

Holding Democracy Together

A common European baseline
for trustworthy digital democracy
in Europe

Authors:

Gabriela Rogowska
Diego Dylan Domenici
(*Trust-IT Services*)

Contributors:

Luca Ceselli (*ICTLC*),
Laurien Coenen (*KUL*),
Christian Fuchs (*UPB*),
Xenia Klinge (*DFKI*),
María Ruiz de Assín
de los Santos (*CIB*),
Fatih Yilmaz (*BtH*)

DOI:

10.5281/zenodo.21026681



Executive Summary

Europeans believe in democracy but increasingly doubt that it works. They see the risks to digital democracy clearly — distrust of institutions, disinformation, and opaque AI-driven political content — but lack the infrastructure to turn that concern into participation: transparent platforms, reliable feedback, and trusted public-interest tools. Digital democracy applications promise to close the gap, yet the conditions that make them legitimate — accountability, hybrid access, visible impact, human oversight, and security — are slow and costly to build, and the market has not built them.

Drawing on eighteen months of INNOVADE research — a citizen survey, a questionnaire of 67 public officials, a mapping of 141 platforms, an expert survey of 331 specialists, twenty country interviews, and validation through real-world Living Labs — this brief sets out ten recommendations for a common European baseline for trustworthy digital democracy, designed for direct uptake into procurement, regulatory, and funding instruments.

- I. Support pillars (1–3)** are the conditions every digital democracy initiative must meet before launch: a Minimum Viable Legitimacy standard for procurement; mandatory impact accountability, so no contribution disappears into a “black box”; and proportional identity, matched to what is genuinely at stake.
- II. State-of-the-art design (4–6)** governs how digital democracy tools are built regardless of provider: parity between online and offline participation, disclosed and human-supervised AI, and participation formats chosen to fit the objective rather than complexity for its own sake.
- III. Foundation conditions (7–10)** are the investments no single digital democracy tool can deliver: permanent funding for participation operations, platforms treated as trust-sensitive public infrastructure, civic and digital literacy as a prerequisite, and public-interest and open-source alternatives to big tech.

The brief is a direct contribution to the operationalisation of the European Democracy Shield — most immediately to its societal resilience and citizens’ engagement pillar, and to the integrity of the information space where participation tools intersect with it — and is offered as an input to the work of the European Centre for Democratic Resilience, operational since February 2026.

One principle runs through all ten recommendations: a common European baseline, implemented along country-specific paths. Legal and cultural context varies too much across Member States for a single uniform model to deliver legitimacy evenly. The aim is to fix the baseline at EU level: covering legitimacy standards, proportional identity, impact accountability, and the foundation conditions above, while leaving implementation to follow national traditions, infrastructure, and social context. Thoughtfully governed digital tools, legitimate before they launch, well built, and sustained over time, can make democracy more open, fair, and responsive.

The Challenge

Digital tools promise scale and efficiency, but the conditions that make them legitimate (accountability, hybrid access, visible impact, human oversight) are slow and expensive to build. That tension runs through every policy layer, from the European institutions to the local town hall.

Special Eurobarometer 568 “Protecting and promoting democracy” (May 2025), captures a public committed to democratic values yet anxious about how democracy functions. Nearly half of the respondents (49%) name growing distrust of democratic institutions as the single most serious challenge facing EU democracy, ahead of foreign manipulation, interference and disinformation (42%), and the lack of transparency around

1. <https://europa.eu/eurobarometer/surveys/detail/3383>

AI-promoted political content (32%). Around digital processes the picture is sharper still: 79% worry that voters will base decisions on disinformation, 67% fear manipulated election results, and 85% want platforms to block fake accounts and AI bots, disclose the source of political messages, and give parties equal access. Yet behaviour lags concern — only 18% verify online information often, and the countermeasures citizens trust most are human and institutional (critical-thinking education, independent fact-checking, awareness campaigns) rather than platform-level technical fixes.

