POSITIONING PAPER

PROPOSALS FOR IMPROVING THE DIGITAL OMNIBUS, REBALANCING DATA PROTECTION AND E-PRIVACY DISCIPLINES WITH INNOVATION

By Luca Bolognini and Francesco Capparelli [1]

February 2026 – DOI: 10.5281/zenodo.18598414

Abstract

In this brief positioning paper, we intend to share some critical ideas and a list of constructive proposals so that the GDPR and the e-privacy directive can improve their balance and proportionality, coherence with other European regulations, with a view to greater competitiveness and a regulatory framework enable sustainable innovation. The ideas presented here are the result of original work by the authors and a selection of key points that emerged during a public discussion organised by the Italian Institute for Privacy and Data Valorisation on 10 September 2025 in Rome.

The authors of this positioning paper propose a pragmatic re-balancing and re-calibration of EU data protection and e-privacy rules to better align rights protection with competitiveness and sustainable innovation, introducing a set of proposals to be considered by the EU legislator, in addition to the already bold amendments envisaged

[1] Luca Bolognini is the President of the Italian Institute for Privacy and Data Valorisation – L.Bolognini@istitutoprivacy.eu
Francesco Capparelli is Board Member of the Italian Institute for Privacy and Data Valorisation – F.Capparelli@istitutoprivacy.eu

in the Digital Omnibus. The authors advance a priority approach - which would entail essential general "horizontal" fixes and improvements on principles - focused on amending key GDPR Recitals (4, 6, 10, 26) to (i) reaffirm proportionality and the need to balance data protection with other Charter rights and innovation, (ii) require DPAs to assess cross-rights impacts, and (iii) replace "high level" with "adequate level" of protection to enable reasoned calibration. In addition, this "horizontal" priority approach would include targeted updates to Article 5 principles, like the following ones: taking a pragmatic and practical approach to transparency (toward explainability for AI), recognising secondary use authorised by the EU Data Strategy, ensuring a more functional and proportionate notion of minimisation (i.e. properly balancing privacy with bias prevention), embracing a fair and equal approach to accuracy (i.e. in case of evaluative AI outputs), extending storage for lawful secondary purposes, and embedding proportional accountability.

A secondary "vertical" approach is proposed, with a list of surgical measures which would refine lawfulness conditions, in particular focusing on: Art. 6(1)(b) on contractual necessity of personal data processing; Art. 6(1)(f) on legitimate interest, to explicitly include the "exercise of other rights and freedoms"; Art. 7(4) on consent requirements, aligned with C-252/21 on paid alternatives; Art. 9(2) on prohibition exemptions for special categories of data processing, where intrinsic to a contractual obligation, and in case of legitimate or public interests subject to appropriate technical safeguards; clarifications for XR biometrics; alignment of Art. 9(4) with EU law on health-data secondary use (e.g. EHDS); and institutional safeguards and duties for Data Protection Authorities, with mandatory impact assessments in Art. 58(4) and revising Art. 70(4) for EDPB consultations. The authors of this paper also propose to modernise e-Privacy discipline, moving the online tracking to GDPR legal bases, and to better harmonise security measures (Art. 32 GDPR with references to ENISA and international standards, consistent with NIS2/CRA/DORA).

Table of contents

I. Priority approach: a proposal for amendments to some GDPR Recitals, for better Proportionality, and to the General Principles

Innovation is essential for safeguarding and advancing fundamental rights, including privacy. It empowers us to address emerging challenges and to expand how these rights are manifested in practice. For innovation and progress to be truly sustainable, fundamental rights must be carefully considered and balanced, ensuring that novel solutions benefit all individuals by respecting and advancing their diverse rights and interests. The European legislator has defined the right to personal data protection, on the one hand, and the right to privacy and confidentiality of communications, on the other, as fundamental rights enshrined in the Charter of Nice and the Treaty on the Functioning of the European Union, but not as 'tyrannical' rights. On the other hand, it is precisely the EU Charter of Fundamental Rights that establishes the principle of proportionality in its Article 52 and prohibits the absolutist exploitation of one right to the detriment of other fundamental rights in its Article 54. The well-known Recital 4 of the GDPR states that *'The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity*."

