Group of the Progressive Alliance of
Socialists & Democrats
in the European Parliament

European Parliament
Rue Wiertz 60
B-1047 Bruxelles
T +32 2 284 2111
F +32 2 230 6664
www.socialistsanddemocrats.eu

Brussels 11 November 2025

To the attention of Executive Vice-President for
"A Europe Fit for the Digital Age"

**Subject: Safeguarding Europe's Regulatory Leadership in the Upcoming Digital Omnibus**

Dear Executive Vice-President Virkkunen,

As the European Commission finalises the forthcoming Digital Omnibus, we wish to express, by means of this letter, our concerns about the potential risks of deregulation and weakening of the EU's carefully constructed digital legal framework. The global regulatory leadership of the EU that brought us a 'Brussels Effect' on tech legislation is under pressure, in a geopolitical context where Big Tech companies are openly challenging our rules. The Omnibus exercise may not undercut the enforcement of our rules, and we should be careful when opening discussions on legislation democratically adopted only recently.

Europe's digital acquis is anchored in the General Data Protection Regulation (GDPR), e-Privacy Directive, the Free Flow of Non-Personal Data Regulation, the NIS 2 Directive, the AI Act, the Data Act, the Data Governance Act (DGA), and the eIDAS Regulation and represent a coherent and human-centric approach to the digital economy. These legal instruments together safeguard fundamental rights, enhance trust, and enable innovation in the European Union.

Our European digital framework is more than a collection of individual acts. It is a regulatory model that has inspired international partners and positioned Europe as a normative power in global tech governance. Backtracking or deregulating would weaken the EU's influence in ongoing global dialogues on data protection, AI, and cybersecurity. Maintaining regulatory coherence is thus not only a matter of internal governance, but also of strategic sovereignty and credibility abroad.

Any broad deregulatory exercise risks upsetting Europe's unique balance between technological progress and public interest. Streamlining and clarification can be considered where they reduce unnecessary overlap and unjustified burden. However, simplification must not come at the cost of legal certainty, enforcement capacity, or the protection of individuals' fundamental rights.

**1. Preserving the integrity of personal data protection under the GDPR and e-Privacy Directive**

The GDPR remains the cornerstone of the European digital regulation, safeguarding in fulfilment of the two fundamental rights enshrined in Art. 7 and 8 Charter everyone's personal data and granting individuals control over their information while enabling free movement of personal data and business operations. The GDPR pioneered the Brussels effect and inspired countries worldwide to adopt rights-based data protection frameworks. The S&D Group will oppose any attempt to weaken these foundations, lower the level of personal data protection, or narrow the GDPR's scope.

At a time when commercial and state surveillance through spyware, profiling, biometric systems, and data retention continue to erode privacy, data protection, and even the freedom of demonstration and of political participation, Europe must not dismantle the very standards and safeguards that define its digital acquis. We are deeply concerned by the proposed erosion of the GDPR's core principles, most notably the watering-down of the definition of personal data in Article 4(1). This definition creates significant legal uncertainty and huge loopholes for companies and would drastically shrink the Regulation's scope. It bears the question, if this Regulation still has any addressees at all.

What is unacceptable is the weakening of the protection of sensitive data in Art. 4(15) and Article 9. Under the proposed changes, only information that *directly* reveals a person's characteristics would be protected, while all inferred or derived data, such as indications of religion, health status, sexual orientation, or political opinions, could be freely processed or even used to train AI systems under legal bases like "legitimate interest." Such a change would deprive Article 9 of its very purpose, contradict established CJEU case law, and open the door to discriminatory profiling and the commercialisation of intimate personal inferences.

The S&D Group is equally concerned by other proposed changes that would restrict the rights of data subjects under Articles 12 *et seq*., especially by limiting their use to narrowly defined "data protection purposes" and by allowing controllers to reject requests as "abusive." This would severely undermine the individuals' right to access guaranteed in Article 8 of the Charter of Fundamental Rights.

We are also profoundly alarmed by the prospect of changing the ePrivacy framework to introduce all the GDPR legal bases for tracking technologies. Proposals such as Articles 88a-88b would expand the current "storage or access" rule to permit active manipulation of terminal equipment, potentially even allowing companies to alter user data on devices. Combined with new, industry-driven mechanisms for consent and broad exceptions for media providers, this would effectively legalise pervasive tracking and remove meaningful user control. The result would be an ad-tech free-for-all where companies rely on "legitimate interest" rather than consent, erasing years of progress in protecting privacy and communication confidentiality. Such a broad legal basis for accessing device data and personalised advertising based on legitimate interest also contradicts the express will of the vast majority of consumers in the EU.

