la villa numeris

Position paper

GDPR : revising to simplify

Spring 2026

Table of Contents

Acknowledgments

Our work was conducted under the direction of **Jeanne Bossi Malafosse**, a member of the Paris Bar, to whom we extend our warmest thanks, as well as to the individuals who answered our questions during interviews: **Michel Combot**, former Director of Technology at the CNIL; **Thomas Dautieu**, Director of Legal Support at the CNIL; **Thomas Honnet**, Data Protection Officer, City of Marseille; **Patricia Le Large**, Data Protection Officer at Orange France; **Fabrice Mattatia**, Data Protection Officer at the Ministry of the Interior; **Hugues de Maupeou**, Government Affairs and Public Policy Manager at Google France; **Juliette Rouilloux-Sicre**, Group Data Protection Officer at Thales; and **Laurent Teyssandier,** Data Protection Officer at Criteo, and all those who preferred to remain anonymous.

Thank you to **France Charruyer,** founding partner of Altij Avocats and president of the public interest association Data Ring; **Clothilde Hocquard**, Regulatory Affairs and Advocacy Lead at France Digitale; **Nathalie Laneret**, Director of Public Affairs at Criteo, **Ariane Thomas**, Director of Sustainable Development Technology, L'Oréal, and **Olivier Esper**, Head of Institutional Relations, Google France, for their insights and contributions, and to **Arthur Brodmann** for his careful review.

Mykaïa's Perspective

Foreword

Recognizing, based on feedback from its members and the market, the need to initiate a discussion on the evolution of the General Data Protection Regulation (GDPR), La villa numeris took the initiative as early as in the summer of 2025 to undertake work in this area, building on its initial publications such as “GDPR: 5 Years, Time to Celebrate?” in 2023, and sustained research on international data transfers.

Methodological Note

Noting that the European Commission has released its omnibus proposal aimed at simplifying European data rules by incorporating the GDPR into its scope, La villa numeris has refocused its work to conduct an initial analysis of the omnibus proposal based on interviews with individuals recognized for their expertise (business leaders, legal experts, DPOs from public and private organizations, regulators) and a study led by Jeanne Bossi Malafosse, an attorney at the Paris Bar.

The position paper that follows is based on these interviews and this analysis. The quotes in quotation marks are taken from interviews conducted by La villa numeris with executives and experts, most of whom wished to remain anonymous in order to speak freely, out of concern for not publicly committing their organizations and exposing them to controversy on a subject that is inherently contentious. In fact, we have chosen not to attribute any quotes, as they reflect a prevailing sentiment among the individuals we interviewed.

We extend our warmest thanks to the representatives of companies and public institutions who agreed to contribute to our work in this way.

Context and Motivation

Ten years have passed since the adoption of the General Data Protection Regulation (GDPR), which came into effect in May 2018 and has become a symbol of individual protection…
and a certain degree of administrative complexity.

Despite the initial difficulties in implementing the regulation’s requirements and the rushed compliance process for some, the regulation has fostered a genuine culture of data protection and increased accountability among stakeholders, a development that deserves recognition.

However, for many stakeholders today, especially smaller businesses and startups, which lack specialized legal resources to navigate regulations deemed “incomprehensible”, the need for clarification and simplification remains clear.

Above all, we observe that depending on how the text is applied, certain legal professionals, often DPOs, adopt a stance that is sometimes rigid and does not serve the purpose of data protection.

In light of this, our philosophy leads us to promote a model where data protection principles do not hinder innovation and the development of business activities but, on the contrary, become a competitive advantage and a source of trust while reaffirming the primacy of the human element.

Context of the Omnibus

The European Commission’s initiative. The proposed Regulation published on November 19, 2025, aims in particular to provide “immediate relief” to businesses and to boost competitiveness through targeted technical amendments. We welcome this initiative.

It also comes at a time when the legislative landscape is saturated by the successive and uncoordinated entry into force of a series of European texts dealing with data: the Data Governance Act, the AI Act, the Data Act, and the European Health Data Space, to name just a few. This situation further exacerbates the legal complexity faced by businesses and inevitably creates a climate of legal uncertainty when the provisions of these texts impose new obligations on stakeholders that do not always align with one another.

