Courtesy translation -

Proposal for a European resolution on behalf of the Committee on European Affairs of the French Senate, on the European Digital Omnibus

EXPLANATORY MEMORANDUM

Ladies and Gentlemen,

On November 11, 2025, the European Commission presented a **digital simplification omnibus package**. This initiative is part of the simplification effort launched by the European Commission in early 2025 to support competitiveness. The so-called "digital omnibus package " is the 7th simplification omnibus since 2025.

It follows in the wake of the Draghi report published on September 9, 2024, titled "The Future of European Competitiveness," which advocates for **simplification and harmonization of European rules on data, cybersecurity, and artificial intelligence (AI)**, **to benefit European innovation in the digital sector**, by reducing the burden on companies in the sector.

Comprising two parts—one focusing on AI, the other covering the broader fields of digital technology, data, and cybersecurity— the Digital Omnibus is **a highly comprehensive package that covers a large portion of the European digital legal framework**. Presented by the European Commission as a package of "targeted" simplification measures and technical amendments, it nevertheless raises several substantive issues, notably the reduction in the level of protection for digital rights guaranteed by the GDPR, which has become an international standard.

First, the proposed regulation on the AI framework, known as the "**Digital Omnibus Package on AI**[1]," aims to amend the 2024 AI Regulation[2], which has not yet fully entered into force, as its implementation was scheduled to be phased in through 2027. The main measure aims to postpone the obligations imposed on AI systems classified as "high-risk." Various other amendments to the AI Regulation are proposed, some of which go beyond the scope of simplification.

In an effort to postpone the obligations applicable to certain AI systems that were set to take effect on August 2, 2026, **the timeline adopted for this aspect was characterized by the speed of the negotiations**. A third trilogue concluded on May 7, 2026, less than four months after the publication of the proposed regulation in its French translation.

On this point, the Committee on European Affairs considers that the evolution of the rules must not be rushed, without an impact assessment, **at the risk of being dictated by the digital industry, undermining their clarity for businesses, and contributing to a democratic deficit**.

---

[1] *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonized rules on artificial intelligence.*

[2] *Regulation (EU) 2024/1689 establishing harmonized rules on artificial intelligence.*

Furthermore, the omnibus package includes a second proposed regulation known as the "**Digital Omnibus Regulation**[3]" which more broadly addresses the digital sector, cybersecurity, and data regulation, including personal data. This component **concerningly revises the General Data Protection Regulation (GDPR)**, which has nonetheless become a global gold standard for data protection.

In particular, the proposal amends the definition of "personal data," with potentially dangerous consequences for the protection of digital rights and freedoms.

As the Committee on European Affairs has already highlighted in a recent report[4], the application of the European Union's digital regulatory framework is now being challenged; it remains, however, crucial to ensure the maintenance of a regulatory framework conducive to the economic development of this sector, yet one that is both **ethical and consistent with European values**. This is also true for the protection of sensitive data, for which AI cannot be granted special privileges without sufficient safeguards.

Consequently, this proposed European resolution **calls for the pursuit of a balance** — fragile, yet necessary — **between innovation and the protection of rights, and between simplification and regulation of the digital sector.**

While the very large online platforms and the main AI systems dominating the European market are American and Chinese, this is not the time for **the European Union to waver or compromise in applying the innovative and ambitious legal framework it has begun to build to regulate AI and the digital sector**. On the contrary, it should aim to make the AI Regulation an international standard in this field, much like the GDPR did eight years ago in the area of personal data protection.

Finally, the Committee on European Affairs considers that a genuine industrial policy for the digital sector must be implemented, including, in particular, rules on European preference in public procurement; otherwise, the proliferation of European regulations is doomed to failure.

---

[3] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, and (EU) 2023/2854, as well as Directives 2002/58/EC, (EU) 2022/2555, and (EU) 2022/2557, with regard to the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150 and (EU) 2022/868, as well as Directive (EU) 2019/1024.

[4] Report No. 444 (2024–2025), by Catherine MORIN-DESAILLY and Florence BLATRIX CONTAT, submitted on March 13, 2025, calling for the strict application of the European Union's digital regulatory framework and urging the strengthening of the conditions for genuine European digital sovereignty.

