EUTA's Feedback on the General Data Protection Regulation's Report

February 2024

The adoption of the General Data Protection Regulation (GDPR) marked a significant milestone, setting the stage for data protection principles in the EU economy and enhancing consumer trust. GDPR has also become an international standard, inspiring other non-EU countries to adopt similar laws. Members of the EUTA invested significantly to align their services with GDPR requirements.

Despite GDPR's ambition to ensure a harmonised EU application, diverging interpretations by national data protection authorities across the EU create legal uncertainty. Companies face high costs in adapting to localised requirements and challenges in determining what good compliance looks like across multiple jurisdictions. A more consistent and harmonised approach should be embraced. While the new GDPR procedural regulation marks progress, it falls short of achieving full harmonisation.

The interpretation of the GDPR has so far been very legalistic, neglecting the practical implications for businesses and their operational realities. Presently, DPAs overlook the risk-based approach, which should ensure a more equitable balance between the right to personal data and other fundamental rights. DPAs should not have readings that disadvantage certain companies unfairly, leading to distortions in competition.

Furthermore, to ensure legal clarity, DPAs should foster greater engagement with the industry. Currently, most DPAs primarily function as GDPR enforcers, unable to support companies in achieving compliance by facilitating or endorsing codes of conduct and certifications.

Interactions between DPAs, controllers/processors, and subjects remain intricate and resource-intensive. Additionally, navigating new guidelines and litigation developments poses challenges in keeping abreast of these advancements.

Last but not least, the interaction with other laws should also be addressed, particularly concerning conflicts between GDPR and the e-Privacy Directive.

Exercise of data subject rights

- The access to data (Article 15), and data portability (Article 20), seem to either overlap or clash, especially given the rarity of portability requests and the absence of established standards. While the concept of data portability appears sound in theory, its practical application remains, to our knowledge, largely un-used by data subjects. This means that companies have to invest considerably to prepare for potential demands that may never materialise.
- The access to data right should remain proportional and have a clear benefit for the data subject. DPAs should not lose sight of the important workload and cost that such requests can represent for companies.
- The transparency requirements present a challenge, as being simultaneously precise and easy to understand can be incompatible. Moreover, access requests are increasingly

being used strategically, weaponized to gather evidence or support claims against companies rather than upholding data protection rights.

- Exemptions to subject rights, such as 'legal privilege', lack standardisation across EU jurisdictions, posing challenges in their concrete application.
- The need for similar technical standards extends to consent management. As SAAS and cloud-based solutions become more prevalent in workplaces, the absence of international technical standards for consent data capture and withdrawal persistence is surprising and inefficient. Establishing these standards could benefit software providers, enabling them to incorporate standardised processes into their products and services.
- Right to erasure: Personal data for which the data subject exercises the right of erasure/right to object or withdraw consent may also be used to train an algorithmic model. Therefore the limits of these rights should also be interpreted in light of the current technological developments and within the limits of how far a model can "unlearn".
- There is an intrinsic tension between the obligation to implement privacy-by-design measures such as pseudonymisation and the need to identify the data subject to properly respond to a right request and to limit the risk of unauthorised access to data. Reliance on an ID card may be a solution but some DPAs have been refusing this as being too intrusive. Companies are therefore left in a very difficult situation, facing an impasse, despite their willingness to do things right.
- It would be welcomed if the Commission could try to ensure that legal cases are serving the purpose of the GDPR and have enough merit to go to Court. The Courts should also recognise that companies live in a data driven economy.
- For information, the malicious use of data subject rights was already mentioned in the first GDPR multi stakeholder report in 2020 (see page 9).

Use of representative actions under Article 80 GDPR

Article 80 of the GDPR is more and more used, especially in the framework of collective redress mechanisms. The representative actions are intended to guarantee that legal proceedings prioritise safeguarding the rights of individuals rather than serving as avenues for financial gains for legal practitioners.