We must also guard against a sometimes observed tendency toward “over-compliance” on the part of certain stakeholders who are multiplying compliance measures: the proliferation of unnecessary registry records, a tendency to conduct data protection impact assessments (DPIAs) for processing operations that do not require them, obtaining consent when it is not necessary, and so on.

Consequently, the aim is to prevent Europe from “feeding itself with legislation” that lacks overall coherence.

Presentation of the Digital Omnibus Bill

The bill aims to amend several digital laws to simplify the interpretation of certain obligations, reduce administrative burdens, and clarify certain gray areas (particularly regarding AI and research). On this last point, and independently of another European Commission proposal, the AI Omnibus, aimed at revising certain provisions of the AI

Regulation adopted on June 13, 2024, the Digital Omnibus also includes provisions that could impact the AI Regulation.

Regarding the timeline for adopting the text, a swift adoption, by the end of 2026, is expected.

---

1 | Be ambitious: promote openness and innovation

Several measures could promote open data and innovation while ensuring appropriate implementation conditions.

1.1 - Definition of the concept of personal data and the European Commission's implementing acts

The European Commission's objective appears to be to resolve the difficulties in interpreting the concepts of pseudonymization and anonymization by adopting a new definition of personal data as it currently appears in Article 4 of the GDPR.

This is a delicate undertaking, as it involves modifying the foundational definition of data protection, which holds that whenever a natural person is theoretically identifiable (directly or indirectly), the data concerning that person constitutes personal data subject to the principles of personal data protection.

The European Commission relies on the recent CJEU ruling known as "SRB" of September 4, 2025, which holds that for a data controller who retains the ability to identify the data subjects, pseudonymized data remains fully personal data; however, for a recipient who does not have means that could reasonably be used to re-identify the individuals, the same information ceases to be classified as personal data within the meaning of the GDPR.

This is therefore an important clarification by the CJEU that the Commission proposes to incorporate into Article 4 of the GDPR as follows: *"Information relating to a natural person does not necessarily constitute personal data for any other person or entity, merely because another entity can identify that natural person… "*And in Recital 27, the Omnibus Directive further specifies that to determine "*whether a natural person is identifiable, all means likely to be reasonably used to identify that natural person directly or indirectly must be taken into account*."

Let us first note that in practice, and for certain projects involving multiple stakeholders, it can indeed be very difficult to comply with personal data protection principles, particularly when reusing a natural person's data: how can one inform that person of this new reuse when the pseudonymized data available does not allow for it, except by committing unreasonable material, financial, and human resources. Article 11 of the GDPR thus provides that *"If the purposes for which personal data are*

processed do not or no longer require the controller to identify a data subject, the controller is not required to retain, obtain, or process additional information to identify the data subject for the sole purpose of complying with this Regulation."
This clarification by the CJEU is particularly important as it concerns the concept of personal data, which lies at the heart of the GDPR. It is therefore essential that it be applied in a harmonized manner not only by data protection authorities but also by all national courts. Only by codifying this case law can we ensure consistent interpretation within the internal market and a level playing field at a time when data has become a strategic asset sought after by European companies to develop artificial intelligence.

This reality thus effectively calls for work on the status of pseudonymized data, which must necessarily lead to a re-examination of the definition of personal data.

1.2 - Definition of scientific research: presumption of compatibility with the original purpose

To remove a major barrier to innovation, the challenge lies in being able to reuse data collected for subsequent research projects without having to seek consent again.

The Digital Omnibus proposes an amendment to Article 5(1)(b) of the GDPR, stating that there is a presumption of compatibility (whereas the current text refers to a presumption of non-incompatibility) between further processing of data and the initial processing when the processing is carried out for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes (and provided that the provisions of Article 89(1) are complied with).

Most importantly, unlike the current wording of the GDPR, the Digital Omnibus specifies that this compatibility is assessed independently of Article 6(4) of the GDPR.

In other words, it would no longer be necessary for such data processing to conduct a compatibility test between the initial processing and the subsequent processing.

As a reminder, this compatibility test requires the data controller to verify:

- the existence of a link between the purposes for which the data was collected and the purposes of the subsequent processing;
- the context in which the data was collected, and in particular the relationship between the data subjects and the data controller;
- the nature of the data being processed, and in particular the presence of sensitive data;
- the possible consequences of the envisaged further processing for the data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

This therefore represents a significant development, allowing for greater freedom in the reuse of data for further processing, without lowering the level of protection for the rights and freedoms of data subjects.