Proposal for a European resolution on behalf of the Committee on European Affairs, pursuant to Rule 73 *quinquies* B of the Rules of Procedure, on the European Digital Omnibus

(1) The Senate,

(2) Having regard to Article 88-4 of the Constitution,

(3) Having regard to the Treaty on the Functioning of the European Union, in particular Article 114 thereof,

(4) Having regard to the Charter of Fundamental Rights of the European Union,

(5) Having regard to the Convention for the Protection of Human Rights and Fundamental Freedoms,

(6) Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), known as the "GDPR",

(7) Having regard to the White Paper of February 19, 2020, entitled "Artificial Intelligence: A European Approach for Excellence and Trust," COM(2020) 65,

(8) Having regard to the report by Mario Draghi of September 9, 2024, on the future of European competitiveness,

(9) Having regard to the European Commission's strategy for the Data Union of November 19, 2025, COM(2025)835 final,

(10) Having regard to the Action Plan for the AI Continent, presented by the European Commission on April 9, 2025, COM(2025)165,

(11) Having regard to the proposal for a regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, and (EU) 2023/2854, as well as Directives 2002/58/EC, (EU) 2022/2555, and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150 and (EU) 2022/868 as well as Directive (EU) 2019/1024,

(12) Having regard to the proposal for a regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonized rules on artificial intelligence,

(13) Having regard to the proposal for a regulation of the European Parliament and of the Council on the establishment of European digital identity portfolios for businesses, COM(2025) 838 final,

(14) Having regard to the joint opinion (No. 2/2026) of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) on the proposal for a Digital Omnibus Regulation, of February 10, 2026,

(15) Having regard to the report by Arthur Mensch, Mistral AI, “European AI: A playbook to own it,” of April 2026,

(16) Having regard to the report “Toward a deployment of artificial intelligence in line with European values,” No. 483 (2022–2023) by Mr. André GATTOLIN, Ms. Catherine MORIN-DESAILLY, Mr. Cyril PELLEVAT, and Ms. Elsa SCHALK on behalf of the Committee on European Affairs, as well as European Resolution No. 100 (2022–2023),

(17) Having regard to Report No. 444 (2024-2025) by Ms. Catherine MORIN-DESAILLY and Ms. Florence BLATRIX CONTAT, submitted on March 13, 2025, as well as Resolution No. 106 (2024-2025) aimed at the strict application of the European Union’s digital regulatory framework and calling for the strengthening of the conditions for genuine European digital sovereignty, which became a Senate resolution on April 18, 2025,

(18) Having regard to Senate Information Report No. 279 (2018–2019) by Messrs. André GATTOLIN, Claude KERN, Cyril PELLEVAT, and Pierre OUZOULIAS, prepared on behalf of the Committee on European Affairs, entitled “Artificial Intelligence: The Urgency of a European Ambition,” submitted on January 31, 2019,

(19) Having regard to Senate Information Report No. 627 (2021–2022) by Messrs. Marc-Philippe DAUBRESSE, Arnaud de BELENET, and Jérôme DURAIN, on behalf of the Committee on Laws, entitled “Biometric Recognition in Public Spaces: 30 Proposals to Avert the Risk of a Surveillance Society,” submitted on May 10, 2022,

(20) Having regard to the report “Europe, a colony of the digital world?” No. 443 (2011–2012) by Ms. Catherine MORIN-DESAILLY on behalf of the Committee on European Affairs,

(21) Having regard to the information report “A new role and strategy for the European Union in global Internet governance” No. 696 (2013–2014) by Ms. Catherine MORIN-DESAILLY, on behalf of the Senate’s Joint Fact-Finding Mission on Internet Governance, as well as European Resolution No. 122 (2014–2015),

(22) Having regard to the conclusions of Senate Report No. 7 (2019–2020) of October 1, 2019, entitled “The Duty of Digital Sovereignty: Neither Resignation Nor Naivety,” prepared on behalf of the Commission of Inquiry on Digital Sovereignty,

(23) Having regard to Bill No. 220 (2025–2026) on the establishment of a presumption of use of cultural content by artificial intelligence providers, adopted by the Senate on April 8, 2026,

(24) Considering the central role of digital technologies in our societies from socio-economic, societal, and environmental perspectives;

(25) Considering the growing role of artificial intelligence (AI) technologies and the opportunities as well as the risks that these technologies pose for our societies and economies, particularly for the competitiveness of European businesses, but also for the efficiency of public services, security, and the well-being of our societies;

(26) Whereas this process of AI deployment must under no circumstances undermine the protection of fundamental rights, including the high level of personal data protection currently

enjoyed by Europeans, and whereas these technologies must serve people and be subject to the values, principles, and fundamental rights of the European Union;

(27) Whereas artificial intelligence technologies pose risks to respect for human dignity, privacy, and the protection of personal data, data security, and non-discrimination on the basis of gender, ethnic origin, age, religion, and economic status;

(28) Whereas, for Europe to fully capitalize on the economic and societal potential of AI, it is necessary to ensure greater legal certainty, which requires the development of rules that are clear, precise, understandable to all, and sufficiently stable over time;

(29) Whereas there is a high risk of regulatory capture facing national and European public institutions in the digital sector, and particularly in AI, given the complexity and pace of technical developments and the information asymmetries between these public actors and private actors, notably large non-European platforms;

