Public Consultation on Regulation 1/2003 and its implementing regulation, Regulation 773/2004

CCIA Europe Response

September 2025

The Computer & Communications Industry Association (CCIA Europe) welcomes the opportunity to submit comments in response to the European Commission's (Commission) Public Consultation regarding the procedural framework for the implementation of Regulation 1/2003 and Regulation 773/2004 (together the "Regulations") released for public comment on July 10, 2025.[1]

CCIA Europe supports a procedural competition framework that ensures effective and harmonised competition enforcement, legal certainty, and upholds the principles of fairness and due process. As the Commission reassesses its framework for enforcing EU competition rules, maintaining the balance between protecting competition and ensuring due process is critical. Any updated framework must balance enforcement powers with the fundamental principle of legal certainty and harmonisation among European member states. In response to this consultation, CCIA Europe thus offers the following recommendations:

1. Maintain the current legal framework on the principles of territoriality and investigatory powers.
2. Maintain the current legal tests and framework for interim measures and adopt guidelines facilitating earlier commitments.
3. Implement a confidentiality ring system that ensures access by both external and in-house legal counsel.
4. Adopt a fully harmonised approach to competition law enforcement in the EU by extending the convergence rule to unilateral conduct.

I. Maintain the current legal framework on the principles of territoriality and investigatory powers

Recommendations:

1. Maintain the current legal framework based on the principles of territoriality, which is crucial for the exercise of the Commission's coercive powers under Articles 101 and 102 TFEU.
2. Adopt a targeted approach for Requests for Information (RFIs), focusing on strictly necessary information that is proportionate to the investigation's needs.
3. Ensure that digital inspections are not used as substitutes for targeted and proportional RFIs, and are based on the same set of procedural and substantive safeguards that protect the rights of undertakings during physical inspections.
4. Maintain current investigatory powers, without adding potential disproportionate tools such as compulsory summons.

---

[1] European Commission, "*EU antitrust procedural rules (revision)*" (Jul. 10, 2025), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14729-EU-antitrust-procedural-rules-revision-_en.

II. Maintain the current legal tests and framework for interim measures and adopt guidelines facilitating earlier commitments

Recommendations:

1. Maintain the balance between protecting competition and ensuring due process by keeping the current legal tests and framework for interim measures.
2. Adopt clear and predictable timelines and guidelines for implementing interim measures.
3. Adopt guidelines that facilitate earlier commitments and proactive engagement by the Commission with the parties regarding potential commitments.

III. Implement a confidentiality ring system that ensures access by both external and in-house legal counsel

Recommendations:

1. Implement rules allowing parties access to all relevant evidence in a timely manner, granted via remote access to a secure platform.
2. Include both external and in-house legal counsel in the confidentiality rings system.
3. Adopt rules that allow parties sufficient time to produce non-confidential versions during the investigation procedure.
4. Adopt measures to help mitigate the risks of leaks, misuse, or inadvertent disclosure of highly sensitive information within confidentiality rings.

IV. Adopt a fully harmonised approach to competition law enforcement in the EU by extending the convergence rule to unilateral conduct

Recommendations:

1. Promote legal certainty by extending the convergence rule to unilateral conduct, ensuring harmonisation in competition law among the member states.

Introduction

The Computer & Communications Industry Association (CCIA Europe) welcomes the European Commission's ongoing consultations on the review of the procedural framework for the implementation of Regulation 1/2003 and Regulation 773/2004.

With growing digitalisation across the economy, regulations governing competition law must adapt to increase efficiencies, reduce regulatory burdens, and foster innovation. For this review to be meaningful, CCIA Europe believes a neutral, fact-based approach is essential, and one that enables the Commission to fully assess what changes, if any, are required of the Regulations, as well as the potential benefits, negative impacts, and unintended consequences of said reforms.

I. Maintain the current legal framework on the principles of territoriality and investigatory powers

1. Keep the current legal framework on the principles of territoriality, which is critical for the exercise of the Commission's coercive powers under Articles 101 and 102 TFEU.

With the growing digitalisation of the economy across a number of sectors, companies have been increasingly relying on cloud storage and third-party servers to store their data. Despite these servers sometimes being physically located in different jurisdictions, the current legal framework allows the Commission to access the relevant information it may require. As grounded in EU case law, undertakings under investigation have an enforceable general duty to preserve reasonably available evidence, and failure to do so can result in severe penalties. This duty, and the obligation on undertakings to cooperate with the Commission, guarantees competition enforcers access to the required information.