The presumption of compatibility with the original purpose must be affirmed. Thus, the “A Lever for Data” proposal moves in a direction that should be welcomed and affirmed.

However, the effectiveness of this measure depends on a necessary clarification of the very definition of “scientific research” proposed by the Digital Omnibus in Article 4(38). To provide full legal certainty for investors, the legislator should explicitly state in the text that, regardless of whether a commercial purpose is pursued, research may be funded by private or public funds. Without this clarification, the ambiguity regarding the scope of this presumption risks perpetuating uncertainty that is detrimental to European R&D.

1.3 - Flexibility for AI: new legal basis and possibilities for processing sensitive data

The Omnibus Bill proposes to explicitly provide that legitimate interest may serve as a legal basis for training AI language models, thereby addressing a strong demand from the industry to safeguard its investments.

1.3.1 Article 88ter: Securing Legitimate Interest for AI Training

We welcome the Omnibus’s aim to explicitly confirm that legitimate interest constitutes a valid legal basis for the development and operation of AI models. This is an *essential* prerequisite for meeting industry demands and securing European investments. However, for this recognition to be effective, the text must ensure full harmonization across the Single Market: the provision allowing national laws to circumvent the GDPR by requiring consent at the national level must be removed, lest it create unmanageable regulatory fragmentation. The same applies to the procedures for applying legitimate interest.
Surprisingly, the current wording of Article 88ter restricts the use of legitimate interest by limiting the balancing test solely to the interests of the data controller, effectively excluding those of third parties. This approach not only constitutes a legal departure from Article 6(1)(f) of the GDPR and established case law, which expressly allow for the consideration of legitimate interests pursued by a third party, but also amounts to technological nonsense. Indeed, artificial intelligence is, by its very nature, a technology whose economic and societal benefits extend far beyond the single company that develops or improves a model. In order to reflect the reality of this technology and avoid stifling European innovation, the legislator must amend the text to explicitly include the interests of third parties in this balancing test.

1.3.2 Article 9(5): Adopt a risk-based approach for sensitive data

Allowing the processing of special categories of (sensitive) data is crucial for detecting and correcting biases in AI algorithms. This is a pragmatic step forward that most stakeholders welcome.

Indeed, the Digital Omnibus proposes, in particular, to add a new exception to the prohibition on processing sensitive data, thereby supplementing the list in Article 9 of the GDPR.

It proposes allowing the processing of sensitive data in the context of developing and operating an AI system or model, provided that the principles governing the processing of personal data (Article 5 of the GDPR) are respected.

This new exception aims to stimulate the development of artificial intelligence systems or models in the European Union by allowing the collection of sensitive data for the training of these systems or models.

The Digital Omnibus would, however, establish a strict framework by requiring the implementation of appropriate technical and organizational measures to prevent the collection of sensitive data. If, however, these measures do not prevent the processing of such data, then the data controller must ensure that such data is deleted. If deletion proves impossible, the data controller must protect the data against any use of such data to produce results and against any disclosure or other form of making the data available to third parties.

Thus, while the Digital Omnibus provides some leeway for training artificial intelligence systems and models, this proposal aims to ensure that no sensitive data is disclosed in the output data of artificial intelligence systems.

The practice of regulatory “sandboxes” should also be encouraged to test innovation without the risk of immediate sanctions. Data protection authorities should devote more resources to this practice, which today better reflects the reality of the processing operations in question rather than their often highly theoretical and doctrinal examination of the formalities files submitted to them.

2 | Being practical

Several concrete measures could ease the obligations of economic actors without calling into question the principles of personal data protection.

2.1 - Individuals’ rights

Simplify to inform. When information notices are too long or too repetitive, they are neither read nor understood. The current information overload, particularly with endless legal disclaimers, undermines trust and genuine understanding on the part of the user. More concise and readable information must be implemented.

In this regard, the Digital Omnibus proposal aims to simplify the obligations regarding the information that must be provided to data subjects.

On the one hand, it clarifies the scope of the current GDPR exception set forth in Article 13.4, which provides that a data subject who already possesses the information covered by the text need not be informed again, while

specifying that this exception applies if there are *"reasonable grounds to assume that the data subject is already aware of the identity of the controller and the purposes of the processing."* On the other hand, it provides for other exceptions to the information obligation when the data has been collected in the context of a clear and limited relationship between the data subjects and the controller carries out an activity that is not data-intensive.

