European Digital Rights

EDRi Contribution to the European Commission's GDPR Implementation Dialogue (Post-Meeting Submission)

EDRi welcomes the opportunity to participate in the European Commission's Implementation Dialogue on the GDPR and thanks DG JUST for facilitating an open and constructive exchange. This post-meeting submission builds on our initial contribution and reflects additional input following the discussion held on 12 July 2025. We offer these remarks in the spirit of continued engagement and a shared commitment to a strong, rights-based implementation of the GDPR.

1. Further simplification/reduction of administrative burden

Q: What are your views on possible further simplification of the GDPR, going beyond the recent Commission's proposal to simplify the record-keeping obligation (1)?

In 2024, the European Commission carried out a detailed assessment of the enforcement of the GDPR as part of its second evaluation report. It found no evidence to justify structural reform. On the contrary, the Commission reaffirmed that the Regulation is effective in achieving its objectives, proportionate in its obligations, and adequately future-proof to respond to evolving technological and societal challenges. The vast majority of recommendations focused on non-legislative, supportive measures to strengthen enforcement. Notably, Chapter 6 of the report was titled 'The GDPR as a cornerstone for EU policy in the digital sphere,' highlighting how in practice, the GDPR is not an obstacle to innovation or competitiveness but a foundational framework that underpins trust, rights protection, and the EU's broader digital strategy.

EDRi remains strongly opposed to the proposal in COM(2025)501 to amend Article 30(5) and finds it concerning that - especially with the GDPR Procedural update only just having been agreed - 'further simplification' is already being proposed. The proposed change to 30(5) is not a neutral simplification. It removes a key safeguard, introduces unjustified exemptions based arbitrarily on the size of the controller rather than the risk of processing, and ultimately creates legal uncertainty, rather than reducing it.

The proposal is not based on evidence, lacks an impact assessment, and would likely result in irresponsible actors avoiding documentation entirely, while many controllers would continue documenting for liability or internal governance reasons, having such systems already well established. It risks normalising differential treatment of rights: some controllers would maintain minimal records, while others would be rewarded for abandoning documentation altogether. This creates a compliance asymmetry that runs counter to the GDPR's risk-based logic.

Simplification is not neutral. It must be asked: simplification for whom? The burdens imposed on people trying to understand and exercise their rights are often far greater than those imposed on controllers by documentation obligations. The Commission should focus on the real sources of complexity: inconsistent enforcement, lack of guidance, and an opaque compliance industry that thrives on uncertainty. Effective simplification must come through better implementation, not deregulation.

At the same time, EDRi recognises that practical and genuine simplification measures are both possible and desirable, provided they strengthen rather than weaken protections. In our view, the most effective measures to reduce compliance burden without lowering the level of protection should include:

- The development of standardised, pre-approved templates (e.g. for ROPAs, DPIAs, privacy notices) to reduce uncertainty and legal costs, especially for SMEs;
- The promotion of sector-specific, risk-based compliance models co-developed with DPAs. These could take inspiration from the CNIL's former *normes simplifiées*, which provided standardised ROPAs for common processing activities. Organisations could declare adherence to these predefined frameworks to demonstrate compliance, provided they stayed within clearly defined limits. More complex or high-risk processing would still require a bespoke approach. A modernised version of this model could offer legal certainty and reduce burden without lowering protection standards;
- The adoption of joint guidance by the EDPB on key areas of GDPR implementation where organisations often face uncertainty and/or where national guidance is either lacking or fragmented. This could include, but is not limited to, legal bases, risk assessments, accountability tools, transparency obligations, and data subject rights. This will reduce fragmentation and make compliance expectations more predictable across Member States;
- We also strongly support the implementation of the EDPB Helsinki Statement as a framework for coordinated simplification, focusing on aligned enforcement methodologies, practical tools, and accessible interpretation.

Real simplification means accessible guidance, clear interpretation, and targeted support for compliance, not weaker rights or reduced accountability. With the EU's broader simplification agenda already watering down key rights and justice protections across many areas (for example Corporate Sustainability Due Diligence), simplification must not be allowed to be a Trojan horse for deregulation.

Q: Which targeted amendments would appear potentially useful to reduce administrative burden of controllers and processors, while maintaining the GDPR's risk-based approach and ensuring the high level of data protection?

We do not support any legislative amendments at this time. The GDPR is a future-proof, principles- and rights-based framework that is already proportionate and allows for reasonable flexibility. Reopening the text would distract from the real challenges and risks inviting deregulatory changes that would undermine the Regulation's core purpose.

