unione europea
e diritti

The Digital Omnibus and the GDPR: Balancing Data Subjects' Rights with Controllers' Interest

Annagiusy Verde*

SUMMARY: 1. Reducing Complexity in the Digital Acquis: A Focus on the GDPR. – 2. From an Absolute to a Relative Approach: Identifiability of Pseudonymized Data. – 3. Regulating AI Under the GDPR: Legitimate Interest and Residual Processing of Sensitive Data. – 4. Moving Beyond Cookie Banners: Centralization of Privacy Preferences and Machine-Readable Signals. – 5. Final Remarks.

1. *Reducing Complexity in the Digital Acquis: A Focus on the GDPR*

On 19 November 2025, the Commission officially presented the Digital Omnibus[1] with a view to modernizing the European Union's digital regulatory framework.

This initiative belongs to a broader political agenda outlined in its Communication on "A simpler and faster Europe",[2] which takes stock of the recommendations contained in Mario Draghi's report[3] on the negative impact of the progressive accumulation of rules on Europe's competitiveness and productivity.

* Laureata in Giurisprudenza, Alma Mater Studiorum Università di Bologna.

[1] European Commission 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) 2019/1024 (Digital Omnibus), 19 November 2025.

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A simpler and faster Europe: Communication on implementation and simplification, COM(2025)47 final, 11 February 2025.

[3] M. DRAGHI, The future of European competitiveness, European Commission, 2024.

The drive towards simplification has encompassed, throughout 2025, several policy areas, including agriculture, single market, corporate sustainability, and defense. A case in point is the recently approved Omnibus Directive I,[4] which aims to simplify green reporting rules and due diligence obligations for businesses respectively under the Corporate Sustainability Reporting Directive[5] and the Corporate Sustainability Due Diligence Directive.[6]

The key legislative technique underpinning these efforts is the use of Omnibus bills, *i.e.* single acts that amend multiple legal instruments across different regulatory sectors. While this approach enables the swift adoption of new legislation, it has also raised concerns in relation to appropriate democratic oversight and procedural integrity of the legislative process.[7]

Against this background, the Digital Omnibus responds to concerns raised by European businesses and other stakeholders regarding regulatory burden, inconsistent enforcement and the cumulative impact of overlapping obligations, especially for small and medium enterprises, in the context of digital legislation.[8] The latter has indeed become increasingly complex over time, as a multitude of legal instruments have been adopted in areas as disparate as electronic communications, personal data protection, data sharing, cybersecurity, and so on. Although these rules are robust in terms of protection of fundamental rights, some are widely regarded as outdated and inadequate for the current technological reality and market practices, while others require streamlining and fine-tuning.

Notably, the General Data Protection Regulation (GDPR)[9] stands out among the relevant legislative instruments affected by the proposal, as the

---

[4] For a critical analysis, see E. CORCIONE, *Meno diritti umani, più competitività? Alcune considerazioni sul pacchetto Omnibus proposto dalla Commissione europea*, in *SIDIBlog*, 2025.

[5] Directive (EU) 2022/2464 of the European Parliament and of the Council, of 14 December 2022, amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting.

[6] Directive (EU) 2024/1760 of the European Parliament and of the Council, of 13 June 2024, on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859.

[7] A. ALEMANNO, *The Omnibus Road to Constitutional Drift, How the Rise of Omnibus Legislation Undermines Procedural Integrity in the EU*, in *VBlog*, 2025; J. OUYANG, *The Omnibus Comeback of the Neoliberal EU: Eroding Sustainability and Depoliticising the Market*, *ibidem*, 2025.

[8] Explanatory Memorandum of the Digital Omnibus, pp. 2-8.

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 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.

Commission intends, on the one hand, to modernize specific core provisions, and, on the other, to align it with a regulatory landscape that now encompasses the Artificial Intelligence Act (AI Act).[10] In fact, while the latter delimits clear conditions of use and imposes specific obligations for the deployment and development of AI technologies, the GDPR remains responsible for ensuring that the processing of personal data within those systems complies with data protection principles.

