Council of the European Union

Brussels, 12 November 2026
(OR. en)

15800/26

Interinstitutional Files:
2026/0011 (COD)
2026/0012 (COD)
2026/0013 (COD)

CYBER 459
JAI 1439
DATAPROTECT 367
TELECOM 554
MI 1184
IND 694
CADREFIN 457
FIN 1605
BUDGET 50
CSC 738
COMPET 1358
ESPACE 185
CODEC 2157
IA 307

COVER NOTE

date of receipt:	12 November 2026
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2] Proposal for a Regulation of the European Parliament and of the Council on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision No 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision No 243/2012/EU - Opinion of the European Committee of the Regions

Delegations will find attached the opinion[1] of the European Committee of the Regions on the above-mentioned proposals..

[1] Other language versions, if needed, can be found on: Cybersecurity Review and Digital Networks Act | European Committee of the Regions.

European Committee of the Regions

ECON-VIII/015

173rd plenary session, 12-14 October 2026

OPINION

Cybersecurity Review and Digital Networks Act

THE EUROPEAN COMMITTEE OF THE REGIONS (CoR)

– underlines that local and regional authorities (LRAs) are expected to secure systems, protecting essential and important services and utilities, manage risks and support infrastructure deployment, despite very different levels of capacity across Europe. LRAs require targeted support, dedicated funding, and stronger involvement of regions in cybersecurity and connectivity governance frameworks;
– highlights that many LRAs operate integrated vendor stacks in which replacement of a single component requires reconfiguration across entire service layers. A proportionality test must be anchored in the text of the regulation so that supply-chain measures do not risk forcing rip-and-replace mitigating measures that exceed LRAs' capacities and disrupt public services on which citizens depend;
– demands that the European Competitiveness Fund digital window earmarks a dedicated envelope of the cybersecurity allocation for capacity building in LRAs with limited administrative or technical capacity;
– stresses that territorial cohesion must remain a central principle in the implementation of the future European framework for digital networks. Faster connectivity must respect subsidiarity and the role of local authorities in territorial planning and protecting the public interest;

ooter

Rue Belliard/Belliardstraat 101 | 1040 Bruxelles/Brussel | BELGIQUE/BELGIË | Tel. +32 22822211
www.cor.europa.eu | @EU_CoR | /european.committee.of.the.regions | /european-committee-of-the-regions | @EU_regions_cities

EN

Rapporteur:

Zdeněk HŘIB (CZ/GREENS), Member of the Local Assembly of the City of Prague

Reference documents:

COM(2026) 11 – Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881

COM(2026) 13 – Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]

COM(2026) 16 – Proposal for a Regulation of the European Parliament and of the Council on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision No 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision No 243/2012/EU

Opinion of the European Committee of the Regions –
Cybersecurity Review and Digital Networks Act

I. RECOMMENDATIONS FOR AMENDMENTS

Amendment 1
COM(2026) 11
Recital 33
Amend

Text proposed by the European Commission	*CoR amendment*
To support Union shared cybersecurity situational awareness, ENISA, in close cooperation with the Member States, should prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats, based on publicly available information, its own analysis and reports shared with it by Member States' CSIRTs or the national single points of contact on the security of network and information systems ('single points of contact') provided for in Directive (EU) 2022/2555, both on a voluntary basis, Europol and CERT-EU. That report should be made available to the Council, the European External Action Service, EU-CyCLONe, the CSIRTs network, the Commission and Europol.	To support Union shared cybersecurity situational awareness, ENISA, in close cooperation with the Member States, should prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats, based on publicly available information, its own analysis and reports shared with it by Member States' CSIRTs or the national single points of contact on the security of network and information systems ('single points of contact') provided for in Directive (EU) 2022/2555, both on a voluntary basis, Europol and CERT-EU. That report should be made available to the Council, the European External Action Service, EU-CyCLONe, the CSIRTs network, the Commission and Europol. ***Local and regional authorities, through their national single points of contact on the security of network and information systems, should receive relevant reports to the extent possible. These reports should be accompanied by executive summaries to administrations with limited capacities; when a Member State has extended the scope of application of Directive (EU) 2022/2555 in accordance with Article 2(5)(a) thereof, public administration entities at local level receive the relevant sections of the report concerning the risks or incidents in their territory through the relevant single point of contact.***

Reason
Access to cybersecurity situational awareness reports ensures that local and regional authorities can fulfil their role in providing cybersecurity. Municipalities' information position regarding cyber incidents on their territory needs to be strengthened. Information should be tailored to the needs and capacities of local and regional authorities with limited capacities.

