Implementation dialogue on the application of the GDPR: Written input

Following the implementation dialogue on the application of the GDPR, we would like to share our views on the four topics (see below) framing the discussions that took place on 16th July.

Topic 1: "Further simplification/reduction of administrative burden"

1. *What are your views on possible further simplification of the GDPR, going beyond the recent Commission's proposal to simplify the record-keeping obligation.*

While we welcome the proposed changes for SMEs, a broader vision is essential to ensure that the original objectives of uniform protection and harmonization of the GDPR are met. As the Draghi report correctly identifies, regulatory complexity is a significant impediment to the EU's global competitiveness. The GDPR's potential is currently constrained not by its core principles, but by fragmented interpretation and administrative friction that affects the entire economic ecosystem.

Therefore, simplification must be a holistic effort that benefits all actors, from startups to large enterprises, avoiding a two-tiered system. The objective should be to reduce administrative overhead and increase legal certainty for all companies in Europe. This is a strategic necessity to unlock investment, enable companies to scale, and continue to translate world-class European research into commercial success, particularly in data-driven fields like AI.

One important simplification measure would be to formally embed the principle of proportionality as a core tenet of GDPR interpretation and enforcement. The lack of a general proportionality principle has led to absolutist interpretations by some authorities, creating limitless and often disproportionate compliance burdens for low-risk processing activities. Explicitly recognising this principle—for instance, in Article 24—would empower organizations to apply a truly risk-based approach, focusing resources where they are needed most.

2. *Which targeted amendments would appear potentially useful to reduce administrative burden of controllers and processors, while maintaining the GDPR's risk-based approach and ensuring the high level of data protection?*

We propose highly targeted amendments to the GDPR which would retain its essential structure and principles while addressing key sources of legal uncertainty and administrative cost. These amendments include:

Reaffirm legitimate interests as one of the GDPR's most innovation-enabling legal bases, e.g. for training AI models[1] – as recognized by the European Data Protection Board.

Provide clarity for scientific research (Article 89): Recognize the collective dimension of data by introducing more flexibility for scientific research, making it clear that people can give 'broad consent' to their data being used for a general area of scientific inquiry, whether public or commercial.

Streamline the international data transfer regime (Chapter V):

- Proposal: Increase legal clarity in relation to data transfers that take place under Standard Contractual Clauses (SCCs), e.g., by developing common guidance that can help alleviate the complexity and burdens for companies, or by allowing organizations to conduct a single, scalable assessment for a set of similar transfers, rather than having all transferring entities having to do separate and individual transfer impact assessments for a significant number of countries in a legally uncertain context. We recommend creating a self-certification mechanism for intra-group transfers, obviating the need for SCCs/TIAs within a corporate group that adheres to specified principles. In addition, the Commission should explore ways to support companies in assessing the laws and practices of non-adequate third countries, particularly with regard to national security concerns (e.g. common criteria for assessing government access risks).

- Justification**:** The post-Schrems II transfer regime is one of the single greatest administrative burdens under the GDPR. A "global TIA" approach and an intra-group certification would drastically reduce compliance costs and complexity without lowering the standard of protection.

Simplify the ePrivacy and "Cookie" rules:

- Proposal**:** The 2002 ePrivacy Directive is a major source of friction and a prime candidate for simplification. The over-reliance on consent for low-risk activities has led to widespread 'consent fatigue' among citizens and imposes significant costs on businesses. Processing currently under Article 5(3) of the ePrivacy Directive should be moved into the GDPR and benefits from a wider range and more open legal bases, or, if kept in, low-risk processing -

[1] See IAB Europe white paper on "Artificial Intelligence and Europe's Digital Advertising Frontier"

such as reducing ad frequency, cybersecurity and preventing ad fraud, displaying ads or measuring ad delivery - should be rendered more flexible by allowing cookie placement without consent.

- Justification: Low-risk processing, such as reducing ad frequency, cybersecurity and preventing ad fraud, displaying ads or measuring ad delivery, have become essential to the functioning of the ad supply chain, enable positive consumer outcomes and do not adversely impact user privacy. Integrating this into the GDPR would allow organizations to rely on legitimate interests for essential, low-risk processing, reducing unnecessary consent banners and aligning the rules with a more practical, risk-based approach that citizens and businesses can better understand and manage, while maintaining the same level of protection for data subjects.

Embrace Privacy-Enhancing Technologies (PETs):

- Proposal**:** We propose to recognise that PETs offer a powerful means to protect data while enabling value creation. To unlock their potential, the EU needs a smart regulatory framework that creates clear incentives for their use.

