2024d; OpenAIRE, 2022).

The detailed technical implementation (repositories such as Zenodo or others, exact metadata template, Creative Commons licence options, and preferred formats such as CSV/XLSX/SPSS) is defined in D7.2 for ITHACA. In case of divergence, the legal and ethical constraints defined in this data governance framework prevail.

All ITHACA partners must apply the rules provided herein whenever they process data related to the ITHACA project in any way, regardless of whether the data are ultimately open, restricted or closed. R&I projects developing CEPs can adopt the same structure as a project-wide baseline for data interoperability and open science.

7.1 Metadata Standards and FAIR Principles

ITHACA adopts the FAIR principles (Findable, Accessible, Interoperable, Reusable) as the key reference baseline for all datasets and related documentation. The same approach is recommended for other R&I projects on CEPs, to ensure that participation-related data can be located, understood and reused within and beyond the project.

7.1.1 Minimum metadata requirements

Metadata are mandatory for every dataset created or substantially transformed in the project. Each dataset must be registered in the central project dataset inventory (maintained under D7.2) using a common metadata template. As a minimum standard, metadata shall include:

- i. Title, short description, creator(s), affiliation
- ii. Date of creation / last update and related WP / Task / pilot
- iii. Data type and formats (e.g. CSV, XLSX, SPSS)
- iv. Access level (open / restricted / closed) and justification
- v. Licence (for open data) or access conditions (for restricted data)
- vi. Persistent identifiers (e.g. DOI) and links to related publications, code or documentation.

Metadata should be structured and machine-readable (e.g. JSON-LD, XML) and, where possible, use standard vocabularies and code lists (European Commission, 2024e).

7.1.2 Findability and accessibility

To ensure datasets are findable, all public datasets deposited in external repositories receive a persistent identifier, while the central dataset inventory records all Persistent Identifiers, repository links and access conditions.

To ensure datasets are accessible, open or shared datasets are deposited in Zenodo or other trusted repositories defined in D7.2. Repository access levels (open, embargoed, restricted) must match the access level described in the metadata, and repositories should support long-term preservation and export to open formats.

7.1.3 Interoperability and reuse

To ensure interoperability, data should be stored and shared in non-proprietary, widely used formats (e.g. CSV for tabular data, JSON for semi-structured or log data). Proprietary formats (e.g. XLSX, SPSS) may be kept for convenience but not as the only option. Where feasible, data structures and metadata should align with common EU and domain standards (e.g. DCAT-AP-inspired catalogues, standard survey metadata fields) (European Commission, 2024e).

For reuse, open datasets will be published under Creative Commons licences (e.g. CC BY, CC BY-SA, CC0), as specified in D7.2 and consistent with the project's IPRs and exploitation plans. Each dataset will be accompanied by sufficient documentation (e.g. codebook, methodology, processing steps) to enable meaningful reuse, and its versions, known limitations and potential biases will be clearly recorded, especially for datasets used to train or evaluate AI components.

7.2 Open Data and Interoperability Obligations

This section describes the obligations adopted in the ITHACA project regarding open data, APIs and technical interoperability. At the same time, it proposes these obligations as baseline standards for AI-enabled CEPs developed in R&I projects, in line with Horizon Europe open science requirements, the Open Data Directive and the emerging Interoperable Europe framework (European Commission, 2024d; European Parliament & Council of the European Union, 2019a, 2024c; European Commission, 2024b).

7.2.1 Scope of open data

In the ITHACA project – and, by extension, as a recommended standard for CEPs – the principle “as open as possible, as closed as necessary” applies. Data and documentation should be made open whenever legally and ethically possible, while any restrictions (e.g. due to GDPR, confidentiality, security or IPR) must be minimised and clearly justified.

Within ITHACA and comparable CEP deployments, typical candidate open datasets include:

- Aggregated pilot statistics and engagement metrics;
- Anonymised or synthetic datasets derived from citizen interactions;
- Evaluation or configuration datasets for AI tools, where personal data and sensitive attributes are properly protected.

Where ITHACA platform – or another CEP – generates datasets aligned with high-value themes (e.g. public participation, public-sector performance), operators should prioritise publication in machine-readable formats and under open licences, to support reuse by researchers, civil society and public authorities (European Parliament & Council of the European Union, 2019a; European Commission, 2024b).