Despite its normative strength, the GDPR has revealed several structural challenges that require targeted legislative intervention. They relate to interpretative uncertainty regarding key concepts and arising from the persistent lack of a clear legal framework governing the processing of personal data in the context of AI development, an issue that calls for timely regulatory intervention given the increasing societal and economic centrality of artificial intelligence. Moreover, the current structure of cookie policy has proven both burdensome for controllers and detrimental for data subjects. Additional compliance challenges arise from the proliferation of information duties and data breach notifications, also in low-risk scenarios, and the existence of abusive access requests.[11]

Taken together, these factors contribute to making compliance with the GDPR particularly costly and burdensome for economic operators, highlighting the necessity to strike a more balanced framework between data subjects' rights and controllers' interests.

The potential impact of the Digital Omnibus on the EU data protection framework must be assessed in light of the constitutional role of the GDPR, widely regarded as the cornerstone of the EU digital *acquis* and a central pillar of European citizens' digital rights. Its normative strength lies in the high level of protection it affords to personal data, rooted in the constitutional status of data protection as a fundamental right enshrined in the Charter of Fundamental Rights of the European Union (Charter), by ensuring that the economic and technological developments in the digital sphere remain aligned with such status. Further, its rights-oriented approach has contributed to the GDPR's

[10] Regulation (EU) 2024/1689 of the European Parliament and of the Council, of 13 June 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828.
[11] R. MAHIEU, *The Ominous Omnibus: Dismantling the Right of Access to Personal Data*, in *VBlog*, 2025.

emergence as a global regulatory model,[12] exporting and shaping data governance standards at the international level.

In light of the above, the objective of the present analysis is to assess to what extent the Commission's proposal is capable of addressing the shortcomings currently displayed by the GDPR, while ensuring an effective balance between the protection of data subjects' rights and controllers' interests. More precisely, it will focus on three key relevant areas: the definition of personal data, the treatment of personal data in the context of AI development, and the substantial revision of the longstanding EU cookie policy. Through an analytical assessment of the relevant proposed provisions, the present analysis argues that, while some appear to merely formalize possibilities already envisaged at the level of judicial interpretation or regulatory guidance, with the aim of enhancing legal clarity in certain domains, others are likely to prioritize the interests of controllers, thereby raising concerns that such a shift may come at the expense of an optimal protection of users' rights.

2. *From an Absolute to a Relative Approach: Identifiability of Pseudonymized Data*

Under the current definition, "personal data" means any information relating to an identified or identifiable natural person. As highlighted in the Commission's Staff Working Document[13] accompanying the proposal, stakeholders consulted during the drafting process stressed the need for additional clarifications as to when a natural person should be regarded as identifiable and, consequently, whether the GDPR applies to specific data. The definitional issue is of practical relevance,[14] as it is closely interconnected with the use of pseudonymization techniques and with the disclosure or transfer of pseudonymized data to third parties. The contention stems from what is perceived as a specific risk inherent in data pseudonymization, given that it encompasses a range of operations aimed at dissociating the information

[12] M. L. RUSTAD, T. H. KOENIG, *Towards a Global Data Privacy Standard*, in *Fla. L. Rev.*, 2019.

[13] Commission Staff Working Document, SWD(2025)836, 19 November 2025.

[14] For academic comments on the definition of personal data, see A.B. MENEZES CORDEIRO, *The Personal Data Under the GDPR: Concepts, Elements, and Boundaries*, in *GPLR*, 2023, pp. 82-92; B. WONG, *Delimiting the Concept of Personal Data After the GDPR*, in *Legal Studies*, vol. 39, no. 3, 2019, p. 517 ff.; F. DAL POZZO et al., *They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR*, in *IDPL*, vol. 10, no. 1, 2020, p. 11 ff.

from the individual to whom it relates, while preserving the possibility of reidentification using additional information. This residual possibility of reidentification has led the European Data Protection Board (EDPB), the main administrative authority in the realm of data protection, to adopt a strict position, by consistently maintaining that pseudonymized data must nevertheless be regarded as personal data.[15]

By contrast, the Commission's proposal seeks to depart from this rigid approach, placing an excessive burden on data controllers when handling pseudonymized data, and to embrace a more flexible, context-dependent assessment.

