Connect Europe and the GSMA views on the Digital Omnibus

October 2025

Connect Europe and the GSMA, representing the European telecommunication sector, welcome the opportunity to comment on the European Commission's 'Digital Omnibus' and to offer our views on how this initiative can help to simplify the regulatory landscape related to data, cybersecurity and artificial intelligence. We appreciate the European Commission's ambition to simplify the EU rulebook and to 'stress-test' the current digital rules, resulting in lower administrative costs, more coherent regulation, and a harmonised regulatory framework in line with the EU's goals for a more competitive Europe. We also see the need and added value of effective regulation that strikes the right balance between safeguarding individuals' fundamental rights and enabling innovation and competitiveness.

An overly complex regulatory landscape, marked by the proliferation of legislative instruments and their unclear and fragmented interplays, risks undermining the very objectives set out by EU institutions. To effectively protect individuals' rights while promoting innovation and competitiveness, it is essential to ensure that companies are not overwhelmed by disproportionate bureaucracy, excessive paperwork, or unrealistic expectations (e.g., due to obstacles they cannot control). For instance, efforts and investments should be directed toward implementing effective and meaningful measures, rather than being consumed by administrative burdens. Geopolitical and market realities must be acknowledged, and the interactions and cumulative (in some instances, redundant) effects of obligations across different EU legal texts must be clarified to avoid legal uncertainty and regulatory fatigue.

Based on the scope of the current call for evidence, GSMA and Connect Europe members are concerned that urgent and necessary regulatory simplification in the telecoms sector is being de-prioritised, relative to efforts to simplify or streamline regulation on digital platforms. While we are supportive of common-sense modifications to reporting requirements under the EU's Digital Aquis, these efforts must be matched if not exceeded in terms of pace and ambition with simplification of the telecoms regulatory framework; recognising the regulatory asymmetry that exists between digital services and telecoms operators. In this regard, we believe that the Commission can be more ambitious in tackling regulation that truly hinders innovation and competitiveness, particularly with regard to the ePrivacy Directive and cybersecurity framework simplification. We believe that only a high level of ambition will result in real change and will strengthen European players

We share our views on the ePrivacy Directive, the 'data acquis', the cybersecurity framework, and the AI Act below.

ePrivacy Directive

European telecommunications providers continue to struggle with the fragmented and duplicitous nature of the ePrivacy Directive, with the Directive's legal obligations applying exclusively to telecom operators placing operators at a comparative disadvantage. As such, we would like to reiterate our concerns surrounding its application, as well as encouraging the European Commission to broaden its scope of simplification to better examine how foundational provisions of the Directive could be better applied in existing or future EU legislation. We do not consider the Digital Omnibus' unilateral focus on the cookies' rules to be sufficiently ambitious.

Repeal of the ePrivacy Directive and deferral to other relevant current and upcoming legislation

Connect Europe and the GSMA strongly encourage the European Commission to reevaluate the scope of its simplification efforts on the ePrivacy Directive. While we commend the Commission's efforts to pursue simplification of the Directive, we would strongly encourage a broader scope of exploration beyond the issue of cookies, given the raft of persisting issues with respect to the Directive's implementation. In that vein, Connect Europe and the GSMA **reiterate our call for the repeal of the ePrivacy Directive entirely**, and the **incorporation of the principle of the confidentiality of communications into existing and/or future horizontal EU law**.

The ePrivacy Directive has explicit impacts on the telecommunications industry, with full implementation marred by disproportionate obligations, fragmented legal application and legislative inconsistencies with existing EU law. More specifically, the Directive (article 6) imposes unique legal requirements exclusively on telecommunications operators that do not apply to other digital service providers. This creates regulatory asymmetries that place telecom operators at a competitive disadvantage, distorting the level playing field within the digital single market. Furthermore, the implementation of the ePrivacy Directive has varied significantly across Member States, resulting in a fragmented regulatory landscape that generates legal uncertainty across markets. As a consequence of this, the current legal framework casts limitations on the adoption of the large-scale innovative services, such as the GSMA Open Gateway Initiative, advanced anti-fraud and security-related technologies that could otherwise add significant benefits to enhancing consumer protection. It also questions the management of operators' data in the context of AI transformation.