To address disparities, forestall redundant actions, and ease the administrative strain on local courts and companies stemming from numerous claims under Article 80 of the GDPR concerning the same issue, we propose considering a more consistent approach between Member States.

Experience with Data Protection Authorities

The interpretation of the GDPR has so far been very legalistic, often overlooking the practical implications for businesses and their day-to-day operations.

Data Protection Authorities (DPAs) and the European Data Protection Board (EDPB) should strive for greater engagement with industry stakeholders, including trade associations and companies. This engagement is crucial not only to ensure legal certainty but also to grasp market dynamics, prevalent practices, and the potential or actual risks to individuals. An approach grounded in shared practices and practical examples will foster innovation while addressing the prevailing confusion surrounding sanctions imposed by DPAs. Moreover, it will ensure the GDPR's adaptability to technological advancements. Currently, most DPAs primarily

function as enforcers of the GDPR and do not adequately support companies in achieving compliance.

In some countries, engaging with DPAs and gaining their insights into data protection practices or market realities can be extremely challenging. While there have been some positive developments, such as the establishment of regulatory sandboxes and legal assistance programmes, the number of selected projects remains insufficient to meet industry needs.

Such collaboration should extend to the drafting of guidelines. European tech companies would appreciate the opportunity to contribute to the initial drafts of guidelines issued by DPAs and the EDPB. DPAs need a clearer understanding of industry practices when providing guidance. To facilitate this collaboration with the industry, DPAs and the EDPB should enhance transparency in their activities and functioning (e.g. better explain how subgroups operate or explain why certain inputs to consultation are accepted or rejected).

It is essential that guidelines remain confined to interpreting the law and do not impose additional obligations on companies beyond the GDPR's requirements. The legal status of numerous EDPB guidelines requires clarification, as does the extent to which companies are bound by them and how courts should consider them.

The issuance of guidelines by DPAs at the national level poses challenges, as the GDPR calls for full harmonisation. Ideally, all guidelines should be issued by the EDPB, except for provisions allowing for national specifications. The multitude of national guidelines creates complexity and confusion for European companies engaged in cross-border activities. These differing national interpretations by DPAs recreate barriers to the internal market that the GDPR aimed to remove, making it difficult for companies to implement European-wide programmes or launch products. This situation also fosters competition distortions and encourages forum shopping. DPAs' interpretation of the GDPR should not distort competition or jeopardise the competitiveness of European tech companies.

Currently, most DPAs overlook the risk-based approach mandated by Recital 4, which should ensure a fair balance between the right to personal data and other fundamental rights. For example, the 2014 guidelines on pseudonymisation and anonymization fail to adopt this risk-based approach. The industry awaits updates by the EDPB, as such techniques are invaluable for companies to protect data while innovating.

A critical issue is the inconsistent application of the one-stop mechanism, leading to prolonged complaint handling for example. Simplifying this process is essential, requiring a centralised repository for clear and accessible guidance. The vast and detailed EDPB guidelines, while useful, need practical grounding and a more defined legal status within the GDPR.

Another issue is how DPAs have been playing with the lack of clarity on the relationship between the GDPR, the one-stop-shop and the e-privacy directive.

Experience with accountability and the risk-based approach

The accountability principle was introduced to replace the administrative burden of prior authorisations and declarations under the Directive with the requirement for companies to demonstrate the organisational and technical measures they have internally implemented to comply with the GDPR.

However, there are drawbacks to the accountability principle. It could result in a scenario where privacy appears robust on paper but lacks actual implementation in real-world scenarios. For instance, in some enforcement actions, the emphasis is placed on the quantity of privacy documentation (e.g., Records of Processing Activities, Legal Information Bulletins, Privacy Impact Assessments) rather than on operational compliance, sending the wrong message that documentation outweighs actual compliance.

