IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

*Brussels, 25 January 2024*

# Executive Summary: IAB Europe's Response to the European Commission's GDPR Multistakeholder Expert Group Questionnaire for the 2024 Report

This executive summary outlines IAB Europe's response to the European Commission's GDPR multi-stakeholder expert group questionnaire for the 2024 report on the application of GDPR. As the European-level association for the digital advertising and marketing ecosystem, IAB Europe (Transparency Register: 43167137250-27) underscores several priority issues requiring attention under the GDPR. These include the imperative for more consistent application of data protection laws, enhanced education and awareness about the GDPR, and the necessity to support research and development into innovative data protection technologies by better applying the risk-based approach.

1. To promote a **more consistent application of the GDPR**, we advocate for aligning national rules and harmonising domestic procedures among Member States. This approach aims to address inconsistencies, prevent duplicative actions, and alleviate administrative burdens on local courts and companies dealing with multiple claims on the same matter. We emphasise the need to avoid divergence in interpreting the GDPR between Data Protection Authorities (DPAs) and national courts during civil proceedings.

2. Most importantly, **we argue against ruling out the choice of legal bases a priori**. Instead, we propose a case-by-case assessment, accompanied by clear guidance applicable across the EU that does not disproportionately restrict digital businesses and is applicable across the EU.

3. In refining **GDPR concepts**, we recommend additional guidance to clarify specific definitions, including the interpretation of 'unlawfully processed data'. We stress the importance of aligning enforcement actions with the principle that **joint responsibility does not imply equal responsibility**. This entails delineating clear responsibilities between joint data controllers to avoid placing disproportionate expectations on individual companies.

4. We advocate for the **improved functioning of DPAs** through enhanced personnel training and increased communication with the industry. Additionally, we highlight concerns about the **zero-risk approach by DPAs**, which contradicts the concept of appropriateness and hinders the development of anonymisation techniques.

5. Regarding the EDPB Guidelines, IAB Europe suggests an **improved consultation process** to ensure comprehensive stakeholder input, including from business associations, before

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

the initial draft is produced. Furthermore, in the context of Codes of Conduct (CoC), we **recommend a simplified drafting process**, active DPA engagement in code development, and the recognition of tools like **IAB Europe's Transparency & Consent Framework (TCF)** as a transnational GDPR Code of Conduct. This approach would offer substantial compliance benefits to consumers and the industry, fostering improved market coverage and a streamlined user experience, particularly in inherently transnational sectors such as digital advertising.

6. IAB Europe encourages striking a **balanced approach between data protection and innovation,** considering the diverse impacts of technologies on user privacy. We stress the importance of a meticulous assessment and articulation of the GDPR's interaction with laws like the AI Act, DSA, DMA, and Data Act, without necessitating the reopening of the GDPR.

Our response is rooted in the lessons learnt by our members while striving to comply with GDPR rules. It underscores the need for a consistent application of the GDPR in the EU and clearer guidance from data protection enforcers. Finally, we express our commitment to an ongoing dialogue on GDPR enforcement with policymakers to serve the interests of both businesses and consumers.

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

# IAB Europe's response to the European Commission's questionnaire on the application of the General Data Protection Regulation (GDPR)

## I. General Comments

The GDPR adoption was a substantial milestone, establishing the principles of data protection for the whole EU economy, and indeed explicitly, in the digital advertising context.

IAB Europe's members have invested material, time and resources to ensure that their services meet GDPR requirements. This document pulled out some lessons learnt from our efforts to comply with the EU data protection rules.

In our view, the following priority issues need to be addressed under the GDPR:

- The need for more harmonised data protection laws across the EU.
- The need for more education and awareness about data protection rights and responsibilities.
- The need to support research and development into new data protection technologies and solutions by better applying the risk-based approach.

By addressing these priority issues, we can continue to improve the protection of personal data in the digital age. This is key to delivering on the initial objective of the GDPR to support innovation and investment in the EU's digital economy to the benefit of EU consumers and businesses

<u>A more consistent interpretation of the rules</u>

The initial ambition of the GDPR was to achieve consistent and homogenous application of the rules on the protection of natural persons concerning the processing of personal data and the free movement of such data. However, this has fallen short and resulted in instability and uncertainty. Across the EU, the industry faces diverging interpretations of GDPR concepts.

