26 August 2026

Vodafone response to BEREC Call for Inputs on interfaces for mobile networks

Executive summary

Vodafone welcomes BEREC's Call for Inputs and supports the development of a competitive, innovative and well-functioning European market for Network APIs. Standardised Network APIs, particularly those developed through CAMARA and GSMA Open Gateway allow developers and application providers to access advanced network capabilities through common interfaces, reducing fragmentation and enabling new digital services to scale across operators and countries.

Network APIs can support important European policy objectives including digital competitiveness, cybersecurity, fraud prevention, trusted digital identity, industrial digitisation and high-performance connectivity. Early market traction is strongest in identity, authentication and anti-fraud use cases, while emerging network programmability APIs, such as Quality on Demand, can support future applications requiring more predictable network performance.

Vodafone's central regulatory message is that the market needs clarity and consistency across markets more than new layers of regulation. Industry standardisation is progressing, but inconsistent interpretation of privacy, ePrivacy, traffic data, location, Open Internet and national telecoms rules can block or delay deployment of otherwise standardised APIs.

These challenges are not theoretical. Vodafone's internal regulatory work identifies specific barriers affecting secure authentication, Branded Calling, Quality on Demand, anti-scam APIs, Location APIs and broader cybersecurity APIs. BEREC can support market development by helping clarify how existing rules should apply to Network APIs in a proportionate, outcomes-based and innovation-enabling way.

Vodafone therefore encourages BEREC to support a framework that combines industry-led technical standardisation with clear, proportionate and consistent regulatory interpretation across Member States. This would help developers build once and scale, enable operators to invest with confidence, and allow Europe to capture the innovation and consumer-protection benefits of Network APIs.

Key messages for BEREC

- **Network APIs are pro-innovation and pro-consumer:** they expose advanced network capabilities in a standardised, secure and controlled way and help protect consumers from scams, fraud and cyber threats. They also have the potential to improve customer experiences and enhance digital service that benefit consumers
- **Open standards are necessary but not sufficient:** CAMARA and GSMA Open Gateway reduce technical fragmentation, but regulatory fragmentation can still prevent scale – in order to scale we also need consistency across regulations and their interpretation otherwise industry standardisation isn't enough
- **BEREC should focus on clarity, consistency and proportionality:** the key ask is to ensure the regulatory framework *supports* the development of network APIs, taking the opportunity of the Digital Networks Act (DNA) to modernize the rules applying to network APIs, such as ePrivacy and Open Internet; and then ensuring a harmonised interpretation of these rules, especially privacy, ePrivacy, traffic data, location data and Open Internet rules.
- **Regulation should focus on purpose and safeguards:** for anti-fraud, cybersecurity, location and QoD use cases, the assessment should consider consumer benefit, proportionality, minimisation, auditability and the absence of harm to other users.
- **Europe needs a level playing field:** operators should not be structurally prevented from using network-derived data for consumer protection where comparable third-party device or SDK-derived data can be used for similar purposes without the application of disproportionate regulation.
- The Open Internet framework is currently blocking the improvement of customer experience and digital services through Quality on Demand – we ask that these regulations are modernised to allow QoD to scale to the benefit of consumers.

Draft responses to BEREC questions

1. What roles has each player in this complex ecosystem?

Mobile Network Operators provide the network capabilities and data that underpin Network APIs. These capabilities are exposed through standardised, secure interfaces so that developers and application providers can use them without needing to integrate separately with each operator's proprietary systems.

MVNOs and MVNEs may participate depending on their technical architecture, commercial role and access to underlying network capabilities. In some cases they may act as API consumers or channel participants; in others, the relevant network capability will be provided by the host MNO.

Aggregators, channel partners and CPaaS providers simplify market access by offering developers a single technical and commercial route to APIs from multiple operators. Network vendors provide exposure platforms and underlying technical capabilities. Cloud providers can integrate Network APIs into developer environments. Developers and application service providers build the end-user services, while end users benefit from improved security, authentication, connectivity, fraud prevention and digital experiences.

2. Can you provide publicly available information on market demand, predictions and market development?

Market demand is being driven by the need for trusted digital identity, fraud prevention, secure authentication, anti-scam capabilities, location-enabled services, network insights and more predictable connectivity. Demand is particularly visible in sectors such as financial services, e-commerce, cybersecurity, media, transport, manufacturing and public services.