Allowing the Commission to compel access to cloud storage or third-party servers located in non-European Economic Area (EEA) countries would raise questions as to the extraterritorial investigation powers of the Commission. These concerns were also raised when discussing the adoption of the Digital Markets Act (DMA), and the Commission's decision to address gatekeepers not established in the EEA through EEA-based points of contact is also appropriate in these circumstances. The effectiveness of EU competition law does not require such extraterritorial powers.

2. Adopt a targeted approach for RFIs, focusing on strictly necessary information that is proportionate to the needs of the investigation.

Depending on how the RFI is designed, requests can potentially be extremely broad, resource-intensive, and costly for undertakings, and in turn for the Commission. As such, all parties involved would benefit from a more tailored approach, focusing requests on information that is strictly necessary and proportionate to the investigation's needs.

Clear engagement and coordination with undertakings before the RFIs are issued would be particularly useful for RFIs requesting internal documents and data, which can be very burdensome. To ensure that requests are as targeted as possible, the Commission should collaborate with the parties to define the parameters of requests based on their knowledge of their business and IT systems, particularly in cases where search terms are used to identify documents.

3. Ensure that digital inspections are not used as substitutes for targeted and proportional RFIs, and are based on the same set of procedural and substantive safeguards that protect the rights of undertakings during physical inspections.

The existing framework covering physical inspections under Regulation 1/2003 and its implementing rules provides an adequate set of procedural and substantive safeguards that protect the rights of undertakings, ensure proportionality, and uphold fundamental rights. If digital inspection powers were to be introduced, they should include similar safeguards to those of physical inspections. In particular:

1. **Legal basis and written authorization**: Any digital inspection must be based on a formal, written decision that clearly states the scope, purpose, and legal basis for accessing digital records, including the specific data or systems to be accessed.
2. **Scope and specificity**: Digital inspections should be limited to data and records directly relevant to the investigation.
3. **Notification and consultation with National Competition Authorities (NCAs)**: Where data is stored in multiple EU jurisdictions or in the cloud, the Commission should be required to notify and consult with relevant NCAs, particularly when the data controller or processor is established or where the data is physically located.
4. **Participation of company representatives and legal counsel**: Company representatives, including internal and external legal counsel, should be allowed to be present at all times during the digital inspection process, in the same manner as they are when inspections are conducted on the Commission's premises. The right of the investigated parties to be assisted by external legal counsel is paramount and must be respected during any digital inspection.
5. **Protection of Legal Professional Privilege (LPP) and confidential, sensitive personal data or out-of-scope information**: Digital inspection protocols must include mechanisms for identifying, flagging, and excluding documents protected by LPP or containing trade secrets/confidential information, sensitive personal data, and out-of-scope documents before being reviewed or copied by the Commission.
6. **Record-keeping and transparency**: A detailed record should be maintained of all digital actions taken during the inspection, including the data accessed, searched, and/or copied; the individuals responsible; and the dates of the actions. This record, including access to the documents/data retained by the Commission, must be made available to the company and its advisers for review and for use in any subsequent legal challenge.

Additionally, the Commission should not use any digital inspection power as an alternative to formulating targeted and proportionate document and data requests. Digital inspections may lead to increased costs, as undertakings would likely need to invest in secure data transfer protocols, monitoring tools, and IT support providers to facilitate remote inspections and protect sensitive information. Digital inspections are more intrusive than RFIs, and should only be used when there is a specific urgency requiring their use rather than issuing a targeted and proportionate RFI. Without appropriate procedural safeguards, including sufficient measures to prevent data and privacy breaches, digital inspection powers risk litigation challenging their scope, proportionality, and legality, resulting in increased costs and delays.

4. Maintain current investigatory powers, without adding potential disproportionate tools such as compulsory summons.

The current framework already grants the Commission robust investigatory powers, and there is insufficient evidence to suggest that compulsory interviews are necessary for effective enforcement. Such powers seem a disproportionate tool for antitrust implementation, are likely to increase the administrative burden on Commission investigations and raise serious concerns regarding due process and the safeguarding of the rights of individuals and undertakings.

Inadequate safeguards and compulsory interviews may infringe upon the right to remain silent or not to incriminate oneself, as protected under Article 6 of the European Convention

on Human Rights and Article 48 of the EU Charter of Fundamental Rights, and recognized in EU Courts' case law.[2] Forced participation can pressure individuals to disclose incriminating facts and potentially lead to conflicts of interest.