7.2.2 APIs and platform interoperability

ITHACA's platform and related services will expose documented, stable APIs (e.g. REST/JSON) to support data access and integration. The same approach is recommended as a good practice for CEPs developed in R&I projects:

- API input/output schemas, authentication mechanisms and usage policies should be documented (e.g. in a technical annex such as ITHACA D7.2) and version-controlled.
- Data structures and identifiers used by these APIs should, where feasible, align with relevant European interoperability specifications, with any deviations duly documented and justified.
- Public APIs serving open data should be accessible under fair, non-discriminatory terms, facilitating reuse and avoiding lock-in.
- Access-controlled APIs must comply with the strong security and access-control rules defined in this document (e.g. role-based access control, logging, encryption in transit and at rest).

In ITHACA these requirements are binding for the project platform; for other CEP-related R&I projects they can be adopted as a reference interoperability profile, ensuring that platforms emerging from research are compatible with the broader Interoperable Europe framework.

The project's data governance lead (as defined in D7.2 for ITHACA) oversees the consistent application of these rules with input from all Work Packages. For CEPs more broadly, an equivalent function (e.g. data/AI governance board or data controller) should be formally designated. In all cases, where there is tension between openness and the protection of fundamental rights, the protection of individual rights prevails.

8. Conclusion

The present Data Governance Framework outlines the legal, ethical and practical experience of the ITHACA project. By covering the full data lifecycle and integrating the results of the Data Protection Impact Assessment, this framework ensures that sensitive personal data, political opinions, vulnerable groups and AI-assisted functionalities within the ITHACA project are handled with clear safeguards, documented responsibilities and enforceable decision paths.

While grounded in the concrete experience of the ITHACA project, this document consolidates this experience into a practical governance blueprint for CEPs that is both compliant with evolving regulatory requirements and responsive to democratic and ethical concerns.

When people participate through digital platforms, they expose their views, experiences and sometimes their vulnerabilities. They will only do so at scale if they can trust that their data are treated lawfully, fairly and securely, and that algorithmic tools do not distort or manipulate debate.

9. References

- **Berryhill, J., Heang, K. K., Clogher, R., & McBride, K.** (2019). *Hello, world: Artificial intelligence and its use in the public sector* (OECD Working Papers on Public Governance No. 36). OECD Publishing. <https://doi.org/10.1787/726fd39d-en>
- **Cortés-Cediel, M. E., Cantador, I., & Gil, O.** (2019). Citizen participation and the rise of digital media platforms in smart governance and smart cities. *International Journal of E-Planning Research*, 8(1), 19–39. <https://doi.org/10.4018/IJEPR.2019010102>
- **European Commission.** (2024c). *Web accessibility directive: Standards and harmonisation*. Shaping Europe’s Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/web-accessibility?utm>
- **European Commission.** (2024d). *Open science* [Policy page]. Research and Innovation. https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/our-digital-future/open-science_en?utm
- **European Commission.** (2024e). *DCAT-AP: DCAT application profile for data portals in Europe*. EU Vocabularies / Interoperable Europe. <https://op.europa.eu/en/web/eu-vocabularies/dcat-ap>
- **European Data Protection Board.** (2017). *Guidelines on data protection impact assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679* (WP248 rev.01). https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711
- **European Data Protection Board.** (2019). *Guidelines 4/2019 on Article 25: Data protection by design and by default*. [Guidelines 4/2019 on Article 25 Data Protection by Design and by Default | European Data Protection Board](https://edpb.europa.eu/our-work-and-activities/guidelines-standards-recommendations-and-advices/our-guidelines/guidelines-4-2019-on-article-25-data-protection-by-design-and-by-default_en)
- **European Data Protection Board.** (2020). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. [Guidelines 07/2020 on the concepts of controller and processor in the GDPR | European Data Protection Board](https://edpb.europa.eu/our-work-and-activities/guidelines-standards-recommendations-and-advices/our-guidelines/guidelines-07-2020-on-the-concepts-of-controller-and-processor-in-the-gdpr_en)
- **European Parliament and Council of the European Union.** (2016a). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L 119. [Regulation - 2016/679 - EN - gdpr - EUR-Lex](https://eur-lex.europa.eu/eli/reg/2016/679/oj)
- **European Parliament and Council of the European Union.** (2016b). Directive (EU) 2016/2102 of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies. *Official Journal of the European Union*, L 327. [Directive - 2016/2102 - EN - EUR-Lex](https://eur-lex.europa.eu/eli/dir/2016/2102/oj)
- **European Parliament and Council of the European Union.** (2019a). Directive (EU) 2019/1024 of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive). *Official Journal of the European Union*, L 172, 56–83. [Directive - 2019/1024 - EN - psi directive - EUR-Lex](https://eur-lex.europa.eu/eli/dir/2019/1024/oj)
- **European Parliament and Council of the European Union.** (2019b). Directive (EU) 2019/882 of 17 April 2019 on accessibility requirements for products and services (European Accessibility Act). *Official Journal of the European Union*, L 151. [Directive - 2019/882 - EN - EUR-Lex](https://eur-lex.europa.eu/eli/dir/2019/882/oj)
- **European Parliament and Council of the European Union.** (2022a). Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). *Official Journal of the European Union*, L 277. [Regulation - 2022/2065 - EN - DSA - EUR-Lex](https://eur-lex.europa.eu/eli/reg/2022/2065/oj)
- **European Parliament and Council of the European Union.** (2022b). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*, L 333. [Directive - 2022/2555 - EN - EUR-Lex](https://eur-lex.europa.eu/eli/dir/2022/2555/oj)