Moreover, Connect Europe and the GSMA continue to observe that many key provisions of the ePrivacy Directive are already laid down as part of the GDPR, which specifically provides a robust and uniform legal basis for personal data protection, including vigorous requirements related to data transparency, accountability, and data security.

While elements of the ePrivacy Directive are largely regulated for under the GDPR, Connect Europe and the GSMAconsider the principles of confidentiality of communications and user privacy (Article 5 (1) and (2)), as fundamental pillars of the existing Directive, must be preserved. In view of repealing the ePrivacy Directive, we strongly encourage the Commission to consider incorporating such principles on confidentiality within an EU horizontal law. The remaining provisions of the Directive should be repealed (with special attention to Articles 6 and 9, which are more burdensome for telecom operators).

The 'Data Acquis'

With the entry into application of the Data Act, Connect Europe and the GSMA encourage the European Commission to consider several aspects to support innovative industrial data sharing in Europe, all the while safeguarding commercially sensitive data. Clear involvement of industry in multistakeholder discussions, particularly in the development of EU-level guidelines, will be critical to ensure the continued vibrance, fairness and transparency of the data sharing ecosystem.

Furthermore, Connect Europe and the GSMA reiterate our full support for a considered simplification of the GDPR, which we believe would enhance legal certainty, reduce administrative burdens, and help to responsibly innovate without lowering the high level of data protection in the EU. While we believe that the GDPR remains a cornerstone of the EU digital framework as well as a global standard, there remain some areas which could still benefit from further refinement to improve its overall effectiveness. Owing to this, we propose some solutions to refine how the GDPR should be applied, without undermining its foundational goals, and without a broader reopening of the Regulation.

Data Act

Provide further clarity on key aspects pertaining to the scope of the Data Act, Business to Business (B2B) and Business to Consumer (B2C) data sharing

While Connect Europe and the GSMA laud the efforts carried out to date by the European Commission, particularly with respect to the Data Act FAQ, there are still several aspects that require further work in order to support a clear and comprehensive implementation of the Data Act.

Given the significant and sophisticated nature of the current data value chain, which is expected to grow exponentially over the coming years, further clarity is still needed for actors on the specific types of products and services that are required to comply with the Data Act.

For instance, article 2(5) of the Data Act defines a "Connected Product" as an item that collects or generates data on its use or environment, can communicate such data, and whose primary function is not the storing, processing, or transmission of data for third parties.

The Commission's FAQ (p.9) further specifies: products primarily used for storing, processing, or transmitting data (e.g., servers and routers) fall outside Chapter II data-sharing obligations unless they are owned, rented, or leased by the user.

This addition risks undermining the Regulation's own definition. Article 2(5) already excludes devices whose main function is to process or transmit data on behalf of others. Routers, modems, femtocells, wi-fi amplifiers, set-top boxes and, in general, other equivalent electronic communications and audiovisual equipment, clearly fall into this category: they enable communication flows that necessarily involve third parties (e.g., ISPs). As such, they should remain excluded from the definition of "Connected Product." We consider this exclusion as supported by Data Act's recital 16, which states that equipment is necessary for the provision of intermediary services (e.g., servers in the case of cloud infrastructure, but extensible also to ISP's routers should not be covered by the Data Act. The FAQ carve-out, however, creates the risk that leased or rented equipment provided by ISPs could be pulled back into scope. This would contradict both the intention expressed in the FAQ itself and the Regulation's objectives, by unintentionally extending data-sharing obligations to network infrastructure supplied by providers.

We therefore request:

- An explicit list of **excluded devices** in the Regulation, as was partly the case in the original proposal of the Data Act (Recital 15). This list should extend to servers, routers and set-top boxes.
- Removal of the FAQ carve-out "unless they are owned, rented, or leased by the user."

We have welcomed the various opportunities to engage directly with the Commission throughout the Data Act's implementation process, however, further stakeholder engagement is still needed, with a clear rationale to ensure that industry stakeholders across the data value chain are involved in the development of clear guidelines, including on compensation for B2B and B2C data sharing. This will ensure that the compensation regime is co-created in a fair and transparent way. Further action is needed to reduce unnecessary regulatory hurdles and legal complexities, including through simplification of cross-border deployments, paving the way for a far more innovative and navigable industrial data sharing ecosystem. The adoption of open standards and comprehensive interoperability protocols will be critical mechanisms to support general compliance with the Data Act's provisions and to unlock the Data Act's tangible benefits to the EU Single Market. In this perspective, the definition of common EU-wide standards represents a key factor to optimise implementation costs, reduce duplication, and foster broader collaboration across industries and

sectors.