The new GDPR procedural regulation is a positive step towards harmonising cross-border procedures but falls short of achieving harmonisation within the EU. In particular, as private litigation increases, so does the risk of discrepancies between DPAs' interpretation and implementation of GDPR by civil courts in damage claim lawsuits. The risk is even higher when the lead DPAs and the civil court are not located in the same country.

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

We advocate for harmonising regulations and ensuring a uniform interpretation of GDPR concepts to strengthen law enforcement. To support this, we suggest:

- Ensuring consistent interpretation of the GDPR across Europe.
- Providing guidelines to handle new technical or business models in a legally secure manner throughout the EU

Creating a unified privacy and data protection regime at the EU level would benefit both consumers and businesses, aligning with the broader objective of establishing a single European data market space.

## II. Data Subjects Rights

**Privacy-by-design vs user protection**

There is a continuous conflict between implementing privacy-focused measures like pseudonymisation and access to information necessary to identify data subjects for addressing rights requests and reducing security risks. Data Protection Authorities overlook the safety and security obligations related to data subject rights, making compliance challenging for businesses.

**Recommendation**: The GDPR needs clearer guidelines on the scope of Article 11 of the GDPR, especially regarding security-related data processing and identity verification.

**Access to data (Article 15)**

The 'right to access data' faces challenges due to its undefined scope. Interpretations influenced by court decisions and DPA guidance lead to broad access requests. This leads to a high regulatory burden for companies often resulting in highly technical and non-user-friendly information. Additionally, there is ambiguity over the vague concept of 'manifestly unfounded or excessive' requests.

**Recommendation**: We suggest excluding certain technical details from accessible information to users and promoting scalable solutions like transparent privacy policies to streamline GDPR compliance at scale.

**Erasure (Article 17)**

The challenges in implementing erasure rights are centred on determining unlawfulness and dealing with complexities related to the reuse of data. The concept of 'unlawfully processed' data is unclear, making it difficult for controllers to determine the legality of their data practices. This involves a complex balancing test between freedom of expression and information and data subjects' rights, creating uncertainty.

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

**Recommendation**: We propose additional guidance to clarify 'unlawfully processed' data and recommend reviewing the EDPB's limiting stance on legal bases to only one. This revision aims to enhance flexibility in data reuse, ensuring alignment with technological advancements.

**Data portability (Article 20)**

Data portability under Article 20, poses challenges in two key areas. Firstly, there is a lack of clarity about the originating service's responsibility in evaluating potential destinations for service-to-service data transfers. Secondly, the GDPR lacks explicit standards or guidelines for such transfers, emphasising the need for clearer criteria.

**Recommendation:** Provide guidelines for data transfer between services, addressing the absence of clear criteria in the GDPR and clarifying the responsibility of the originating service in evaluating potential destinations for service-to-service data transfers.

**Tools or user-friendly procedures to facilitate the exercise of data subject rights**

Despite significant investments by industry players to provide accessible privacy controls, there remains a challenge as users frequently opt for non-automated methods over controllers' self-service tools for data subject requests. Controllers also struggle with addressing complaints unrelated to GDPR user rights.

**Recommendation:** DPAs should require complaints to be made in good faith, exhausted through internal procedures, and specifically concerning GDPR-defined personal data processing during their assessments.

**Exercise of Data Subject Rights by Children**

Under the GDPR, data subjects, including children, have rights regarding their personal data.

**Recommendation:** We suggest clarifying the uncertainties regarding the extent of parental authority to exercise these rights on behalf of their children.

## III. Use of representative actions under Article 80 GDPR

There is an increased use of Article 80 GDPR due to collective redress mechanisms. The representative actions should ensure that litigation prioritises protecting individuals' rights over financial gains for lawyers.

**Recommendation:** We suggest harmonising domestic procedures among Member States to address inconsistencies, prevent duplicative actions, and alleviate administrative burdens on local courts and companies arising from multiple claims under Art. 80 GDPR on the same matter.

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

## IV. Experience with Data Protection Authorities (DPAs)

**Experience in obtaining advice from DPAs**

The GDPR is designed to be a regulation that remains relevant in the face of evolving technologies and trends. However, challenges persist in some DPAs' understanding of emerging technologies, vital in today's swiftly evolving digital landscape.

Several DPAs appear reluctant to collaboratively engaging with industries, particularly in offering practical advice for broad compliance efforts. Another challenge for companies is the lack of a formal process for engaging with DPAs. Some Data Protection Authorities (DPAs) limit discussions on innovation by preferring to give oral advice through trade associations. Meanwhile, the current regulatory sandboxes are inadequate in meeting industry needs.