In particular, the first two new proposed sentences clarify that «Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person» and that «Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity».

Moving forward, the third sentence of the proposed change states: «such information does not become personal data for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates». Through this intervention, the Commission seeks to facilitate compliance for data holders, who would otherwise be required to assess, on a case-by-case basis, whether each potential recipient has the means to identify the data subject and, consequently, whether the GDPR applies to the processing at issue.

These changes are certainly rooted in the Commission's intention to soften the absolute rule endorsed by the supervisory authorities and to shift the focus towards a factual assessment of the concrete ability of a given entity to identify a data subject, by incorporating in the legislative text contextual factors and complementary considerations which can already be found in the judicial reasoning and in the relevant Recital.

In fact, it should be emphasized that the abovementioned additions reflect a stance developed by the Court of Justice, which has progressively admitted a subjective, relative notion of identifiability, requiring the assessment at issue to be carried out from the perspective of the data holder concerned, focusing on the respective reidentification capabilities.

[15] European Data Protection Board, Guidelines 01/2025 on Pseudonymisation, adopted on 16 January 2025.

This line of thought emerged in the Court's reasoning before the GDPR came into force. A case in point is the *Breyer* judgment,[16] concerning the application of Directive 95/46/EC,[17] the predecessor of the GDPR, classifying dynamic IP addresses as personal data for a website operator only when that operator had means reasonably likely to be used to obtain the additional information needed to identify the data subject. Identifiability, therefore, had to be assessed by reference to the specific controller and realistically available means.

This stance was recently reiterated in *Deloitte*,[18] decided shortly before the publication of the Commission's proposal, where the Court explicitly stated that «pseudonymized data must not be regarded as constituting, in all cases and for every person, personal data […] insofar as pseudonymization may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject […]».

Furthermore, Recital 26 of the GDPR endorses a relative, context-dependent assessment of identifiability, as it provides that, in order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, either by the controller or by another person. The Recital further specifies the criteria to be considered, including the costs and the time required for identification, the available technology at the time of processing and foreseeable technological developments.

In this context, the joint reading of the Commission's Staff Working Document and proposed Recital 27, indicate the future elaboration of specific guidelines aimed at identifying the relevant criteria and means for determining when pseudonymized data can no longer be considered personal data. The stated purpose of these guidelines is to promote legal certainty and consistent application of the Regulation, particularly in business relations involving data sharing, by assisting controllers in conducting identifiability assessments in a predictable and harmonized manner. This shows that the Commission

[16] Judgment of the Court of Justice of 2 December 2016, Case C-582/14, *Breyer*. For an academic comment, see N. PURTOVA, *From Knowing by Name to Targeting: The Meaning of Identification Under the GDPR,* in *IDPL*, vol. 12, no. 3, 2022, p. 163 ff.

[17] Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[18] Judgment of the Court of Justice of 4 September 2025, Case C-413/23, European Data Protection Supervisor/Single Resolution Board. For an academic comment, see T. CABRAL, *Relative or Objective: The End of the Saga Concerning the Interpretation of the Concept of Personal Data: SRB v. EDPS (C-413/23)*, in *ELL*, 2025.

acknowledges that the highly technical nature of such assessments makes it necessary to provide additional support to controllers in the application of this proposed updated definition of personal data.

3. *Regulating AI Under the GDPR: Legitimate Interest and Residual Processing of Sensitive Data*

The General Data Protection Regulation was adopted at a time preceding the widespread deployment and the technological maturity of artificial intelligence systems. However, its growing societal and economic centrality has underscored the need to introduce *ad hoc* provisions in the Regulation at issue, given that the development of artificial intelligence systems typically involves the processing of wide and heterogeneous data sets, often including personal data, for purposes such as training, testing, validation, bias mitigation and performance optimization. In this sense, the use of AI represents one of the greatest challenges for regulatory instruments, due to the numerous risks associated with the application of these technologies, namely in terms of protection of personal data.

