Date 08-07-2025

EDRi Contribution to the Public Consultation on the Proposal for a Regulation on Burden Reduction and Simplification for Competitiveness of Small Mid-Cap Enterprises

Executive Summary

- While EDRi supports the goal of making EU regulation more navigable for smaller organisations, we strongly oppose the framing of fundamental rights safeguards as administrative burdens and reject the proposal's redefinition of core accountability obligations.

- The proposed amendment eliminates the current exemption's cumulative safeguards (occasional, low-risk, and non-sensitive processing), replacing them with a single, vague threshold of 'likely high risk'. This change allows routine and systematic data processing to be undocumented, creating legal loopholes and disincentivising compliance. The removal of the term 'occasional' in particular dismantles a critical check against untraceable and potentially harmful data practices.

- This shift also undermines the structural logic of the GDPR, which treats documentation as a foundational element of transparency, enforceability, and security. The proposal weakens the ability of individuals to exercise their rights, obstructs regulatory oversight, and erodes cybersecurity resilience. It introduces legal uncertainty for controllers and misaligns professional and legal standards, placing responsible actors at a competitive disadvantage.

- Moreover, the proposal was introduced without an impact assessment, without evidence of disproportionate burden, and outside the normal processes for amending fundamental rights legislation. This procedural shortcut contravenes the Commission's own Better Regulation Guidelines and threatens to normalise *ad hoc* deregulation of rights-based frameworks.

- Finally, the proposed changes send a damaging signal to global partners. The GDPR has been a global benchmark for data protection; diluting its core provisions on economic grounds risks undermining the EU's credibility and digital diplomacy.

- The amendment appears to reflect a broader deregulatory trend that threatens not only the integrity of the GDPR, but the coherence of the EU's entire digital rulebook. Using 'competitiveness' as a justification to weaken rights-based frameworks risks normalising

procedural shortcuts, lowering legal standards across digital legislation, and eroding the EU's credibility as a global leader in fundamental rights protection.

- EDRi urges the Commission to withdraw the proposed amendment to Article 30(5) GDPR. We also call on co-legislators to oppose the use of omnibus simplification instruments to alter fundamental rights legislation. The GDPR does not need to be reopened: it needs to be properly enforced and supported with tools that enable, rather than undermine, compliance.

I. Introduction

European Digital Rights (EDRi) is the largest network of civil society organisations and individuals in Europe committed to defending fundamental rights in the digital environment. We welcome the opportunity to provide feedback on the Commission's proposal for the Fourth Omnibus Regulation (COM(2025)501 final), and in particular the proposed amendment to Article 30(5) of the Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR).

EDRi does not oppose competitiveness or the aim of ensuring that smaller organisations can navigate EU regulation effectively. However, we strongly reject the false dichotomy between competitiveness and fundamental rights. The GDPR is not a burden to be minimised, but a cornerstone of the EU's constitutional framework under Article 8 of the EU Charter of Fundamental Rights (Charter), and notably of the EU's digital rulebook. It is a rights-based instrument designed to protect individuals, regardless of the economic profile of those who process their data.

The proposed amendment to Article 30(5) GDPR would dramatically reduce accountability obligations for nearly all organisations operating in the EU. It removes the requirement to document processing activities unless they are deemed 'high risk' while eliminating the current safeguard that exempts only 'occasional' and low-risk processing. We are afraid that this shift is not a simplification, but a structural weakening. It does not clarify obligations; it redefines them in a way that undermines transparency, impairs enforcement, and shifts power further away from individuals and supervisory authorities. It also lowers the baseline for security preparedness and breach response, as organisations would no longer be required to maintain internal records that are crucial to identifying, containing, and addressing data breaches.

The proposal is being introduced through a general 'simplification' initiative, outside the normal processes of rights-specific legislative reform. This raises serious concerns about procedural legitimacy and democratic scrutiny. No impact assessment has been published, no evidence of disproportionate burden has been presented, and no legal analysis has been offered to explain how the change complies with the Charter or the GDPR's risk-sensitive but fundamentally rights-driven logic.