However, the Digital Omnibus immediately tempers this desire for simplification for stakeholders by stating that these exceptions cannot be invoked if the data controller:

- transfers the data to other recipients;
- transfers the data to a third country;
- engages in automated decision-making, including profiling;
- or if the processing is likely to result in a high risk to the data subjects.

This development may be welcome for data controllers insofar as it simplifies this information obligation for processing operations that pose little risk to data subjects. For example, this exception will prevent the inclusion in certain contracts or privacy policies of information clauses whose sole purpose was to comply with regulations but which did not address any actual data protection concerns.

However, it will be necessary to clarify what constitutes a non-data-intensive activity.

It is regrettable that the text does not include the exception currently provided for in Article 13 of the GDPR (prior knowledge of the information by the data subjects). Thus, a restrictive interpretation of the concept of a "clear and limited relationship" could reduce the exceptions to the information obligation, as eligibility for the current exception would be subject to all the new conditions (notably a clear and limited relationship).

It is therefore essential to obtain clarification on the interpretation to be adopted in order to ensure that this text does indeed constitute a simplification measure.

Furthermore, the Digital Omnibus proposal adds an exception to the obligation to provide information when processing is carried out for scientific research purposes and the provision of such information proves impossible or would involve a disproportionate effort on the part of the data controllers, or compliance with this obligation would be likely to render impossible or seriously compromise the conduct of the research itself.

While this exception is of interest to a data controller who wishes to reuse, for scientific research purposes, data already collected from data subjects and who does not have, or no longer has, the contact details of the data subjects, it will only be effective if the conditions for its application are precisely defined.

It would, however, be useful in certain cases, particularly in the field of medical research, where researchers seeking to reuse data originally collected for another purpose regularly face significant practical difficulties in complying with the individual obligation to provide information.

It must also be consistent with national laws.

But beyond these simplifications, is it not appropriate to ask whether prior and individual notification should be maintained as a matter of principle in all cases? Given that in their daily lives, connected citizens constantly access information, could we not consider that the obligation to provide information could be satisfied in many cases by general information, while always allowing the possibility to object within a defined timeframe?

It is worth noting that the Omnibus text refers to the possibility of making the information required under the individual notification requirement publicly available whenever such notification is impossible. Provided that the assessment of this impossibility is defined much more broadly than it is today.
Combating abuse in cases of excessive requests. Citizens' right of access is often misused, deviating from its intended purpose, which is to verify the lawfulness of processing, to serve as leverage in commercial disputes, such as those involving dissatisfied consumers, or in competitive situations. Therefore, a principle of proportionality must be applied. Consequently, companies should be able to refuse manifestly abusive or repetitive requests without incurring disproportionate legal risk.

With regard to data subjects' right of access, Article 12 of the GDPR already allows the data controller to refuse a request or charge for the costs incurred in the event of a request deemed *"manifestly unfounded or excessive*," particularly due to its repetitive nature.

The text proposed in the draft Digital Omnibus Regulation goes further by adding the possibility for the data controller to refuse the request or charge for the costs incurred in the context of a request for access based on Article 15 of the GDPR when the data subject abuses the rights conferred by the GDPR for purposes other than the protection of their data.
It will be interesting to monitor this concept of abuse of rights to determine exactly what it encompasses.

This amendment introduced by the Digital Omnibus is undoubtedly a response to the case law of the CJEU, which has so far ruled on several occasions that this right may be exercised for any purpose, including in litigation or for the production of evidence. However, the recent ruling by the same Court, published on March 19, 2026 (Case C-526/24), appears to reverse this position, as it specifies that an initial request for access may, under certain circumstances, be considered excessive and therefore abusive, particularly if it is made for the sole purpose of subsequently seeking compensation for an alleged violation of the GDPR.

Indeed, it has become common practice, for example, for employees, in the context of pre-litigation proceedings before labor courts, to exercise their right of access in order to gather the necessary evidence for the upcoming dispute.

Some organizations thus find themselves burdened with significant work analyzing and compiling data in order to respond to a request for access within a particularly tight deadline (one month), as these requests are in no way related to the protection of their

personal data but rather to gathering evidence in their favor or the desire to harm their former employer.

