



Digital local and regional governments

The interests of European local and regional governments in the EU's digital policies and their implementation

CEMR position paper

June 2025



CEMR key messages

As Europe continues its digital transformation, local and regional governments (LRGs) are at the forefront of ensuring that digitalisation is inclusive, sustainable, and accessible to all citizens. LRGs play a pivotal role in providing essential public services and implementing key EU digital policies. However, significant challenges remain, including gaps in digital infrastructure and implementation, disparities in digital skills, and rising cybersecurity threats.

To ensure that no one is left behind in the digital transition, CEMR calls on European institutions to:

- 1. Bridge the digital divide by investing in digital infrastructure in underserved regions, promoting EU-based technologies to reinforce digital sovereignty at the local level, and improving digital connectivity and accelerating high-speed internet deployment through public-private partnerships.**
- 2. Guarantee accessibility and inclusion by supporting LRGs with technical and financial assistance to design digital services available and accessible by all.**
- 3. Strengthen local cybersecurity capacity by increasing funding for secure infrastructure and services, providing tailored guidance on implementing cybersecurity legislation, and fostering cross-border cooperation to share best practices and improve preparedness.**
- 4. Support local capacity-building through funding for training programmes focused on AI and other digital technologies, and promoting digital literacy through awareness campaigns for citizens of all ages.**

Background

Local and regional governments (LRGs) are at the heart of Europe's digital transformation. They provide essential public services, including healthcare, education, transportation, waste management, water supply, social services, and fibre infrastructure, and are key actors in implementing digital policies such as the Data Act, Interoperable Europe Act, AI Act, and Single Digital Gateway. As many public services are increasingly digitalised, LRGs are crucial in ensuring that these services and digitalisation remain inclusive, sustainable, efficient, and allow citizen engagement.

The 2030 Digital Compass sets ambitious goals for digitalising public services, highlighting the essential role of LRGs in ensuring that digital transformation aligns with local needs.

How LRGs contribute to the digital transformation

To ensure inclusive digital transformation, LRGs work closely with communities, educators, social workers, and civil society actors to promote digital literacy and ensure equitable access to online and public services. This helps develop local strategies to support citizens with limited digital competencies, offering training opportunities in local spaces and providing user-friendly and accessible digital public services. These efforts help residents develop the competencies to engage with digital services and participate in civic life. Municipalities are leading efforts to expand connectivity and high-speed broadband access in areas where infrastructure gaps persist.

Challenges for LRGs

However, despite progress, significant challenges remain: financial and geographical gaps in digital infrastructure, cybersecurity threats, regulatory burdens, and lack of digital skills. This has an impact on increasing the digital divide, with persisting gaps among regions and municipalities in the accessibility to digital infrastructure, skills, or financial resources to deal with these issues. Ensuring territorial cohesion and equal opportunities across municipalities, including rural and less-connected areas, is essential to achieving an inclusive digital society.

These challenges are exacerbated by the profound societal, economic and technological changes caused by the current geopolitical situation, particularly the outcomes of the COVID-19 pandemic and the war in Ukraine. While the pandemic amplified inequalities by dividing those who had digital access, skills, and equipment, able to adapt and maintain their daily life, from those who did not, the war in Ukraine has further strained public resources and heightened digital vulnerabilities, especially in border regions and areas already facing infrastructure concerns. Many aspects of public life and services offered to citizens take place online. All these challenges show that it is essential for European institutions to engage with LRGs when developing new policies on digitalisation to ensure alignment with local realities. These issues, ranging from infrastructure, inclusion, and cybersecurity to digital skills, are deeply interconnected. Addressing them effectively requires a coordinated approach across all levels of governance and policy areas to prevent fragmentation and ensure coherence.