Amendment 2
COM(2026) 11
Add new recital 131a

Text proposed by the European Commission	*CoR amendment*
	Decisions to designate a third country pursuant to Article 100, as well as the list of high-risk suppliers pursuant to Article 104, should be accompanied by a published non-confidential summary of the evidence and criteria on which the assessment was based, without prejudice to the protection of classified information and trade secrets, including a summary of the economic and operational impact assessment.

Reason
It is necessary to protect classified information, trade secrets and trade sensitive information and sensitive security information. These should not be a part of a non-confidential summary ipso facto. We added an executive summary requirement but not the proposed alternatives to avoid influencing open market and public procurement. However, in order for the summary to be useful to businesses and administrations, it should also reflect the practical consequences of the decision.

Amendment 3
COM(2026)11
Article 25(1)
Amend

Text proposed by the European Commission	*CoR amendment*
The Management Board shall be composed of one member appointed by each Member State ***and*** two members appointed by the Commission. All members shall have the right to vote.	The Management Board shall be composed of one member appointed by each Member State**,** two members appointed by the Commission ***and one member appointed by the European Committee of the Regions***. All members shall have the right to vote.

Reason
One permanent CoR representative is a proportionate adjustment that aligns governance with the implementation reality and closes a long-standing accountability gap.

Amendment 4

COM(2026) 11

Article 103

Add new paragraph 2a

Text proposed by the European Commission	*CoR amendment*
	As part of the assessment referred to in paragraph 4(b), and before adopting implementing acts pursuant to paragraphs 1 and 2, the Commission shall consult representatives of the types of entities referred to in Annexes I and II to Directive (EU) 2022/2555 that are expected to be affected by the proposed measures, including representatives of local and regional authorities, where such entities are operated by, or provide services to such authorities and shall take due account of the operational and financial impact of those measures. The assessment shall cover the degree of dependency on the supplier concerned, service continuity, the availability of suitable alternative suppliers and the need for realistic transition periods depending on the level of dependency and the criticality of the relevant services.

Reason
Mitigating measures impact local IT and services, yet only Member States and suppliers are consulted. Including local/regional input ensures practicality and respects subsidiarity.

Amendment 5

COM(2026) 11

Article 104

Add a new paragraph 7

Text proposed by the European Commission	*CoR amendment*
	When identifying high-risk ICT providers, the Union-wide procedure shall assess the potential operational, service continuity and financial impacts of the resulting measures on local and regional authorities operating critical infrastructure or essential services, including the extent of their dependence on the ICT provider concerned, and the representative bodies of those authorities shall be consulted

	where appropriate. The assessment should also address, where justified by the scale of technological dependency, migration costs, interoperability or essentiality of the services concerned, whether realistic transition periods are needed and whether adequate alternative providers are available. The measures and transitional periods shall be proportionate to the level of identified risk.

Reason
Local and regional authorities manage critical infrastructures and services that may be directly affected by the designations of high-risk ICT providers. The aim is to enable a consultation process where appropriate procedures ensure that operational realities form the basis for decision-making, support viable risk mitigation and strengthen the evidence base for implementation. Local and regional authorities may also be directly affected by decisions relating to high-risk ICT vendors. The assessment should therefore cover service continuity, costs, dependencies, transition timelines and practical options for deploying alternative solutions.

Amendment 6

COM(2026) 13

Add a new Recital 9bis

Text proposed by the European Commission	***Amendment***
	Member States should be able, in accordance with their legal system, to designate or recognise entities with cybersecurity responsibilities at regional level and to involve them appropriately in the implementation, supervision and enforcement of Directive (EU) 2022/2555 within their respective fields of competence, including, where applicable, as CSIRTs that may participate in the CSIRTs network in accordance with Union and national law. Union and national financing instruments should provide stable and accessible support for the development and operation of regional cybersecurity capabilities, including shared cybersecurity services.

Reason
The Directive should accommodate decentralised governance models and avoid presuming that all cybersecurity responsibilities are exercised exclusively at national level. In this regard, the sustainable development of regional cybersecurity capabilities should be promoted.