Nevertheless, since its entry into force, we have witnessed a phenomenon of 'dominance' of the GDPR over other regulations and legislation; the majority of ordinary legislation (EU directives / regulations but also Member States law) contains in its Recitals and first Articles safeguard clauses and references to the "primacy" of personal data protection legislation, in particular the GDPR.

This phenomenon has transformed the GDPR itself into a source with the substantial characteristics of a higher-level law, sometimes 'tyrannical' in its interpretation and application, i.e. a sort of *pseudo-constitutional secondary horizontal legislation*, concretely superordinate to other laws and secondary regulations. One could provocatively paraphrase the ancient Latin saying, *summum ius, summa iniuria,* transforming it into *summum GDPR, summa iniuria.*

For these reasons and in order to strike a better balance and proportionality, it is recommended to amend and elevate certain points already contained in the first Recitals of the GDPR, specifically:

a) **It is suggested supplementing Recital 4, adding the explicit mention of the necessary balance between data protection and innovation** as manifestation of other rights and freedoms, and including a reference to the prohibition of the exploitation of the right to personal data protection to the detriment of other fundamental rights and freedoms, referring to **Articles 52 and 54 of the Charter of Nice**; moreover, it should be specified that the application of the GDPR should leave the contractual autonomy of data controllers and data subjects unaffected, in compliance with Union or Member State law: in this sense, since there is no hierarchy between legal bases, according to the GDPR, if a contract was agreed which includes the processing of personal data, such a contract as legal basis cannot and should not be deemed inadequate. We also recommend strengthening the requirement to ensure proportionality and balance between data protection and innovation as manifestation of other rights and freedoms,

by elevating it to the Articles of the GDPR (preferably in Art.5 as guiding principle);

b) **In the same Recital 4, reference could be made to the duty for Data Protection Authorities to conduct impact assessments in order to assess the proportionality, balance, and effects of the application of personal data protection on other rights, substantial public interests, and sustainable innovation**. This principle should also be explicitly added to Article 51 GDPR, specifying the need for Data Protection Authorities to ensure balance and proportionality as per Recital 4, and Articles 52 and 54 of the Charter;

c) In both Recital 6 and Recital 10, where the European legislator has introduced references to the obligation to ensure a consistent and high level of protection of natural persons and a high level of protection of personal data, it should be better specified that this obligation should always be considered to be balanced, with proportionality and reasonableness, with other rights, freedoms and interests. This proportionality-factor should lead to the need to weigh the risk of varying likelihood and severity for the rights and freedoms of natural persons, on a case-by-case basis. Therefore, **the terms 'high level' should be replaced by 'adequate level'**, to allow interpreters and authorities a more proportionate and balanced reading of the right to personal data protection.

The authors of this positioning paper believe that, by amending the above-mentioned GDPR Articles and Recitals, a more balanced, proportionate, and sustainable interpretation and implementation of the GDPR would be achievable. By making complementary surgical changes to several Articles of the Regulation—which are specifically illustrated below—it would be possible to achieve an even greater balance, fair and coherent interpretation, and application of the European personal data protection legislation, in step with the times and friendly to sustainable innovation. This is why we propose that the European legislator consider, in addition to the already

widely positive proposals contained in the Digital Omnibus, the amendments envisaged in this positioning paper.

Coming now to the general principles of personal data protection, enshrined in Article 5 of the GDPR, they struggle to fit increasingly frequent and 'normal' scenarios, particularly when Artificial Intelligence is involved. For instance, data minimisation, purpose limitation, data retention limitation, and transparency principles are challenging to apply. These challenges appear concretely, in cases involving the training of AI models and systems - due to their intrinsic complexity, need for big amount of data for long-lasting, variable, and adaptable objectives - for augmented reality (AR) / mixed reality (MR) scenarios, where human characteristics data necessarily combine with machine non personal data. Ass already the recommended amendment of Recitals (4, 6, 10) and articles could help overcome the described challenges by allowing for an interpretation and application of the GDPR general principles in a more proportionate and more modern way, in order to better balance them with innovation and other rights, freedoms, and public interests.