While the AI Act adopts a risk-based approach aimed at ensuring a socially sustainable development of artificial intelligence technologies, it does not regulate the collection and further processing of personal data in this context, which remain within the scope of the GDPR, whose provisions are to be accordingly updated to this new technological reality.[19]

In light of the above, the Digital Omnibus seeks to clarify and delimit the scope of the lawfulness of such data processing operations.

Admittedly, this aspect has already been addressed at the interpretative level by the European Data Protection Board, which has acknowledged that AI developers may in principle rely on the legal basis of legitimate interest provided under Article 6(1)(f) of the GDPR.[20] Specifically, in Opinion 28/2024,[21] the EDPB clarified that controllers may invoke this clause for AI

[19] P. DEWITTE, *AI Meets the GDPR: Navigating the Impact of Data Protection on AI Systems*, in N.A. SMUHA (ed.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge, 2025, p. 432; B. HOHMANN, *Reflections on Data Protection Compliance of AI systems Under the EU AI Act*, in *Cogent Soc. Sci.*, vol. 11, no. 1, 2025; P. FALLETTA, A. MARANO, *Intelligenza artificiale e protezione dei dati personali: Il rapporto tra Regolamento Europeo sull'intelligenza artificiale e GDPR*, in *Rivista italiana di Informatica e Diritto,* 2024.

[20] A. DALY, *The Legality of Data Processing under the GDPR: The Case of Legitimate Interests*, in *Comput. Law Secur. Rev.*, 2020.

[21] European Data Protection Board, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted on 17

development, by referring to the three-step assessment already envisaged when controllers intend to rely on legitimate interest as a legal basis.

This assessment requires preliminarily the identification of a legitimate interest pursued by the controller, followed by an evaluation of the necessity of processing for achieving the interest, and a balancing test as a final step to determine whether the legitimate interest is not overridden by the fundamental rights and freedoms of the data subjects. In conducting this balancing test, supervisory authorities are expected to consider a range of contextual factors, including the nature and the source of data, whether the data were publicly available, the relationships between the controller and the data subject, and the reasonable expectations of the individual concerned.

Against this background, the Commission's idea is to codify the possibility envisaged by the EDPB, by introducing a new Article 88c to explicitly recognize the use of legitimate interest as a lawful basis in the context of AI development for admissible purposes, such as bias detection and mitigation, or improvement of accessibility to certain services.

At the same time, the proposal provides for stringent applicability conditions, with safeguards encompassing strict compliance with the principle of data minimization laid out by Article 5 GDPR, which entails a mandatory *ex ante* assessment on the necessity of collecting certain data, active measures to prevent the disclosure of residually retained data, and the recognition of an unconditional right for data subjects to object to the processing of personal data.

The allowance under Article 88c is nevertheless subject to important limitations, as it does not apply where processing is prohibited under Union or national law, as in the case of the restrictions imposed on "gatekeepers" under Article 5(2) of the Digital Markets Act (DMA), nor where the balancing test demonstrates that the interests or fundamental rights of the data subject prevail over those of the controller.

Besides this, the proposal goes far beyond a mere legitimization of AI in the realm of data protection by introducing a significant derogation from the general prohibition on the processing of special categories of personal data under Article 9 GDPR.[22]

December 2024; for an academic comment, see V.L. RAPOSO, *The AI Gospel According to the EDPB-An Overview of Opinion 28/2024 on Data Protection Aspects in AI models*, in *Comput. Law Secur. Rev.*, 2026.

[22] F. BIEKER, K. NOLAN, *European AI FOMO: The European Commission Sacrifices the Digital Acquis at the Altar of AI Hype,* in *VBlog*, 2026.