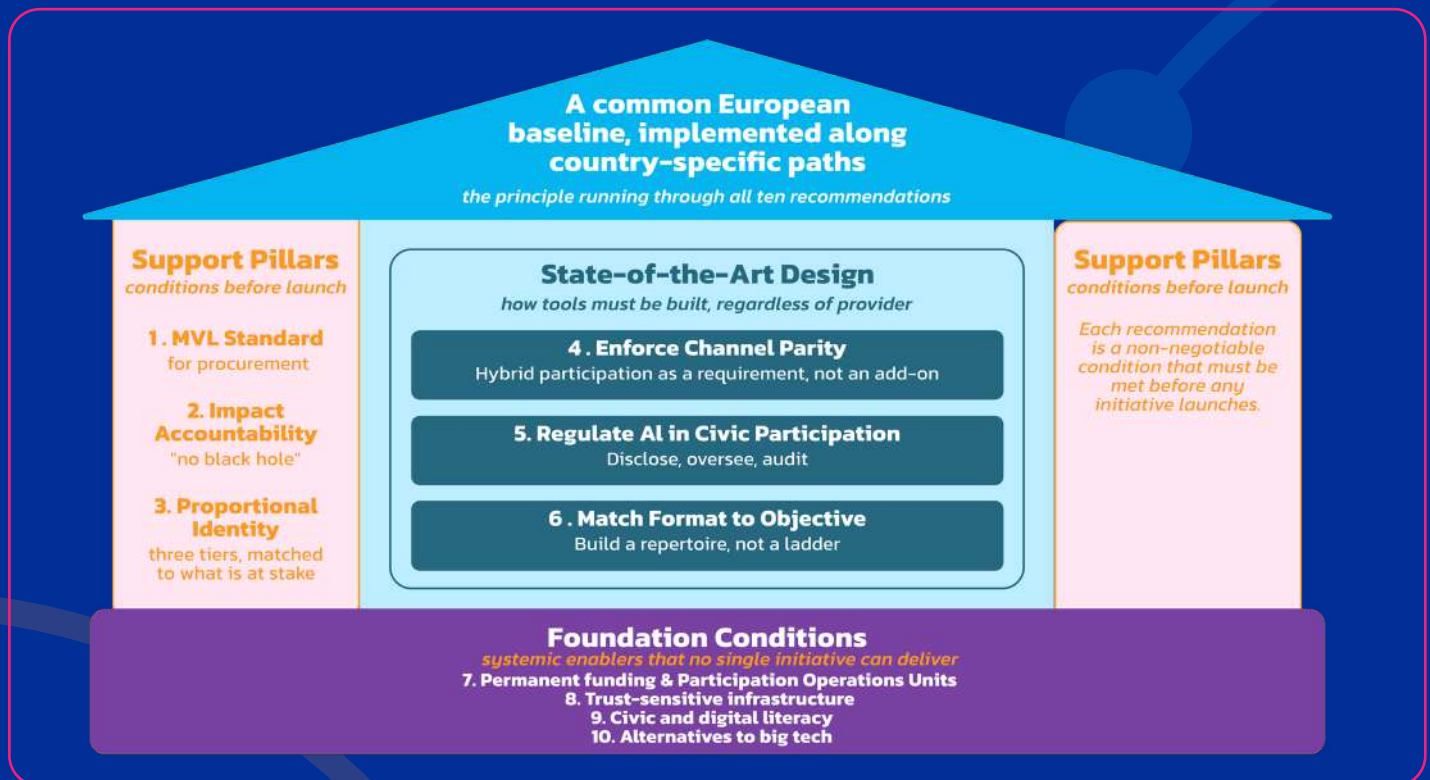
Two structural gaps complete the picture. The first is that participation is rare and though this needs careful reading. More than nine in ten Europeans (91%) have taken no part in any EU-level participatory process in the past five years and 78% are barely aware such mechanisms exist. That is no surprise: participation is best organised at the level closest to citizens, the local one, and few would expect high engagement with distant European processes. The more telling question — local participation rates aggregated across Europe — is one the Eurobarometer does not answer, and it deserves attention in future research. The second is that digital tools are not yet the gateway. Asked what would encourage them to engage, citizens put transparency and clear information first (40%), ranking online participation platforms (25%) below local in-person debates (34%).

The stakes of getting this right are well documented. The Joint Research Centre's 2026 study on the impact of citizen engagement², drawing on public administrations across twenty Member States, finds that embedded engagement improves policy quality, legitimacy, and trust in government — 97% of responding administrations would run engagement processes again — but warns that legitimacy erodes precisely where follow-up fails and citizens cannot see what their input changed. Demand, in other words, is proven; what is missing is the infrastructure of trust.