Amendment 7

COM(2026) 13

Add a new recital 10

Text proposed by the European Commission	*CoR amendment*
	(10) The grounds for withholding information, and the confidentiality safeguards provided for in this directive, are specific in nature and are intended to protect operationally sensitive or classified information. In particular, the amendments introduced by this directive to Article 21(5) concerning cybersecurity risk-management measures, and to Article 23(12) and (13) concerning reporting obligations and the handling of operationally sensitive or classified information, should be interpreted in that context. In respect of public administration entities, those provisions should not be construed as establishing a general basis for reducing the transparency of public administration, for restricting democratic scrutiny, or for withholding from parliaments or other elected bodies information of public interest that would otherwise be accessible under Union or national rules on access to documents and public accountability.

Reason
Confidentiality clauses (Art. 21(5) & 23) protect only sensitive info, not general admin. The recital clarifies this, ensuring transparency and accountability while safeguarding sensitive data.

Amendment 8

COM(2026) 13

Article 1(5)

Amend

Text proposed by the European Commission	*CoR amendment*
in Article 7(2), the following point (k) ***is*** added: '(k) for the transition to post-quantum cryptography, taking into account the transition timelines and relevant requirements set out in applicable Union legal acts and policies.';	in Article 7(2), the following point***s*** (k) ***and (l) are*** added: '(k) for the transition to post-quantum cryptography, taking into account the transition timelines and relevant requirements set out in applicable Union legal acts and policies***, as well as the need for risk-based prioritisation, realistic timelines and coordinated support for the***

	relevant public actors.' ***and '(l) measures to promote balanced territorial access to cybersecurity capabilities, expertise and support, including in rural, peripheral and sparsely populated areas.';***

Reason
When transposing this directive and allocating cybersecurity resources, expertise and funding, Member States should take into consideration balanced territorial coverage, so that rural, peripheral and sparsely populated areas, and smaller public entities, are not left without access to cybersecurity capabilities and support. The transition to post-quantum cryptography should be gradual and risk-based, and accompanied by guidance, funding and coordinated support, in order to ensure that responsibility is not passed on to individual local and regional authorities.

Amendment 9

COM(2026) 13

Article 1(5)

Add a new paragraph after (5)

Text proposed by the European Commission	***CoR amendment***
	Article 14(3) is amended as follows: The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service and European Committee of the Regions shall participate in the activities of the Cooperation Group as observers. The European Supervisory Authorities (ESAs) and the competent authorities under Regulation (EU) 2022/2554 may participate in the activities of the Cooperation Group in accordance with Article 47(1) of that Regulation. ***Where appropriate, the Cooperation Group may invite the European Parliament and representatives of relevant stakeholders to participate in its work.*** ***The Commission shall provide the secretariat.***

Reason
LRAs should be included in the cooperation group mechanism that operates effectively for Member State authorities.

Amendment 10

COM(2026) 13

Article 1(5)

Add a new paragraph after (5)

Text proposed by the European Commission	*CoR amendment*
	Article 14(4) is amended as follows: (t) to develop voluntary guidance on the equal treatment of public administration entities, in particular at local and regional level, which operate their network and information systems through shared structures such as inter-municipal ICT consortia, regional SOCs, shared platforms, or regional shared-service agencies, including on assessing their size and risk profile on an aggregate rather than entity-by-entity basis where appropriate.

Reason
Shared IT services (like inter-municipal consortia) are not treated in a uniform manner. The Cooperation Group should provide guidance to standardise this at the aggregate level, keeping the scope fair and unchanged. The guidance should also ensure that supervision, reporting and documentation do not lead to duplication or disproportionate administrative burden for the participating authorities. The guidelines are a voluntary helping hand, not a binding compliance document that would interfere with the guidelines at national level.

Amendment 11

COM(2026) 16

Article 88(2)

Amend

Text proposed by the European Commission	*CoR amendment*
Where Member States establish that, in light of national conditions, retail prices for the services referred to in Article 87(1) are not affordable, because consumers with low income or special social needs are prevented from accessing such services, they shall take measures to ensure affordability for such consumers of adequate internet access service and voice communications services at least at a fixed location.	Where Member States establish that, in light of national conditions, retail prices for the services referred to in Article 87(1) are not affordable, ***either*** because consumers with low income or special social needs are prevented from accessing such services, ***or because the transition from copper to fibre networks entails additional costs that put consumers who would have otherwise had access at risk of exclusion,*** they shall take measures to ensure affordability for such consumers of adequate internet access service and voice communications services at least at a fixed location.

Reason
The societal impacts that LRAs can see unfolding should be catered for.