The new clause would permit the processing of data revealing sensitive information, such as ethnic origins, political opinions, religious beliefs or sexual orientation, where this occurs in the context of AI development, through an ambiguously structured set of obligations imposed on controllers, whereby the subsequent obligation replaces the preceding one in the event of non-compliance of the latter. Accordingly, controllers are required to adopt the appropriate organizational measures to prevent the processing of special categories of data where they are not necessary for the intended purposes (what is commonly referred to as "residual processing").

Where, despite the adoption of such measures, such data are nonetheless collected, the controller is required to remove them. However, when removal would entail a disproportionate effort, the controller may retain the data, provided that it is not used to produce outputs, nor disclosed or otherwise made available to third parties.

In broad terms, it can be argued that, despite conferring legislative status to the possibility previously envisaged by the EDPB, proposed Article 88c does not resolve the operational issues surrounding the use of legitimate interest for AI developers. In fact, the provision remains broadly framed and refrains from setting out an exhaustive list of criteria to be considered in the balancing test, referring only partially to elements already identified by the EDPB's guidelines. Consequently, the assessment of lawfulness continues to depend on a case-by-case evaluation, ultimately left to the supervisory authorities and to the Court of Justice. Therefore, while the proposal formally ensures legal certainty, it does not substantially improve the current state of play concerning the practical application of Article 6(1)(f) on the AI context.[23]

Furthermore, while the derogation from Article 9 aims at providing clarity in response to longstanding concerns raised by stakeholders regarding the absence of a clear regulatory framework for residual processing in AI systems, the pursuit of legal certainty is ultimately undermined by the indeterminacy of key concepts. In particular, the notion of "disproportionate effort" is left largely undefined, and the absence of commonly accepted technical standards for assessing the adequacy of the organization measures put in place by controllers, raises significant concerns in terms of enforcement. Moreover, by explicitly referring to the reengineering of an AI system as an example of disproportionate effort, without offering corresponding illustrations of what

[23] EDPB-EDPS Joint Opinion 2/2026 on the Proposal for Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), adopted on 10 February 2026, p. 16.

would conversely qualify as proportionate, the proposal risks to appear more concerned with the interests of controllers rather than those of data subjects.[24]

In light of these shortcomings, the adoption of implementing acts clarifying the practical application of the new provisions appears essential to ensure a consistent and effective level of data protection.

4. *Moving Beyond Cookie Banners: Centralization of Privacy Preferences and Machine-Readable Signals*

Cookie policy arguably represents the most affected domain by the Digital Omnibus proposal.

Technically, cookies are text files that enable web providers to store or gain access to information, including personal data, already stored in users' terminal equipment, such as mobile phones and personal computers. Under the current legal framework, the use of cookies demands the prior consent of the user. From a legal perspective, the consent requirement is set out as a general rule under Article 5(3) of the E-privacy Directive,[25] while the subsequent processing of personal data collected through cookies is governed by the GDPR, creating, according to the Commission's view, an unnecessary dual regulatory structure.[26]

In practice, consent is generally expressed through cookie banners, which are consent management tools that inform website visitors about the use of cookies or similar tracking technologies, enabling them to accept, refuse or customize their privacy preferences.

Their pervasive use across the web has given rise to the phenomenon of "cookie consent fatigue",[27] whereby users, constantly exposed to cookie

[24] H. RUSCHEIMER, *Reforming the GDPR: Dilution or Progress?*, in *VBlog*, 2025.

[25] Directive 2002/58/EC of the European Parliament and of the Council, of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector. For an academic comment, see R. BOND, *The EU E-Privacy Directive and Consent to Cookies*, in *Bus. Lawyer*, vol. 68, no. 1, 2012, p. 215 ff.; F. DEBUSSERÉ, *The E-Privacy Directive: A monstrous Attempt to Starve the Cookie Monster?*, in *Int.J.L.&Info.Tech.,* vol. 13, no. 1, 2005, p. 70 ff.