The ten recommendations that follow respond to that gap. They distil eighteen months of INNOVADE research triangulating several work streams: a citizen survey of more than 400 respondents and two participatory workshops in Geel (Belgium) and San Martín de la Vega (Spain) (D4.1); a questionnaire of 67 European public officials (D4.1); a structured mapping of 141 digital democracy platforms (D4.2); the Interdisciplinary Knowledge Base on Digital Democracy (D2.1); the Futures of Digital Democracy Survey of 331 international experts; and 20 expert interviews across five Member States (ICTLC) — all validated through the INNOVADE Living Labs, near-real-world testing grounds bringing together policymakers, citizens, civil society, industry, and researchers.

Layer	Central questions	Primary sources
(I) Support Pillars	Is this initiative legitimate before it starts?	D4.1/D4.2; Living Labs LL2/LL3/LL5; ICTLC
(II) State-of-the-art Design	Is this tool built to honour that legitimacy?	D4.1; Living Labs LL3/LL4/LL5; D2.1; ICTLC
(III) Foundation Conditions	Is the ecosystem viable, sovereign, and trustworthy? Does the surrounding society support it?	Living Labs LL2/LL5; D2.1; the Futures of Digital Democracy Survey; ICTLC; D4.2

2. DUNLOP, T., KOZAREV, V., GUIMARAES PEREIRA, Â. and ROSA, P., Impact of Citizen Engagement – Making a difference to policy, institutions and society, Publications Office of the European Union, Luxembourg, 2026, <https://data.europa.eu/doi/10.2760/3912442, JRC145690>.



Ten Recommendations: A Common European Baseline

(I) Support Pillars

Conditions that must be met before any digital democracy initiative launches

1. Establish a Minimum Viable Legitimacy (MVL) Standard for Procurement
2. Make Impact Accountability Mandatory
3. Adopt Proportional Identity Models — Neither Full Anonymity Nor Full Identification

(II) State-of-the-art Design

How digital democracy tools must be built, regardless of provider

4. Enforce Channel Parity: Hybrid Participation as a Requirement, Not an Add-On
5. Regulate AI in Civic Participation: Disclose, Oversee, Audit
6. Match the Format to the Objective — Build a Repertoire, Not a Ladder

(III) Foundation Conditions

Investments that no single digital democracy tool or initiative can deliver alone

7. Fund Participation Operations as Permanent Infrastructure
8. Treat Digital Democracy Platforms as Trust-Sensitive Public Infrastructure
9. Invest in Civic and Digital Literacy as a Prerequisite, Not an Afterthought
10. Support Alternatives to Big Tech: invest in public service internet platforms, digital commons projects, and open-source software

(I) Support Pillars

Conditions that must be met before any digital democracy initiative launches

Recommendation 1

Establish a Minimum Viable Legitimacy (MVL) Standard for Procurement

WHY

Digital democracy tools tend to implement visible features (polling, ideation) well but fall short on the ones that build legitimacy and are trust-critical: documented security, identity management, and transparency controls. Citizens trust public and non-profit operators most, and private international platforms least. Contracting authorities currently lack shared criteria.

HOW

Develop a **Minimum Viable Legitimacy** checklist for procurement, covering accessibility evidence; audit trails and transparency features; identity and anti-bot controls proportionate to the use case; AI disclosure and oversight requirements; and a resourcing plan covering staffing, moderation, and analysis capacity. Convert the checklist into model contract clauses so contracting authorities do not reinvent due diligence for each initiative.

Based on: D4.1; D4.2; ICTLC expert interviews; Living Labs LL2–LL5..

Recommendation 2

Make Impact Accountability Mandatory

WHY

Across every Living Lab, across the citizen survey, and in the qualitative workshops, citizens did not primarily ask for more features. They asked for fewer broken promises. The single most cited legitimacy killer — described repeatedly in participants' own words — is what researchers call the "black box effect": input that enters a platform and never returns in any form. Citizens want what one Living Lab participant called a "parcel-tracking model of participation": the ability to follow their submission from entry through deliberation to a final institutional response, including a clear and honest explanation when their input was not acted upon. This is not an unreasonable demand. It is the minimum condition for trust, and trust is the condition without which everything else fails. Process opacity disproportionately discourages already disengaged groups.

