Alliance Digitale

Position Paper on the upcoming Commission evaluation report on the GDPR

Summary

- Since 2018, the GDPR benefited the society as a whole in particular with regards to increased transparency and trust between citizens and economic actors, as well as better management and governance of personal data.
- However, there is room for improvement in many areas such as harmonization, interpretation by different national Data Protection Authorities ("DPAs"), or simplification of procedures.
- Alliance Digitale shares the Council's conclusions dated November 17, 2023, regarding the application of the GDPR[1], particularly concerning the burden imposed on Small and Medium Enterprises ("SMEs") and Intermediate-Sized Enterprise ("ETIs") to comply with the GDPR, clarifying the status of pseudonymized data, and the necessary alignment of the regulation with the EU's recent digital initiatives.
- Alliance Digitale shares **nine concrete proposals to amend or adapt the GDPR to difficulties, constraints, and uncertainties faced by the digital marketing sector**.

1. Simplifying procedures and constraints associated with the GDPR compliance
    - **Exempting small companies which do not process sensitive data from the obligation to maintain a record of processing activities** to avoid hindering their economic development.
    - **Clarifying which data are covered by the exercise of rights in a code of conduct**, thus establishing a market standard benefiting all stakeholders.
2. Adapting the GDPR to new technological challenges and innovations
    - **Developing guidelines and opinions through the EDPB on the relationship between the GDPR and AI** to clarify applicable rules and prevent diverging national interpretations by DPAs.
    - **Distinguishing the risk level associated to anonymized and pseudonymized data, through detailed EDPB guidelines** as requested by the EU Council in order to remove prejudicial legal uncertainties for the entire sector**.**
3. Strengthening and harmonizing the governance of the GDPR at both French and European levels
    - **Strengthening the role of EDPB to allow the emergence of a true European independent authority responsible for the GDPR** in order to better harmonize decisions at the European level and avoid damaging national initiatives.
    - **Proposing a better articulation between privacy (e-Privacy directive) and personal data (GDPR) issues** by distinguishing the authorities responsible of ePrivacy and the GDPR, especially in France.
    - **Mandating the anonymization of actors targeted by injunction procedures** led by the CNIL to avoid associated damages.
    - **Reverting to a risk-based approach as initially envisaged by the GDPR**, particularly regarding data transfer and inference issues, to avoid "overprotection" for market players.
    - **Fostering the advisory role of Data Protection Authorities (DPAs)** for professionals and consider documents exchanged as covered by trade secrets by default.

[1] Position of the Council of the European Union - 17 November

Since its implementation in 2018, the General Data Protection Regulation (GDPR) has benefited the society at large. By clarifying the regulatory framework for personal data, the regulation has fostered increased transparency and trust between citizens and economic actors. GDPR compliance translated in substantial investments on the part of economic actors, which in turns enable better management and governance of personal data. Furthermore, many subsequent international laws and standards have used the GDPR as both an inspiration and a model highlighting the EU's pioneering role in this regard.

However, there is room for improvement to reach better harmonization, interpretation by various national Data Protection Authorities ("DPAs"), and simplification of procedures. Alliance Digitale thus aligns with the Council's conclusions on the application of the GDPR dated November 17, 2023[2], especially concerning the compliance burden imposed by the GDPR on small and medium-sized enterprises ("SMEs") and intermediate-sized enterprises ("ETIs"), clarification of the status of pseudonymized data, and the necessary alignment of the regulation with the EU's recent digital initiatives.

With this position paper, Alliance Digitale, representing the digital marketing sector in France and nearly 250 diverse businesses, aims to present its recommendations focusing on three objectives:

1. Simplifying the procedures and constraints associated with the GDPR.
2. Adapting the GDPR to new technological challenges and innovations.
3. Strengthening and harmonizing the governance of the GDPR at both French and European levels.