II. Maintain the current legal tests and framework for interim measures and adopt guidelines facilitating earlier commitments

1. Maintain the balance between protecting competition and ensuring due process by keeping the current legal tests and framework for interim measures.

The Commission's power to impose interim measures under Article 8 of Regulation 1/2003 is a key tool to help prevent anticompetitive harms during ongoing investigations, and replicates the legal test applied by the Court of Justice of the European Union (CJEU) in interim measures cases.[3] However, this power can have a considerable impact on investigated parties by prohibiting them from engaging in certain business practices. As such, it is imperative to ensure that due process and the rights of the defence are safeguarded. Interim measures should only be imposed in cases of urgency, serious and irreparable harm, and on the basis of a *prima facie* finding of infringement.

2. Adopt clear and predictable timelines and guidelines for the adoption of interim measures.

To increase the level of legal certainty regarding the imposition of interim measures, clear and predictable procedural guidelines, including clear timelines, should be introduced to help safeguard core procedural rights. By ensuring that the judicial review of interim measures rulings is clear and timely, the Commission can strike a proper balance between protecting competition and ensuring due process.

3. Adopt guidelines facilitating earlier commitments and proactive engagement by the Commission with the parties regarding possible commitments.

The legal framework established by Regulations 1/2003 and 773/2004 regarding the adoption of commitment decisions is an effective mechanism for resolving Commission investigations. However, many procedural efficiencies can be realized that help incentivise parties to propose and agree to earlier commitments by issuing guidelines implementing certain key reforms.

The Commission should proactively engage with the parties at an early stage in the investigative process by allowing for preliminary discussions of potential commitments before a Statement of Objections is issued. Additionally, the Commission should ensure early access to the case file and an advanced commitment to a State of Play meeting where the Commission's concerns can be articulated in more detail to the parties. By providing

[2] *See, e.g.*, CJEU, 384/87, *Orkem;* C-682/20 P, *Les Mousquetaires and ITM Entreprises v Commission;* C-690/20 P *Casino, Guichard-Perrachon and Achats Marchandises Casino v Commission, and* C-693/20 P, *Intermarché Casino Achats v Commission.*
[3] CJEU, 792/79, *Camera Care;* GCEU, T-44/90 *La Cinq.* Cf. *Camera Care*, para. 19, which states that IMs must be of a "temporary and conservatory nature and restricted to what is required in the given situation."

clearer guidance on the types of commitments likely to be accepted, the Commission can actively encourage parties to offer commitments to resolve potential concerns, and ensure that commitments are appropriately tailored and implementable.

By committing to early and proactive engagement with parties, the Commission would reduce legal uncertainty, lessen the need for extensive information gathering, and allocate limited resources more effectively. This in turn would allow the Commission to shift the focus toward assessing proposed commitments, likely mitigating the potential of protracted negotiations and revisions. Earlier discussions can clarify the Commission's concerns and the types of remedies that might be acceptable.

III. Implement a confidentiality ring system that grants access to both external and in-house legal counsel

1. Implement rules allowing parties access to all relevant evidence in a timely manner, granted via remote access to a secure platform.

Access to all relevant evidence in a timely manner allows parties to prepare their defence, present their case effectively, and address the allegations against them. Investigated parties require access to all evidence collected by the Commission and placed in its file, not only evidence referred to in the Statement of Objections or otherwise supportive of the preliminary or final conclusions of the Commission, but also other evidence which could be exculpatory.

Given the inefficiency of physical data rooms and the related security risks, access to relevant evidence should also be provided to parties remotely via a secure platform. Importantly, confidentiality must be protected during the access to file process. As noted in the consultation documents, the process for creating and granting access to non-confidential versions of documents in the Commission's file is highly resource-intensive, time-consuming, and costly. The burden has increased with digitalisation and the increasing volume of data/documents.

2. Include both external and in-house legal counsel in the confidentiality rings.

Depending on the level of confidentiality required, there are clear advantages to using confidentiality rings for access to files. In particular, they are likely to reduce the burden of producing non-confidential versions of all material related to the file while ensuring access to authorized parties. However, it is of paramount importance that both external and in-house legal counsel are included in the confidentiality rings and have access to this information.

External legal counsel is generally bound by ethical and regulatory confidentiality obligations, as are in-house counsel. As external counsel is unlikely to have sufficient knowledge of the business/markets at issue, It is crucial for both parties to have access to the information, which allows external counsel to effectively seek instructions from clients.