There are serious concerns as to whether the far-reaching fundamental weakening of the GDPR and ePrivacy is compatible with the heart of two fundamental rights enshrined in the Charter: the right to privacy and the confidentiality of communications. Recent revelations from the data broker scandal once again highlight the dangers of a shadow industry trading in our movements, emotions, and relationships. Instead of dismantling these hard-won achievements, our efforts must focus on

strengthening them, through clearer guidance, stronger enforcement, and genuine accountability. The Commission cannot bargain away the right to privacy and protection of personal data and trade off our values and civil liberties for the false promises of deregulation. Privacy and data protection are not obstacles to innovation, they are the foundation of a free and democratic digital society.

**2. Strengthening the Data Act, Data Governance Act and Free Flow of Data Regulation as pillars of the EU data economy**

The Data Act and the Data Governance Act together form crucial pillars of Europe's data space architecture. The Data Act establishes fair access and use conditions for industrial and connected-device data, ensuring that data generated in the EU benefits European businesses and consumers alike. The DGA, in turn, creates the institutional framework for trustworthy data sharing, through mechanisms such as data intermediaries, data altruism, and the reuse of public-sector information. The Free Flow of Data Regulation ensures that non-personal data can circulate freely across Member States. Proposal to improve coherence and consistency between the different text can be considered. However, we warn against merging bits and pieces together as such an approach could result in a more complex legal regime and could fail to consider specificities of the respective legal acts. Additionally, we underline that any changes that would blur the boundaries between personal and non-personal data or weakens the role of supervisory authorities would fragment compliance regimes, erode public confidence and be unacceptable for the S&D.

**3. Maintaining Europe's ambition in cybersecurity and resilience**

The NIS 2 Directive is a vital pillar of the Union's cybersecurity architecture. At a time of increasing geopolitical tension and hybrid threats, regulatory consistency and preparedness are crucial. Streamlining should not dilute sectoral obligations or reporting duties that underpin collective resilience. The Digital Omnibus should reinforce, not relax, the principles of risk management, transparency, and accountability that NIS 2 embeds.

**4. Protecting trust and interoperability under eIDAS**

The eIDAS Regulation, and its recent revision introducing the European Digital Identity Wallet, form the foundation for trusted digital interactions across the Union. It ensures interoperability and mutual trust in electronic identification and trust services. Any attempt to weaken the regulatory safeguards around qualified trust service providers, authentication standards, or certification mechanisms could undermine both security and user confidence. The Omnibus should therefore focus on facilitating consistent implementation and supporting Member States' technical alignment, rather than reopening the substantive obligations that guarantee reliability and cross-border acceptance.

**5. Preserving the AI Act protection for individuals**

The AI Act forms the backbone of Europe's emerging AI economy by setting a framework for trustworthy AI. We are deeply concerned that the Commission intends to amend the AI Act before it is fully in force and without fact-based assessment, thus contradicting its commitment under Better Regulation.

The S&D firmly opposes any delay or "stop the clock" which would only generate legal uncertainty and expose citizens to the very risks and harms the Act proportionally addresses. Rather than reopening the Act, the priority must be swift finalisation of harmonised standards and guidance from the AI Office to clarify interplay with other legislation.

The S&D will firmly oppose any attempt to reduce the level of protection owed to our citizens. Removing Article 27 from the proposal would be a red line for our Group and would go far beyond a so-called 'simplification exercise'. Similarly, we oppose any attempt to modify the scope of the AI Act such as by modifying the Annex III or the definitions. Furthermore, AI literacy must be enhanced by AI providers and deployers in order to promote an efficient and safe use of AI systems. We are also extremely worried about the risk of weakening of transparency and accountability provisions by reducing registration obligations. From a data protection and privacy perspective, we are concerned about extending the possibility to process special categories of personal data to correct bias. At a time where important problems emerge due to AI systems, it would appear irresponsible to lower the level of protection provided by the AI Act.

In conclusion, we strongly urge the Commission to ensure that the Digital Omnibus reinforces, rather than relaxes, the integrity of the EU's digital legal order. Simplification and coherence should serve the Union's long-term strategic vision for a competitive, secure, and rights-based digital economy rather than short-term deregulatory goals. It should not take away the focus and resources of the much-needed enforcement efforts of landmark rules like the Digital Services, Markets and AI Acts. We encourage you to focus the Digital Omnibus on improving coherence, transparency, and regulatory guidance without undermining the level of protection achieved so far.

We are looking forward to engaging in a constructive dialogue to achieve these objectives in a manner that protects both innovation and individuals' rights.

Yours sincerely,

Alex Agius Saliba MEP
*Vice-President for Digital Agenda*

Birgit Sippel MEP
*LIBE Coordinator*

Brando Benifei MEP
*AI Act Rapporteur*

Laura Ballarin MEP
*IMCO Coordinator*

Christel Schaldemose MEP
*DSA Rapporteur*

Romana Jerkovic MEP
*Rapporteur eIDAS*