[26] European Commission, Evaluation and review of Directive 2002/58 on privacy and electronic communications sector, 2022.

[27] P. NAITHANI, *Standardised Cookie Banner: A Solution to the Cookie Consent Problem*, in *Int. Rev. of Law Comput. Technol.*, vol. 39, no. 2, 2025; T. BISELLI ET AL., *Supporting Informed Choices about Browser Cookies: the Impact of Personalised Cookie Banners*, in *Proc. Priv. Enhancing Technol.*, vol. 1, 2024, p. 171 ff.; J.M. BAUER ET AL., *Are You Sure You Want a Cookie? - The Effects of Choice Architecture on User's Decisions about Sharing Private Online Data*, in *Comput. Hum. Behav.*, 2021; L.N. JAYAKUMAR, *Cookies 'n'*

banners in their daily online interactions, become overwhelmed and consequently inclined to provide consent in an automatic, non-critical manner. The legal requirements of a freely given, specific and informed consent, as established by Articles 4(11) and 7 GDPR, are thus significantly undermined by this psychological effect.

Furthermore, the validity of consent is jeopardized by questionable practices adopted by web providers in relation to the design of cookie banners, commonly known as "dark patterns".[28] This term describes deceptive interfaces and manipulative techniques that nudge users towards consent or otherwise make refusal more difficult. The extensive use of dark patterns has been documented by several empirical studies, showing that these practices are not isolated but rather systemic, and has resulted in the imposition of significant fines by national data protection supervisory authorities. The scale of the problem is clearly illustrated by a joint large-scale study conducted by the Karlsruhe Institute of Technology and IT University of Copenhagen,[29] which found that approximately 72% of European websites deploy at least one misleading element in their cookie banners, such as unequal prominence among different options or pre-ticked consent boxes.

In light of these shortcomings, the proposal intends to introduce a long-awaited overhaul of the current framework, with the objective of streamlining users' online experience, given the inadequacy of cookie banners as a valid consent mechanism.

While the protection of users' privacy represents a core objective, the Commission further highlights that the current rules entail a substantial economic and regulatory burden for businesses. In fact, the use of cookie banners as the main mechanism to obtain consent requires constant legal, technical and organizational efforts. Moreover, impact assessments and stakeholders consultations indicate that these costs are particularly burdensome

---

Consent: An Empirical Study on the Factors Influencing of Website Users' Attitude towards Cookie Consent in the EU, in *DBS Bus. Rev.*, vol. 4, 2021; R. BORNSCHEIN ET AL., *The Effects of Consumers' Perceived Power and Risk in Digital Information Privacy. The Example of Cookie Notice*, in *J. Public Policy Mark.*, vol. 39, no. 2, 2020, p. 135 ff.

[28] See M. MARTINI, C. DREWS, *Making Choice Meaningful - Tackling Dark Patterns in Cookie and Consent Banners through European Data Privacy Law*, in *SSRN*, 2022; J. LUGURI, L.J. STRAHILEVITZ, *Shining a Light on Dark Patterns*, in *JLA*, vol. 13, no. 1, 2021, p. 43.

[29] B. M. BERENS ET AL., *Cookie Disclaimers: Dark Patterns and Lack of Transparency,* in *Comput. Secur.*, 2024. Similar conclusions were drawn by NOYB, an Austrian non-profit organization for the protection of digital rights, which, in a comparative analysis of cookie banners based on the relevant guidelines issued by the EDPB and national supervisory authorities, highlighted systematic practices aimed at directing users towards acceptance, via omissive or manipulative mechanisms.

for small and medium-sized enterprises, which often lack in-house and technical expertise, and that these burdens are likely to be exacerbated by the current status of the relevant legal regime as a Directive, as divergent national transpositions and uneven enforcement practices across Member States could lead to a fragmentation that undermines the ultimate objective of a single harmonized digital market.[30]

For these reasons, the proposal primarily aims to minimize consent fatigue for users, while reducing regulatory fragmentation and operational costs for controllers.