The drafting of the Digital Omnibus is therefore welcome, provided that abuse of rights is clearly defined in this context and does not undermine the balance that must always be maintained between protecting the rights of data subjects and safeguarding the interests of businesses.

2.2 - The announced relaxations that must not call into question the liability of the parties involved

2.2.1 - List of processing operations subject to an impact assessment
Currently, the list of data processing operations subject to a data protection impact assessment (DPIA) depends on the interpretation of each data protection authority, even though the GDPR defines the broad categories.

The Digital Omnibus proposal suggests delegating to the European Data Protection Board (EDPB) the task of defining a list of processing operations for which an impact assessment is required, and a list for which such an assessment is not required.

The Board then forwards these lists to the Commission.

Assigning this authority to the EDPB is therefore certainly intended to establish a common position across all European countries by reducing differences in interpretation among EU member states, a development that is likely to be welcomed by stakeholders.

Furthermore, the Digital Omnibus provides that the EDPS shall develop a common methodology for conducting impact assessments, a development at the European level that would indeed be welcome.

In a risk-based approach, it must be reaffirmed that the DPIA should focus on actual “high risks” and not become a systematic bureaucratic formality.

2.2.2 - Conditions for reporting a data breach

Avoiding over-reporting is more necessary than ever. The plan to align the notification (to the authority) and communication (to individuals) regimes risks diluting the warning effect and unnecessarily increasing the burden for minor incidents.

Thus, the criteria for determining severity would benefit from being stated more clearly so that only incidents posing a real risk to rights and freedoms are reported, thereby avoiding overwhelming DPOs and authorities.

The Digital Omnibus proposal includes several measures aimed at streamlining and simplifying data breach notification obligations and restoring the provision’s true purpose.

Thus, the deadline for notifying the supervisory authority in the event of a data breach is extended to 96 hours from the time of discovery, compared to the current 72 hours, which will undoubtedly avoid additional notifications that burden the procedure.

The Digital Omnibus proposal also refers to the establishment of a single point of entry for reporting breaches, introduced by Directive (EU) 2022/2555 and still awaited in practice to address the various reporting obligations imposed by European legislation (notably the GDPR and the NIS 2 Directive).
Finally, it refers to the European Data Protection Board (EDPB) for the development of a common notification template as well as a list of circumstances in which a personal data breach is likely to result in a high risk to an individual's rights and freedoms, a template that must be adopted by the Commission through an implementing act. This point is particularly anticipated, as the concept of "high risk" remains unclear at this time and continues to raise questions about whether data breaches must be notified to data subjects, although the examples already developed by the EDPB are helpful in this regard.

3 | Missed Opportunities

3.1 - Governance: Role and Conditions for Intervention by the EDPB and Commission Implementing Acts

The EDPB - Although this issue is not directly addressed in the draft text, stakeholders would like to see the functioning of the European Data Protection Board (EDPB) reformed. The EDPB is still perceived as too "opaque," producing guidelines that are disconnected from operational reality.

To address this, it would be appropriate to provide for stakeholder consultation before, rather than after, the drafting of guidelines. This would avoid dogmatic or maximalist stances by prioritizing dialogue.

For example, the EDPB could adopt a more constructive approach toward the business community by agreeing to meet with representatives from the relevant sectors.

Imposing more transparent voting rules on the EDPS regarding its position statements and the deadlines for producing guidelines would also help strengthen its authority.

For example, the faster production of its updated guidelines on anonymization might have helped avoid more radical positions on the definition of personal data as currently proposed by the Commission in the Digital Omnibus.

There is a need at the European level for a governance body that is far more effective, responsive to stakeholders, and whose authority is thus more widely recognized.

Toward genuine harmonization: the EDPB's powers should be strengthened to unify legal doctrine, which would prevent the fragmentation of approaches and interpretations by national authorities, such as the CNIL, from adding "overlays" or

additional requirements. This inherently fragments the single market.

The Commission - Draft Article 41a provides that the Commission may adopt implementing acts to specify the means and criteria for determining whether pseudonymized data still constitutes personal data for certain entities.