Amendment 12

COM(2026) 16

Article 129(1)

Add a new letter (l)

Text proposed by the European Commission	*CoR amendment*
	(l) to hold a prior consultation with the representatives of local and regional authorities on specificities of local markets and impact on public interest in the region.

Reason
LRA representatives should be included in the institutional set-up of BEREC so that they are consulted at an early stage and not just at the end of the decision-making process.

Amendment 13

COM(2026) 16

Article 135

Add a new letter (l)

Text proposed by the European Commission	*CoR amendment*
	(l) to hold a prior consultation with the representatives of local and regional authorities on specificities of local markets and impact on public interest in the region.

Reason
LRA representatives should be included in the institutional set-up of RSPB so that they are consulted at an early stage and not just at the end of the decision-making process.

Amendment 14

COM(2026) 16

Article 136 (4)

Amend

Text proposed by the European Commission	*CoR amendment*
4. The Chair shall report to the European Parliament and to the Council on the performance of the RSPB's tasks when invited to do so.	4. The Chair shall report to the European Parliament***, to the European Committee of the Regions,*** and to the Council on the performance of the RSPB's tasks when invited to do so. ***These reports shall cover its territorial impact and specific recommendations for public***

	administrations.

Reason
Access to information that specifically affects them ensures that LRAs can fulfil their role in providing cybersecurity.

II. POLICY RECOMMENDATIONS

THE EUROPEAN COMMITTEE OF THE REGIONS (CoR)

CSA 2.0

1. welcomes the Commission proposal's ambition to strengthen trust in public authorities in an evolving threat landscape; trust also originates at local and regional level and is essential for effective governance. In this context, European cybersecurity certification schemes, including certificates and EU statements of conformity, can help reinforce trust;

2. underlines that local and regional authorities (LRAs) are expected to secure systems, protecting essential and important services and utilities, manage risks and support infrastructure deployment, despite very different levels of capacity across Europe. LRAs require targeted support, dedicated funding, and stronger involvement of regions in cybersecurity and connectivity governance frameworks;

3. calls for dedicated training programmes for LRAs, including continuous and multi-annual programmes, standardised guidelines and implementation models, joint exercises and exchanges of best practices, access to technical expertise and specialised consultancy, as well as the development of coordinated response and support mechanisms at European, national and regional level;

4. recognises that cooperation between ENISA (European Union Agency for Cybersecurity), MSAs (Member State Authorities) and LRAs should include practical guidance tailored to LRAs, in particular guidance helping to understand their obligations and identify optimal compliance approaches in light of the applicable national implementation of Directive (EU) 2022/2555, including where they operate their network and information systems through shared structures such as inter-municipal ICT consortia or regional shared-service agencies, applied training programmes and exchanges of experience between public authorities managing critical infrastructure;

5. highlights that many LRAs operate integrated vendor stacks in which replacement of a single component requires reconfiguration across entire service layers. A proportionality test must be anchored in the text of the regulation so that supply-chain measures do not risk forcing rip-and-replace mitigating measures that exceed LRAs' capacities and disrupt public services on which citizens depend; calls for realistic transition periods and dedicated technical assistance for LRAs in regions with permanent geographical disadvantages and limited capacity;

6. calls therefore for the CoR and LRAs to be consulted before issuing any mitigation measures currently envisaged by Article 103 of the regulation;

7. calls on the Commission to ensure that LRAs are represented in any expert group or advisory body supporting the EU-level assessment of high-risk ICT vendors, to ensure timely information-sharing by Member States with affected LRAs following the identification of such vendors;

8. highlights the importance of applying the EU ICT SCS Toolbox[2] and complementary national or ENISA-developed measures, including guidance for LRAs on public procurement requirements and supplier management, in a clear and simplified manner;

9. underlines the potential of voluntary pooling frameworks for procurement and delivery of cybersecurity services among LRAs. These can preserve subsidiarity while making operational cybersecurity affordable at local level;

10. demands continued support for regional intermediary structures, such as European digital innovation hubs, regional cybersecurity agencies, regional security operations centres and shared platforms, territorial computer security incident response teams and cyber campuses, as key vectors for capacity building; calls for stable, long-term funding and stronger cooperation between these structures, ensuring that their expertise and services can be shared where needed;

