Ref. Ares(2025)10600012 - 02/12/2025

Verisure´s contribution to the draft BEREC 2026-2030 Strategy

Introduction to Verisure

Verisure is the leading European provider of professionally monitored security systems which protects almost 6 million customers (households and small/medium businesses) across 13 countries in Europe and 4 in Latin America and has more than 30,000 employees worldwide. We operate as *Verisure* in most of our markets, and as *Securitas Direct* in Spain, Portugal, and Sweden. In 2020 *Arlo Europe,* which is Europe's leading provider of Smart Security Cameras, became part of *Verisure*.

Verisure's mission is to bring peace of mind to families and small business owners by providing them with the best security solutions and services. A pioneer in innovation and technology, *Verisure* continuously invests in providing effective, intelligent, and reliable security solutions. This includes research & development centers in Geneva, Madrid and Malmö with more than 1,700 technologists developing new products, or external partnerships with industry leading technology companies.

Verisure Group stands as a premier provider of private security and teleassistance services, acknowledged as essential services in several countries where we operate. This recognition underscores the critical role these services play in ensuring the safety and security of end users.

To deliver unparalleled security solutions, Verisure leverages cutting-edge IoT devices, seamlessly integrated through robust mobile network communications. As one of the largest IoT service providers in the European Union, Verisure has established a formidable presence with devices managing an impressive volume of over **1.4 trillion signals in 2024**, ensuring a continuous and responsive security infrastructure.

Verisure' s commitment to innovation and reliability has solidified its position as a leader in the security sector, dedicated to providing top-tier protection and peace of mind to our clients.

C1-Public

Verisure is member of Confederation of European Security Services (CoESS), *Euralarm, EENA* and takes part in European Committee for Electrotechnical Standardization (CENELEC) national committees, with direct presence in 8 of them.

Verisure welcomes the possibility of contributing to the public consultation on the draft BEREC Strategy 2026-2030, a relevant strategic guide to align BEREC's actions with upcoming market, technological, and regulatory developments over the coming five years. **Verisure contribution is focused on giving our feedback to 'Priority 3: empowering end-users', as we leverage this opportunity to address a critical issue for our operations regarding the phase-out of mobile technologies and its impact on end-users**. It elaborates on the issue, offers key references, and suggests actions for BEREC to address the problem and include strategic actions in its strategy.

1. Current challenges in the face of network changes

Need to secure continuity of emergency and essential services before migrating to new technologies

The planned phase-out of 2G and 3G networks in favor of 4G and 5G poses significant challenges. In Europe, many monitoring and alarm response services still depend on 2G/3G networks. The transition has been complicated by the fact that 2G/3G shutdowns are outpacing the deployment of 4G/5G infrastructure. This also requires careful consideration of the needs of end-users, associated costs, and the complexities of operator migration planning, impacting products and services in utilities and commodities, such as monitored security and safety systems, critical infrastructure, vehicle eCall services, and the broader IoT ecosystem.

2G and 3G networks have been the backbone of mobile connectivity for many years, supporting a wide range of IoT services. These networks are especially important for security and safety systems that depend on reliable emergency signaling. The sudden phase-out of these networks without adequate preparation can lead to significant disruptions, affecting the reliability of these crucial services. This was most recently seen in Australia, where the attempt to phase out last year had significant implications for both consumers and businesses, notably with a loss of connectivity and access to emergency services.

C1-Public

One of the major challenges is the disparity between the life-cycle of IoT devices and that of mobile networks. IoT devices, particularly those installed in customer premises, often have a long life-span of up to 20-25 years. In contrast, mobile networks have increasingly shorter life-cycles. This mismatch means that IoT devices may outlive the networks they rely on, necessitating premature and frequent replacements, which can be both costly and logistically challenging.

The shorter life-cycle of communication networks forces replacement of fully functional equipment, involving very significant additional cost and operational diversion.

Additionally, the faster obsolescence of networks contributes to the growing problem of electronic waste, which poses significant environmental and health risks. Finally, changing IoT devices installed at customer premises is not a straightforward task. It requires user intervention, as the change must be done inside homes and offices. This adds another hurdle, which at best involves inconvenience for the end-users and at worst means that critical IoT devices are not replaced, with risk to safety and security.