LRGs are committed to contributing to the efforts for a safer, more sustainable, and inclusive digital transition. To do so:

- They build capacity within their administrations and strategically leverage available EU and national funding to **implement digital solutions tailored to local needs**, ensuring that public services remain efficient, transparent, and citizen-centric
- Being the **closest to citizens' needs**, LRGs monitor and measure the digital divide to assess disparities in digital access, skills, and infrastructure. This allows LRGs to know better which targeted policies are needed to close the digital gap. They also collaborate with their local communities, facilitators, and social workers to promote digital literacy and inclusion, and extend their impact. The Union of Skills and other frameworks can provide necessary support in this regard.
- They ensure ethical and transparent AI use in public services by using guidelines on algorithmic decision-making and data governance. AI usage must align with EU values, ensuring its applications are fair, explainable, and non-discriminatory. Through open data initiatives and citizen engagement, **LRGs increase transparency, foster trust, and ensure that digital transformation serves the public interest.**

This position paper highlights the main areas where a more coordinated action is needed to support LRGs in their digitalisation efforts.

Bridging the digital divide and promoting accessibility

The digital divide remains a significant challenge across Europe, disproportionately affecting rural and remote areas, low-income households, older adults, and other vulnerable populations. For LRGs, this divide is not only a societal issue but also a governance challenge, as it hinders their ability to deliver inclusive and efficient digital services. Gaps in digital infrastructure, literacy, and access to technologies prevent citizens from fully participating in the digital society, reinforcing existing inequalities and creating barriers to social inclusion. Many cities, rural and peripheral areas face systemic disadvantages in terms of connectivity, service provision, and access to digital innovation.

Addressing these gaps requires a strong commitment to territorial cohesion. This includes targeted investment in digital infrastructure and support for public-private partnerships that can accelerate broadband rollout and local innovation. In addition, supporting the development of EU-based digital infrastructures would enhance Europe's digital autonomy and reinforce the capacities of local authorities to meet their communities' needs.

Inclusive digital transformation also requires attention to accessibility. Public digital services must be designed to be inclusive of, among others, persons with disabilities, older adults, and those with

Digital local and regional governments

The interests of European LRGs in the EU's digital policies and their implementation

June 2025

limited language proficiency. Applying universal design principles ensures that e-government platforms and tools are intuitive and usable by all, thereby reinforcing democratic participation and social inclusion. Nonetheless, digital public services must also remain accessible in-person to accommodate citizens who prefer or require face-to-face interaction.

CEMR calls upon the European institutions to:

- **Ensure adequate EU investment in digital infrastructure** to bridge the digital divide, prioritise underserved regions, and support the development of EU-based systems that strengthen digital sovereignty and empower LRGs.
- **Provide guidance, financial, and technical assistance**, such as capacity building and trainings, to help LRGs ensure accessibility in digital public service design.
- While efforts are being made to close infrastructure and skills gaps, especially in smaller LRGs and remote areas, **guarantee that all citizens can continue accessing public services through non-digital means**, preventing further exclusion during the digital transition.
- **Promote public-private partnerships** to expand high-speed internet access and other infrastructure across Europe.

Ensuring cybersecurity and digital resilience

Municipalities manage vast amounts of sensitive data and operate critical infrastructure that is increasingly targeted by cyber threats. Ensuring strong cybersecurity measures is essential not only for protecting data but also for maintaining public trust and ensuring the continuity of essential services.

Enhancing cybersecurity resilience requires a multi-level governance approach. Cooperation between local, national, and EU institutions can improve threat intelligence sharing, incident response coordination, and crisis preparedness. Cross-border collaboration also enables municipalities to benefit from shared expertise, best practices, and collective defence mechanisms.

EU cybersecurity regulations, such as the NIS2 Directive requires stronger security policies and incident response mechanisms. Many municipalities, especially smaller ones, lack the technical expertise and financial resources to comply with these regulations effectively. In this context, fragmented monitoring and compliance requirements across different EU digital regulations can further complicate implementation for LRGs. Greater alignment and simplification of these mechanisms would reduce administrative burden and support more coherent cybersecurity practices. Tailored guidance, technical assistance, and sustainable funding are essential to help LRGs building the necessary capacity.

Digital local and regional governments

The interests of European LRGs in the EU's digital policies and their implementation

June 2025

Moreover, investing in secure digital infrastructure is equally critical. Strengthening cloud security, data protection frameworks, and robust authentication systems helps LRGs protect public services from cyber threats. Reducing reliance on external providers, when appropriate, by promoting European-based cybersecurity solutions also reinforces digital sovereignty and resilience.