The market is developing in phases. Early deployments are concentrated around identity and anti-fraud APIs such as Number Verify and SIM Swap. The next phase is expected to include more advanced capabilities such as Quality on Demand, connectivity insights, location services, edge discovery and other network programmability use cases.

Industry-led initiatives such as GSMA Open Gateway and CAMARA have improved the outlook by creating a common framework for implementation. This reduces integration friction for developers and increases the likelihood of cross-border scale.

3. Can you provide publicly available information on business models and pricing models?

Network API business models are still developing, but several models are emerging. Identity and anti-fraud APIs are often suited to usage-based or transaction-based charging, for example per API call or successful verification event. Other API categories may support subscription, tiered usage, bundled or outcome-based models.

Aggregators and channel partners may package APIs from multiple operators into propositions for developers and enterprises. This can simplify procurement and integration, but it requires transparent commercial terms, reliable service levels and sufficient operator coverage.

The appropriate pricing model will depend on the API category, customer use case, value delivered, required service levels and ecosystem role of the provider. For network programmability APIs such as Quality on Demand, commercial models will also depend on the regulatory classification and safeguards expected by regulators.

4. In what way can Open APIs enable or support a dynamic and well-functioning European market?

Open APIs reduce fragmentation. Historically, developers needed to integrate with individual operators and local proprietary interfaces. Standardised APIs allow application providers to build once and scale across different networks and countries.

This supports competition by lowering barriers to entry for developers and digital service providers. It also supports investment by enabling operators to monetise advanced network capabilities through consistent, scalable products.

For Europe, Open APIs can support digital sovereignty, trusted identity, cybersecurity, industrial digitisation, high-performance connectivity and new digital services across sectors. However, Open APIs will only deliver this benefit if technical standardisation is matched by consistent regulatory interpretation.

5. How can adoption of Network APIs be accelerated?

Adoption can be accelerated through continued industry standardisation, consistent implementation of CAMARA APIs, broader operator participation in GSMA Open Gateway and regulatory clarity. Without regulatory consistency across markets, adoption is restricted.

Regulatory clarity and standardisation are critical. Developers and operators will invest more confidently where there is an effective, consistent and predictable interpretation of privacy, ePrivacy, traffic data, location, data protection and Open Internet rules across Europe. Without this, a technically standard API can still become commercially fragmented market by market and this is currently hampering efforts to scale across markets.

Developers need simple onboarding, clear documentation, predictable commercial terms, testing environments, transparent performance information and access to APIs through the channels they already use, including aggregators, CPaaS providers and cloud platforms – which is why continued standardization is important to accelerate adoption and growth.

Adoption would also benefit from broader regulatory recognition of network-derived data as a trusted source for compliance use cases. For example, in areas such as age verification, acceptance of network signals can vary by country, with some markets recognising them as valid evidence while others do not. This fragmentation limits scalability, increases implementation complexity and weakens the business case for pan-European services. Greater consistency in the acceptance of network-based credentials and signals would help create stronger demand and accelerate market adoption

6. What are the main drivers for successful adoption of Open APIs in Europe?

The main drivers are interoperability, standardisation, geographic coverage, demonstrable business value, developer experience, trust, privacy and regulatory certainty.

APIs must be technically consistent across operators; commercially easy to access; and legally predictable across Member States with consistent regulation that facilitates adoption. Without these conditions, developers may not see sufficient scale to justify adoption.

European adoption will be strongest where APIs solve clear problems, such as fraud reduction, secure customer journeys, scam prevention, industrial automation, quality-sensitive applications and operational resilience. BEREC can support adoption by ensuring that the regulatory framework enables these legitimate use cases with proportionate safeguards.

7. What are the main technical and commercial challenges?

Technical challenges include achieving consistent API behaviour across networks, integrating new exposure capabilities with legacy environments, managing different levels of network maturity, ensuring interoperability across network vendors and delivering reliable performance information.

Commercial challenges include creating sufficient geographic coverage, proving return on investment, building developer awareness, establishing sustainable pricing models and simplifying contracting across multiple operators and markets.

Regulatory uncertainty is also a commercial challenge. If operators and developers cannot predict whether a use case will be permitted, whether consent is required, whether network-derived data can be used, or whether QoD can be offered under Open Internet rules, investment and go-to-market decisions are delayed.

8. Do you see any regulatory challenges?

Yes. Vodafone's primary concerns are regulatory uncertainty and regulatory fragmentation. Network APIs are increasingly designed as standardised, cross-border digital services, but applying relevant regulations can be very challenging, compounded by the fact that regulatory interpretation can vary significantly by market and by API category. This can affect launch timelines, product design, technical architecture, contracting models and developer confidence.

