CIVIL LIBERTIES UNION FOR EUROPE

# Civil Liberties Union for Europe:

# Response to the Call for Evidence for the Digital Fitness Check

11 March 2026

## 1. Executive Summary

Liberties welcomes the opportunity to provide input to the Digital Fitness Check Communication. However, it is unfortunate that this opportunity only comes after the digital omnibus proposals were launched in November 2025. Second, we strongly oppose the presumption which derives from the presentation of this consultation, which implies that the accumulation of rights-protecting rules inherently undermines businesses' ability to operate in Europe. This framing risks misrepresenting *simplification* as synonymous with innovation, when it is, in reality, an attempt to deregulate the Digital Acquis that the EU has been building for the last 20 years. In our view, the problem with digital legislation is not bureaucracy but widespread **under-enforcement**. In a geo-political context where the EU may feel tempted not to enforce its own laws to appease the US administration and align with Big Tech and European corporate lobbying, it should do just the opposite. This is the moment for Europe to stand firm and oppose foreign interference and attacks on our citizens, with our laws and our principles, including respect for the rule of law and an international rules-based order.

The EU's digital rulebook — including the **Digital Services Act (DSA)**, **Artificial Intelligence Act (AI Act)**, **General Data Protection Regulation (GDPR)**, and the **ePrivacy Directive** — is grounded in the **Charter of Fundamental Rights of the European Union**, particularly Articles 7 (privacy), 8 (data protection), and 11 (freedom of expression and information). These rights are not "bureaucratic burdens"; they are the primary-law baseline, the constitutional foundation of EU digital governance.

Before even contemplating changes to the European digital rulebook, the Fitness Check must prioritise:

- **Meaningful enforcement of existing laws;**
- **Legal clarity through guidance from supervisory and enforcement authorities;**
- Performing **thorough impact assessments and meaningful consultation** processes with stakeholders, including civil society**;**
- **No dilution of fundamental rights.**

## 2. Fundamental rights are not “red tape”

The Commission’s consultation and the overall narrative about the many proposed Omnibuses suggest that the “accumulation of rules” undermines competitiveness. As a civil rights organisation, we oppose this narrative, which is based on a selective interpretation of the Draghi Report. In fact, we believe that centring digital legislation on public service goals and fundamental rights creates legal certainty. Furthermore, it allows European businesses and people to thrive and compete innovatively outside the data-exploitative business model Big Tech has created. Furthermore, legal certainty ensures fairness and transparency in the tech industry. Citizens, along with small and medium-sized European companies, would be the main beneficiaries of such an approach to digital legislation.

A narrative claiming that high standards uniquely burden SMEs is invalid. The EU digital acquis does not impose *uniform* obligations on all actors. In practice, several instruments already embed **risk-based** and **size-based** differentiation. It means that the most resource-intensive duties are bound to actors such as Big Tech and other resource-rich companies with sufficient capacity, rather than SMEs. The GDPR, the DSA, and the AI Act each exempt certain companies from the most stringent obligations. The truth is that SMEs often struggle with uncertainty, inconsistent interpretation, lack of oversight support and duplicative procedures, things that deregulation will not solve.

The Digital Omnibus claims to reduce bureaucracy and burdens by proposing a widespread number of changes to critical digital legislation. Paradoxically, this undermines legal certainty, as businesses that were adapting to the digital acquis now see that their preparatory work will need to change if the many changes become law. Legal certainty benefits all market actors, particularly SMEs, by preventing fragmentation and reducing compliance risk. Renegotiating foundational instruments would cause **legal instability**, could deter investment, and may favour incumbents with greater capacity to absorb regulatory uncertainty.

From a fundamental rights point of view, this is even more worrisome. The proposed changes to the AI Act, GDPR and ePrivacy Directive are already undermining the core basis of the digital legislation that the co-regulators adopted, with a careful balance between protecting fundamental rights and ensuring that laws do not unduly restrict the digital single market. We are concerned with the trend of continuing the dismantling of digital legislation.

Specifically, we encourage the European Commission to protect not only the laws mentioned before in the previous paragraph but also the Digital Services Act (DSA) and the Digital Markets Act (DMA). Both laws are only in their infancy, and it is too early to propose changes when we are just beginning to enforce them, with core staff still being incorporated into the enforcement teams in the European Commission as we write these lines.

We must also highlight the spillover effect of European legislation, which has set a global standard in data protection. The responsibility of European legislators to uphold democratic values and the rule of law is a core principle of the EU. By dismantling our core digital protections in Europe, the “Brussels effect” may lead this time to similar deregulation efforts worldwide.

## 3. Fix enforcement gaps, not legislation

We believe that the European Commission should focus on enforcing existing legislation at both the EU and national levels, rather than removing protections. Below, we have noted several aspects that highlight the lack of enforcement of the laws currently under review.

## 3.1 GDPR Enforcement Statistics

The GDPR remains the EU's principal data protection framework, yet enforcement challenges persist. Noyb, the Austrian data protection civil society organisation, has repeatedly documented that, on average, only about **1.3 % of cases before national data protection authorities result in fines**, highlighting systemic under-enforcement. These statistics show that the problem is not *too much law*, but **too little bite** in implementation.