**Recommendation:** Enhancing the knowledge and capabilities of DPAs' personnel through appropriate resources and training as well as increasing communication with industry could facilitate a more comprehensive understanding of the evolving landscape and the dynamics of personal data processing within it.

**Guidelines adopted by the EDPB supporting the practical application of the GDPR**

The process preceding EDPB guidelines publication lacks transparency and stakeholders' involvement. The selection and scope of new guidelines lack explanatory details, and the absence of preliminary stakeholders' consultations limits the guideline's adaptability to technological and commercial developments. Moreover, the non-binding nature of EDPB guidelines for DPAs results in diverging interpretations across jurisdictions, including reliance on said guidelines in enforcement proceedings against companies, thereby hindering harmonisation and impeding companies' reliance on these guidelines for compliance.

**Recommendation:** Article 70(4) of the GDPR outlines a consultation process, yet it should be improved to ensure comprehensive stakeholders' input, including from business associations ***before*** the first draft of the guidelines is produced. Guidelines should not be used in enforcement proceedings.

**DPAs' guidance**

National DPAs have updated their guidance on the interplay between GDPR and ePrivacy's directive, impacting digital advertising. However, diverging interpretations of valid consent conditions create legal uncertainty, which prevents the industry from adopting an EU-wide approach to GDPR compliance. In addition, the broad interpretation of the ePrivacy directive that requires consent tends to undermine the choice of legal bases in Article 6 of the GDPR for any other downstream processing activity.

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

Inconsistencies persist in defining 'freely given' consent, especially concerning 'pay-or-consent walls' for revenue generation, leading to contrasting stances among DPAs. There is uncertainty about using legitimate interests for data processing within the digital advertising sector, as some local interpretations disqualify this legal basis, such as the Dutch DPA that considers that commercial interests cannot constitute legitimate interests, contrary to the intentions of the EU co-legislators.

All companies in the broad digital advertising ecosystem - advertisers and advertising agencies on the buy side, news publishers and other ad-funded sites and online services on the sell side, and technology providers serving both sides - have clear economic and consumer satisfaction interests in the collection and processing of non-sensitive personal data (often in the form of pseudonymous data) for various purposes such as contextual advertising or audience measurement. The ability to leverage the legitimate interest legal basis cannot be excluded where adequate transparency (Art. 5(1)(a) GDPR), case-specific balancing tests (as required by Art. 6(1)(f) GDPR), and the user's right to object (Art. 21 GDPR) are implemented.

**Recommendation:** We contend that the choice of legal bases should not be ruled out a priori but depends instead on an assessment of the specific situation at hand, and supplemented by clear guidance that does not disproportionately restrict digital businesses and is applicable across the EU.

## V. Experience with accountability and the risk-based approach

The risk-based approach is one of the guiding principles of the GDPR. The right to the protection of personal data is not absolute but has to be weighed against the rights and freedoms of other third parties, such as the legitimate interests of data controllers. (see recital 4 of the GDPR) This is often disregarded and should be more clearly enshrined in the GDPR.

### The Implementation of the Principle of Accountability

The GDPR established accountability as a key principle for self-assessment and documentation of data processing compliance by companies. The introduction of the accountability principle aimed at fostering a data protection strategy that promotes risk management. The implementation of GDPR has led DPAs to avoid giving practical advice or legal support, citing the accountability principle. Despite expectations that codes of conduct and certification would streamline GDPR compliance, companies face challenges such as limited flexibility and a lack of dialogue with DPAs.

It leaves companies with no legal certainty that the approach they have taken in terms of risk assessment will be accepted by their DPA in case of investigation. This is particularly the

case in situations where companies are considered jointly responsible with other companies for a given processing operation. DPAs artificially amplify the scope of data controllers' accountability obligations in their enforcement action as a means to hold companies responsible for ensuring compliance with all GDPR requirements associated with the data processing at stake without delineating responsibilities between each joint data controller.

**Recommendation:** We suggest aligning enforcement actions with the principle that joint responsibility does not equate to equal responsibility. This involves delineating clear responsibilities between each joint data controller, avoiding disproportionate expectations on individual companies. Such a revision in the approach would provide legal certainty to companies, encouraging them to invest in proportionate technical and organisational measures for compliance with the General Data Protection Regulation (GDPR).

**Pseudonymised data vs. personal data**

As highlighted in this document, interpreting the GDPR in the EU poses uncertainties, particularly regarding the broad definition of personal data. This has resulted in court cases questioning whether pseudonymised data should be classified as personal data.

