Title: i2Coalition Response to the European Commission's Call for Evidence: European Data Union Strategy
Submitted via: Have Your Say Portal
From: Christian Dawson, Executive Director, Internet Infrastructure Coalition (i2Coalition)

July 15, 2025

About the i2Coalition

The Internet Infrastructure Coalition (i2Coalition) represents the companies that build and maintain the Internet's foundational layer.

Our members include cloud infrastructure providers, domain name registrars and registries, data centers, managed services providers, and web hosting companies. Together, they form the ecosystem on which digital services depend. With membership across the U.S., Europe, and beyond, i2Coalition advocates for sound policy that supports a stable, open, and innovative global Internet.

1. The Internet Is Global. The Strategy Must Be, Too.

A successful European Data Union Strategy must reflect the interoperable, cross-border nature of Internet infrastructure. Infrastructure operators maintain global systems through ongoing coordination that spans jurisdictions. Legal fragmentation and inconsistent rules create barriers to participation and limit Europe's digital leadership.

We recommend that the Commission:

- **Prioritize harmonization** of national and EU-level data laws to eliminate legal uncertainty.
- **Acknowledge that infrastructure providers cannot localize operations** without undermining competitiveness or efficiency.

- **Avoid legal frameworks** that pressure providers to exit or avoid EU markets due to regulatory risk or complexity. This includes addressing national-level laws that may contradict or exceed EU objectives, such as those that led to Cisco's exit from France and Belgium.

2. Infrastructure Providers Need Legal Clarity

Infrastructure companies are not content creators. They typically do not see or control the data they transmit. Assigning content-related responsibilities to infrastructure providers misunderstands their technical role and exposes them to disproportionate liability and compliance burdens.

We ask the Commission to:

- **Preserve and strengthen safe harbor protections** and intermediary liability frameworks based on proportionality.

- **Differentiate clearly between infrastructure-level and content-level actors** in all legal and regulatory contexts.

- **Avoid assigning filtering, monitoring, or moderation responsibilities** to foundational infrastructure services.

Additional Recommendation: To align GDPR with modern Internet architecture, the Commission should introduce an exemption for passive transmission providers from obligations related to personal data they neither access nor control. With the increasing use of end-to-end encryption, such providers cannot meaningfully process or interpret user data, which remains unintelligible to them.

The i2Coalition is available to support clarification of these roles and to help develop comprehensive solutions that also respect the interests of content creators.

3. Build the Strategy on Trust and Privacy-First Infrastructure

Strong privacy protections and secure infrastructure are not obstacles—they are the foundation for public trust and sustainable innovation. Infrastructure providers already implement privacy-by-design, end-to-end encryption, and data minimization, aligning with the principles enshrined in the GDPR.

We recommend the Commission:

- **Affirm support for lawful end-to-end encryption** and reject proposals for mandatory scanning, client-side scanning, or technical backdoors.

- **Ensure cybersecurity and privacy frameworks are interoperable, practical, and accessible to SMEs.**

- **Design regulatory requirements with usability in mind**, minimizing complexity and ambiguity for infrastructure implementers.

Additional Recommendation:

To promote the adoption of privacy-first infrastructure, the Commission should consider introducing a **targeted exemption from GDPR obligations for data that is fully end-to-end encrypted and inaccessible to the data holder due to the absence of decryption keys**. Such an exemption would align with data minimization principles and recognize the reality that infrastructure providers cannot process or interpret encrypted content. It would also **create a regulatory incentive for the deployment of strong encryption**, reinforcing user trust and security across digital services.

4. Cross-Border Data Mobility Is Key

The EU has the opportunity to become a global hub for responsible data exchange—but only if the underlying infrastructure can operate across borders without undue legal risk or operational friction.

Current data localization pressures and unresolved international transfer mechanisms, particularly under the GDPR, create legal uncertainty and discourage participation in the European market. Infrastructure providers can support robust compliance frameworks—but they need legal clarity, technical feasibility, and risk-appropriate approaches.

We urge the Commission to:

- **Advance interoperable frameworks for international data flows** that balance privacy with operational mobility and cross-border functionality.

- **Include infrastructure providers in the co-creation of technical compliance tools and standards**, ensuring that obligations are grounded in real-world infrastructure practices.

- **Avoid mandating infrastructure changes** that conflict with global Internet architecture or foundational principles such as DNS and hosting neutrality.

Additional Recommendation:

The Commission should adopt a **more flexible, risk-based approach to international data transfers**, allowing such transfers to third countries where the level of protection is not *materially lower* than that of the EU—even if not strictly equivalent. This would align with principles of proportionality and legal certainty, particularly for infrastructure providers with no access to data content.

Further, **Transfer Impact Assessments (TIAs)** should only be required in specifically defined, high-risk circumstances. This targeted approach would reduce compliance burdens while preserving strong privacy protections and encouraging responsible global data flows.

5. Make the Data Union Strategy Work for SMEs

Small and medium-sized infrastructure providers are essential to a competitive and resilient Internet, but they often lack the legal and administrative resources to navigate overlapping regulatory requirements. Complex compliance frameworks can unintentionally exclude SMEs from participating in Europe's digital transformation.

We suggest the Commission:

- **Simplify and unify compliance pathways** for SMEs across privacy, cybersecurity, and AI-related regulations.
- **Provide templates, model practices, and implementation guidance** specifically tailored for infrastructure operators.
- **Ensure that European innovation funding and support programs** explicitly include digital infrastructure SMEs.

Additional Recommendation:

To reduce administrative burdens and enhance legal certainty for infrastructure operators, the Commission should **allow for a defined set of "recognised legitimate interests"**—such as cybersecurity, national security, emergency response, crime prevention, and internal administrative transfers—that can be **relied upon as a lawful basis for data processing without requiring a strict balancing test**. This would bring much-needed clarity to operators acting in the public interest and reduce legal risk for those supporting essential services.

6. Governance Must Include Infrastructure Voices

Effective governance of the European Data Union Strategy depends on sustained, structured engagement with the infrastructure providers who operate the Internet's backbone. These actors possess critical operational insight that must inform the design, implementation, and evaluation of data-related policies.

To ensure governance reflects technical reality, we recommend the Commission:

- **Guarantee representation from the Internet infrastructure sector** on strategic governance bodies, including the European Data Innovation Board.
- **Institutionalize ongoing consultation mechanisms** to include infrastructure providers in regulatory design, implementation, and review processes.
- **Fund infrastructure-specific research and pilot programs** focused on data stewardship, privacy-respecting protocols, and cross-border interoperability.

Infrastructure operators are essential allies in Europe's digital future—if their voices are systematically included in the strategy's development and evolution.

7. Conclusion and Next Steps

The European Data Union Strategy presents a timely opportunity to position Europe as a global leader in ethical, privacy-driven data innovation. But success depends on grounding the strategy in the technical, legal, and economic realities of the Internet's foundation.

Infrastructure providers can serve as trusted partners in this effort—**not as afterthoughts, but as architects**. With coherent, proportionate, and globally interoperable rules, Europe can foster both trust and technical excellence.

The i2Coalition stands ready to:

- **Facilitate technical dialogue** between policymakers and the infrastructure community.
- **Provide implementation insight** to ensure rules are workable across diverse operational environments.
- **Support policy design** that protects core Internet architecture while advancing European values.

We look forward to continued collaboration with the European Commission and other stakeholders in building a sustainable, inclusive, and interoperable European Data Union.

Christian Dawson
Executive Director
Internet Infrastructure Coalition (i2Coalition)
https://i2coalition.com | dawson@i2coalition.com