Considering these challenges, it is imperative that national governments, telecom operators, and industry players work together to establish clear and inclusive transition plans. In line with BEREC draft strategy, we support the need for closer monitoring of the process and planning of phasing out legacy to prevent negative impacts. The shutdown plans should ensure continuity for all essential services, including private security services, and consider the long life-cycle of IoT devices. It is natural for consumers and industry to expect the availability of services to maintain connections and reach out for assistance when needed.

Need for a well-planned and coordinated approach

A well-planned and coordinated phase-out of 2G and 3G networks, developed in close collaboration with all affected stakeholders, including private security services, is crucial to avoid significant societal and economic disruptions and ensure uninterrupted service. However, this is not the case today. The lack of coordinated national strategies has resulted in high levels of uncertainty, absence of proper impact assessments, fragmented shutdown schedules, low public awareness, and increasing risks of essential service interruptions or

C1-Public

disconnections. Indeed, comprehensive network transition plans seem absent today in part due to insufficient transparency and collaboration among stakeholders.

In France, a report by the Parliamentary Higher Commission for Digital Technology and Postal Services from April 2025[1] has highlighted the lack of communication and preparation among stakeholders regarding the 2G/3G shutdown. The report calls for stricter regulations on the 2G/3G network phase-out to ensure that affected stakeholders are not adversely impacted.

In December 2023, the Finnish Ministry of Communications noted after performed impact analysis including public consultation that 2G networks were still heavily used by IoT devices for critical services (such as energy) and that migrating over 90% of these services was not feasible before the end of 2029. Consequently, the Ministry approved changes to operator licenses[2], requiring the maintenance of the 2G band until December 31, 2029, and mandating operators to provide end users at least one year's notice for any changes.

Similarly, in Norway, the Parliament requested an impact assessment of the 2G network shutdown in March 2025, following concerns about its implications. The government instructed the National Communications Authority (Nkom) to conduct this assessment. In its report, published in July 2025, Nkom recognized that among others home alarm systems, SOS buttons in cars, lift alarms and social alarms would stop working, but still considered that the shutdown could start in 2025 in a controlled manner given that the main network provider, Telenor, would keep its network open and could serve as a backup network provider if needed. Network provider Telia will also maintain readiness after shutdown and can switch on its 2G network if required for life and health[3].

Even for 4G/5G capable devices, there remain open questions on the impact of 2G/3G sunset. This is especially related to the use of SMS. SMS is an important communication channel for many IOT devices. Today, it relies on the 2G/3G networks. However, GSMA's recent report on SMS continuity post-sunset recognizes that there remains uncertainty on the different technical approaches operators may choose to take. There is limited to no

[1] Avis-n°2025-02-du-10-avril-2025-sur-les-consequences-de-la-fin-des-technologies-2G-et-3G.pdf

[2] https://lvm.fi/en/-/changing-licence-terms-for-telecom-operators-2g-technology-to-be-maintained-until-end-of-2029

[3] https://www.nrk.no/nyheter/regjeringen-slukker-2g-nettet-1.17483476.

C1-Public

public data today on the subject. This uncertainty makes it difficult for IOT operators to plan on how to ensure service continuity on a go-forward basis.[4]

All of the above shows that urgent and coordinated action is needed and BEREC should play a key role in ensuring coordination and certainty among Member States governments must work with telecom operators and industry players to establish clear, inclusive transition plans that ensure continuity for all essential services, including private security services.

2. Broader challenges linked to technology shifts: Action needed

Increase NRAs role on Spectrum management

Action of the NRAs in each of the Member States is key to addressing the critical issue of ensuring service continuity for IoT services that rely heavily on mobile communication networks. As mobile networks are a fundamental input for the provision of millions of IoT services, **we urge BEREC to call national regulators to intervene to prevent negative impacts when these networks undergo changes or shutdowns.** At the same time, we ask BEREC to support any regulatory development which reinforces Member States´s power to intervene in any mobile network changes or shutdown plans that could potentially impact on the services provided over these networks, for example, through the future Digital Networks Act that the European Commission plans to publish by end of 2025.