HOW

Require every publicly funded digital democracy initiative to publish an **Impact and Feedback Protocol** before launch, specifying what is being decided, at what level and with what degree of influence (consultative or advisory vs. binding); the decision timeline; and what response each participant will receive by when. Introduce a **Participation Debt metric** — the proportion of submissions without a public status update after a defined period — as a reportable indicator in EU-funded projects. Progress tracking should be treated as a standard feature requirement, not an option.

Based on: Living Labs LL2, LL3, LL5; D4.1.

Impact & Feedback Protocol

every submission is tracked from entry to institutional response



The "black box" effect

input enters the platform and never returns in any form



Participation Debt

% of submissions with no public status after X days

Recommendation 3

Adopt Proportional Identity Models — Neither Full Anonymity Nor Full Identification

WHY

One of the most persistent and unresolved tensions in digital democracy is the conflict between anonymity and accountability. Citizens are divided: many value privacy and fear that identification will deter participation. Governments strongly prefer robust user verification, and for several reasons. The first is integrity: verification helps prevent bot manipulation, coordinated inauthentic behaviour, and the submission of harmful or baseless contributions. The second is dialogue: feedback loops and the "parcel-tracking" model of participation only work if you know who submitted what. If a contribution arrives anonymously, there is no way to enter into direct dialogue or to report back accurately on what happened to it — accountability and anonymity pull in opposite directions. The third is security: democratic participation is a sensitive context, and strong authentication safeguards citizens' data within it. Unauthorised access and identity theft can do real and lasting damage to fundamental rights.

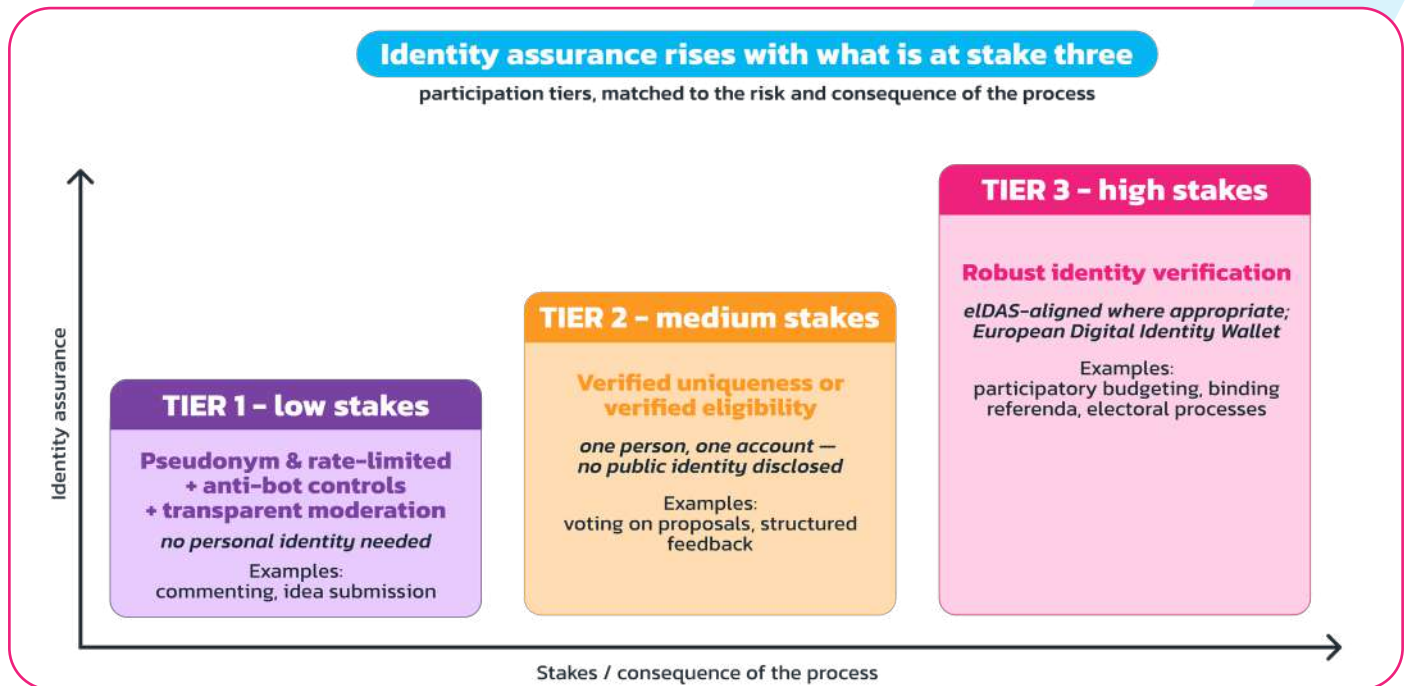
Both sets of concerns — the citizens' and the governments' — are legitimate. The mistake is treating them as a binary choice. Imposing full identification as a default excludes people for whom privacy is a condition of free expression, as surveillance creates a chilling effect on democratic participation. Permitting full anonymity, on the other hand, opens platforms to abuse and erodes the equal-weight principle that democratic processes depend on.