This is pursued through the consolidation of the relevant rules under the GDPR and the introduction of new Articles 88a and 88b.

The new framework upholds consent as a general basis for the use of cookies, while a whitelist of low-risk purposes, where accessing and processing of personal data stored in user's devices is deemed lawful without the necessity of consent, is established by paragraph 3 of Article 88a, thus reducing the number of situations in which consent must be obtained.

However, the most significant innovation consists in the replacement of cookie banners by simplified and intelligible manners to express privacy preferences, such as single click buttons or equivalent means, whenever consent is used as a legal basis. In particular, according to Article 88b, such preferences should be communicated to controllers through automated, machine-readable indications, transmitted via web browsers, operating systems, or mobile applications[31]

The article allows the use of such signals both to express consent, provided that all the conditions for its validity are satisfied, and to refuse consent or to exercise the right to object pursuant to Article 21(2) GDPR, where the processing is based on the legitimate interest of the controller.

Moreover, the proposal introduces a six-months moratorium during which controllers are prohibited from requesting consent again where it has already been declined, with a view to avoiding the replication of intrusive consent requests.

It is worth stressing that the idea of replacing cookie banners is not entirely new, as it dates back to 2009, when Recital 66 of Directive 2009/136/EC[32]

[30] Commission Staff Working Document Accompanying the documents, 19 November 2025.
[31] M. HILS ET AL., *Privacy Preference Signals: Past, Present and Future*, in *Proc. Priv. Enhancing. Technol.*, vol. 4, 2021, p. 249 ff.
[32] Directive 2009/136/EC of the European Parliament and of the Council, of 25 November 2009, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the

introduced the principle that users should be able to express their preferences through browser settings or other applications. Accordingly, new mechanisms were introduced, such as the Do Not Track Header,[33] a technical standard that indicated user's privacy preferences to websites. However, its purely voluntary nature and the absence of a legal obligation for websites to comply with the signals prevented a widespread adoption. Subsequently, the proposal for a Regulation on Privacy and electronic Communications in 2017[34] reaffirmed the possibility of automated consent signals, making them binding for web providers, a feature now reinstated by paragraph 2 of Article 88b of the Digital Omnibus.

In light of the above, the Commission's initiative should be welcomed as it marks a renewed legislative effort to successfully integrate machine readable expressions in the European privacy framework after earlier failed attempts, although it remains vague as to the concrete technical solutions to implement the new consent regime; a gap that will be inevitably filled by technological actors and subsequently shaped by the oversight of supervisory authorities.

5. *Final Remarks*

As anticipated, the proposed changes to the GDPR analyzed in this article are part of the Commission's broader commitment to streamline the European digital regulatory framework, which has been increasingly criticized for its excessive stratification.

With this respect, the core question becomes whether the Commission has succeeded in drawing up a proposal that strikes an appropriate balance between enhancing regulatory effectiveness, while upholding a consistent protection of data subjects' rights.

Overall, this analysis suggests that some of the changes under scrutiny are less innovative than they appear at first glance, as they codify practices already emerged in the context of judicial interpretation and regulatory guidance. This is the case for the departure from any automatism between pseudonymized

processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[33] I. KAMARA, E. KOSTA, *Do Not Track Initiatives: Regaining the Lost User Control*, in *Int. Data Priv. Law*, vol. 6, no. 4, 2016, p. 276 ff.

[34] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.

data and their qualification as personal data, an approach already implicit in Recital 26 of the GDPR and in judicial reasoning.

Likewise, the explicit recognition of the possibility for AI developers to rely on legitimate interest as a valid legal basis for processing does not constitute a substantive departure from the existing framework.

By contrast, more controversial are the provisions concerning the processing of special categories of data in the context of AI development.

In fact, the introduction of a permissive framework for the residual processing of sensitive data, amounts to a *de facto* derogation from the general rule in the absence of commonly agreed technical standards, potentially hollowing out the principle of data minimization, which is one of the cornerstones of the GDPR. Moreover, while it is undeniable that AI systems generally employ vast datasets, including data that may reveal sensitive information, this technological reality cannot lead to increased risks for data subjects, especially considering well-known phenomena connected to AI systems such as data leakage, AI hallucinations and data regurgitation.