(30) Considering the hybrid and systemic risks that AI tends to create for Member States in a shifting geopolitical context;

(31) <u>On the principle of a digital omnibus:</u>

(32) Calls on the European Union not to waver or compromise in the application of the innovative and ambitious legal framework it has begun to build to regulate AI and the digital sector;

(33) Welcomes the European Commission's commitment to simplifying the applicable framework and reducing the administrative burden and compliance costs, particularly for small and medium-sized enterprises (SMEs) and small mid-cap enterprises (SMEs), with a view to improving their competitiveness;

(34) Welcomes the technical measures aimed at improving the coordination of the various European standards in the digital sector, for the sake of clarity and legal certainty;

(35) Regrets that the proposal goes beyond the sole objective of simplification in some respects, tending to complicate an already complex and dense regulatory framework, at the risk of undermining its clarity and acceptance by businesses and citizens,

(36) Regrets the absence of an impact assessment, which hinders a proper understanding of the proposals put forward by the European Commission and their incorporation into European Union law;

(37) Emphasizes that regulatory developments in the digital sector must not be pursued with excessive haste, at the risk of being dictated by the digital industry;

(38) Regrets the very tight schedule for negotiations on the AI component, which did not allow for the full involvement of all stakeholders and Member States;

(39) Regrets the lack of clarification regarding the legal framework for copyright in the context of AI, even as courts begin to rule on specific cases and legal solutions have been identified to ensure remuneration for cultural content used by AI systems, in particular the proposed law

establishing a presumption of use of cultural content by artificial intelligence providers, adopted by the Senate on April 8, 2026;

(40) Regrets that the digital omnibus package on AI did not provide an opportunity to ensure greater consideration of the environmental footprint of AI, particularly given the significant use of water and raw materials it entails;

(41) Calls on the European Commission to consider supplementing existing reporting obligations regarding energy consumption with obligations regarding targets for reducing such consumption, as well as to consider future environmental reporting obligations covering the entire lifecycle of AI systems applicable to major AI providers;

(42) On the postponement of obligations imposed on certain AI systems:

(43) Takes note of the postponement of obligations imposed on certain high-risk AI systems decided during the trilogue on May 7, 2026, considering that a postponement to a fixed date promotes greater legal certainty and enhanced predictability for companies in the sector;

(44) Regret that this postponement has been extended to the transparency obligations set out in Article 50 of the AI Regulation, delaying the labeling of AI-generated content by six months, to the detriment of the benefits expected from this measure both in terms of copyright protection and transparency for AI users;

(45) Considers, however, that this postponement is indicative both of the difficulty in regulating a rapidly evolving technical sector and of the limitations of the European decision-making process in balancing agility with the stability of standards;

(46) On efforts to simplify the regulatory framework for AI:

(47) Welcomes efforts to simplify administrative obligations for small and medium-sized enterprises (SMEs) and small and mid-cap enterprises (SMEs) in the AI sector;

(48) Regrets the insufficient simplification of the coordination between cybersecurity requirements for AI service providers, as set forth in the AI Regulation, and those arising from the existing framework, notably the Cyber Resilience Regulation;

(49) On expanding the prohibited uses of AI:

(50) Supports the proposal to ban AI systems capable of generating, manipulating, or reproducing content depicting a person's private parts or sexually explicit activities without their consent ("nudification");

(51) Regrets that the ban on AI systems capable of generating, manipulating, or reproducing child pornography content (images, video, audio) was not adopted;

(52) Calls, in general, for a ban on any AI practice likely to exploit potential economic, personal, or social vulnerabilities of a given person or group of people, in a manner that causes or is likely to cause harm to that person, that group, or a third party, and in particular any AI practices likely to undermine human dignity;

(53) Considers that education and continuing training in digital technology and AI must be strengthened to improve European citizens' literacy in these areas, including knowledge of their rights and freedoms and of the avenues of redress in the event of abuse;

(54) On regulatory sandboxes for AI:

(55) Takes note of the establishment of regulatory sandboxes, including cross-border ones, to encourage European innovation and facilitate the scaling up of European AI startups;

(56) Calls for vigilance regarding real-world testing of high-risk AI systems in certain critical sectors (healthcare, critical industries, etc.);

(57) Considers it particularly desirable that national data protection authorities be systematically involved in the operation of such sandboxes, particularly in these critical sectors, including with regard to the cross-border sandbox;

(58) On governance and enforcement of the AI regulatory framework:

(59) Recalls that a balanced distribution of powers between the European Commission and national supervisory authorities is an essential prerequisite for effective regulation of the digital sector and AI;

(60) Calls on the European Commission to strengthen its AI Office solely for the purpose of enhancing expertise and the ability to anticipate developments in the sector, by enabling the recruitment of technical and legal experts, without undermining national capabilities;