This contribution outlines why the proposed changes to Article 30(5) GDPR should be withdrawn. It calls on the Commission and co-legislators to preserve the structural safeguards that make the GDPR enforceable, and to support SMEs through guidance and resourcing, not through deregulation that undermines people's rights.

II. Analysis of the Proposed Amendments

1. A Substantive Rewriting of the GDPR's Architecture

The proposed amendment is not a technical clarification. It is a structural change to the GDPR's logic. The GDPR is a rights-based framework grounded in Article 8 of the Charter, which guarantees the right to data protection regardless of the type of processing or size of the controller.

The amendment reframes Article 30(5) by removing the requirement that processing be 'occasional' to qualify for exemption, and by conditioning record-keeping on whether the processing is likely to result in a high risk to individuals' rights and freedoms.

This move substitutes the current three-part, cumulative test (low risk, occasional, no sensitive or criminal data) with a single, weakly defined threshold: : whether the processing is 'likely to result in a high risk.' It is not simplification. It is a redefinition of who is accountable, and when, under the GDPR.

The shift towards a 'high risk' threshold mirrors the logic of the AI Act, but this resemblance is misleading. The AI Act adopts a risk-based approach precisely because it assumes the foundational protections of the GDPR are already in place. It regulates systems, not rights holders. Its framework is built on the premise that baseline rights safeguards - including documentation, transparency and purpose limitation - are guaranteed by the GDPR. Undermining those safeguards in the GDPR collapses the very floor on which the AI Act rests. As the former Article 29 Working Party (now EDPB) made clear: 'Rights granted to the data subject by EU law should be respected regardless of the level of the risks.[1]' By embedding risk assessment into the very applicability of documentation duties, the proposal makes enforceability contingent rather than guaranteed, reversing the logic of rights protection by making it dependent on a vague and self-defined threshold.

2. Removing 'Occasional': A Gateway to Routine, Opaque Processing

Under the current Article 30(5), only controllers whose processing is occasional, not likely to result in a risk, and does not involve special category or criminal data are exempt from record-keeping.

The term 'occasional' is not a vague embellishment. It is a foundational limitation. It ensures that only marginal, once-off or rare processing escapes documentation. Its removal would have dramatic negative consequences.

Systematic, continuous or large-scale processing, including profiling, adtech operations or employment-related surveillance, could now be undocumented, as long as the organisation deems it not high risk. This would remove a key check on cumulative harm and repetitive interference, particularly in everyday services that people depend on, such as education, employment or social protection.

---

1 14/EN WP 218 Statement of the WP29 on the role of a risk-based approach in data protection legal frameworks

The sole justification given in the Staff Working Document[2] is that 38% of SMEs have employees, which implies that their processing of personal data is not 'occasional' under the current GDPR exemption. According to the Commission, this makes them ineligible for the current derogation and thus burdened by the record-keeping obligation. However, this particular issue could be addressed in a much more targeted way without also exempting companies whose core activities consists of processing personal data on a large scale.[3]

The deletion of the 'occasional' requirement would degrade the GDPR's structural logic, in which frequent processing demands accountability. The loss of 'occasional' is not just a drafting issue. It is a legal opening for routine rights infringement without internal traceability.

3. 'High Risk': Vague, Self-Serving, and Legally Unfit for Article 30

The new trigger - likely to result in a high risk - is lifted from Article 35 GDPR (on Data Protection Impact Assessments). However, Article 35 is not meant to define exemption thresholds. It is a forward-looking tool for identifying the need for prior assessment, not a filter for whether documentation should exist.

The Commission provides no binding criteria to determine what is or isn't high-risk. DPIA guidance[4] (e.g. WP248rev.01) is non-binding and not tailored to the documentation function. There is also no obligation to consult supervisory authorities, and no requirement to record the rationale for the self-assessment.