For the GDPR's accountability principle and approach to succeed, a fluid, open, and ongoing dialogue between companies and regulators are needed to align on what constitutes a risk and the appropriate level and granularity of the company's compliance approach. We regret to see that there isn't such a fluid, open, and ongoing dialogue between companies and DPAs. It is regrettable to observe that discussions on risk assessment and legal arguments predominantly occur during the enforcement phase before the DPA or in court.

The accountability principle has led to significant legal uncertainty and has failed to achieve its intended objectives. Companies spend considerable time implementing technical and organisational measures, documenting their activities, all while facing the threat of substantial sanctions without legal certainty that their risk assessment approach will be accepted by the DPA, despite acting in good faith.

Furthermore, DPAs have often adopted strict interpretations of the GDPR, sometimes disregarding the risk-based approach allowed by Articles 25 and 32, as well as Recital 4 of the GDPR.

It would be beneficial if DPAs could better recognise the efforts made by companies to mitigate the risk to their processing activities, such as through pseudonymisation techniques and by applying a risk of identification test. However, some DPAs have declined to consider this as a mitigating factor in enforcement cases, despite companies' investments in risk reduction and enhanced personal data protection. This may discourage companies from further investing in such techniques.

Moving forward, improved transparency on how fines are determined would be welcomed. Companies would appreciate a clearer correlation between the fines imposed and the harm suffered by individuals due to non-compliance.

DPAs should strive to encourage compliance alongside their enforcement efforts.

Finally, DPAs should maintain objectivity and consider various stakeholders' positions, whether from NGOs or the industry, in their decision-making processes.

Data protection officers (DPOs)

The role of a DPO can be quite challenging, involving tasks that sometimes seem contradictory in practice (e.g. how to ensure they are not making decisions related to the purposes and means of the data processing but are consulted before making one).

When referring to "sufficient resources", it is often perceived as having enough staff. However, the evolving responsibilities of DPOs now require them to have access to and work with effective tools used by controllers and processors. Companies should be able to use specific tools

tailored to their business models or company needs. This lack of clarity means DPOs might find themselves having to put in extra effort to guide their organisations/companies in detail, aligning with the accountability principle and supporting their tasks effectively.

Controller/processor relationship (Standard Contractual Clauses)

Use of Standard Contractual Clauses has been ok and widely accepted by vendors.

International transfers

The lack of risk based approach related to data transfers has created a lot of bureaucratic work for European digital companies that have not led to any impact or improvement on data protection of the data subjects. The complicated rules and lack of a practical approach mean companies are spending too much time and resources on unnecessary processes, instead of actually improving the protection of users' data.

The idea of international data transfers is important, but needs to be clearer and more practical. We need an approach that can fit different businesses and scenarios. European tech businesses would appreciate having clear global rules making international data transfers easier.

Even though Standard Contractual Clauses (SCCs) are commonly used, they have problems like extra costs and unclear criteria for 'essentially equivalent' protection.

Binding Corporate Rules (BCRs) provide a unified standard for data protection across a multinational corporation. This consistency ensures that all subsidiaries and branches of the company adhere to the same high standards of data protection, irrespective of their geographical location and BCRs also serve as a testament to the company's dedication to maintaining high standards of data privacy. However, it takes some time (several years) to get BCR's approval.

Moving forward, European digital businesses need a unified and practical approach to solve these international data transfer challenges and create an environment that focuses on effective protection without unnecessary bureaucracy.

Problems with the national legislation implementing the GDPR (e.g., divergences with the letter of GDPR, additional conditions, gold plating, etc.)

Fragmentation is taking place across various facets of the GDPR implementation.

To ensure the smooth operation of the single market, Member States through their DPAs and the EDPB should align their interpretation of the GDPR provisions. This alignment could enable national courts to refer to prior decisions taken by foreign EU DPAs and resolve legal matters.

Another challenge to the digital economy functioning is the debate around consent as the legal foundation for processing personal data; how can users validly provide consent and who bears responsibility for data control. For instance, in Germany, uncertainty persists regarding the voluntariness of consent under the German privacy law, TTDSG.

