BoR (26) 88_6

BEREC'S POSITION ON RESILIENCE AND PREPAREDNESS

2 June 2026

Key messages

- BEREC supports the DNA focus on resilience and commits to contribute to this aim within its field of expertise. However, the interplay among different authorities involved as well as among different EU legislations should be better defined.
- The elaboration of the Preparedness Plan should be assigned to BEREC, with the support of the ODN, considering the expertise and resources required. Along these lines, the timing for the preparation of the Plan should be more flexible, considering the complexity of the matter.
- To ensure legal certainty, a definition of "critical communications" should be included in the DNA.
- Withdrawing the right to provide networks and services is a last resort structural measure, extremely rarely imposed due to the impact on market structure and end users. NRAs' discretion in relation to the general authorisation must also be preserved in relation to the CSA 2 obligations.

Commission proposal:

Key resilience-related proposals in the DNA include:

EU-wide Preparedness Plan for Digital Infrastructures

The proposal introduces a comprehensive Union Preparedness Plan for Digital Infrastructures, aimed at enhancing coordinated crisis preparedness and response to natural disasters, foreign interference, cybersecurity incidents, and other systemic risks affecting critical networks. This plan will include operational recommendations, data collection and a consistent approach across Member States to strengthen continuity and redundancy in digital infrastructure.

Strengthened Security and ICT Supply Chain Requirements

Under the DNA, network and service providers will be subject, within the General Authorisation regime, to additional obligations related to security and resilience with a particular focus on mitigating ICT supply chain risks. The framework intends to align with and complement existing EU cybersecurity instruments such as NIS2 and the proposal for a revised Cybersecurity Act (CSA2) to ensure robust risk management and incident prevention strategies.

Enhanced Emergency Communication and Public Warning Provisions

The proposal aims to strengthen the resilience of emergency communications, including obligations for network preparedness, testing, and ensuring reliable access to emergency services (e.g., 112) even under stress or disruption.

Reduced Dependencies and Strategic Autonomy

By targeting strategic dependencies within the connectivity ecosystem and fostering EU-level cooperation mechanisms, the DNA aims to build a more resilient single market for connectivity, reducing vulnerabilities stemming from fragmentation and uncoordinated responses to crises.

BEREC's assessment:

BEREC's role and support for resilience measures

BEREC notes the enhanced role foreseen for NRAs and for BEREC and the ODN in resilience and preparedness. As recognised by the DNA, coordination among NRAs, BEREC, the ODN, and other EU and competent national stakeholders is central to achieving harmonised resilience outcomes across the Union. As a matter of fact, these sovereignty aspects, which may be vital for the EU's continuity of economic activities and preservation of human lives during crises, have rarely fallen under the competence of NRAs, being rather generally under the remit of other competent authorities to date. Therefore, the definition of this new role and the associated skills, in accordance with competence breakdown among Member State administrations, needs to be carefully assessed and set up. Furthermore, national security regulations on classified information will impose restrictions on the data that may be shared with BEREC and the ODN.

BEREC notes that the expanded responsibilities under the DNA will require adequate staffing, expertise and resources at both, NRAs within BEREC and ODN. Ensuring that NRAs and BEREC are sufficiently equipped and resourced is essential to effectively deliver on strengthened resilience objectives and to maintain regulatory effectiveness.[1]

BEREC also notes that the proposed resilience-related provisions may place additional regulatory obligations on network providers. Therefore, due consideration must be given to the interplay with related horizontal legislation and potential duplicities of obligations, including in reporting obligations. It is also necessary to ensure that both Member States and NRAs can issue binding instructions to entities to enforce the new obligations, otherwise, the intended objectives may not be achievable.

Terms that are central to the scope of the DNA, such as "critical communications" need to be defined and the proposed timelines for the delivery of the Union Preparedness Plan for Digital Infrastructures (12 months after the entry to force according to Article 6(1)), as well as of the template for data gathering (6 months according to Article 7(4)), deserve careful consideration, especially with a view to the need to reinforce expert resources on this area and the complexity of the task.

More specific comments on the DNA proposals on resilience and their relation with the CSA2 proposal are provided in the following sections:

Resilience – Articles 4–8

In the DNA, new provisions are proposed concerning the overarching objective of enhancing resilience, against challenges arising from natural or man-made disruptions. While BEREC welcomes the initiative to enhance the resilience of networks at the EU level, as stated and explained above, the proposal could create a complex regulatory framework with overlapping provisions across different legal acts (NIS2, CSA2, DNA), which needs to be addressed carefully. The delineation between the DNA and other legal acts in the field of cybersecurity, as well as its implications for national legislation in the Member States, should be clearly analysed and clarified.

One example of the above issue is Article 5 of the proposed DNA Regulation, which addresses ensuring continuous availability of electronic communications networks and services. Regulation in

[1] This requirement is already included in the Draft CSA2 Art. 112(3): *"Member States shall ensure that their competent authorities have appropriate powers, sufficient human and technical resources and relevant expertise to effectively carry out the supervisory and enforcement measures referred to in Article 114".*

this area will likely address issues relating to security measures, such as requirements for redundancy and backup power, which are regulated in some of the Member States under the national NIS2 transposition and may be further specified in national regulations issued on this basis. If providers are subject to both the proposed DNA Regulation and the NIS2 Directive, there is a risk of overlapping regulatory requirements.

The proposal to establish a Preparedness Plan for Digital Infrastructure at EU level presupposes, as follows in more detail from Article 7 DNA, the collection of information on national critical infrastructure. BEREC notes that in many Member States such information may be classified for national security purposes and therefore cannot be disclosed to EU institutions. It may therefore be questioned whether data collection of the intended kind at EU level is feasible in practice.