This opens a serious legal loophole. Controllers are left to self-certify their non-accountability, with no duty to demonstrate how they assessed risk. SMEs and small mid-caps, under pressure to reduce overheads, are structurally incentivised to underestimate or downplay risks. Even well-intentioned organisations may lack the expertise to conduct reliable assessments without guidance or oversight. Inexperienced organisations may assume their processing falls below the new threshold without properly considering the associated risks or if a documentation duty applies, precluding the benefit those organisations gain from that preliminary analysis. In fact, assessing whether processing is 'high risk' may itself require compiling a record of processing activities, particularly for mapping flows applying EDPB guidance. This pushes many organisations towards costly external legal or consultancy support.

DPAs, meanwhile, are left in the dark: they cannot verify the validity of a self-assessment when there are no records to review, and cannot easily determine whether a controller was ever subject to documentation duties in the first place. This disables early detection of systemic issues, frustrates the handling of complaints, and undermines targeted supervision. It also creates uncertainty for processors, joint controllers and third parties who rely on clear documentation to understand data flows and roles. In practice, the proposal would disincentivise compliance, make breaches harder to trace, and erode the foundations of trust and legal predictability across data ecosystems.

---

2 SWD(2025) 501 final, page 13

3 A targeted approach is taken in recital 10 of the proposal, where it is clarified that processing of personal data due to legal obligations in the field of employment should not, as such, require records of processing to be maintained.

4 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01

This undermines the principle of legal foreseeability under Article 52(1) of the Charter. People cannot rely on the law if it is discretionary and unverifiable in application.

While the idea of a 'risk based approach' is generally accepted, it must be operationalised through clear thresholds and legal provisions that ensure certainty for all actors. It is entirely unclear what would constitute a 'high risk',which is also detrimental for controllers. An inaccurate assessment could lead to fines of €10 million or 2% of annual turnover. Such legal uncertainty tends tends to increase reliance on lawyers and consultants resulting in actual administrative burden and thus unnecessary costs that wouldn0t arise under a clearly defined threshold.

3bis. Risk Reinterpretation Through Recital: Undermining Safeguards for Special Category Data

The amended Article 30(5) removes the explicit reference to special category data as a trigger for documentation duties. Under the current GDPR, processing such data disqualifies a controller from exemption. Under the proposed text, the only condition is whether the processing is 'likely to result in high risk'.

In this context, the new recital proposed alongside the amended Article 30(5) plays a critical interpretive role. It asserts that processing special category data under Article 9(2)(b) – particularly in employment and social protection contexts – does not, in itself, trigger a record-keeping obligation. While recitals are not legally binding, they guide interpretation. In this case, the proposed recital invites controllers and regulators to treat structurally sensitive and power-asymmetric contexts as inherently low risk, a stance that departs significantly from the original GDPR's logic and its emphasis on heightened safeguards for 'sensitive data'.

This approach is not only legally incoherent, it is in direct tension with Recital 10 of the GDPR, which recognises that such contexts are likely to involve high risk. The risk is compounded by the fact that Article 30(5) is now conditioned on a vague, self-assessed risk threshold, with no obligation to document or justify the assessment. The recital could therefore exacerbate the loophole: organisations could claim low risk, omit records, and cite the recital as interpretive support, even when processing highly sensitive data in hazardous settings.

4. Undermining Transparency and Individual Rights

Record-keeping under Article 30 is not an administrative burden. It is the basis for:

- fulfilling transparency obligations under Articles 13 and 14, including mandatory information about third-country transfers,
- enabling data subject rights under Articles 15 to 22 (access, rectification, erasure, objection),
- ensuring demonstrable compliance under Article 5(2),
- and providing evidence in disputes before DPAs and courts.