HOW

Identity assurance should be matched to what is actually at stake in a given process, using **three participation tiers**. Tier 1, for low-stakes engagement such as commenting or idea submission, requires pseudonymity with strong anti-bot controls and transparent moderation — no personal identity needed. Tier 2, for medium-stakes participation such as voting on proposals or structured feedback, requires verified uniqueness (one person, one account) or verified eligibility without disclosing public identity or more personal data than necessary. Tier 3,

for high-stakes decisions such as participatory budgeting, binding referenda, or electoral processes, requires robust identity verification aligned with applicable national and EU electronic identification frameworks, including eIDAS where appropriate. The applicable tier must be disclosed publicly in every initiative's pre-launch documentation, so citizens know exactly what they are signing up for. EU digital identity infrastructure, including eIDAS compliant solutions and the European Digital Identity Wallet, should therefore be designed and implemented as an enabling layer for proportionate identity assurance, not as single default gateway for all forms of democratic participation.

Based on: ICTLC expert interviews (Germany, Belgium, Italy, Spain, and Greece); D4.1; D2.1.



II) State-of-the-art Design

How digital democracy tools must be built, regardless of provider

Recommendation 4

Enforce Channel Parity: Hybrid Participation as a Requirement, Not an Add-On

WHY

Digital-only platforms systematically exclude citizens by age, connectivity, literacy, or cultural preference. Combining online tools with physical touchpoints is not an accessibility add-on but a democratic integrity requirement. Physical location of participation touchpoints — a totem in a public space, a supported terminal in a library, an info point — is a stronger predictor of actual participation rates than any feature of the digital tool. Both citizens and governments identify hybrid design as a success driver, not an accessibility courtesy. Offline and online participation do not serve the same purpose: digital tools are better for scale and reach; offline formats are better for social cohesion (trust-building, and inclusion of those who are less digitally fluent) and community building.

HOW

Introduce a **Channel Parity Rule**: offline inputs must enter the same tracking and audit workflow as online inputs, with equal visibility and response guarantees. No participant should be penalised — in terms of response speed, feedback quality, or influence on outcomes — for choosing to participate offline rather than online. Publicly funded participation initiatives should be required to designate physical touchpoints — in libraries, civic centres, or local authority buildings — staffed with support capacity for those who need it. Digital-only compliance should not satisfy public consultation obligations under EU or national law.

Based on: Living Labs LL3, LL5; D4.1; D2.1

Recommendation 5

Regulate AI in Civic Participation: Disclose, Oversee, Audit

WHY

AI-assisted features (proposal clustering, guidance layers, moderation) are valued for efficiency but only when accompanied by visible disclosure and meaningful human oversight. Undisclosed AI involvement risks eroding the trust that the entire participation process depends on. The EU AI Act classifies AI that influences voting behaviour as high-risk. At the same time, governments are under pressure. Administrative capacity is a near-universal constraint, and AI is increasingly seen as a way to cope with the volume of citizen input that well-designed participation generates. That is a legitimate use — but it carries conditions.

HOW

Require **mandatory plain-language disclosure** of any AI component interacting with end users, explaining its role in the participation process— not in technical terms, but in terms a citizen can act on. Procurement standards should require **documented human oversight mechanisms**, audit rights, and an explicit EU AI Act risk classification of each component before deployment. Where AI is used for moderation or analysis, human review of AI-generated outputs must be the default for consequential decisions. AI can handle scale but humans must handle judgement.

Based on: Living Labs LL4, LL5; ICTLC expert interviews; EU AI Act; D4.1.