However, Article 5 could be specifically amended as follows:

a) **The principle of transparency**, as referred to in Article 5(1)(a) and further elaborated in Articles 12-13-14-15 of the GDPR, should be considered with regard for Article 52 of the Charter, Recital 4 GDPR, the risk-based approach, and ultimately parallel internal market objectives of the GDPR, which require a more balanced, proportionate and balanced approach to transparency. **In this light, it would be appropriate to better define and clarify "transparency", from an innovative and more effective perspective**, taking into account the peculiarities of data processing in the digital environment and in the context of Artificial Intelligence systems, both for the input and output phases. In particular, due consideration should be given to the objective impossibility or impracticability (due to the black box effect in certain scenarios) of providing

exhaustively all the information specified in Articles 13, 14 and 15 of the GDPR, placing greater emphasis instead on ensuring explainability. For his purpose, **relevant Articles could also be amended with provisions inspired by the digital transparency modalities contained in Article 26 of the Digital Services Act (DSA), to be intended as a possible best practice** (of course, being understood that it would not make sense to conflate the DSA and GDPR competence plans, since both pursue different objectives), reducing the amount of information to be provided *ex ante* and giving much more weight to meaningful transparency in form of downstream explanations (e.g. enabling users to understand why and how personalised content is provided).

b) **The principle of purpose limitation, referred to in Article 5(1)(b), should be rebalanced, taking into account the numerous cases of secondary use of data**, including personal data, permitted by the new regulations deriving from the European Data Strategy (Data Governance Act, Common Data Spaces, Data Act) and the forthcoming Data Union Strategy within the AI Continent Action Plan, as well as national legislation that has introduced options for secondary data processing, as was the case with the Italian law on Artificial Intelligence (see Article 8). In this regard, it would be appropriate to expressly provide for – in addition to compatibility with storage in the public interest, statistical activities and scientific or historical research – **the compatibility of processing for the purposes of**

   a. **Both public and private research, more widely subject to appropriate safeguards;**
   b. **Pseudonymisation, anonymisation and anonymised creation of synthetic data and the further use of such data; or**
   c. **where there are legal bases for the secondary use of personal data, as provided for by Union or Member State law.**

c) As regards the principle of **data minimisation**, considering that in many cases minimisation could have a negative impact on the prevention of bias in the development of Artificial Intelligence systems, it would be appropriate to supplement Article 5(1)(c) of the GDPR with a provision that **this principle must be applied in a proportionate way which ensures balance with other rights, freedoms and interests**, such as in particular with regard to objectives of preventing bias in the input data for training AI models and systems.

d) With regard to the principle of **data accuracy, it should be limited to data of an objective and non-evaluative nature**, **and it should not be extended to inferred data where Article 22 GDPR will not be applicable**. This specification would make it possible to avoid always considering the output results, which are the result of processing by AI systems and are only of a trend, statistical or probabilistic nature, to be in violation of the general principles.

e) With regard to the principle of **storage limitation, it would also make sense to extend the cases of legitimate further storage linked to secondary purposes permitted by the new regulations** deriving from the European Data Strategy (Data Governance Act, Common Data Spaces, Data Act) and the forthcoming Data Union Strategy within the AI Continent Action Plan, and national legislation that has introduced options for secondary data processing, as well as processing for the purposes of pseudonymisation, anonymisation and anonymised data synthesis and the further use of such non-personal data;

f) The principle of **accountability**, referred to in Article 5(2) of the GDPR, should be supplemented with a condition of reasonableness and proportionality, for example by including a clause that provides for the demonstration of compliance *'by reasonable means and taking into account the balance with other rights and freedoms*'.