3. Adopt rules allowing parties a sufficient period of time to produce non-confidential versions during an investigation procedure.

Given the particular importance of confidentiality in the documents that undertakings are required to produce, non-confidential versions of documents could be created for a wider group of individuals, as considered necessary by legal counsel for the rights of the defence. Nevertheless, undertakings must have sufficient time to prepare and submit them. The time allocated should also take into account the volume of documents to be redacted.

4. Adopt measures to help mitigate the risks of leaks, misuse, or inadvertent disclosure of highly sensitive information within confidentiality rings.

There are some concerns associated with the confidential information that is being provided. Particularly regarding the risk of leaks, misuse, or inadvertent disclosure - especially when the information is highly sensitive. As such, the Commission may consider adopting several measures to mitigate these risks. For example:

1. **Detailed confidentiality undertakings**: each confidentiality ring member should sign a robust confidentiality agreement, including clearly defined obligations and liabilities.
2. **Redaction and tiered disclosure**: redacting particularly sensitive content and/or a tiered disclosure approach, where some information is only shared with a "higher confidentiality tier" in the same or another confidentiality ring.
3. **Monitoring and auditing**: include the ability to monitor use, track access, and conduct audits to detect improper handling or breaches early.
4. **Use of secure platforms**: require all disclosures to be made via secure document review platforms with watermarking, access logs, and download restrictions.
5. **Notification System:** A system for notifying breaches (including inadvertent breaches) of confidentiality, along with incentives for individuals to report breaches. Breaches of confidentiality obligations may be difficult to identify and prove.

IV. Adopt a fully harmonised approach to competition law enforcement in the EU by extending the convergence rule to unilateral conduct

---

1. Promote legal certainty by extending the convergence rule to unilateral conduct, ensuring harmonisation in competition law among the member states

The current system, in which member states can adopt and apply stricter national laws on unilateral conduct, undermines the benefits of the otherwise harmonised system that applies across the EU. Additionally, there is little to no relevant case law or guidance on the scope of Article 3(2) of Regulation 1/2003, or a clear overview of the rules it covers. Thus, the scope of the possibility for stricter national laws on unilateral conduct is not entirely clear in practice, creating legal uncertainty.

Given the limitations of Articles 11(4) and 11(6) of Regulation 1/2003, a new type of intervention is required by revising the aforementioned Articles, incorporating the DMA to ensure its consistent application. Here, Article 7a of the 2009 Telecoms Framework Directive can provide a good starting point when considering how the new intervention can

be designed.[4] This provision enables the Commission to comment on measures taken by member states. If disagreement persists after a reconciliation process, the Commission may adopt a binding recommendation regarding the remedies to be imposed. A more harmonised framework would provide a number of benefits, such as:

1. **Reduced complexity**: removing the ability for member states to apply stricter national laws would simplify the legal framework, reducing the need for businesses to navigate a patchwork of national rules in addition to EU law. This would streamline compliance and enforcement processes.
2. **Lower compliance costs for businesses**: The proliferation of stricter national rules has led to legal uncertainty and increased compliance costs. Undertakings, especially those operating cross-border, would benefit from a single set of rules, reducing the need for multiple legal assessments and compliance strategies tailored to different member states.
3. **Ensure a level playing field**: the current system results in fragmentation and a "patchwork" of rules, undermining the aim of a level playing field across the EU single market. Undertakings should be subject to the same rules on unilateral conduct regardless of where they operate in the EU.
4. **Ensure better overall coherence and effectiveness of competition law enforcement**: the enforcement of abuse of dominance rules would be more consistent if all authorities applied the same substantive provisions. This would, additionally, enhance legal certainty.

Alternatively, the Commission should consider extending the convergence rule at least to unilateral conduct, subject to the most stringent national rules that contribute most to regulatory fragmentation across the EU.

Conclusion

As markets continue to evolve, it is crucial to adapt existing Regulations to ensure effective competition enforcement while balancing the need to safeguard due process rights. CCIA Europe encourages the Commission to seize this opportunity to implement necessary changes to the Regulations and foster harmonisation of competition laws across member states.

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross-section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policymaking since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

Visit ccianet.eu, x.com/CCIAeurope, or linkedin.com/showcase/cciaeurope to learn more.

[4] European Commission, *Directive 2009/140/Ec Of The European Parliament And Of The Council*, Article 7, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF.

For more information, please contact:

CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org