I. Simplifying Procedures and Constraints Associated with the GDPR

Exempting Small Businesses from Record-Keeping Requirements

The Council believes the burden imposed by certain provisions of the GDPR on SMEs and startups is at times too important and a challenge for small companies. In its conclusions, the Council thus encourages the development of practical tools and calls on the EDPB to enact targeted guidelines on the obligation to maintain records of processing activities. This core is a priority for both France and Germany which are jointly advocating for "adjustments [to the GDPR] to effectively relieve SMEs and startups from the obligations to provide information, documentation, and proof of compliance."[3]

The GDPR applies indiscriminately to all economic actors. Some small companies, including SMEs or startups facing disproportionate obligations even though their main activity is not the processing of personal data and/or the processing of directly identifying data. The exemption outlined in Article 30.5 of the GDPR is often interpreted restrictively by DPAs, resulting in an actual obligation to maintain records of processing activities.

Record-keeping (such as processing records, privacy policies, etc.) requires significant human, financial, and legal resources. Seeking external counsel or hiring an internal specialist comes with substantial costs. Additionally, companies face a profound inequality between what a very large enterprise and a startup can bear for the same violation especially when fines are imposed by DPAs.

> Our proposal
>
> Introduce a principle of proportionality by exempting startups and small and medium enterprises with fewer than 50 employees from maintaining records of processing activities and remove the term "occasional" from paragraph 5 of Article 30 of the GDPR. As specified in the same Article 30, this exemption would not apply if the processing they carry out is likely to result in a risk to the rights and freedoms of the data subjects.

[2] Position of the Council of the European Union - 17 November
[3] Réduire la bureaucratie en ces circonstances sans précédent - Papier franco-allemand sur le « mieux réguler » et la modernisation de l'administration en Europe - 12/10/2023 - Lien

Addressing uncertainties associated with the exercise of rights of the data subjects

The exercise of rights by individuals is a cornerstone of data protection law to which Alliance Digitale is committed. However, we would like to draw your attention to several crucial points:

1. Responding to a request for the exercise of rights by a data subject regarding its personal data is costly: Alliance Digitale members estimate that responding to any single request would cost a minimum of around 300 euros. Some companies, especially smaller ones, would therefore be unable to respond to several simultaneous requests, as is the case for certain actors in the sector.
2. The type and extent of the data to provide is sometimes significant, with no real benefit for the user: In the absence of clear guidelines on the type and extent of data to provide as well as the limits of this right of access, companies provide all available data, mostly without real added value for the user. However, the extraction, processing, and reworking of this data involves significant resources. This observation is reinforced in cases where companies only deal with pseudonymized data that they cannot reidentify themselves. Some companies are thus forced to provide data including information covered by trade secrets law, such as correspondence tables linking data from different operators. Conversely, when companies choose to limit themselves to reasonable and useful data from the user's perspective or protect their confidential data, they face damaging legal uncertainty.
3. Identity verification is complex, and its application is uncertain: A majority of digital marketing and online advertising actors use pseudonymized personal data in their activities (cookies, universal identifiers, etc.). When an individual exercise its rights of access to personal data, the company must request an identity document and the cookie identifier before providing the data. But this procedure which is necessary to verify identity and ensure that data is not transmitted to an unauthorized third party is disputed and has led to procedures and fines, such as the CNIL's decision in 2023 against Criteo. The authority believed that this request violates the imperative of easy access to data. This double constraint puts actors in the sector in a legally untenable situation.

> Our proposal
>
> Clarify in a code of conduct the extent and type of personal data that should be submitted when an individual exercise his/her right to access.. This would allow the emergence of a standard for the exercise of rights regarding personal data, benefiting all stakeholders, be them individuals or companies. A clear framework will allow an effective use of these rights by individuals.
>
> Finally, it is necessary to clarify the conditions of the right of access to pseudonymized data. Given the non-identifying nature of this data, we believe that this data should be explicitly excluded from the scope of Article 11 of the GDPR

II. Adapting the GDPR to New Technological Challenges and Innovations

Specifying the Applicable Framework of the GDPR in the Field of Artificial Intelligence

The GDPR should be adapted to emerging technologies and new uses of data. Yet the regulation implemented in 2018 does not fully integrate the challenges posed by artificial intelligence and is also out of sync with the general evolution of the digital marketing sector. For instance, stakeholders question the necessity of seeking consent for each reuse of data intended for training a model.