CEMR calls upon the European institutions to:

- Provide tailored guidance and technical assistance to LRGs on **implementing the NIS2 Directive and related cybersecurity regulations**.
- **Increase funding opportunities for LRGs** to enhance cybersecurity measures, including investment in secure digital services and resilient digital infrastructure.
- **Streamline regulatory reporting frameworks related to digital and cybersecurity policies** to enhance clarity, reduce overlap, and facilitate implementation at local level.
- **Facilitate cross-border cooperation on cybersecurity strategies**, enabling LRGs to benefit from shared expertise and best practice.
- When appropriate, **support to use of European alternatives to foreign service companies**.

Fostering digital skills and capacity building

LRGs already play a central role in equipping their workforce with the expertise needed to effectively implement digital policies, such as the AI Act, the Interoperable Europe Act, and cybersecurity regulations, and provide digitalised public services. They are required to invest in training for local public officials to help them oversee digital applications, maintain human oversight in decision-making, and ensure compliance with European standards.

AI-related skills are particularly important locally to ensure that LRGs retain control over AI-driven public services, guaranteeing an AI deployment according to local needs and ethical considerations. Training local officials is needed to strengthen their ability to govern AI effectively. In this regards, interregional cooperation enables knowledge-sharing and innovation, helping municipalities navigate regulatory challenges and implement best practices.

Strengthening digital competencies at all levels enables inclusive, secure, and citizen-oriented digital services and reduces dependence on external providers. However, while most of these responsibilities fall on the shoulders of LRGs, they often lack the adequate financial resources, technical support, and institutional recognition to effectively fulfil them. This gap is particularly critical given the growing emphasis at EU level on the importance of skills, as underscored by the recent *Union of Skills* communication. Digital transformation can only succeed if LRGs, their staff, and their communities possess the necessary skills to navigate, manage, and shape new technologies.

Digital local and regional governments

The interests of European LRGs in the EU's digital policies and their implementation

June 2025

Without sufficient support, many local and regional governments risk falling behind in building the capacities required to meet the digital ambitions set at national and EU levels.

Cybersecurity also requires substantial investment in digital skills for which LRGs should be supported. As regions and municipalities become more digitally connected, developing the digital skills of public sector employees is crucial for effectively implementing and maintaining cybersecurity measures, protecting sensitive data, and ensuring resilient public services. Cybersecurity training should not be limited to IT teams but should be embedded across all levels of public administration to build a culture of security awareness. Collaborating with national authorities and EU institutions can further enhance local cybersecurity capacities, providing LRGs with the tools and resources to improve their defences and enable better incident response, data protection, and infrastructure resilience.

Digital transformation should ensure that citizens and businesses can actively engage with public services. To this end, strengthening digital education, from school-age programs to lifelong learning, fosters digital literacy and enhances public trust. Involving communities in shaping digital services ensures that technological solutions reflect actual needs.

In addition, collaboration between municipalities and across regions accelerates digital innovation and reduces redundancies. Platforms facilitating knowledge exchange allow LRGs to share best practices, model use cases, and strategies for AI implementation, digital governance, and cybersecurity. This collective learning ensures a more balanced and equitable digital transformation across Europe.

To concretely support these aspects, CEMR calls upon the European institutions to:

- **Increase funding for regular local training programmes with a strong focus on AI**, ensuring public sector employees can manage and are fit to apply digital technologies responsibly.
- **Support the promotion of digital literacy** among all age groups through training and awareness-raising campaigns.

Contact

Hamza Bennis

Advisor – Employment, Digitalisation and Public Services

Square de Meeûs 1, 1000 Brussels

+ 32 470 88 33 42

hamza.bennis@ccre-cemr.org



Local &
Regional
Europe

Council of European Municipalities and Regions
Conseil des Communes et Régions d'Europe

+ 32 2 511 74 77 \ info@ccre-cemr.org \ www.ccre-cemr.org

Scan the QR code and follow us on social
media