11. notes that for the effective implementation of the EU cybersecurity certification framework, local and regional administrations should benefit from additional EU-level support focused on skills and operational enablement. This should cover:

    a) EU-funded, ECSF-aligned training pathways aligned with national schemes for key certification roles (policy leads, technical evaluators, procurement officers, auditors and accreditation staff), coordinated under the Cyber Skills Academy to ensure consistency and mutual recognition across Member States;

    b) A dedicated ‘train-the-trainer’ programme and practical exercises (workshops, scenarios, implementation clinics) building on ENISA methodologies, to strengthen operational capacity and standardise exercise criteria;

    c) Operational toolkits supporting rollout, including templates, checklists and procurement guidance mapped to assurance levels and existing and upcoming schemes;

    d) Access to shared EU testing and evaluation capabilities (e.g. CSoA preparedness testing) and expert communities via the ECCC/NCC network, including short secondments and peer exchanges to transfer knowledge from early adopters;

    e) Targeted multi-annual funding agreed under the MFF 2028-2035 explicitly earmarked for ‘skills-for-certification’ capacity building in public administrations and regional

2 EU coordinated risk-mitigation framework for security of supply (SCS).

ecosystems with special attention to LRAs with limited administrative or technical capacity, including the costs of operations, maintenance, updates, expert staff and technology renewal during the lifecycle of the financed capacities

12. underlines that large European cities are critical institutional infrastructure for the EU and should therefore be considered strategic partners in EU cybersecurity policies, including resilience exercises, crisis drills and pilot projects with innovative technology;

13. notes that LRAs need to migrate early to post-quantum cryptography (PQC) but this should take place on the basis of a risk analysis and following an agreed migration plan; notes the CoR's foresight study on quantum technologies for LRAs (June 2026), which provides a roadmap for this transition; calls for dedicated PQC funding, expertise and coordinated support, including an ENISA-led taskforce and cooperation with national governments and EU-funded digital skills academies, to support implementation;

NIS 2 +

14. notes that the advantages of a more uniform approach will be realised gradually over several years, not immediately. LRAs note that they should be allowed to enjoy any simplification regimes stemming from current national rules, while preparing for the introduction of a new certification-based system; calls for proportionate transition periods, clear practical guidance and targeted financial and technical support, ensuring that the new system does not create additional administrative burdens for LRA;

15. calls for a proportionate, risk-based approach that avoids unnecessary administrative and financial burdens, with requirements aligned to the criticality of the service and stricter obligations reserved for high-risk or essential ICT services; stresses that simplification measures should aim to ensure that requirements only need to be met once, that existing national contact points are re-used and that any duplication of supervisory or reporting requirements is avoided; stresses the need to provide or facilitate technical assistance for entities with limited administrative or technical capacity, including entities with populations below 50 000 inhabitants or equivalent technical thresholds;

16. emphasises that access to and implementation of funding programmes by LRAs are becoming increasingly complex in the context of growing European and national cybersecurity and connectivity requirements;

17. demands that the European Competitiveness Fund digital window earmarks a dedicated envelope of the cybersecurity allocation for capacity building in LRAs with limited administrative or technical capacity; calls for simplified and direct access to this funding, based on transparent territorial criteria and with particular attention to small municipalities and rural, remote and border regions;

18. notes that the underutilisation of cybersecurity support schemes in some Member States highlights the need for greater awareness and stronger incentives to improve cybersecurity. Such incentives may include an information portal, change-management programmes and

measures linking public support and funding to a minimum level of cybersecurity maturity among beneficiary organisations;

DNA

19. welcomes the proposal to harmonise and streamline the governance of digital networks across the EU, enhancing predictability and investment; stresses, however, that implementation should avoid disproportionate administrative burden and compliance costs for businesses and public authorities;

20. welcomes the preservation of technological and service neutrality, while stressing that these principles must remain compatible with public-interest objectives such as an open internet, fair competition, digital inclusion, sustainability and network resilience; reiterates the importance of preserving and strengthening net neutrality safeguards, including by codifying relevant CJEU case law principles; the CoR stresses that network resilience measures must specifically take into account data centres, underwater cables, island connectivity and critical cloud services; calls, in particular, for the specific needs of island regions and other territories with geographical constraints to be factored in when developing resilience measures for digital networks and continuity of communications;

21. calls upon LRAs to carefully assess the proposed coordination mechanisms to avoid creating duplicative or administratively burdensome processes that would unduly burden the capacities of stakeholders without providing adequate benefits for the security and resilience of digital networks;