In addition, regarding data processing services switching, the Data Act does not sufficiently address situations where services are resold, for example when operators resell hyperscalers' products or services to their customers. Furthermore, many European companies act as intermediaries or resellers of cloud services and do not have the technical means to facilitate switching as required under the regulation. The absence of specific provisions or guidance in such cases creates legal uncertainty on roles and responsibilities and how switching obligations apply in practice, and where responsibilities lie across the value chain.

Support a competitive Business to Government (B2G) data sharing framework

Opaque and far-reaching provisions on government access requests to sensitive commercial data, specifically, unclear "exceptional need" provisions, risk negatively impacting European innovation. Without clear guiding principles, industry is left uncertain about how they should comply with such requests, as well as to details on fair compensation afforded for sharing such commercially sensitive data. As such, we reiterate the importance of targeted and proportional data access requests, made exclusively in the event that existing market-based solutions have either been exhausted or are insufficient. Further, emergency access requests often come at times of increased strain to industrial actors. As such, Connect Europe and the GSMA welcome the opportunity to engage with the Commission on the creation of a **clear, transparent and mandatory EU-wide compensation scheme** to underpin emergency access requests.

GDPR

Reinforce the risk-based logic of the GDPR

Connect Europe and the GSMA believe that the GDPR was designed with a risk-based approach in order to tailor compliance obligations based on actual risks, rather than perceived risks, to personal data. We believe that overly rigid views on how this can be achieved have undermined this approach. Connect Europe and the GSMA call on the European Commission to consider further clarification and harmonisation of risk evaluation and enforcement criteria across EU Member States. This should, in our view, encompass factors such as scale, sensitivity, safeguards, and likelihood of harm. We believe this more refined approach would significantly reduce administrative burden, ensure better allocation of companies' resources and better position EU companies to innovate and compete globally.

In general, to ensure the success of the EU digital regulatory framework, the European Commission should streamline obligations, clarify the interaction between digital laws, and provide guidance that harmonises requirements across frameworks.

Interplay between legislation

We underline the importance of harmonising compliance processes across key European legislation on data and digital technologies (such as the GDPR, Data Act, AI Act, NIS2 and DORA), through a common operational approach supported by EU-wide shared guidelines. Such an approach would enable a more consistent and objective assessment of compliance, reducing divergent national interpretations and ensuring a level playing field across Member States. At the same time, it would foster greater internal consistency within companies, helping organisations to evaluate in a uniform way that is permissible under each regulation and to apply proportionate and harmonised mitigation measures. This would streamline administrative requirements and strengthen regulatory clarity across the entire digital ecosystem.

Support a clearer interplay between the GDPR and the AI Act

The concurrent application of the GDPR and the AI Act raises substantial legal complexities and hurdles that we believe could be better addressed. Recital 47 of the GDPR underpins the concept of legitimate interest of data controllers to process certain data. This concept should be clearly extended for the purposes of training AI systems as a recognised legitimate interest.

Such processing of personal data for the training of AI systems and models would include clear guardrails, such as the exclusion of sensitive data sources, limitations of data categories, early pseudonymisation or anonymisation, transparency towards data subjects, and a risk-based evaluation of relevant safeguards, as well as the preservation of the right to object by data subjects, as provided for under Article 21 of the GDPR. We believe the Commission should foresee that the processing of personal data for the training of AI systems and models is a recognised legitimate interest under GDPR, with the appropriate safeguards in place.

We underline the importance of introducing EU-wide common guidelines on Data Quality and Data Minimisation for artificial intelligence (AI) systems, in order to ensure the responsible, proportionate and transparent use of data.
Such guidelines should provide clear operational rules to:

- Reduce bias and inefficiencies in AI models.
- Ensure data traceability and quality throughout the lifecycle.
- Promote data management practices consistent with the principles of privacy by design.

While both the AI Act and the GDPR establish the principles of data quality and data minimisation, they do not specify how these should be implemented in practice.

We therefore propose that the European Commission develop a common set of operational guidelines, including for example:

- Minimum data quality metrics (completeness, consistency, accuracy).
- Dataset labelling with trust metadata.
- Pseudonymisation and minimisation by design.
- Traceability and documentation of data transformations.