In addition to what has already been covered in the above responses, we see additional regulatory challenges.

Open Internet: For Quality on Demand, the key challenge is how temporary, purpose-specific quality enhancements should be treated under the Open Internet Regulation (and its national implementation). QoD is not intended to create permanent 'fast lanes', or block competing services or degrade best-effort internet access. It is a temporary, narrowly scoped and controlled capability for defined interactions, with admission controls and network policies.

However, as these use cases involve network differentiation for specific content or categories of content, they must be viewed through the highly complex and restrictive prism of the open internet regulation, specifically the 'specialised services' compliance criteria. While some services may potentially fit within existing exceptions, making this determination requires extensive legal, technical and commercial assessment and, even with this, typically remains within a regulatory grey area. And this assessment must be done from scratch for each individual use case. As a result, we are forced to design services around regulatory risk rather than customer need, limiting functionality, reducing consumer benefits and discouraging innovation. The challenge is compounded by the fragmented nature of implementation across Europe. Even where a use case may be considered compliant in

one Member State, there is no guarantee that other national regulators would reach the same conclusion or impose the same conditions. This lack of predictability creates significant barriers to scaling innovative services across the Single Market and undermines incentives for investment in advanced network capabilities

Vodafone asks BEREC to (1) support the use of the Digital Networks Act to modernize the open internet framework for Europe, to allow for flexible development of enterprise use cases, whilst maintaining key open internet guardrails; (2) continue in its efforts to ensure a harmonised application of the open internet rules across member states, in particular as concern network API use cases.

Data Protection: For anti-scam and fraud-prevention APIs, the challenge is how network-derived traffic data can be used responsibly to protect consumers. Services such as Scam Signal can use limited call-context or derived risk indicators to help banks detect social engineering fraud. Vodafone asks BEREC to support a proportionate approach that recognises fraud prevention and consumer protection, and that avoids disadvantaging operators compared with non-telco providers using comparable device or SDK-derived signals.

For Location APIs, the challenge is how consent, delegated consent, refresh periods and transparency obligations should operate in practice across use cases such as fraud prevention, IoT asset tracking, workforce safety and geofencing. Vodafone asks BEREC to provide clarity on proportionate consent models, including when delegated consent may be acceptable and whether differences in granularity, accuracy or use of derived yes/no outputs should affect regulatory treatment.

For cybersecurity use cases, Network APIs can help detect and prevent SIM swap attacks, account takeover, credential compromise, device cloning and social engineering attacks. Vodafone asks BEREC to clarify whether cybersecurity uses that are designed to prevent malicious activity can be supported under similar principles to anti-fraud uses, subject to appropriate safeguards.

Licensing: Finally, local interpretations and licensing requirements can prevent standardised APIs from scaling. Vodafone's internal work identifies examples where launches can be blocked by uncertainty about whether an API is an electronic communications service, whether an identifier is traffic data, whether delegated consent is acceptable, how caller ID rules apply to Branded Calling, or whether aggregators need additional licences. Some examples are outside the EU, but they illustrate the risk that regulatory fragmentation creates for a market built on standardisation. BEREC can help by promoting consistent, proportionate and outcomes-based interpretation across Europe.

9. To what extent are current APIs truly interoperable across operators and vendors in Europe?

Interoperability has improved significantly through CAMARA and GSMA Open Gateway, especially for mature API categories. However, interoperability is a journey rather than a binary outcome.

Differences may remain because operators have different network architectures, vendor environments, deployment timelines, 5G Standalone maturity and national regulatory requirements. These differences can be more pronounced for newer network programmability APIs than for mature identity and fraud-prevention APIs.

Continued standardisation, testing, certification, implementation alignment and close cooperation between operators, vendors, aggregators and developers will be important to achieve consistent interoperability at scale. Regulatory consistency is also part of interoperability: a common technical API is less valuable if a developer cannot use it consistently across markets because the legal interpretation differs.

Closing comments

Vodafone encourages BEREC to support an approach that enables innovation while preserving trust. The most effective path is to support industry-led technical standardisation, promote interoperability, and encourage consistent, proportionate regulatory interpretation across Europe. In particular, BEREC should help clarify how existing privacy, ePrivacy, traffic data, location and Open Internet rules apply to Network APIs so that beneficial use cases in secure authentication, anti-scam protection, cybersecurity, location-enabled services and Quality on Demand can scale responsibly across the European market.