- **European Parliament and Council of the European Union.** (2022c). Regulation (EU) 2022/868 of 30 May 2022 on European data governance (Data Governance Act). *Official Journal of the European Union*, L 152. [Regulation - 2022/868 - EN - EUR-Lex](#)
- **European Parliament and Council of the European Union.** (2024a). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, L 206. [Regulation - EU - 2024/1689 - EN - EUR-Lex](#)
- **European Parliament and Council of the European Union.** (2024b). Regulation (EU) 2024/2847 of 13 March 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). *Official Journal of the European Union*. [Regulation - 2024/2847 - EN - EUR-Lex](#)
- **European Parliament and Council of the European Union.** (2024c). Regulation (EU) 2024/903 of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act). *Official Journal of the European Union*, L 2024/903, 1–33. [Regulation \(EU\) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union \(Interoperable Europe Act\) | Interoperable Europe Portal](#)
- **European Telecommunications Standards Institute.** (2021). EN 301 549 V3.2.1: Accessibility requirements for ICT products and services. [ETSI EN 301 549 - V3.2.1 - Accessibility requirements for ICT products and services](#)
- **European Union Agency for Cybersecurity.** (2025a). *Technical implementation guidance on cybersecurity risk management measures in the NIS2 Directive* [ENISA Technical implementation guidance on cybersecurity risk management measures version 1.0.pdf](#)
- **European Union Agency for Cybersecurity.** (2025b). *Cyber Resilience Act implementation via EUCC and applicable technical elements*. [Cyber Resilience Act implementation via EUCC and its applicable technical elements - European Union Cybersecurity Certification](#)
- **Fabbri, M.** (2025). The role of requests for information in governing digital platforms under the Digital Services Act: The case of X. *Journal of Open Access to Law*, 6(1), 41. <https://www.mdpi.com/2673-5172/6/1/41>
- **Farina, (2014).** *Designing an online civic engagement platform: Balancing “more” vs. “better” participation in complex public policymaking* [Article]. Scholarship@Cornell Law: A Digital Repository. <https://scholarship.law.cornell.edu/facpub/1387/>
- **Fasel, M., & Weerts, S.** (2024). Can Facebook’s community standards keep up with legal certainty? Content moderation governance under the pressure of the Digital Services Act. *Policy & Internet*, 16(3), e391. <https://doi.org/10.1002/poi3.391>
- **ITHACA Consortium.** (2025). *D5.5 – White paper with policy recommendations* [Project deliverable]. Horizon Europe project “ITHACA – artificial Intelligence To enHance Civic pArticipation” (Grant Agreement No. 101094364).
- **Khatri, V., & Brown, C. V. (2010).** Designing data governance. *Communications of the ACM*, 53(1), 148–152. <https://doi.org/10.1145/1629175.1629210>
- **Nelimarkka, M.** (2014). Comparing three online civic engagement platforms from the perspective of the Spectrum of Public Participation. In *Internet, Politics, and Policy Conference 2014 (IPP2014)*. Oxford Internet Institute. https://blogs.oii.ox.ac.uk/ippconference/sites/ipp/files/documents/IPP2014_Nelimarkka.pdf?utm_source=ippconference&utm_medium=email&utm_campaign=ipp2014
https://blogs.oii.ox.ac.uk/ippconference/sites/ipp/files/documents/IPP2014_Nelimarkka.pdf?utm_source=ippconference&utm_medium=email&utm_campaign=ipp2014
- **OECD.** (2019a). *Artificial intelligence in society*. OECD Publishing. <https://doi.org/10.1787/eedfee77-en>
- **OECD.** (2019b). *The path to becoming a data-driven public sector*. OECD Publishing. https://www.oecd.org/en/publications/the-path-to-becoming-a-data-driven-public-sector_059814a7-en.html