- Justification**:** Legally recognising the use of PETs as a key technical safeguard in data processing and as a strong supporting factor in legitimate interests assessments would encourage their adoption, enabling innovative uses of data while strengthening fundamental rights protections.

Should the Commission propose these amendments, the legislative process should stay within the original scope and genuinely simplify the implementation of the regulation.

Topic 2: "Increasing legal certainty, reducing fragmentation and further harmonising enforcement"

1. *What are the measures you would consider useful to increase legal certainty, to reduce the fragmentation in the application of the GDPR and to further harmonise its enforcement?*

Fragmentation and inconsistent interpretation and enforcement are major barriers to the Digital Single Market. To create a predictable regulatory landscape, we propose:

Mandate inter-regulatory cooperation: Introduce a statutory duty for national competent authorities (including DPAs) to consult with other relevant regulators when issues overlap between the GDPR, AI Act, DSA, etc. A structured, official inter-regulators forum - like the UK DCRF or the EDPS' Digital Clearinghouse - could provide the formal structure for such consultations.

Introduce duties on DPAs and EDPB: In addition, member state DPAs and the EDPB should have duties to have regard to the effect of their work on innovation, competitiveness and growth. All authorities should be required to prioritise aiding organisations' compliance and producing actionable and workable guidance that supports long-term decision-making and continuity of business. This will establish a more stable and predictable regulatory climate and inform investment decisions.

Ensure consistent and consultative guidance: All guidance issued by the EDPB should be binding on national DPAs to end fragmentation. Guidelines clarifying divergent interpretations of GDPR rules across Europe should be prioritized by the EDPB (e.g. DPIAs or DSARs). Furthermore, all guidance must be subject to mandatory prior public consultation with key stakeholders to ensure it is practical and well-informed. Guidance must be in place to inform company compliance and before any enforcement action is considered.

Harmonise the definition of high risk activities: Article 35 defines what is a high risk processing activity with a clear list of criteria but also provides for DPAs to establish their own local lists. This creates complexity and lack of legal certainty for European controllers looking to implement cross-border processing activities, having to deal with a huge number of lists with different use cases and taxonomies that are often impossible to reconcile. Similar to the AI Act, the GDPR should establish a single list. Alternatively, only the EDPB could provide for a single list of high-risk activities which is binding on DPAs.

Topic 3: "Facilitating compliance with GDPR"

1. *What are your views on the various tools under the GDPR, e.g. codes of conduct and certification, that could be exploited to facilitate compliance with the GDPR?*

We regret the absence of greater investment in codes of conduct and certifications by regulators, which has meant that opportunities to facilitate compliance by companies and enforcement by regulators have been missed. In six years, only two codes of conduct have been approved by the EDPB at EU level. These tools, which have been underused, were supposed to specify the GDPR obligations in various sectors and create a continuous dialogue between DPAs and industry on what compliance looks like, thereby increasing legal certainty. A higher prevalence of codes of conduct would likely have resulted in fewer fines.

2. *What challenges have you faced in relation to the use of such tools and what solutions would you propose to address these challenges?*

Main challenges include:

- High cost of financing a monitoring body for businesses.
- Lack of resources allocated by DPAs to work with industry to set up these tools.

Going forward, the development of these tools should be easier, faster, and susceptible to being based on established voluntary industry standards. To support this, the Commission should consider removing the obligation for a monitoring body for codes of conduct and include a clear obligation for DPAs to work on codes of conduct and certifications with organizations. DPAs should also invest in deeper technical expertise, to engage more confidently on complex issues.

Topic 4: "Clarifying the articulation with other digital legislation"

1. *Is there a need to further clarify the interplay of the GDPR with other EU digital legislation?*

   Yes.

2. *Can you provide some specific examples of provisions for which the interplay of the GDPR and other digital legislation has appeared to be challenging?*

The current overlap of digital laws creates legal uncertainty, increases costs, and deters innovation. A clear articulation of rules and responsibilities is critical.

GDPR and AI Act: The interplay is challenging. Due to its horizontal scope, the GDPR applies to all data processing activities. As a result, some activities may be considered high risk by DPAs, including use cases that do not fall under the AI Act's high-risk definition. To improve legal certainty and coherence, any high-risk classification of AI-related data processing by DPAs that is not included in Annex III of the AI Act should only be allowed if supported by empirical evidence of serious, existing risks to individuals' rights and freedoms.

GDPR and Data Act: The obligation to share data under the Data Act creates uncertainty regarding the GDPR legal basis for that sharing. Clarifying the rules on joint controllership and streamlining data transfer mechanisms, as proposed above, is essential to making data sharing under the Data Act practical and legally certain.