GDPR and Data Act Interplay

The Data Act restricts data holders' ability to use both personal and non-personal data, creating conflicts with GDPR provisions:

- **Personal data**: Article 8(4) may lock datasets unless released at a user's request, undermining GDPR grounds such as contract performance (Art. 6(1)(b)) or legitimate interest (Art. 6(1)(f)). This could harm industry's ability to use data legitimately, e.g., for AI.
- **Non-personal data**: Article 4(13) limits use of non-personal data to explicit contracts, yet it is unclear what constitutes "non-personal data of the user," especially when datasets combine personal and non-personal data. Where users are legal entities, such data is closer to confidential information or trade secrets, better handled under existing regimes (e.g., Directive 2016/943).

Cybersecurity

European telecommunications providers face several challenges related to the EU cybersecurity legislative landscape, often due to overlapping and inconsistent frameworks like NIS2 Directive, DORA, CRA, and the RED Delegated Regulation. **A more cohesive regulatory framework is needed to**

streamline compliance, reduce unnecessary complexity, and avoid any undue impacts on innovation.

Redundant laws or national implementations should be repealed where sector-specific regulations overlap with horizontal ones, such as NIS2 or CER. For instance, when other laws impose security requirements on service providers already regulated by NIS2, compliance with NIS2 should be deemed sufficient, with no need for additional or unnecessary audits or regulatory oversight.

The European Commission should ensure that national laws transposing legislation (e.g., NIS2, CER) effectively repeal existing sectoral provisions in national telecom laws, including those implementing Articles 40–41 of the EECC and any other national regulations on quality or resilience. The EU should provide formal guidance, request a cost-benefit analysis for any provisions proposed to be retained, and publish a roadmap with key timelines to achieve simplification.

The use of international standards should be promoted to facilitate compliance (i.e., ISO 27001), and penalties for non-compliance should be proportionate and avoid discouraging proactive cybersecurity measures. New regulations should also provide minimum and clear transition periods to allow companies to prepare and implement necessary measures.

Reporting Obligations

Multiple EU laws require telecommunications and digital service providers to report security incidents and vulnerabilities. However, inconsistent procedures, thresholds, and designated authorities across these frameworks lead to duplicated efforts. **Administrative burdens should be reduced, reporting requirements and competent authorities should be streamlined across relevant legislation, and the efficiency of security incident management should be enhanced, in full recognition of the current cybersecurity threat landscape.**

To streamline the reporting process, the following measures should be taken:

- Simplify and harmonise reporting requirements and procedures across regulations, based on best practices, including definitions, what needs to be reported, timelines, thresholds, reporting authorities, and tools (platforms, reporting templates or other).
- Centralisation of security incident management through the once only principle, meaning that just one notification would need to be submitted through a single- entry point in each Member State, making the same report available to all relevant competent authorities. This principle is not widely applied in practice across Europe. ENISA could play a key role in developing best practice guidelines that integrate the practices of all Member States. For cross-border incidents or those affecting one company in multiple Member States, more than one company under majority ownership, or market activity of a Group with business activities in the same or multiple Member States, a single report can optionally be submitted to the single-entry point of the country where the most relevant legal entity is established. The national competent authority has to submit the report to ENISA and share it with other relevant stakeholders. The one-stop shop principle should also be extended to follow-up questions, which are time-intensive for companies to answer and divert resources away from incident response and risk management (i.e., where the Group of entities has its main establishment in the Union).
- These changes are expected to reduce the complexity of security incident management, allowing more resources to focus on incident resolution rather than on reporting. They will also improve awareness of incidents among relevant agencies and provide greater legal certainty for all parties involved through simpler and more consistent legislation.

NIS2 Directive

NIS2's flexibility in sector and entity classification leads to inconsistent interpretations. A centralised EU repository should clarify registration processes and scope across Member States, and requirements should be based on international standards, should apply. National authorities should be encouraged to harmonise their approaches to technical requirements and guidelines.

The "main establishment" concept creates jurisdictional challenges, particularly for telecom groups offering services across multiple Member States and must be clarified. To avoid duplication, pan-European audits and international certifications, mutual recognition, harmonised and standardised audit approaches, and an EU framework for auditor approval, should reduce compliance burdens. Finally, flexibility should be allowed for incident reviews, and logging requirements streamlined with non-binding guidance from ENISA.