Record of Processing Activities are also a necessary precondition for fulfilling other GDPR obligations, including mapping data transfers and conducting DPIAs, both of which require a

structured understanding of processing operations.Without records, privacy notices risk becoming generic, incomplete or misleading. Access requests cannot be meaningfully answered. DPAs are left without any documentation to investigate complaints or verify legal compliance. Individuals are left with no structural tool to check, contest or understand how their data is used

In this sense, the change does also not seem to reach the objectives to simply the law. In fact, companies must logically collect an overview of the processing the undertake to even make a proper risk assessment. Removing this requirement based on the assumed outcome of the process seems fundamentally unlogical.

In reality, the change may have very limited practical impact, as responsible controllers will continue to update their records to comply with other GDPR provisions (such as Articles 5(1)(a), 5(2) 13, 14, 15 or 32). The GDPR's overall architecture requires organisations to maintain a comprehensive overview of the processing they carry out.

Removing documentation for most organisations functionally disables the exercise of rights, even if they remain formally listed in the Regulation. The removal of documentation obligations also undermines organisational and cybersecurity resilience. Record-keeping is not only about accountability to individuals or regulators: it is a core operational tool for internal oversight, breach detection, and forensic analysis. Without clear records of processing activities, organisations may be unable to swiftly identify the scope and source of a data breach, notify affected individuals, or contain further harm. In practice, this weakens both preventive and reactive security capabilities. The proposal thus runs counter to broader EU Cybersecurity Strategy and the GDPR's own principles of security by design and by default (Article 25 and 32).

5. Company Size and Turnover: Misaligned Metrics

The Commission proposes raising the threshold to 750 employees, with potential reference to turnover. This scale is disconnected from data protection realities.

Size does not equal risk. Small companies frequently engage in intrusive processing. Adtech vendors, data brokers, credit scoring firms and AI developers often employ under 50 people. With the Commission's over-broad simplification proposal, some of these companies will be required to designate a data protection officer (DPO) under Article 37, but exempted from the record-keeping obligations in Article 30.

Enforcement statistics show that major GDPR fines overwhelmingly target large firms with persistent, systemic violations, not small firms penalised for minor issues. The GDPR already embeds proportionality into enforcement. Supervisory authorities are empowered to take into account size, capacity and intention when applying sanctions.

Granting automatic exemptions to the majority of EU-based organisations based solely on economic metrics is *de facto* deregulation (more on this below). According to Eurostat, over 99.9 % of EU companies fall below the 750-employee threshold[5]. The exemption becomes the rule, and accountability becomes selective rather than structural.

5 Structural business statistics overview https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Structural_business_statistics_overview

6. No Evidence, No Assessment, No Justification

The Commission claims this change will reduce administrative burdens and save €66 million annually for micro, small, and small mid-cap companies. But this number seems highly speculative. It is based on the assumption that organisations only spend 30 minutes per year updating their Article 30 records. No empirical data backs this assumption. Figures are presented without any source, sectoral context or cost breakdown. It is unclear whether it refers to recurring or one-off costs, or whether it includes external legal advice or GDPR implementation more broadly. A single unverified example, devoid of methodological clarity, cannot justify weakening a foundational accountability obligation that applies across all sectors of the economy. The proposal is not accompanied by a cost-benefit analysis, nor any enforcement data demonstrating that the Article 30 obligation has produced disproportionate burdens.

The Commission frames the deletion of record-keeping obligations under Article 30(5) GDPR as an extension of 'mitigating measures'. As mentioned, this is conceptually flawed, as it enables organisations to demonstrate compliance, supports data subject rights, and facilitates regulatory oversight, and detect, contain and respond to security incidents such as data breaches. Weakening documentation obligations removes a key internal control for operational and cybersecurity preparedness, undermining both legal accountability and technical resilience.