In accordance with what is foreseen in Priority 3, BEREC should encourage actions by Member States to oversee the planning of Operators' networks and mitigate any adverse effects on end users. To achieve this, Member States should:

[4] GMSA, *Ensuring SMS Continuity for IOT after 2G/3G sunset,* May 2025 (SMS-for-IoT-after-2G-3G-Shutdown.pdf

C1-Public

- Establish requirements for telecommunications providers to inform each national Regulator about their network transition plans and specific shutdown dates.
- Require Operators to keep Regulators informed about any developments related to their shutdown plans and timelines.
- Consider intervening or even vetoing shutdown plans if service continuity is not assured.
- Regulatory oversight, including the power to intervene or veto shutdowns plans if service continuity or citizens' rights might be at risk.

By promoting these measures, and reinforcing the role of national authorities, we can ensure that the transition to new technologies is managed in a way that preserves the reliability and accessibility of essential services, thus preventing any disruption to the millions of IoT services that depend on mobile communication networks.

Need to ensure end-users protection

As stated in the draft Strategy 2026-2030 as 3rd priority:

*"While end users are increasingly being given the opportunity of benefitting from new and enhanced connectivity thanks to the migration to VHCN**, the process for phasing out legacy networks will have to be closely monitored to prevent negative impacts."***

As we transition towards advanced digital networks, it is imperative to establish robust safeguards to protect end-users and maintain service continuity. The complexity and criticality of mobile networks, especially for providers such as Verisure, requires a thorough and preemptive approach to any network changes.

One of the **principal reasons for the necessity of these safeguards is the current lack of comprehensive analysis before implementing significant network changes**. Presently, there is an alarming absence of detailed information on the number of customers affected, the types of services impacted, and the potential implications for network performance. Without conducting a proper impact assessment beforehand, we run the risk of unintended consequences that could severely disrupt services. This oversight is

C1-Public

particularly concerning for sectors dependent on uninterrupted connectivity, such as the Internet of Things (IoT) service providers.

It is important to define an inclusive approach to identifying individuals who may be considered vulnerable during this process, such as customers who are more likely to use older devices and therefore depend on legacy technologies. This includes implementing specific actions to ensure that these groups are not excluded. Ofcom's report, "3G and 2G switch-off: Our expectations of mobile providers (Feb. 2023)," outlines various regulatory initiatives aimed at mitigating these risks. Another significant issue is the insufficient real-world testing before emergency systems are deployed. Often, mobile networks, user devices, and Public Safety Answering Point (PSAP) systems are not tested together, leading to the discovery of major problems only during actual emergencies, which poses risks to users. It is crucial to regularly and comprehensively test all components of the emergency communication system to identify and resolve these issues before they impact real-life situations. Without such testing, issues are likely to emerge during real emergencies, putting users in significant danger.

Furthermore, **before retiring legacy systems, public authorities, mobile operators, and emergency service providers must collaborate to ensure that new technologies meet or exceed the levels of accessibility, resilience, and functionality provided by the existing systems**. It is crucial that emergency communications remain uncompromised during the digital transition. The expectation is that these new networks will provide enhanced capabilities, but without the proper safeguards, we may inadvertently introduce vulnerabilities that could have been avoided with thorough planning and cooperation.

To mitigate these risks, Verisure asks **BEREC to support any regulatory development (through upcoming EU Digital Networks Act) that emphasizes that any changes to communication networks impacting the continuity of end users' services should protect their rights** through the following measures:

C1-Public

- Conduct public consultations to identify challenges and risks for users and sectors.
- Require that operators provide a minimum of 7-year advance notice to ensure visibility and preparedness.
- Implement nationwide information campaigns to keep all stakeholders fully informed.
- Ensure the continuity of emergency and essential services, if needed through continued legacy network availability for such services.
- Offer targeted support to ensure vulnerable populations maintain access.

Additionally other regulatory measures can be temporarily implemented to ensure technology availability such as has been the case with the Universal Service Obligations in some countries in the past. BEREC should support any measure that entitles Member States to define **remedies based on national roaming on a given network which will guarantee services for a sufficient period of time** even if the rest of the operators begin the shutdown process.

In conclusion, in order to keep fulfilling BEREC mission of fostering independent, forward looking, consistent and high-quality regulation of digital infrastructures and services for the benefit of Europe and its citizens, measures proposed in this contribution are a necessity to ensure a smooth transition to new network technologies. By proactively addressing potential issues and coordinating actions at European level, BEREC can promote collaboration and protect end-users, while reliability and efficiency of critical services is ensured during periods of transition.

July 2025

C1-Public