DORA

The statutory responsibility under DORA should remain with financial entities. To the extent that financial entities involve electronic communications providers as ICT third-party service providers in their compliance efforts, these providers' NIS2 compliance should be considered sufficient for conducting risk-based audits of ICT providers and to harmonise oversight.

Furthermore, guidance or more explicit language is required to clarify the definition of 'ongoing basis' that could lead to misinterpretation, and the limitation of the scope of 'financial performance' to the 'impacts on the client's information system' focusing on significant effects related to DORA. Additionally, in the key contractual provisions, audit rights should be moderated by allowing mutual agreement on alternative assurance levels. Audit rights should also be limited to what is necessary and proportionate, ensuring they do not exceed the scope mandated by DORA. Regarding threat-led penetration tests a **risk-based approach** should be followed in order to prevent service disruptions in multi-customer environments.

The EU should allow global ICT providers to comply with DORA for their worldwide network infrastructure by relying upon requirements that parallel the contractual assurances concerning the reliability and security the ICT providers use today with large financial customers and other institutions, such as certifications with ISO and other standards organisations, which should be presumed sufficient for meeting DORA compliance requirements. This will further support harmonisation and reduce duplication. Furthermore, we believe that Pan-European audits and certifications should be accepted by all Member States as evidence of conformity, without the need for additional national-level audits or certifications. This approach will enhance legal certainty, reduce administrative burden, and support the development of a true digital single market. Regarding key contractual provisions, it should be clearly specified that the relevant service provider (rank 1 - direct supplier) is the company that directly delivers the ICT services, regardless of reseller relationships or arrangements.

Lastly, registration and supply chain obligations should be limited to direct ICT suppliers to align with the scope of NIS2.

Cyber Resilience Act and RED Delegated Regulation

NIS2 supply chain requirements are closely linked to product rules under the RED Delegated Regulation and the CRA, with overlapping obligations, particularly for importers and distributors, but delayed standards leave businesses with little time to prepare. These standards may also become outdated due to upcoming CRA obligations. For NIS2-regulated entities, a product verified as

compliant with CRA/RED DR should meet NIS2 and similar supply chain requirements. The harmonised standards developed for the RED DR must be maintained for the CRA.

The enforcement of the RED Delegated Regulation should be delayed, or a grace period should be introduced. If there are delays or unavailability of a complete CRA standard, CRA implementation deadlines should be extended, or self-certification should be temporarily accepted.

AI Act

Successfully integrating AI into electronic communications networks (ECN) is essential for promoting state-of-the-art connectivity, innovation, and competitiveness. To this end, we are taking this opportunity to share our views regarding the classification of AI systems as high-risk and the adoption of standards, the definition of safety components and interactions between the AI Act and the Radio Equipment Directive below. These elements are necessary to take into account for the successful implementation of the AI Act.

Ensuring timely harmonised standards for high-risk AI compliance

The effective implementation of the AI Act likewise depends on the timely development and adoption of harmonised standards, particularly for high-risk AI systems. These standards are essential to provide legal certainty, support compliance efforts, and uphold proportionality. Based on current trajectories we expect that many of these standards will be neither available on time nor compatible with existing international standards. From an industry perspective, it is important to stress that the implementation and internal compliance processes can only start once these standards are completed.

Given that it is likely that many standards are not going to be in place with sufficient time to prepare for implementation in companies' respective systems, we call for the application of the relevant provisions for high-risk AI systems to be postponed by one year. This would allow all the actors in the AI value chain the necessary time to adapt, while ensuring that the AI Act's objectives of innovation, competitiveness, and the protection of fundamental rights are not compromised. Moreover, the harmonised standards should be compatible with existing standards, such as the integrated management system (i.e., ISO 9001, ISO 31000).

Regarding the definition of standards, we call for setting up a unified certification framework in order to simplify implementation by all entities. Additionally, full coherence among the evolving standards should be ensured to reduce ambiguity.

Furthermore, the successful application of the AI Act in the telecom sector is currently challenged by considerable ambiguity stemming from vague definitions and an unclear scope of application—particularly in the context of electronic communications networks (ECN). To ensure consistent and effective implementation, it is crucial that the European Commission provides clear and detailed guidance, while further specifications in the AI Act would be welcome.