Recommendation 6

Match the Format to the Objective — Build a Repertoire, Not a Ladder

WHY

Digital democracy currently converts poorly from awareness to action. Current civic interaction is largely transactional (administrative tasks, petitions), co-creation and co-production remain rare. The D4.1 citizen survey found that nearly half of respondents (47%) have taken part in online petitions, and 37.4% have reported a local issue — both low-barrier, low-commitment actions. Co-creation with government staff has been used by fewer than one in ten (9.9%). Co-deciding on budgets by just over one in ten (11.3%). This is not evidence that citizens do not want deeper participation. It is evidence that the pathway from first engagement to meaningful co-production has not been designed. The government survey reveals an equally significant gap on the other side: what public actors actually want from future tools — more co-design, more co-production, more substantive involvement. Both citizens and governments identify a gap between what tools currently enable and what they would value.

Designing for depth is necessary but not sufficient on its own. Furthermore, D2.1 adds another warning: it is not only the level of participation that matters, but its substance. Trivial or tokenistic applications of civic technology — what the INNOVADE Interdisciplinary Knowledge Base calls the “park bench problem” — damage trust and reduce future participation rates, regardless of how collaborative the format is. A community can co-design intensively around something that ultimately changes nothing, just as it can deliver real value through a light-touch, advisory exercise that brings a neighbourhood together. The lesson is therefore not to participate more deeply, but to participate more deliberately: to match the format to the objective, and to make sure that objective genuinely matters to the people taking part.

HOW

Build a **repertoire of participation formats** into platform design, from low-barrier and familiar (reporting local issues with resolution tracking, voting and rating on proposals, transparent dashboards linking citizen input to decisions) through to more intensive ones (design sprints, structured deliberation). Where deeper involvement serves the objective, make the step into it easy and well-signposted — for instance, inviting those who voted on a proposal to help define its implementation trade-offs. But depth is an option, not a destination. Success should be measured neither by registrations and downloads, nor by the complexity of the formats used. What matters is choosing the method deliberately, according to the project’s goals, rather than defaulting to what is familiar — too often, simply letting citizens comment on something. The repertoire is there to be drawn on as the objective requires, not climbed for its own sake. Public authorities should be encouraged to match the format to the need, and to experiment.

Based on: D4.1; D2.1.

Co-creation is a broad, umbrella term. It covers citizens and public authorities working together across the whole life of a policy or service — from shaping ideas to delivering them.

Co-design is co-creation at the planning and design stage: jointly deciding what a service or policy should be. Example: residents and planners redesigning a neighbourhood mobility plan together.

Co-production is co-creation at the delivery and implementation stage: jointly producing, running, or sustaining a service. Example: citizens reporting potholes through an app and tracking the repair, helping deliver the maintenance service.

(III) Foundation Conditions

Investments that no single digital democracy tool or initiative can deliver alone

Recommendation 7

Fund Participation Operations as Permanent Infrastructure

WHY

Insufficient resources, staff capacity, and administrative burden are near-universal blockers in the government survey (D4.1) and across all Living Labs. The most common cause of digital democracy failure is not bad technology — it is good technology abandoned. Structural viability is a systemic risk: 7.8% of mapped platforms are inactive or discontinued, and long-term operation correlates with sustainable funding rather than project grants. There is no sustainable business model for civic participation that does not compromise public values — and governments rarely budget for ongoing participation operations as core infrastructure. Deploying tools without operational continuity actively erodes trust when maintenance or follow-up lapses: citizens who engaged with a tool that subsequently went dark are harder to re-engage than those who were never asked at all.

HOW

Develop dedicated structural funding instruments for civic participation operations — covering staffing, moderation, data stewardship, and platform maintenance — independent of time-limited R&D grants. Require any publicly funded digital democracy initiative to include a binding post-project continuity plan as a condition of approval. Participatory structures must be legally and administratively embedded to survive beyond electoral cycles and political turnover. Consider establishing shared **Participation Operations Units** at national or regional level that municipalities can draw on for facilitation, moderation, legal/GDPR support, and data analysis.

Based on: Living Labs LL2, LL5; D4.1.