II - Proposal for amendments to Lawfulness Conditions

The legal bases set out in Article 6 of the GDPR could be better specified. In particular, the following amendments are proposed:

a) The GDPR does not establish any hierarchy between the different legal bases laid down in Article 6(1) (as reiterated by EDPB in the Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, also mentioning the Opinion of Advocate General Szpunar in Case C-394/23, Mousse - ECLI:EU:C:2024:610). In this light, **in point (b) of Art. 6(1), it is suggested to explicitly specify that the necessity of processing for the performance of a contract to which the data subject is party should be assessed in relation to the subject matter of the contractual relationship, just considering the validity and effectiveness of the contract** under Union or Member State law. This specification would imply, as a logical interpretative consequence, that **if a contract is deemed valid under applicable Member State and Union law, it should also ensure the validity of contractual necessity as a lawful basis**, for the processing of personal data for the performance of the contract: data protection and privacy rights should not automatically override contractual rights and obligations which are a manifestation of other rights, freedoms and interests. This clarification would avoid interpretations by Data Protection Authorities that question the objective and extra-contractual necessity of a specific contractual activity, influencing assessments of the appropriateness of any innovation and the free initiative and self-determination of the parties involved in the negotiations. Furthermore, the contractual necessity should be recognised in any contractual obligation, whether it relates to the data subject or the data controller. However, the mere amendment to Recitals 4 (already

mentioned in this paper, Par. I) and 44 – specifying that the GDPR should leave the contractual autonomy of data controllers and data subjects unaffected, in compliance with Union or Member State law – could bring the interpreter to the same interpretation.

b) The principle of lawfulness, which requires legal grounds for any processing of personal data, should contemplate the existence of conditions of lawfulness deriving from respect for other rights, freedoms and interests; in this sense, **in Article 6(1)(f), it is suggested that 'the exercise of other rights and freedoms and related interests' be added to the category of 'legitimate interests' in order to clarify unequivocally that this legal basis is also appropriate for carrying out the multidimensional balancing tests referred to in Recital 4 of the GDPR**. However, even the mere amendment to Recital 4, as indicated above in this paper (Par. I), could promote such interpretation.

III - Proposal for amendments on Special Categories of Personal Data

In order to overcome limitations on the processing of special categories of data, which have proven to be unnecessarily obstructive to the activities of operators who provide goods or services that inevitably carry sensitive information, the following amendments are suggested:

a) Adding **a specific derogation to the prohibition of processing of special categories of personal data to Article 9(2) of the GDPR for cases where *the processing is strictly necessary, considering the nature of the specific goods or services, for the performance of a contract*** *to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*

b) Further broadening the spectrum, **technology neutral exemptions on legitimate interest and public interest should be included in Article 9(2) GDPR**, subject to appropriate safeguards - also leveraging on **state-of-the-art Privacy Enhancing Technologies (PET) and pseudonymisation / synthetic data generation techniques**;

c) In addition, in Recital 51 of the GDPR, it is suggested to specify that **biometric data consisting of human characteristics strictly necessary for the technical functioning of augmented, virtual, or mixed reality** environments activated by data subjects, users or subscribers **should not be considered as belonging to special categories of data**;

d) Lastly, in paragraph 4 of Article 9, it should be specified that such conditions and limitations must in any case comply with Member States and Union law on the **secondary use and common space of health data**.

IV - Proposal for amendments to the Powers of the EDPB and National Data Protection authorities

In order to avoid negative and unbalanced impacts on other rights, freedoms, and interests of the decisions of the European Data Protection Board and single national authorities, some substantial amendments to Chapters VI and VII of the GDPR are suggested. That said, even the above proposed amendments to Recitals 4, 6, and 10 and Articles of the GDPR could lead to the same interpretation, without the need for specific and surgical amendments, which however we are going to illustrate below.

a) First of all, it could be opportune:
   - to envisage **a provision of principle, of a binding nature, which requires the individual Data Protection Authorities to call for participatory procedures of prior consultation** for their decisions and guidelines, and
   - to identify common principles to guarantee the consistency of the national models of prior consultation.
   - In order to ensure a balance between rights and technological innovation, in all draft general decisions and guidelines, as well as in decisions of a punitive nature, **the supervisory authority should be required to carry out a prior analytical assessment of the impact that such decisions would have on innovation and competitiveness**, including knowledge enhancement and technology transfer, as well as on other public interests or fundamental rights and freedoms. This impact assessment should be notified to the addressee with the provisional decision preceding the conclusion of the proceedings, allowing for a reasonable period of time for a response to ensure the right to be heard. The arguments put forward by the addressee of the decision in their response should be considered in the reasons for the final decision. The

impact assessment should also always be published on the authority's website, omitting any information in accordance with the confidentiality of third parties or business secrecy or other confidentiality obligations under applicable law. For sanctioning proceedings, such publication shall only be made where the publication of the decision as an ancillary sanction is also provided for.