It would also be more constructive to include in these implementing acts a definition of the scope of anonymization, as the long-awaited work by the EDPS on anonymization and pseudonymization has still not been adopted. Waiting for the opinion of the supervisory authorities on this matter, who currently do not share the same view on the evolution of the definition of personal data and who clearly do not intend to take into account the CJEU's judgment of September 4, actually calls for the adoption of implementing acts that interpret the text.

It might also be appropriate to recognize the value of Privacy Enhancing Technologies (PETs), which offer a practical way to implement data protection principles. Indeed, the current procedures for adopting codes of conduct remain very complicated and time-consuming.

3.1 - The practice of regulatory "sandboxes"

This practice should be encouraged to test innovation without the risk of immediate sanctions. Data protection authorities should devote more resources to this practice, which better reflects the reality of the data processing operations being carried out today, rather than their often highly theoretical and doctrinal examination of the formality files submitted to them.

It would make sense for the Digital Omnibus bill to recognize this practice, given that the Artificial Intelligence Regulation enshrines it in Articles 58 and 59.

3.2 - The Incomplete Implementation of the e-Privacy Directive and Consent Fatigue

The Digital Omnibus's ambition to align these rules with the GDPR (via the new Article 88a) stemmed from an excellent intention: to unify the legal framework to ensure more consistent regulation under the sole authority of data protection authorities and through the one-stop-shop mechanism. Unfortunately, this is a missed opportunity. While the Commission has signaled its intent to phase out the ePrivacy Directive, the Omnibus proposal fails to address this. By maintaining a dichotomy where personal data falls under the GDPR while non-personal data related to the same terminal equipment remains under the ePrivacy Directive, the text will force companies to comply with multiple regulators for a single cookie. Far from simplifying the law, this status quo will paradoxically create more jurisdictional conflicts, legal uncertainty, and complexity in enforcement than the current situation.
Adopted in 2002, nearly 25 years ago, the ePrivacy Directive appears to be "completely outdated."

While the Digital Omnibus proposal touches on the subject, it does not venture to address the underlying problem of growing "consent fatigue" among users when accessing

websites and encountering advertising banners.

A new Article 88a would be incorporated into the GDPR and would require consent for the storage of personal data or for access to data already stored on the terminal equipment of natural persons, thereby incorporating the provisions of Directive 2002/58 (e-Privacy) into the GDPR.

Rather than simply merging the rules, the Commission has merely duplicated the rules applicable to cookies (Article 5(3) of the e-Privacy Directive) in the GDPR (new Article 88a). Thus, (1) the rules of the e-Privacy Directive would continue to apply to the processing of non-personal data, and (2) they would also continue to apply to the processing of personal data of legal entities, as such data falls outside the scope of the GDPR. The proposal would create an asymmetry between the exceptions to obtaining consent under the e-Privacy rules and the GDPR, with more exemptions provided for the use of personal data than for non-personal data. For example, access to non-personal data for audience measurement purposes would be subject to user consent, whereas the processing of their personal data for the same purpose would not be. The resulting hybrid approach risks maintaining, or even amplifying, the inconsistencies and compliance burden that the Omnibus was intended to simplify.

In any case, a broader discussion should be conducted to assess the need to maintain a separate legal framework for data access and storage on terminal equipment. This also requires a unified approach by the competent authorities.

Draft Article 88b would concern automated, machine-readable indications of individual choices, as well as compliance with these indications by website providers.

However, bolder measures should be considered while preserving the web's business model, which is primarily funded by advertising, as the requirement to centralize browser signals does not effectively address user fatigue.

The Commission's proposal to introduce a new provision into the GDPR (Article 88b) requiring compliance with standardized, automated, and machine-readable signals expressing users' choices will add a new layer of complexity.

In France, the Competition Authority has demonstrated that centralizing consent at the browser level would significantly strengthen the position of *gatekeepers*.

From a technical standpoint, the mechanism proposed by the Commission is impractical: users interact with digital services through a wide variety of devices and entry points (browsers, *app stores*, AI agents, etc.). Requiring all service providers to comply with universal choices is therefore technically unfeasible. Defining these choices could lead to intractable debates regarding the necessary level of granularity for the consent interface, the various purposes, the definition of consent validity, which should apply across the entire value chain, or the management of consent conflicts (e.g., a user refuses data collection on their connected device but not on their computer).