- **OECD.** (2019/2024). *Recommendation of the Council on Artificial Intelligence* (OECD Legal Instrument No. OECD/LEGAL/0449). OECD Publishing. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
- **OECD.** (2022a). *Going Digital guide to data governance policy making*. OECD Publishing. <https://doi.org/10.1787/40d53904-en>.
- **OECD.** (2022b). *OECD framework for the classification of AI systems* (OECD Digital Economy Papers No. 323). OECD Publishing. <https://doi.org/10.1787/cb6d9eca-en>
- **OECD.** (2022c). *OECD guidelines for citizen participation processes* (OECD Public Governance Reviews). OECD Publishing. <https://doi.org/10.1787/f765caf6-en>
- **OECD.** (2022d). *Building trust to reinforce democracy: Main findings from the 2021 OECD survey on drivers of trust in public institutions*. OECD Publishing. <https://doi.org/10.1787/b407f99c-en>
- **OECD.** (2022e). *The protection and promotion of civic space: Strengthening alignment with international standards and guidance*. OECD Publishing. <https://doi.org/10.1787/d234e975-en>.
- **OECD.** (2025a). *European Data Governance Act (DGA): Regulation (EU) 2022/868*. In *Access to public research data toolkit*. OECD Publishing. https://www.oecd.org/en/publications/access-to-public-research-data-toolkit_a12e8998-en/european-data-governance-act-dga-regulation-eu-2022-868_920b8b28-en.html?utm
- **OECD.** (2025b). *Governing with artificial intelligence in government: The state of play and way forward in core government functions*. OECD Publishing. https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en.html
- **OECD.** (2025c). *A preliminary mapping of measures affecting the cross-border flow of non-personal data* (OECD Trade Policy Papers No. 295). OECD Publishing. https://www.oecd.org/en/publications/a-preliminary-mapping-of-measures-affecting-the-cross-border-flow-of-non-personal-data_0825c57c-en.html
- **OECD.** (2025d). *Tackling civic participation challenges with emerging technologies* (OECD Public Governance Policy Papers No. 72). OECD Publishing. https://www.oecd.org/en/publications/tackling-civic-participation-challenges-with-emerging-technologies_ec2ca9a2-en.html
- **OECD.** (2025e). *AI in civic participation and open government*. In *Governing with artificial intelligence in government: The state of play and way forward in core government functions*. OECD Publishing. https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en/full-report/ai-in-civic-participation-and-open-government_51227ce7.html
- **Ohnesorge, J.** (2025). *Counting without accountability? An analysis of the DSA's transparency reports*. *Digital Society Blog*. Alexander von Humboldt Institute for Internet and Society. <https://zenodo.org/records/17201618>
- **OpenAIRE** (2022). *Horizon Europe: OpenAIRE guides for researchers*. OpenAIRE. <https://www.openaire.eu/horizon-europe-openaire-guides-for-researchers?utm>
- **Shin, B.** (2024). *A systematic analysis of digital tools for citizen participation*. *Government Information Quarterly*, 41(3), 101905. <https://doi.org/10.1016/j.giq.2024.101954>
- **Tsarchopoulos, P., Tsampoulatis, I., & Roman, M.** (2018). *Digital tools for participatory governance*. In *Proceedings of the 20th Conference of the Greek Society of Regional Scientists* (pp. 104–110). Athens, Greece. https://www.tsarchopoulos.com/wp-content/uploads/2018/06/Tsarchopoulos_et_al_Digital_Tools_for_Participatory_Governance2018.pdf
- **Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., ... Mons, B.** (2016). *The FAIR guiding principles for scientific data management and stewardship*. *Scientific Data*, 3, Article 160018. <https://doi.org/10.1038/sdata.2016.18>
- **World Wide Web Consortium** (2018). *Web Content Accessibility Guidelines (WCAG) 2.1*. W3C Recommendation 05 June 2018. <https://www.w3.org/TR/WCAG21/>