Mitigating measures, in the context of simplification, should reduce burdens without dismantling structural safeguards. But this proposal removes the obligation altogether for most organisations, even in contexts of systematic or sensitive processing. Moreover, the removal creates a misleading baseline: many responsible companies will likely continue to keep records voluntarily, especially those operating across jurisdictions or facing supply chain due diligence obligations. This introduces a discrepancy between legal requirements and professional standards, creating legal uncertainty, competitive distortion, and weakening the EU's ability to define and enforce consistent practices across sectors. Additionally, this means the exemption will primarily benefit those least inclined to comply: organisations with weak accountability practices, opaque business models, or high-risk operations. In other words, the reform removes obligations precisely where oversight is most needed, while responsible actors bear the costs of doing the right thing.

Crucially, the Commission explicitly states that no impact assessment was necessary, on the grounds that the proposal is part of a simplification package. This position is deeply problematic given that the amendment in question affects a key safeguard under a fundamental rights-based regulation. Any legislative change that limits or conditions individuals' ability to exercise their rights under the Charter must meet strict standards of necessity, proportionality and transparency. None of these requirements have been fulfilled.

Furthermore, no analysis seems to have been carried out on how the removal of documentation obligations will affect the ability of supervisory authorities to investigate complaints, verify lawfulness, or ensure meaningful redress. There has also been no evaluation of less intrusive alternatives, such as simplified templates, enhanced guidance, or reinforced DPO support, all of which were highlighted as priorities in the Commission's own 2024 report on GDPR enforcement.

This approach fails to meet the European Commission's own Better Regulation standards and contradicts the principle of necessity and proportionality under Article 52(1) of the Charter. The

lack of justification, coupled with the absence of any quantifiable or proportionate assessment, renders the proposed amendment legally and politically indefensible.

Moreover, while the Staff Working Document includes a formal 'interoperability assessment', this is limited to checking for legal contradiction. It does not assess whether the proposed simplifications weaken coherence across digital legislation, such as the Digital Services Act (DSA), Sigital Markets Act (DMA) or AI Act. Reducing documentation duties under the GDPR undermines enforcement interoperability and risks fragmenting core accountability mechanisms across the EU's digital rulebook.

In practice, many companies only prepare Record of Processing Activities when specifically required to do so by DPAs. Weakening this duty removes one of the few points of intervention that prompts proactive compliance.

7. The Omnibus as Procedural Shortcut: Deregulation by Design

The proposed amendment is not merely a question of administrative streamlining. It seems emblematic of a wider deregulatory trend that frames fundamental rights safeguards as obstacles to growth, and uses competitiveness as a pretext for structural erosion. The Fourth Omnibus Regulation introduces changes to the GDPR without a dedicated legislative process, seemingly without fundamental rights impact assessments, and with limited public scrutiny, all under the banner of 'simplification.'

This approach sets a dangerous precedent: rights-based frameworks can be revised through horizontal economic files, rather than through proper democratic processes. Once this route is normalised, the threshold for altering core safeguards in other digital laws will be dangerously lowered. In fact, we are already witnessing growing political appetite to further reopen the GDPR, both through future omnibus packages and via sectoral reforms that quietly revise rights protections. Discussions around the Digital Package expected in Q4 2025 (which will include other laws of the digital rulebook), the Data Union Strategy, and the International Digital Strategy all seem to point toward a sustained institutional interest in revisiting or weakening the GDPR's core provisions.

The legislative manoeuvre at play here mirrors recent procedural shortcuts seen in other files, such as the Corporate Sustainability Due Diligence Directive (CSDDD), where obligations were significantly narrowed through last-minute changes in interinstitutional negotiations. These practices risk turning *ad hoc* deregulation into a systemic mode of policymaking.

In this context, the amendment to Article 30(5) does not look like an isolated simplification but as part of a broader shift towards selective accountability, whereby obligations are removed or diluted based on economic profiling rather than risk or rights impact. This logic is legally unsound and politically corrosive, as it reframes the purpose of EU digital legislation away from protecting people and towards shielding controllers from responsibility.

This cumulative effect risks shifting the Overton window of digital regulation: what once seemed politically unthinkable - weakening the EU's flagship data protection law - is being slowly normalised. Allowing this to happen through procedural backdoors undermines both the rule of law and the EU's commitment to upholding fundamental rights as the foundation of its digital strategy.