Recommendation 8

Treat Digital Democracy Platforms as Trust-Sensitive Public Infrastructure

WHY

Trust in a digital democracy platform is the precondition for the platform's democratic legitimacy. Security experts across multiple countries identify trust as the condition that connects privacy, cybersecurity, usability, and institutional legitimacy. Disruption or cyberattack on a participation platform directly undermines public confidence in democratic processes. Supply-chain risks compound the picture. Security, auditability, and resilience are currently under-documented in the tool landscape (9.2% of platforms have documented security/privacy/compliance features).

HOW

Digital democracy platforms used for high-stakes processes must be subject to **independent security audits** and **documented resilience plans** before deployment. GDPR Data Protection Impact Assessments should be applied rigorously, with Fundamental Rights Impact Assessment-type evaluations wherever political opinion data, location data, or sensitive participation records are processed. Every public authority deploying a digital democracy platform should be required to complete a documented sovereignty and supplier-risk assessment covering data residency, jurisdictional exposure, security capability, incident notification, audit rights, and exit strategy. Privacy and data protection safeguards are democratic legitimacy requirements and should be treated as such in procurement, design, and audit alike.

Based on: ICTLC expert interviews (Belgium, Italy, Spain, Germany, Greece); D4.2.

Recommendation 9

Invest in Civic and Digital Literacy as a Prerequisite, Not an Afterthought

WHY

If people lack the skills, the confidence, the trust, or the time to engage, digital tools alone will not make participation more democratic — they will make it more unequal. This was the consistent message from civil society representatives, local governments, and organisations working with vulnerable groups. Meaningful participation requires enabling conditions that extend well beyond any platform — time, digital skills, motivation, and access to civic education. The structural conditions of participation, including investment in civic and digital literacy, should be treated as policy responsibilities in their own right, not assumed as pre-existing user capacities that technology can bypass. The Futures of Digital Democracy Survey identifies critical digital literacy as the second most urgent policy intervention cited by experts (25% of respondents). Participation initiatives that assume pre-existing capacity systematically reproduce existing inequalities.

HOW

Accompany EU and national digital democracy strategies with **dedicated investment in civic and digital education as a precondition** for deployment, not a parallel track. Every participation initiative should conduct a pre-launch accessibility and inclusion audit that assesses not only technical accessibility but also the time, literacy, and motivational barriers facing the target community — and report on these as part of standard project monitoring. Public service media organisations and educational institutions should be formally engaged as delivery partners for digital literacy outreach. Digital democracy policies that focus solely on platforms and technological solutions, without addressing the human conditions for participation, risk reproducing existing inequalities rather than reducing them.

Based on: Living Lab LL2; D2.1; The Futures of Digital Democracy Survey.

Recommendation 10

Support Alternatives to Big Tech: invest in public service internet platforms, digital commons projects, and open-source software

WHY

The digital democracy tool market is dominated by private-sector providers (D4.2). Citizens trust local municipalities, non-profits, and open-source operators most as platform operators (D4.1); and they trust international private companies least. The Democracy-as-a-Service market is currently 57.4% private-sector, creating procurement dependency and legitimacy risks. This creates a structural contradiction: the tools most widely available for democratic participation are provided by the class of operators that citizens trust least. The Futures of Digital Democracy Survey found that 75% of digital democracy experts call for new EU regulation and reform. The single most urgent measure cited (50.7%) is supporting alternatives to commercial big tech platforms — public service internet platforms, digital commons projects, platform co-operatives, and FLOSS (free/libre open source software).

A structural mismatch

the tools most widely available are provided by the operators citizens trust least

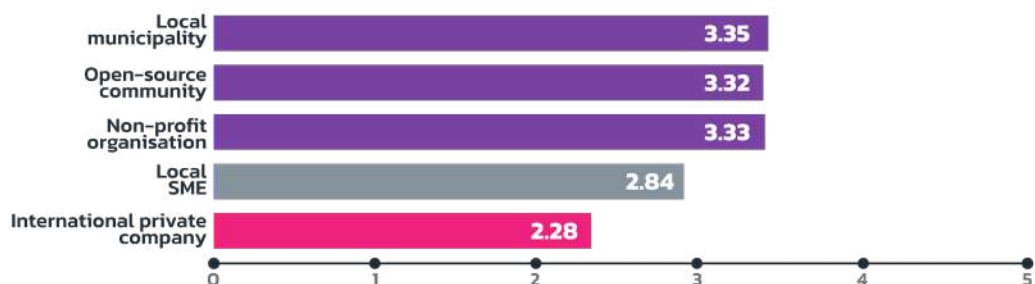
Who supplies the tools

D4.2 landscape mapping of 141 digital democracy platforms



Who citizens trust as platform operators

D4.1 citizen survey, mean trust on a 5-point scale (1 = no trust, 5 = high trust)