- A recent ruling by the General Court of the European Union (EGC) in the case Single Resolution Board v European Data Protection Supervisor, clarified that pseudonymised data sent to a recipient is not considered personal data if the recipient cannot re-identify the individuals. However, it is noted that pseudonymised data can still potentially link to individuals through separately stored information, requiring consideration under GDPR Recital 26.

- The EGC decision aligns with the ECJ's Breyer case, emphasising that the data recipient's perspective matters in determining whether pseudonymised data qualifies as personal data. If the recipient lacks the means to re-identify individuals and legal access to such information, the transferred data is not personal data from the recipient's viewpoint, even if the sender has the means to re-identify.

These rulings show that the capability of the data provider to re-identify individuals does not automatically classify the data transferred as personal information for the recipient. This challenges the prevailing overly broad interpretation of personal data, and we believe this should be promptly considered in the ongoing review of the GDPR.

**Recommendation:** This zero-risk approach by DPAs contradicts the concept of appropriateness and hampers the development of anonymisation techniques. Additionally, DPAs often overlook these companies' efforts using pseudonymisation techniques, impacting enforcement decisions. To counter that, we suggest creating a distinct data

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

category for pseudonymised data to provide a better acknowledgement of companies' efforts in risk mitigation.

## VI. International transfers

We appreciate the Commission's interest in understanding the industry's experience with tools for international data transfers. However, these tools do not effectively address fundamental concerns regarding legal uncertainties in international data transfers. The Commission's requirements add complexity, creating challenges for businesses seeking clarity in data transfers.

**Standard Contractual Clauses for international transfers**

The Standard Contractual Clauses (SCCs) provide certainty to businesses and allow them to plan their international transfers and align their operations accordingly. The CJEU's judgement C-311/18 (Schrems II) rendered Standard Contractual Clauses (SCCs) less reliable and insufficient for international transfers. GDPR enforcement has not fully addressed concerns about data transfers' legal uncertainties, particularly regarding government access in third countries. Additional measures, such as Transfer Impact Assessments (TIAs), are now required for SCCs, adding complexity to transfers.

**Recommendation:** Businesses require a comprehensive and clear approach to international data transfers to ensure certainty and effective use of tools like SCCs.

**Countries with which the Commission should work to facilitate safe data flows**

**Recommendation:** We urge the Commission to collaborate with other global actors to align on how to develop stronger interoperability between European data flow systems and other systems like the Global Cross-Border Privacy Rules. Several countries should be considered for closer cooperation such as the United States, but also, other markets including India, Australia, Indonesia, Singapore and South Africa.

## VII. National implementation of the GDPR & fragmentation/use of specification clauses

Fragmentation is observed in various areas of GDPR implementation, notably in the interpretation of consent requirements and the definition of data controller responsibilities, creating challenges for industry compliance. Other examples of fragmentation are the discrepancies that arose in Germany regarding the voluntary nature of consent under the TTDSG, lacking uniformity in interpretation and organisation, and impacting the digital economy.

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

Inconsistencies persist in transparency standards set by supervisory authorities and initiatives like the Cookie Pledge, highlighting differing approaches to user consent information.

Other discrepancies include variations in minimum age requirements and interpretations of GDPR concepts like personal data, anonymization, and legal bases across Member States.

**Recommendations:** It is necessary for the well-functioning of the internal market and companies that national rules align within the boundaries established by the GDPR. Introducing additional requirements should only occur when permitted and necessary, avoiding unnecessary constraints on businesses.

Additionally, divergence should be avoided in the interpretation of the GDPR between DPAs and national courts in the context of civil proceedings. National courts should consider the prior findings of DPAs in their legal assessment

## VIII. Codes of Conduct

### Use of Codes of Conduct

DPAs predominantly prioritise enforcement actions and penalties rather than exploring alternatives, such as codes of conduct under the GDPR to enhance business compliance. Codes of Conduct, encouraged by Article 40 of the GDPR, hold promise in providing clarity on GDPR application within specific industries or sectors.

Despite their potential to significantly improve compliance, the development of codes is resource-intensive and time-consuming, offering no legal safe harbour to organisations. Consequently, the incentive to create codes remains weak, resulting in few developments since 2018. We emphasise the need for prioritising this compliance approach, especially for transnational codes that mirror the GDPR's harmonisation.