Users generally prefer to make choices for each individual service rather than through browser-level mechanisms. This allows for a clearer context, greater transparency, better control, and ultimately more trust.
Conversely, centralized consent mechanisms provide less visibility and control over which organizations can process the data.

Finally, centralized consent would contradict the principle that valid consent must be specific, purpose-bound, and associated with clearly identified processing operations in order to allow users to make informed and autonomous choices for each processing purpose.
Rather than changing how consent can be given, a better approach would be to ask users for consent only for the most intrusive activities.

Centralizing user choice at the browser level is therefore a false solution and would pose a dual risk to the European ecosystem: by automating user choices at the system level, this mechanism will inevitably dry up the advertising revenue that funds the press and free content publishers. The direct and immediate consequence will be a proliferation of paywalls across all websites that have no other means of financing themselves.
Consequently, the proposed mechanism will have a severe impact on the European economic fabric, particularly SMEs and e-commerce businesses, whose growth, visibility, and customer acquisition rely heavily and increasingly on online advertising.

Furthermore, Article 88ter will automatically drive the flight and concentration of advertising budgets toward closed environments (*walled gardens*). These platforms, which rely on ecosystems of logged-in users, will be immune to these signals, thereby completely distorting competition to the detriment of the open Internet.

Rather than fixating on the form (how centralized consent is collected), lawmakers must shift their paradigm and focus on the substance (*what* consent covers). We must move beyond the current binary logic by adopting a genuine risk-based approach, which involves exempting minimally intrusive processing from the consent requirement.
The inclusion of clear exemptions for contextual advertising and its essential technical operations (audience measurement, capping, and fraud prevention) would achieve a dual objective: drastically reducing the daily display of banners while actively encouraging companies to switch to these privacy-respecting models. This pragmatic approach is, in fact, the solution formally supported and recommended by the joint opinion of the European Data Protection Boards (EDPB/CEPD).

3.3 - Harmonization of Administrative Procedures

Currently absent, the unification of administrative procedural law would represent real progress. Today, companies must navigate 27 different litigation procedures. This fragmented landscape is a serious obstacle for pan-European players and does not foster the emergence of European players capable of competing with their American or Chinese counterparts.

3.4 - Centralized governance

The absence of a truly strong, single European regulator for cross-border players leaves in place a complex “one-stop shop” system that is showing its limitations. With the strengthening of the EDPB’s powers, “a shared foundation common to all organizations” should be considered. This point should be considered in conjunction with the discussion above regarding the EDPS.

Conclusion

The European Commission’s attempt to amend the GDPR as adopted in 2016 and implemented in 2018, to simplify certain provisions, clarify and ease certain obligations, and take into account a rapidly evolving digital landscape, is an initiative welcomed by stakeholders, particularly businesses that rely on personal data to operate.

These stakeholders do not wish to revisit certain obligations imposed by the GDPR, given that they have already implemented procedures, revised their contracts, and organized compliance with the regulation. For example, seeking to limit the maintenance of a record of processing activities to a specific threshold of employees seems unnecessary, given that it serves as a tool for a data controller to monitor compliance across its chain of processors.

On the other hand, they wish for certain measures, which, upon implementation, resemble highly administrative procedures or obligations that in some cases prove very difficult, if not impossible, to comply with, to be reexamined in light of a highly competitive international context now marked by widespread digitization and the use of artificial intelligence tools.
Admittedly, it may seem bold to seek to modify the definition of personal data, given that this definition governs the application of personal data protection principles. But how can progress be made on this issue when, on the other hand, neither the EDPS nor the data protection authorities are proposing practical, effective solutions within timeframes compatible with the reality of an economic and competitive environment that is constantly accelerating?

And the argument often raised, that we must preserve a European model that respects individual rights and freedoms, no longer necessarily holds water when we see, in practice, the relentless insistence on requiring stakeholders to comply with data protection measures that are impossible to implement and therefore meaningless, unless we want to block their projects.

The very meaning of personal data protection must be rethought (rediscovered?) to preserve its spirit and adapt it. This draft digital omnibus bill is an opportunity to be seized to move forward. ❐

la vi//a .
numeris

*unlock the future, make it human**

hello@lavillanumeris.com
+33 7 80 96 11 11
http://www.lavillanumeris.com

**libérez l'avenir, rendez-le plus humain*