(61) Considers, therefore, that the AI Office must not supplant the prerogatives of Member States and their national supervisory agencies within their respective areas of competence and that, in general, any experimentation in the field of AI must be placed under the supervision of agencies independent of the European Commission;

(62) Considers that strengthening the exclusive powers of the AI Office for certain AI systems, particularly those based on a general-purpose AI model, is contrary to the principles of subsidiarity and proportionality, as it deprives national market surveillance authorities of the ability to intervene, including in cases where the AI Office has chosen not to intervene;

(63) Considers, therefore, that for the AI systems in question, a "de-escalation" approach—under which national authorities would be required to step aside whenever the AI Office wishes to conduct oversight in the relevant sectors—would have been preferable and, moreover, conducive to better coordination among national agencies, while strengthening the AI Office's governance for cross-border oversight;

(64) On the amendment of Annex I to the AI Regulation:

(65) Regrets the transfer of the Machinery Regulation from Section A to Section B of Annex I to the AI Regulation, which has the effect of excluding it from the scope of the AI Regulation, noting that, in the absence of an impact assessment, it is not possible to meaningfully assess whether this regulation provides a level of safeguards equivalent to that of the AI Regulation for the relevant products incorporating AI;

(66) Emphasizes the importance, particularly in the critical sectors covered by Annex I of the AI Regulation, of promoting a "safety by design" approach that is consistent with the spirit of the AI Regulation, which is based on a risk-based approach;

(67) On the simplification and clarification measures concerning the various European data-related texts:

(68) Welcomes the European Commission's efforts to harmonize and improve coordination among the texts and to eliminate redundancies;

(69) Supports expanding the possibility to object to the disclosure of data constituting a trade secret, where there is a high risk of unlawful acquisition, use, or disclosure to third countries or entities under their control;

(70) On the creation of a single point of entry for reporting cybersecurity incidents:

(71) Strongly opposes the proposal to create a single point of entry for reporting cybersecurity incidents, given the risk of turning it into a single point of failure;

(72) Doubts ENISA's technical capacity to secure this single point of entry sufficiently to ensure its resilience;

(73) Considers the creation of a single point of entry to be contrary to the principles of subsidiarity and proportionality, given the underlying national security implications of cyber incidents and the strategic importance for Member States of retaining the filtering rights they currently have to decide whether or not to share information on cybersecurity breaches of national critical infrastructure at the European level;

(74) On the transfer of cookie rules from the e-Privacy Directive to the GDPR:

(75) Considers that transferring cookie rules from the e-Privacy Directive to the GDPR would create a dangerous dual regime for the regulation of such cookies, without addressing the challenge of reducing consent fatigue regarding trackers;

(76) On amendments to the General Data Protection Regulation (GDPR):

(77) Recalls that the purpose of the GDPR is not data protection per se, but the protection of the rights and freedoms of the individuals to whom the data pertains;

(78) Considers that the proposed revisions to the GDPR are too substantial and potentially dangerous, given that the text has become a global benchmark for the protection of personal data;

(79) Welcomes, nevertheless, the proposals to harmonize the frameworks and documents relating to data protection impact assessments (DPIAs);

(80) Supports the proposal to extend the deadline for reporting personal data breaches from 72 hours to 96 hours, giving data protection officers more time to manage the emergency before fulfilling their reporting obligations within a reasonable timeframe;

(81) Considers that amending the definition of personal data, by going beyond the parameters defined by recent CJEU case law on pseudonymization, opens the door to potentially serious abuses and would undermine the fundamental right to the protection of personal data of French and European citizens, without providing the legal clarity expected by businesses and data controllers;

(82) Consequently considers that it is not appropriate to amend the definition of "personal data" contained in the GDPR;

(83) Opposes the amendment of the definition of "scientific research" in the GDPR to expand it to include any research supporting innovation, including for purely commercial purposes;

(84) Considers that additional safeguards are necessary to ensure the genuinely "scientific" nature of the processing of personal data for scientific research purposes, by adding to the definition the concepts of verifiability, transparency, and the objectives of scientific research;

(85) Considers that AI should not be granted special privileges regarding the processing of personal data without sufficient safeguards being ensured;

(86) Calls for efforts to preserve the delicate balance between innovation and the protection of fundamental rights arising from the protection of personal data;

(87) Regarding the European Commission's ability to adopt implementing acts:

(88) Considers the provisions allowing the European Commission to adopt implementing acts in several areas (regarding the criteria for defining pseudonymized data, harmonized lists and documents relating to cross-border data transfers, etc.) to be disproportionate, and believes that the relevant European sectoral institutions are better placed to issue the necessary guidelines, where appropriate;

(89) Calls, therefore, for the deletion of this provision;

(90) Calls on the Government to assert this position in the negotiations within the Council.