**Recommendation:** Recognising tools like IAB Europe's Transparency & Consent Framework (TCF) as a transnational GDPR Code of conduct would offer substantial compliance benefits to consumers and the industry, fostering improved market coverage and a streamlined user experience, particularly in inherently transnational sectors such as digital advertising.

### Challenges in the developing and approving of Codes of Conduct

IAB Europe's TCF increases transparency, choice and accountability concerning how personal data is processed by different actors in the digital sector and can be used as an enabler of effective compliance by DPAs. The TCF was proactively introduced and presented to a number of DPAs but was subsequently the subject of an enforcement action by the Belgian DPA.

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

Rather than engaging in a constructive dialogue, the Belgian DPA took an overly broad and flawed interpretation of the concept of data controller to bring an enforcement action against IAB Europe. Although the case has been referred to the Court of Justice of the European Union for a preliminary ruling, the question arises as to how industry associations can develop codes of conduct for their sector if it brings their members no legal comfort and the associations themselves can be deemed joint-controllers for the processing operations the code of conduct aims to cover.

Similarly, there are other examples of pending codes like pseudonymisation and ongoing discussions in France that have stalled, hindering sector-specific GDPR compliance efforts. The lack of DPA assistance in implementing GDPR-compliant solutions for specific sectors is apparent.

**Recommendation:** Codes of Conduct are essential for legal certainty in areas like international transfers, transparency, and accountability, fostering trust and aiding compliance. Simplifying the code drafting process and providing legal assurance for signatory organisations is crucial. DPAs should actively engage in code development, allocate resources, and collaborate with industries instead of unilateral guideline drafting. In addition, timely approval and strong regulatory guidance for Codes of Conduct are critical to incentivise their development and adoption.

## IX. Certification

Similarly, to other tools, certification mechanisms, recognised under the GDPR, have not been commonly adopted at the EU level.

**Recommendation:** Supporting the wider adoption of these certification mechanisms that can enforce appropriate safeguards when coupled with mandatory commitments.

## X. GDPR and innovation / new technologies

**GDPR vs. Innovation and New Technologies**

The GDPR was anticipated to be future-proof, aiming for a technology-neutral, pragmatic, and risk-based approach, fostering innovation. However, we observe that GDPR compliance hinders product development and innovation within the EU, leading companies to launch new products outside the EU first due to time-consuming risk assessments and compliance requirements. The GDPR's rigid interpretation by DPAs, lacking flexibility, has deterred innovation.

Regarding Privacy Enhancing Technologies (PETs), they offer effective privacy protection while facilitating beneficial data use. Encouraging the exploration of innovative solutions

beyond anonymisation is crucial for fostering innovation, especially in machine learning, while safeguarding fundamental rights.

In the context of AI, although the GDPR does not explicitly reference AI, its principles are adaptable to AI systems, mandating transparency, consent, and robust security measures to protect personal data.

**Recommendations:** We encourage striking a better balance between data protection and innovation. At the same time, GDPR consent requirements should make a distinction to avoid treating diverse technologies uniformly and neglecting their varying impacts on user privacy.

**GDPR and new regulation**

Several new EU laws intersect with the GDPR, leading to concerns among our members about potential conflicts and prolonged legal uncertainties, impacting their EU operations, investments, and partnerships. While supporting consumer empowerment initiatives like the Cookie Pledge, it is essential to align proposed solutions with the GDPR and ePrivacy directive.

Regarding the GDPR and the **Data Act**, potential conflicts exist between the GDPR's data minimisation principle and the EU data strategy which is focused on data sharing and reuse. Additionally, the Data Act's coverage of both personal and non-personal data raises concerns about enforcement regimes' clashes, data minimisation, and the separation of personal and non-personal data. Conservative GDPR interpretations may clash with the economic value placed on data by acts like the Data Governance Act and data spaces, designed to promote innovation around data.

Concerning the GDPR and the **Digital Services Package**, the DMA and DSA build upon vague GDPR definitions, causing ambiguity, especially in areas like 'profiling' and 'special category data.'

Lastly, it is crucial to address the ongoing uncertainties stemming from the delayed **ePrivacy Regulation**. The goal should be to achieve synchronisation with the GDPR, particularly in terms of legal bases, competent enforcement authorities, and reliance on the GDPR's consistency mechanism.

**Recommendation:** In the future, careful assessment and articulation of the GDPR's interaction with laws like the AI Act, DSA, DMA and Data Act are crucial. However, such analysis should not necessitate a re-opening of the GDPR, and both the European Commission and EDPB should play key roles in this process.