In the absence of such clarification, standardisation bodies or national supervisory authorities may interpret the rules inconsistently, leading to fragmented enforcement, disproportionate compliance burdens, and significant legal uncertainty. This could ultimately hinder innovation and delay the responsible deployment of AI technologies in ECN.

Below are some elements that the European Commission specifically should take into account when reviewing the high-risk AI rules:

Safety Components

I**t is crucial to distinguish between 'safety' and 'security'**.[1] Cybersecurity and safety differ fundamentally in definitions, threats, risks, objectives, and mitigation measures. While **security** is a property based on a very concrete set of attributes or capabilities (availability, integrity, confidentiality),[2] **safety** is a term closely tied to the concept of avoiding the production of "harm" or "damages" on persons and/or property.

In the context of the AI Act, a "safety component" refers to an AI system that plays a direct role in protecting the health, safety, or physical integrity of individuals or critical infrastructure and property. These components are not necessarily essential for the basic functioning of a system but are crucial in preventing harm in case of failure or malfunction.

Therefore, in the context of digital infrastructures or radio equipment subject to the RED, we consider that components designed solely to prevent the following types of harm **should not be regarded as "safety components"**:

1. **Indirect or consequential damage**, i.e., those that do not result directly from the failure or malfunction of a product.
2. **Non-physical or immaterial damage**, such as moral harm or infringements of rights.
3. **Damages caused by third parties**, including those arising through the use of intermediation services.

The term 'safety component' should therefore be more precisely defined in the law and should remain to be the primary criterion for assessing high risk AI within the scenarios outlined in the AI Act. It should also be clarified in the AI Act that the focus on safety components in digital infrastructure also applies to the interaction with the Radio Equipment Directive, to avoid overlapping or even contradicting interpretations regarding the applicability of the high-risk rules to communication networks and equipment. This distinction is essential to ensure that regulatory obligations remain proportionate and appropriately targeted. **It is imperative to avoid the undue classification of AI systems that serve cybersecurity or operational functions, without a direct safety role, as high-risk.**

Interactions with the Radio Equipment Directive (RED)

There is a need for consistent implementation with regard to the Radio Equipment Directive (RED). Radio equipment devices can incorporate AI-based components. Due to the complexity of the RED, the conditions and obligations under which the AI Act applies to the radio equipment device must be determined, in a coherent manner, aligning with other equipment subject to certifications, particularly regarding cybersecurity (e.g., CRA, NIS2, etc.).[3] Components used for cybersecurity and safety

[1] According to Recital 55 of the AI Act, *"Safety components of critical infrastructure, including critical digital infrastructure, **are systems used to directly protect the physical integrity of critical infrastructure or the health and safety of persons and property** but which are not necessary in order for the system to function. The failure or malfunctioning of such components might directly lead to risks to the physical integrity of critical infrastructure and thus to risks to health and safety of persons and property."*

[2] According to the NIS2 Directive (EU) 2022/2555, the "security" of network and information systems is *"the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems*

[3] According to Article 15 (1) of the AI Act, providers of high-risk AI systems must design and develop these systems in such a way that they achieve an appropriate level of cybersecurity. If a high-risk AI system is also a product with digital elements, Article 8 of the CRA stipulates that the cybersecurity requirements of Article 15 of the AI Act are deemed fulfilled if all CRA requirements are met and covered by the conformity assessment procedure.

components should be clearly differentiated. Cybersecurity is already dealt with within a number of pieces of legislation (i.e., NIS2, CRA, DORA etc.).

In general, **AI-based cybersecurity components in radio equipment should not be categorised as AI high risk for human safety**. As stated above, it is crucial to distinguish between 'safety' and 'security'. Mixing security and safety in the implementation of the AI Act would result in unnecessary regulatory burdens on the use of AI-cybersecurity solutions in radio equipment (not safety components), potentially discouraging innovation in cybersecurity solutions tailored for telecom networks. This in turn could harm industry competitiveness, high level of cybersecurity of such equipment, and result in other regions advancing more rapidly in smarter and more secured 5G networks due to the absence of such restrictions. If such specification is not possible within the AI Act itself, further clarification on the interplay between the RED and the AI Act should be provided with the guidelines on high-risk AI.

Clarification of biometrics definition

The AI Act should be clarified regarding the definition of biometric and emotional AI based tools, especially in the context of GPAI, to better understand the scope of the AI Act rules.