22. stresses that territorial cohesion must remain a central principle in the implementation of the future European framework for digital networks. Faster connectivity must respect subsidiarity and the role of local authorities in territorial planning and protecting the public interest; calls for targeted investment to guarantee affordable, high-capacity connectivity in regions facing permanent geographical or demographic disadvantages, preventing the digital divide from widening further;

23. supports the proposed institutional set-up, maintaining the Body of European Regulators for Electronic Communications (BEREC), transforming the Radio Spectrum Policy Group (RSPG) into a Radio Spectrum Policy Body (RSPB) and strengthening the BEREC Office (now the Office for Digital Networks, ODN);

24. calls on the Commission and BEREC to ensure that LRAs are involved, through structured consultation mechanisms and targeted stakeholder engagement, in the preparation of guidelines, opinions and other relevant outputs concerning matters that significantly affect the deployment or operation of electronic communications infrastructure at local and regional level like the specificities of local markets, public interest and expected societal impact, whether entrusted to the EU or national level;

25. calls for a clear and proportionate definition of the roles of these institutions. Where LRAs have established decision-making and working arrangements that are subject to change, care must be taken to adapt them accordingly;

26. highlights that, where spectrum decisions take place in a more centralised manner, LRAs must be able to feed territorial needs into decision-making processes, particularly for critical or strategic uses. Spectrum-related decisions should consider territorial impact and cohesion objectives; calls for structured consultation with LRAs and for coverage obligations that reflect the needs of emergency services, critical infrastructure and communities in regions facing permanent geographical or demographic disadvantages;

27. stresses that, should plans for transition to fibre optics and copper switch-off become obligatory, LRAs consider it essential that local specificities be considered when developing such plans, including setting appropriate measures to mitigate negative impacts on crisis management and to maintain the continuity of operations;

28. calls, in this context, for LRAs, together with national governments, to be invited to examine any negative social impact due to the copper switch-off, and to contribute to the development of mitigation measures;

29. highlights that digital infrastructure must be able to ensure, inter alia, reliable communication by public security authorities even in crisis situations (e.g. large-scale power outages, natural disasters, hybrid threats and significant network congestion). We support solutions that strengthen the resilience of networks, the protection of emergency communications and the administrations' ability to ensure the security of the population. The CoR stresses that certain regions with permanent geographical or demographic disadvantages are particularly exposed to natural disasters and connectivity disruptions, and calls for dedicated investment in resilient backup infrastructure and emergency communication redundancy in these territories, in cooperation with local and regional civil protection authorities;

30. believes that the European digital transformation must be based on the principles of innovation, security, public trust and streamlined administration, avoiding any unnecessary red tape and favouring the rapid uptake of new secure technologies at the service of the public;

31. urges the European Commission to support the development and uptake of European cybersecurity technologies, reducing strategic dependencies;

32. urges the Commission and BEREC to ensure that local and regional authorities are involved, through the mechanisms and capacities deployed at that level, in managing crisis situations on digital networks under their area of responsibility, especially in cases where their cybersecurity is affected.

Brussels, 13 October 2026.

The President
of the European Committee of the Regions

Kata TÜTTŐ

The Secretary-General
of the European Committee of the Regions

Petr BLÍŽKOVSKÝ

III. PROCEDURE

Title	Cybersecurity Review and Digital Networks Act
Reference(s)	**COM(2026) 11** Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 **COM(2026) 13** Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2] **COM(2026) 16** Proposal for a Regulation of the European Parliament and of the Council on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision No 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision No 243/2012/EU
Legal basis	Optional, Art. 307(3)
Procedural basis	(Rule 41(b)(i))
Date of Council/EP referral/Date of Commission letter	COM(2026) 11: Council (1/4/26), EP (5/2/26), EC (21/1/26) COM(2026) 13: Council (01/04/26), EP (4/2/26), EC (22/1/26) COM(2026) 16: EP (4/2/26), EC (21/1/26)
Date of Bureau/President's decision	3 February 2026
Commission responsible	Commission for Economic Policy (ECON)
Rapporteur	Zdeněk HŘIB (CZ/GREEN+PRO)
Discussed in commission	23 April 2026
Date adopted by commission	6 July 2026
Result of the vote in commission	Majority
Date adopted in plenary	13 October 2026
Previous Committee opinions	• Cybersecurity of hospitals and healthcare providers • EU Cyber Solidarity Act and Digital Resilience
Subsidiarity reference	Subsidiarity check – No Subsidiarity compliance – N/A