The dominant supplier (international private companies) is the operator citizens trust least

HOW

Horizon Europe and successor R&D programmes should allocate significant funding to public service internet platforms, platform co-operatives, digital commons projects, and FLOSS (free/libre open source software) for democratic participation, and make the digital public sphere a key topic in future societal digitalisation calls. The EU should create and financially support a structured network of public service internet and digital commons initiatives — including, for example, the Manifesto for Public Service Media and a Public Service Internet, the Council for European Public Space, the Public Spaces Incubator, and EuroStack — with an institutionalised role in the European Centre for Democratic Resilience and the European Democracy Shield. The goal is not to exclude private providers but to ensure that public and commons-based alternatives exist at sufficient scale to give contracting authorities a genuine choice.

Based on: The Futures of Digital Democracy Survey; D4.2; D4.1.

Digital commons initiatives:

Digital commons initiatives are not-for-profit Internet projects that have the goal to make digital resources available to everyone. Examples are Wikipedia/Wikimedia, Creative Commons, and diamond open access journals, PeerTube (an alternative to YouTube),

Public service Internet platforms:

Internet platforms run by public service media organisations such as ARD and ZDF, France Télévisions, BBC, RAI, RTVE, TVP, etc. that have the public service remit to support information, education, democratic communication, art, culture, etc. All of them are already active on social media and have their own digital media players. They are major players in the EU's media industry.

Platform co-operatives:

Platform co-ops are Internet platforms that are owned, operated, and managed in a democratic manner by their users and workers. Examples are Stocksy (image platform), Resonate (music platform), FairBnB (an alternative to Airbnb).

Free/Libre Open Source Software (FLOSS):

FLOSS is software that has an open source code available to everyone, and that uses a licence that gives users the right to use, share, modify, and distribute the software. Examples of FLOSS software are LibreOffice (alternative to Microsoft Office), Mozilla Firefox (webbrowser), Mozilla Thunderbird (e-mail client), and Mastodon (social network, social media)

To discover more

These recommendations distil a wider body of INNOVADE research. Readers who wish to explore the underlying evidence can consult the following open-access deliverables and outputs:

- ▶ **D2.1 — Interdisciplinary Knowledge Base on Digital Democracy:** foundational research on models of digital democracy, digital deliberation, open governance, e-voting and foreign information manipulation, including ten high-level recommendations for fostering digital democracy. <https://doi.org/10.5281/zenodo.17079016>
- ▶ **D4.1 — Digital Democracy Preference Toolkit:** citizen and governmental perspectives on digital democracy applications, drawing on a stratified EU citizen survey, two participatory workshops, and a questionnaire of European public officials. <https://doi.org/10.5281/zenodo.18258933>
- ▶ **D4.2 — Report on the state of the art in Digital Democracy Technology** including Digital Democracy Landscape Analysis: a structured mapping of digital democracy platforms by provider, licence type and feature maturity, alongside case studies of real-world success drivers and barriers. <https://doi.org/10.5281/zenodo.20341205>
- ▶ **Expert interviews and Living Labs:** 20 semi-structured interviews with privacy, cybersecurity and technology experts across five Member States (ICTLC), and the INNOVADE Living Labs testing the recommendations with policymakers, citizens and civil society. <https://innovade-democracy.eu/living-labs>
- ▶ **The Futures of Digital Democracy Survey (FDDS): Report and Analysis,** an expert survey of 331 digital democracy specialists on the threats facing digital democracy and the reforms needed to counter digital authoritarianism. <https://doi.org/10.5281/zenodo.20753801>

All public INNOVADE deliverables are available via the project website (<https://innovade-democracy.eu/publications>) and the Zenodo open repository (<https://zenodo.org/communities/innovade/records?q=&l=list&p=1&s=10&sort=newest>).



To learn more about the project, the pilot municipalities of Geel, San Martín de la Vega, Thessaloniki, and opportunities to get involved, visit the INNOVADE website: innovade-democracy.eu

INNOVAD

Innovative Democracy Through Digitalisation

Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.



Funded by
the European Union