Instead, we support non-legislative solutions to support compliance in practice. The EDPB's Helsinki Statement provides a useful basis for this approach. We encourage the development of templates, checklists, and practical tools to support SMEs and reduce perceived burdens without lowering the level of protection.

One example of effective simplification is the CNIL's former system of simplified records of processing activities. By providing predefined models for common processing types, CNIL allowed controllers to declare compliance as long as they remained within set parameters. This approach offered genuine support without legal reform and could be replicated or updated at EU level.

Real simplification means accessible guidance, clear interpretation, and targeted support for compliance, not weaker rights protection or documentation of compliance with these rights.

2. Increasing legal certainty, reducing fragmentation and further harmonising enforcement

Q: What are the measures you would consider useful to increase legal certainty, to reduce the fragmentation in the application of the GDPR and to further harmonise its enforcement?

Legal certainty comes from predictable enforcement, clear guidance, and regulatory stability, not from constant legislative revision. Reopening the GDPR creates uncertainty and undermines trust in the regulatory framework, particularly with two significant changes (Procedural Regulation; midcaps omnibus) already under this Commission's belt. We can see a clear warning in what has happened with the EU AI Act, where the Commission's indication that it may reopen the text due to implementation delays have created a self-fulfilling prophecy of implementation delays.

Crucially, enforcement gaps often stem from under-resourced DPAs, as highlighted by the Fundamental Rights Agency (FRA) 2024 report on the experiences, challenges and practices identified by DPAs in implementing the GDPR requested by the Commission. Despite the growing responsibilities assigned to DPAs, the report documents persistent structural shortages in human, financial, and technical resources across many Member States. While DPA resourcing is not the only barrier to effective enforcement (political pressure, fragmentation, and procedural complexity also play a role) it remains a foundational issue. We believe the Commission should take a more proactive role in addressing these disparities, including through funding mechanisms, baseline capacity assessments, and structured cooperation with national governments. Robust enforcement is not possible without well-equipped regulators.

We recommend:

- Strengthening and coordinating enforcement efforts across Member States, including through joint investigations;
- Providing transparent and widely-accessible DPA and court decisions to support legal convergence;
- Supporting the implementation of the Helsinki Statement, particularly regarding aligned enforcement methodologies and templates;
- Enhancing the role and capacity of the EDPB in providing authoritative interpretation while clarifying its relationship to national guidelines.

The Commission's proposal to exempt small and mid-cap companies from certain obligations under Article 30(5) GDPR is based on the misguided perception that larger companies already face heavier compliance burdens. In reality, the problem is not that smaller actors are overburdened, but that dominant ones too often evade meaningful enforcement. The answer is not to lower standards but to ensure robust and consistent enforcement against all actors, especially against actors whose scale and business models pose systemic risks.

3. Facilitating compliance with the GDPR

Q: What are your views on the various tools under the GDPR, e.g. codes of conduct and certification, that could be exploited to facilitate compliance with the GDPR?
Q: What challenges have you faced in relation to the use of such tools and what solutions would you propose to address these challenges?

These tools have significant potential but remain underutilised due to structural and governance challenges. Limited uptake is due to under-resourced DPAs, difficulties in establishing monitoring bodies, and in some cases, attempts by industry actors to use codes and certification to reinterpret core GDPR principles. This has led to justified rejections by DPAs and discouraged further use.

To unlock the potential of these tools, we recommend:

- Providing templates and clearer expectations for drafting and assessing codes and certification schemes;
- Allowing for flexible, tiered schemes (e.g. SME-oriented basic codes with modular enhancements);
- Clarifying roles and criteria for monitoring bodies to reduce administrative barriers;
- Ensuring transparency and participationof a broad range of stakeholders, including civil society organisations, consumer groups, trade unions, independent academics, and representatives of marginalised or impacted communities in the development and approval processes.

These tools should be rights-enhancing, not deregulatory. They must supplement the law, not replace its enforcement or be used to argue that its protections are no longer necessary.

4. Clarifying the articulation with other digital legislation

Q: Is there a need to further clarify the interplay of the GDPR with other EU digital legislation?
Q: Can you provide some specific examples of provisions for which the interplay of the GDPR and other digital legislation has appeared to be challenging?