It is essential to clarify in Articles 5 and 6 of the DNA that measures safeguarding national security fall outside the scope of the Regulation. The scope of activities carried out by BEREC should be limited to fostering cooperation between Member States, ENISA and the Commission on ensuring the continuous availability of electronic communications networks and services, and should not extend to the harmonised implementation of regulatory requirements.

General authorisation and "Single Passport" with a view to CSA2

The requirements associated with General Authorisation are closely linked with the implementation of Directive (EU) 2022/2555 (NIS2) at national level. In particular, Article 9(4)(d) of the DNA covers, among the General Authorisation conditions, also technical and non-technical requirements under the proposed CSA2, which may be further specified through implementing acts. These areas are also covered by the NIS2 Directive. As a result, the full harmonisation of authorisation requirements pursued under the DNA may in principle extend into areas governed by NIS2, which is based on a minimum harmonisation instead.

In addition, according to the DNA proposal, the rules on General Authorisation and "Single Passport" would affect the current allocation of supervisory responsibilities, in a way that, as regards enforcing the General Authorisation conditions, national authorities in Member States where the electronic communications networks and services are provided would lose the exclusive right to exercise supervision over undertakings operating within their territory. While they would retain certain supervisory powers, key enforcement decisions would need to be taken by the NRA of notification (see BEREC paper on General Authorisation).

In relation with that and in the framework of general authorisation, BEREC highlights that, under the proposed DNA, the provision of electronic networks and services would be conditional upon the provider's compliance with the trusted supply chain framework under the proposed CSA2, among other requirements (cf. Article 9(4) DNA). According to the CSA2, any decision on compliance with such framework is made by the CSA2 competent authority, which is the NIS2 authority in the country where services/networks are provided. (Art. 112 (1) CSA2 states "Each Member State shall designate the competent authorities referred to in Article 8 of Directive (EU) 2022/2555 as authorities responsible for taking the supervisory and enforcement measures referred to in Article 114").

According to Article 196 (10), the competent authority under CSA2 may therefore request the DNA authority in the Member State of provision of services to withdraw their rights under the General Authorisation regime or to withdraw individual rights of use of spectrum. In such situations, the role of NRAs appears to be significantly constrained, as they would be required to act on such requests without a meaningful possibility to assess proportionality or the potential impact on the market. In

practice, this would amount to the execution of a decision taken by the CSA2 authority, rather than an independent regulatory assessment. This would imply a deviation from the basic principle that **the authority granting the authorisation should be the one empowered to withdraw it**. It is further noted that withdrawing the right to provide networks and services (market exit) is a last resort structural measure very rarely imposed. While agreeing and supporting the objectives of cybersecurity, there are equally important obligations that providers need to comply with, which allow for a case-by-case assessment of the infringement and some margin to adopt efficient but proportionate measures.

Where the request is made by the CSA2 authority in the Member State of notification, due to concerns related to supply chain security, this would require coordination at national level, as the CSA2 authority and the NRA may be different entities.

Where the request is made by a CSA2 authority in a Member State of provision other than the one of notification, the situation would become even more complex, as the NRA in that Member State would be required to act in relation to rights granted by the NRA of another Member State. This would create a cross-border enforcement scenario with significant implications for the allocation of responsibilities and regulatory coherence.

Hence, BEREC would like to suggest clarifying the following aspects:

- Flexibility is needed for NRAs regarding how the rights or the General Authorisation would be withdrawn (e.g., regarding the timing (cf. f. ex. Art. 196) and any measures to ensure that end users' interests are safeguarded etc. In such a case, Art. 196 (10) should be adjusted
- It has to be addressed how this would work in practice also with regard to legal redress (NRA makes a decision without any or with limited margin of discretion based on the assessment and evaluation of another agency and thereby undoes a general authorisation that was initiated in the MS where the notification was made).
- It has to be clarified if the withdrawal of rights is absolute or relative to the services/networks impacted by the breach of conditions (removal of critical components from high-risk suppliers), as well as either Union wide or limited to the specific country where services/networks have been impacted by the breach. Many providers offer a range of services, fixed, mobile and wireless services, as well as other services that are covered by NIS2 but not by the DNA. Removal of rights to provide DNA services in the scope of the DNA would have a serious impact on the viability of providing these other services.
- The DNA needs to reflect how this information of the withdrawal of rights should be included in the ODN database and how it would impact the current or even future provision of services/networks in other MS. The DNA text seems to consider the withdrawal as final (Art. 196(9) gives the option to suspend or withdraw, while Art. 196 (10) only foresees the withdrawal, perhaps because it is meant as a final resort option if other measures by CSA-Authority are not successful). If this is not intended, the DNA proposal needs to clarify this as well and provide for how rights can be reinstated or whether a new notification is required.

<u>Alternative proposals:</u>

BEREC proposes to include a definition of "critical communications" in the DNA.

BEREC suggests giving more flexibility regarding the timing of the Preparedness Plan to take into account the required resources.

BEREC requests to add clear guidance on how the general authorisation scheme should work with regard to the ICT supply chain security requirements under the CSA 2, based on the questions raised above (see BEREC's position on the General Authorisation regime BoR (26) 88_1_).

BEREC considers that the drafting of the plan should be assigned to BEREC with the support of the ODN, and not just to the ODN, as after all, the plan will be approved and endorsed by BEREC (cf. BEREC's position on Governance, BoR (26) 88_2).