These provisions could be functionally integrated into the aforementioned paragraph 4 of Article 58 GDPR, where it is already provided that '*The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards*'.

b) In addition, and in one, there is a **proposal for action concerning the regulatory powers of the EDPB**. The proposal has two alternatives. On the one hand, for each of the EDPB's regulatory powers, **a detailed and differentiated regulation of consultation procedures could be laid down in prescriptive terms** (the detailed regulation could then be left to the EDPB's internal regulations). On the other hand, and **as an alternative, greater functional autonomy could be conferred on the EDPB, requiring the Board to activate prior consultation of the stakeholders**: the provision could be transposed in Article 70(4), replacing the current wording with the following: *'The Board shall consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.'*

V - Proposal for amendments to the Digital Omnibus / e-Privacy discipline, aligning online tracking legal bases with GDPR

The following amendments to 'Digital Omnibus' (Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and 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, (EU) 2022/868, and Directive (EU) 2019/102) and Directive 2002/58/EC (e-Privacy Directive) are proposed in order to bring the regulations into line with the latest digital market practices and the reasonable expectations of users and subscribers:

a) **Amendment to Article 88a(1) GDPR as proposed in Article 5 of the Digital Omnibus, as follows: *'1. The storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is based on lawfulness conditions referred to in Article 6(1)***.'

b) Deletion of Article 88a(3) GDPR as proposed in Article 5 of the Digital Omnibus.

VI - Proposal for amendment to Article 32 GDPR

The current formulation of **Article 32 GDPR**, which requires controllers and processors to implement technical and organisational measures appropriate to the risk, considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, should be integrated to reflect the regulatory evolution of information security within the European Union and at international level.

In particular, **it would be appropriate to supplement the reference to the state-of-the-art with an explicit mention of the internationally recognised standards in the fields of information security, secure software development and business continuity**, with particular attention to those developed and/or published by the European Union Agency for Cybersecurity (ENISA), as well as by other competent international standardisation bodies. Such standards, while not replacing the risk-based approach of the GDPR, would operate as authoritative and dynamic benchmarks for the identification and implementation of technical and organisational measures aimed at ensuring a level of security appropriate to the risk to the rights and freedoms of natural persons.

The amendment could therefore read as follows: "***Taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, and by expressly referring to internationally recognised standards in the fields of information security, secure software development and business continuity, in particular those developed and/or published by ENISA, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.***"

Such a clarification would ensure greater consistency between the GDPR and the parallel regulatory corpus emerging from the NIS2 Directive, the Cyber Resilience Act, and the DORA Regulation, thereby promoting a uniform and evidence-based

interpretation of the concept of “appropriate measures”. This would also enhance the accountability of controllers and processors by providing a measurable and verifiable framework for demonstrating compliance, aligning the obligations under the GDPR with the evolving technical benchmarks of European cybersecurity governance.

VII – Conclusions

As can be seen, in this positioning paper the authors propose a “horizontal” priority approach, which is focused on amendments to be applied to certain GDPR Recitals (specifically, Recitals 4, 6, 10) and general principles (Article 5), and a “vertical” secondary approach, which would instead surgically amend further individual Articles and provisions of the European Regulation.

It was deemed useful to list, illustrate, and briefly justify the possible amendments to specific GDPR Articles, although the reader might consider them merely a ‘wish list’ or even a ‘book of dreams’, which would require extremely broad political consensus to be voted on and implemented, and therefore unlikely or unrealistic. Nonetheless, in light of the undoubtedly courageous contents of the Digital Omnibus, the authors of this paper believe that a more extensive and specific reform of the GDPR could prove realistic and possible.

We are convinced, however, that even amending the Recitals and the general principles (as indicated in the “horizontal” priority approach) alone could guide the application of all other GDPR Articles in a more modern and balanced manner, without necessarily requiring further specific changes to the text of the Regulation.

Rome, February 2026

www.istitutoitalianoprivacy.it