On this matter, Alliance Digitale aligns with the Council's conclusions and urges the adoption of guidelines at the European Union level to better align the GDPR with challenges and opportunities posed by new technologies and provide for a clear articulation between the GDPR and new legislations in the digital realm, especially with the AI Act.

Our proposal

Align the GDPR with new opportunities offered by the use of artificial intelligence and specify the applicable rules on:

- Limitation of purposes for the processing of personal data;
- The legal basis, with a particular emphasis on the legitimate interest vis-à-vis consent;
- The principle of data minimization that restricts data collection for training purposes;
- Limitation of the retention period which diminishes training opportunities.

In this regard, Alliance Digitale aligns with the Council's recommendations and advocates for guidelines and opinions from the EDPB on the interplay between the GDPR and the AI Act. This will provide for a harmonized interpretation at the EU level and decreases the risk of fragmented interpretation by DPAs at nation level.

Adapting the GDPR to sector-specific and technological practices, particularly concerning pseudonymization

The digital marketing sector has long called for a better understanding and consideration of pseudonymization techniques, which are still not well understood by Data Protection Authorities (DPAs). In this regard, Alliance Digitale agrees with the Council's conclusions to request for a clarification on the requirements related to anonymization and pseudonymization.

Profiling for advertising purposes is primarily based on individualized yet non-identifying data, known as pseudonymized data. This requires significant efforts from industry players to protect users' privacy. Despite these efforts, individualizing and identifying data are still apprehended indiscriminately by authorities even though these types of data are fundamentally different. Considering the existence of a decryption key and the theoretical possibility of reidentification, authorities such as the CNIL associate the same level of risk to these data as if they were directly identifying. In 2023, the CNIL fined Criteo and did not consider the pseudonymization of data as a mitigating circumstance[4].

The DPA does not distinguish between these data even though the matching table allowing reidentification is often not in the possession of the company holding the data or its clients and partners. This lack of risk gradation is particularly damaging to our sector and other economic sectors that innovate and work towards better privacy protection.

The approach adopted by the General Court of the Court of Justice of the European Union ("CJEU") in April 2023[5], advocating for a distinction of pseudonymized data, shows a way forward on this issue. In its judgment, the CJEU concluded that pseudonymous data is anonymous when those who hold it do not have legal and reasonable means in practice to access the information necessary for reidentification.

Our proposal

Distinguish between anonymized and pseudonymized data in detailed guidelines from the European Data Protection Board (EDPB), as requested by the Council. It is crucial for Alliance Digitale that the level of risks (and consequently obligations) associated with these data be adjusted based on the actual possibilities of identification.

[4] Publicité personnalisée : CRITEO sanctionné d'une amende de 40 millions d'euros - CNIL - Juin 2023 – Lien.
[5] TUE, n° T-557/20, Arrêt du Tribunal, Conseil de résolution unique contre Contrôleur européen de la protection des données, 26 avril 2023 - Lien

III. Strengthening and harmonizing the governance of the GDPR at both French and European levels

Clarifying the status of national authorities and establishing an independent European authority with a genuine regulatory role

The increasingly central position occupied by the CNIL in France is a source of uncertainty for the entire online advertising sector. Beyond its legitimate role as a Data Protection Authority (DPA), the CNIL also assumes a regulatory function that complicates its relationships with the market. The CNIL addresses issues – such as recently on email pixels or mobile applications – without necessarily waiting for harmonization at the European level. These practices weaken the aspirations for rule harmonization within the single market and create a certain legal uncertainty and instability. Moreover, they tend to create national barriers in the market that lead to significant competitive imbalances depending on the country of establishment of companies.

Furthermore, the CNIL is one of the 12 national authorities in Europe (out of 27 in total) that addresses both GDPR and privacy-related topics (e-Privacy Directive). Thus, the CNIL interprets certain GDPR concepts through the lens of the e-Privacy Directive and vice versa even though their scope is different. Two examples illustrate these difficulties:

- In France, the CNIL decided that the one-stop-shop mechanism under the GDPR does not apply to matters covered by the e-Privacy Directive to assert its jurisdiction over companies not headquartered in France. Nevertheless, the CNIL enforces matters covered by the e-Privacy Directive based on the GDPR when acting as the lead supervisory authority;
- In Belgium, the APD handled a case related to the e-Privacy Directive based solely on the provisions of the GDPR, as it did not have competence over the directive at that time.