## 3.2 AI Act roll-out

The AI Act establishes a risk-based framework that links compliance obligations to potential harms. Weakening these safeguards under a simplification banner would invite regulatory arbitrage and erode public trust in automated systems. Center for Democracy and Technology Europe has reported the following shortcomings with the rollout of the AI Act:

- "The opacity, lack of transparency and lack of understanding about how an AI system works and whether an AI system was involved in the first place make it more difficult to bring cases based on valid claims with a sufficient likelihood to succeed.
- Limits on the promise of individual litigation, particularly in the context of systemic and at-scale harms caused by AI.
- Costs and length of legal proceedings, especially if expert advice is needed.
- Lack of financial and human resources for enforcement bodies, also in light of the increased expertise that is required to deal with challenges posed by new technologies.
- Lack of harmonisation of some of the rules and the enforcement structures across Member States leads to an uneven playing field and challenges in addressing cross-border infringements."

These shortcomings will not be solved by the deregulatory effort of the AI Omnibus. On the contrary, extending the enforcement deadline risks delaying the fixing of all these problems, creating less legal certainty for businesses and less protection for people in the EU.

## 4. The Charter of Fundamental Rights is binding, not a "nice to have"

The EU's digital regulatory framework is rooted in the Charter of Fundamental Rights, namely in the following articles:

- **Article 7** — Respect for private and family life;
- **Article 8** — Protection of personal data;
- **Article 11** — Freedom of expression and information.

The Charter is binding on EU institutions and Member States as it is primary law. Any assessment of the digital acquis must keep the Charter at the core of any potential reforms and enforcement. The Charter is not an afterthought or a collection of wishes, but a legal obligation for the EU institutions. Therefore, unlike the Draghi and Letta reports, any conclusion that seeks to limit fundamental-rights protection is deeply misguided.

**In the current political context, a "fitness check" that treats fundamental rights obligations as disposable economic costs would contradict the Charter's constitutional weight and disrupt the EU's legal order, bring legal uncertainty, reduce the EU's power against Big Tech in the context of an existing aggressive US oligarchy, and lead to more disinformation and exploitation of people's fundamental rights.**

## 5. If anything needs to be changed: Fix processes, do not lower standards

Companies and citizens alike benefit from **EU-wide harmonisation**. Divergent enforcement would negatively affect the internal market. It is necessary to avoid the weak enforcement of European laws, which creates legal uncertainty for all market players.

In essence, we propose to "fix processes, do not lower standards". The Commission's approach should **not be to** weaken the legal regime but to enhance cooperation among authorities and prioritise guidance to support uniform application. The Commission should keep up with its promise and reduce the administrative burden through **guidance, shared resources, encouragement of swift and robust enforcement of existing legislation, and consideration of one-stop-shop approaches**. But they should pay attention to not eroding rights or enforcement mechanisms.

Rolling back safeguards would not help SMEs or citizens, but it would advantage Big Tech and other large firms that can easily capitalise on regulatory uncertainty and adapt to it.

## 6. Recommendations

Liberties calls on the Commission to:

1. **Reject any current and future proposals to weaken EU rights-based digital frameworks** under the guise of simplification, such as the AI Omnibus and the Omnibus that impacts the GDPR and the ePrivacy Directive.

2. **Prioritise enforcement reform** of GDPR, DSA, DMA, AI Act, and ePrivacy, including resourcing of supervisory authorities.

3. Improve **cross-border coordination and procedural effectiveness** among national authorities.

4. Undertake a **fundamental rights impact assessment and meaningful consultation processes ahead of any** future regulatory changes impacting digital legislation.

## 7. Conclusion

The Digital Fitness Check must not become a pretext for deregulating rights-protecting standards. The real issue facing the EU digital economy is not the volume of rules, but the **failure to enforce and meaningfully apply them**. What European citizens and businesses need is **effective implementation**, **legal clarity**, and **trustworthy digital infrastructure** — not dilution of safeguards that underpin the internal market and fundamental rights.

In conclusion, we believe that the argument to evaluate competitiveness through bureaucratic burdens is a dangerous mischaracterisation. We have argued that foundational laws like the GDPR, DSA, DMA, and AI Act are not mere administrative burdens, but rather the operationalisation of the Charter of Fundamental Rights. Deregulation of safeguards ensured in these frameworks under the guise of a "fitness check" will not empower European SMEs. Legal certainty of harmonised rules to compete fairly is in their utmost interest. Deregulation would primarily benefit Big Tech companies, which possess the resources to exploit regulatory uncertainty and systemic loopholes. True innovation within the European Union must be built on legal clarity and public service goals, not the erosion of civil liberties.

Therefore, the European Commission must focus on robust, meaningful enforcement of existing laws: priority should be placed on adequately financing supervisory authorities, improving cross-border coordination, and providing clear compliance guidance. The European Union cannot afford to lower its standards and compromise its democratic values for the hypothetical promise of economic gains. The EU must protect its citizens from digital exploitation while cultivating a digital single market.