8. Undermining the GDPR's Role as a Global Standard

GDPR is the world's benchmark for data protection. It has inspired legislative reform in Latin America, Africa and Asia. It underpins adequacy decisions and the EU's digital diplomacy.

Weakening core obligations through vague, economically framed reforms sends the wrong signal to other jurisdictions. It erodes the normative power of EU law. It risks inconsistencies with adequacy standards and contributes to a global race to the bottom on rights protections.

This is not 'simplification' but the first step in normalising selective accountability, justified on economic grounds, at the expense of systemic rights protections.

III. Recommendations

In light of the serious legal, procedural and fundamental rights concerns outlined above, EDRi submits the following recommendations:

1. Withdraw the Proposed Amendment to Article 30(5) GDPR

The deletion of the term 'occasional' is a structural weakening of the GDPR. The current text already provides a narrowly defined and proportionate exemption, limited to non-regular, low-risk, and non-sensitive processing. Removing this condition allows systematic and ongoing data processing to escape scrutiny, undermining accountability and transparency for the vast majority of organisations in the EU.

This change must be withdrawn in its entirety. The retention of 'occasional' is non-negotiable.

2. End the Use of Simplification Packages to Amend Rights-Based Frameworks

The GDPR is a horizontal Regulation grounded in fundamental rights. It must not be altered through omnibus instruments designed to deliver economic simplification. This procedural route bypasses rights-specific consultation, avoids legal impact analysis, and risks normalising ad hoc deregulatory interventions without democratic oversight.

Any attempt to weaken core protections in rights-based legislation through these means is structurally unacceptable.

3. Reaffirm That the GDPR Should Not Be Reopened

The GDPR is a living but coherent Regulation. Its architecture is designed to accommodate sectoral guidance, evolving technologies and contextual enforcement. What it requires is proper application, not revision.

There is no justification for reopening the GDPR: not now, not incrementally, and not under the banner of competitiveness. Such efforts shift the legal baseline, distort the political conversation, and create long-term risks for the EU's regulatory credibility and normative leadership in the digital domain.

IV. Conclusion

EDRi welcomes the Commission's commitment to supporting smaller organisations in navigating EU legal frameworks. However, we are deeply concerned that the proposed

amendment to Article 30(5) GDPR departs from the founding principles of the Regulation and risks undermining the integrity of the EU's data protection system.

The GDPR is a rights-based instrument designed to ensure that all individuals in the EU enjoy a high and consistent level of protection, regardless of the controller or processor involved. The proposed changes would significantly narrow the scope of accountability obligations by removing the existing cumulative conditions for exemption and replacing them with a vague, self-assessed 'high risk' threshold. Most notably, the deletion of the requirement that processing be 'occasional' represents a fundamental shift that would allow continuous and systemic data processing to take place without documentation.

This change could weaken transparency, obstruct enforcement, and impair individuals' ability to understand and exercise their rights. It would create significant legal uncertainty for controllers and supervisory authorities alike, while introducing a degree of fragmentation and legal uncertainty incompatible with the objectives of the Regulation.

Equally concerning is the legislative process itself. Amending a core provision of the GDPR through a horizontal simplification initiative, without a dedicated legal analysis, impact assessment, or public consultation on the implications for fundamental rights, sets a dangerous precedent. It invites further erosion of protections through procedural shortcuts, rather than through open, democratic debate.

EDRi therefore urges the Commission to withdraw the proposed amendment to Article 30(5) GDPR. We also call on co-legislators to ensure that the GDPR is not reopened or amended through omnibus instruments or broader deregulatory agendas. The focus must remain on applying and enforcing the existing framework effectively, not on reducing protections that are essential to safeguarding fundamental rights in the digital age.

We remain committed to constructive engagement and are ready to support efforts to improve regulatory clarity and enforcement, provided such efforts strengthen, rather than dilute, the rights and protections the GDPR was designed to uphold.