Finally, we observed that the CNIL sometimes uses warnings against sector actors as a communication tool to the detriment of the targeted actor. The name of the company is sometimes revealed leading to unjustified harm, especially for small actors, even if the impact of the company's actions on the fundamental rights and freedoms of individuals is limited or non-existent (as is often the case in advertising).

> Our proposals
>
> 1. Strengthening the role of the EDPB to enable the emergence of a true independent European authority responsible for the GDPR in order to better harmonize decisions. The objective would be to standardize decisions at the European level, avoid purely national initiatives, and ensure that national authorities do not exceed the requirements enshrined in the GDPR.
> 2. Proposing a better articulation of privacy issues (e-Privacy Directive) and personal data (GDPR) and distinguishing the authorities responsible for each domain.
> 3. Requiring anonymization of actors targeted by warnings issued by the CNIL to prevent associated harms.

Developing the advisory role of professionals by national authorities and ensuring the confidentiality of information exchanged within this framework

The advisory role of the CNIL to professional actors is essential to ensure an interpretation and application of the GDPR that is adapted to the specificities of each professional sector. However, this mission is hindered both by the lack of resources at the CNIL to develop it and by the absence of confidentiality for exchanges and documents that can be transmitted to the CNIL on this occasion. The exchanges and documents transmitted are subject to the right of access to administrative documents provided for by the Code of Relations between the Public and the Administration, including within the framework of the prior consultation procedure provided for by Article 36 of the GDPR. This situation dissuades many companies from making requests for advice to the CNIL out of fear that certain confidential information provided for the purpose of obtaining some advice by the DPA is subsequently disclosed.

Our proposals:

- Encourage national authorities to develop their advisory role for professionals.
- Consider by default that documents exchanged in this context are covered by trade secrets (especially the Impact Assessment related to Data Protection and risk analyses produced by professionals) and therefore not communicable to the public despite their administrative nature

Reverting to a risk-based approach in regulating personal data to avoid over-caution on the market

Due to uncertainties surrounding the management and processing of personal data, online advertising actors adopt an "over-precautionary" approach that hinders market development. Here are two examples:

- Data transfers to third countries, especially the USA: Authorities now seem to rely more on potential violations regarding data transfers to third countries than on actual observed violations. The interruption of international data flows is not sustainable, and the level of legal uncertainty is high for companies, even if they act in good faith and within the framework of European decisions.
- Indirectly sensitive data and the issue of inference: Many actors refuse to respond to certain requests from their clients because access to and processing of certain data could lead to the deduction of new information that would be sensitive or identifying. For example, data on eating habits can lead to data related to religion, health status, or income level.

Our proposal

Alliance Digitale advocates for a return to a risk-based approach as initially provided in the GDPR regarding the use and processing of personal data, particularly concerning issues of transfers and inference. We believe that this approach has gradually been abandoned in favor of an overly protective stance, even when the actual level of risk does not always warrant it.

In addition, we wish to debunk the increasing tendency of DPAs to consider consent as the primary guarantee for privacy protection. Indeed, the GDPR does not establish a hierarchy among the legal bases outlined in Article 6 and does not specify that profiling should "principally" rely on consent. In this regard, we align ourselves with the expert report to the European Commission, "A competition policy for the digital era,"[6] which contends that legitimate interest fosters innovation and competition without diminishing the level of data protection.

Finally, we believe that a collaborative effort led by the European Commission to ensure interoperability of privacy protection frameworks with non-EU countries would be particularly beneficial. This could align with the "Data Free Flow with Trust" initiative promoted by the G7 under the Japanese presidency in 2019.

[6] Commission européenne, Direction générale de la concurrence, Montjoye, Y., Schweitzer, H., Crémer,J., Competition policy for the digital era, Publications Office, 2019, Lien