Lastly, the revision of cookie policy, the latest of a series of unsuccessful attempts to overhaul a manifestly dysfunctional legal framework, should be welcomed, given that the combination of a current mature technological landscape and a clear normative intervention has the potential to achieve the objective of streamlining users' online experiences, while ensuring meaningful control over their personal data and reducing design and maintenance costs for controllers through the elimination of cookie banners.

At the same time, it is undeniable that there are inherent risks, mostly in relation to an increasing reliance on flexible standards and vague concepts, capable of generating further interpretative fragmentation. In parallel, the expansion of exceptions, especially in the context of AI, could gradually lower the level of protection currently afforded to data subjects, while the lack of precise technical guidance may shift excessively the discretion onto controllers and supervisory authorities, potentially undermining legal certainty.

In any event, the proposed changes will be subject to further revision, as they proceed through the legislative process under the oversight of the Council and of the European Parliament, which will address the most opaque or controversial points. Furthermore, the concrete impact of these changes will ultimately depend on the adoption of implementing acts needed to specify assessment criteria and to elaborate technical standards capable of giving practical meaning to indeterminate legal concepts. In fact, a robust and clear implementation framework will be essential to minimize the risk that the

simplification efforts at issue will lead to increased legal uncertainty and uneven levels of protection across the Union.

ABSTRACT (ita)

Il presente contributo offre un'analisi critica delle modifiche che la Commissione europea intende apportare al Regolamento generale sulla protezione dei dati (GDPR), nell'ambito del pacchetto normativo Digital Omnibus presentato ufficialmente il 19 novembre 2025. Dopo aver evidenziato brevemente la *ratio* della strategia di semplificazione normativa perseguita da quest'ultima in settori di intervento trasversali, l'analisi si sofferma sulle criticità sollevate in relazione a difficoltà interpretative e applicative del GDPR, capaci di generare eccessivi costi amministrativi ed obblighi procedurali a discapito dei soggetti vincolati da tale regolamento. In particolare, ci si focalizza su tre novità principali: la definizione di dato personale alla luce di una concezione soggettiva di identificabilità del soggetto interessato, il ricorso al legittimo interesse quale base giuridica per i trattamenti connessi allo sviluppo di sistemi di IA, e l'abolizione dei *cookie* a favore di una centralizzazione delle preferenze di *privacy*. Le risultanze dello studio mettono in discussione il contenuto innovativo della proposta, richiamando prassi interpretative ed applicative esistenti che troverebbero ora una formalizzazione al suo interno. Si sottolinea altresì come l'esplicita valorizzazione degli interessi dei titolari di trattamento alla base della proposta possa incidere negativamente su un corretto bilanciamento tra esigenze delle imprese e tutela dei diritti fondamentali degli interessati.

ABSTRACT (eng)

This work provides a critical analysis of the amendments that the European Commission intends to introduce to the General Data Protection Regulation (GDPR) as part of the Digital Omnibus legislative package, officially presented on 19 November 2025. After briefly outlining the rationale behind the Commission's cross-sectoral regulatory simplification strategy, the analysis takes stock of the concerns raised in relation to interpretative and practical difficulties associated with the GDPR, which are considered to generate excessive administrative costs and procedural burdens for entities subject to the Regulation. Three key innovations are examined in particular: the definition of personal data in light of a subjective notion of the data subject's identifiability, the use of legitimate interest as a legal basis for processing related to the development of AI systems, and the replacement of cookie banners with

a centralized system for managing privacy preferences. The study casts doubts on their innovative impact of the proposal, highlighting how it formalizes existing interpretative practices. At the same time, it is argued that the explicit recognition of data controllers' interests underpinning the proposal may negatively affect a fair balance between business needs and the protection of fundamental rights of data subjects.