The GDPR is a technologically neutral framework and was designed to accommodate emerging contexts without frequent revision. We therefore find in our work that the GDPR is structurally most compatible with newer digital legislation, creating an essential rights-based foundation for rules that deal with personal data. This is particularly important considering that certain newer laws, like the AI Act, do not take a rights-based approach. Without the GDPR's provisions forming a horizontal foundation, the newer acquis would likely fail to meet obligations to protect the rights to privacy and data protection enshrined in the EU Charter.

That said, the interaction between the GDPR and legislation such as the AI Act, Data Act, and DSA raises questions about regulatory consistency. These are not structural incompatibilities but coordination challenges. They should be addressed through joint guidance, institutional cooperation, and shared interpretation, especially around legal bases, risk assessments, and roles of authorities.

We welcome emerging cooperation between the AI Office and the EDPB as a step in the right direction. Similar coordination should extend to the Data Act and eIDAS, among others.

Article 22 of the GDPR contains essential safeguards on automated decision-making and must not be reinterpreted in a way that undermines individuals' right to meaningful human oversight, especially in high-impact contexts such as AI deployment.

We are concerned by calls to reinterpret the scope of 'legitimate interest' as a catch-all basis for AI training, fraud prevention, or data analytics. These uses require careful assessment and often involve high-risk processing that cannot be legitimised by general interest claims alone. Additionally, industry requests for 'safe harbour' treatment of pseudonymised data risk creating broad exemptions without accountability. Pseudonymisation lowers risk but does not eliminate identifiability. The current legal framework rightly treats it as personal data, and this should not be changed.

Regarding the ePrivacy Directive, we note that it protects a separate but related fundamental right: the confidentiality of communications, as enshrined in Article 7 of the Charter. While not subordinate to the GDPR, it must be applied in a complementary and consistent manner. Given its outdated structure and uneven national implementation, it is essential to preserve the level of protection it is supposed to provide. We are particularly concerned by coordinated efforts to weaken the ePrivacy framework by subsuming its safeguards under the GDPR or repealing key provisions, when in fact the focus should be on ensuring meaningful ePrivacy enforcement. Many of the same actors now calling for 'simplification' of the GDPR previously lobbied against the ePrivacy Regulation. Diluting or repealing the Directive would severely undermine individual rights and further entrench pervasive commercial surveillance models.

We are also concerned by the direction taken in the articulation of the forthcoming Data Union Strategy, and echoed in the broader Competitiveness agenda of the European Commission. While the GDPR is not explicitly mentioned, the language and objectives outlined in preliminary discussions appear to implicitly target the Regulation's safeguards, constructing them as obstacles to data sharing and cross-border flows. This signals a dangerous shift in narrative, one that reframes rights-based protections as barriers to competitiveness. Any strategy that fails to reaffirm the primacy of the GDPR and the Charter risks opening the door to piecemeal erosion of fundamental rights under the banner of 'data innovation'. The same applies for the AI Act, ePrivacy Directive, DSA and DMA, the focus of which should be on implementation or enforcement to bring the co-legislators' aspirations for trustworthy tech into reality, not 'simplification' efforts that move us towards a less fair and more uneven playing field.

Clarification of interplay (NOT overlap) must never become an excuse to lower protections or introduce fragmented interpretations that benefit the most powerful players. The goal must be coherent application of fundamental rights across all frameworks.

Final remark

We are increasingly concerned that proposals to 'simplify' the GDPR are not isolated but part of a broader deregulatory agenda that threatens to lower the level of protection across the EU digital rulebook and beyond. The same actors that previously opposed the ePrivacy Regulation are now calling for the ePrivacy Directive to be diluted or repealed. This coordinated narrative reframes fundamental rights as burdens and risks undermining the EU's credibility as a global standard-setter for rights-based digital governance. The future Digital Package (omnibus) slated for December 2025 has fuelled our concerns that the digital acquis hard-won in the last decade – along with protections for nature, water, and justice for people over corporate greed in other omnibus proposals – are being picked apart. Rather than advocating for much-needed but currently-missing protections (such as against commercial surveillance), public interest actors are pushed into a reactive position of defending basic protections.

The GDPR remains the backbone of the EU's digital rulebook and a global benchmark for rights-based regulation. Reopening it, especially under the false promise of simplification, would jeopardise both its effectiveness and legitimacy.

The challenges we face today do not stem from the legal text. They stem from insufficient enforcement, lack of guidance, and uneven application. These problems demand political will, institutional cooperation, and meaningful support, not legal deregulation.

We urge the Commission to stand firm against pressure to reopen the GDPR and instead prioritise enforcement, implementation, and the protection of fundamental rights.