Discrepancies also exist in how supervisory authorities and initiatives like the Cookie Pledge establish transparency standards. This disparity highlights diverse approaches to informing users and obtaining their consent when utilising this legal basis.

Lastly, disparities exist relating to the age at which GDPR applies, and how different countries understand concepts like personal data, anonymization, and legal bases.

Fragmentation/use of specification clauses

The lack of harmonisation between the e-privacy Directive and the GDPR, particularly concerning the equivalence of legal bases, poses a significant challenge for European tech companies. Avoiding clashes between the two laws is impossible due to numerous overlaps. For instance, ePrivacy rules often create the need for burdensome consent solutions where a GDPR legitimate interest legal basis would have been more appropriate (but which is de facto unusable due to the ePrivacy cookie consent requirement), and would significantly facilitate both compliance and the data subject's experience. As another example of fragmentation: data breach notification templates vary across countries making standardised processes difficult for multinational companies.

Codes of conduct, including as a tool for international transfers

Beyond the necessary enforcement of the GDPR, we encourage DPAs to prioritise additional measures, like encouraging the creation and adoption of codes of conduct as outlined in Article 40 of the GDPR. These codes could clarify how the GDPR applies within specific industries.

Although these codes hold the potential to significantly enhance compliance, their development demands substantial resources and time. Furthermore, they do not afford legal protection to companies. Consequently, there is limited incentive for their formulation, resulting in few new codes since 2018. We stress the importance of placing greater emphasis on this mode of compliance, particularly for codes with transnational applicability that adhere to GDPR standards.

The underutilisation of codes of conduct represents a significant missed opportunity. Six years after the implementation of the GDPR, it strains credulity that only two codes have attained EU-wide approval within the same sector. Given the pervasive cross-border use of data across industries, there should be a multitude of codes specifying GDPR across various sectors.

DPAs should allocate more time and resources towards the development of codes of conduct. This could involve establishing dedicated departments that collaborate closely with industry stakeholders, such as trade associations and companies, to provide better support. A sector-specific code of conduct, formulated in conjunction with industry input and overseen by a dedicated regulatory body, would prove more effective than unilateral guidelines imposed by DPAs or the EDPB.

The necessity for codes of conduct was underscored in the initial GDPR multi-stakeholder report of 2020 (see page 35).

For example, we regret to see that:

- In Belgium, a code of conduct on pseudonymisation is pending for approval for several months. There is no indication of when the review and approval will be completed, leaving industries and companies reliant on pseudonymisation in legal uncertainty.
- In France, the CNIL has suspended ongoing discussions regarding a potential code of conduct on advertising due to an investigation initiated by the Belgian DPA citing "DPA loyalty obligation".

Certification, including as a tool for international transfers

Like other tools, certification mechanisms endorsed by the GDPR haven't been widely used across the EU. It's important to encourage more businesses to adopt these certification mechanisms because they can ensure the right protections when combined with mandatory commitments. Unfortunately, 6 years after the entry into force of the GDPR, all the referential have not yet been published by the EDPB and it is still not possible to obtain one single GDPR certification.

GDPR and innovation / new technologies

The GDPR made several positive promises, advocating for a technology-neutral, pragmatic, and risk-based approach that would foster the necessary environment for innovation. However, the interpretation of the GDPR by DPAs fails to fully embody this philosophy, and rather creates challenges to innovation.

As highlighted in the inaugural GDPR multi-stakeholder report of 2020 (refer to page 28), it is imperative not to lose sight of innovation and the imperative for a risk-based approach.

In today's global landscape, prioritising innovation is crucial for the EU.

For instance, embracing artificial intelligence (AI) is essential to stay ahead in the innovation game. It's noticed that other EU data regulations often unintentionally overlap with GDPR. To safeguard our data ecosystem, it's crucial to ensure that emerging legislation, especially the AI Act, aligns with the GDPR and doesn't contradict it. The tension between AI and the GDPR was already mentioned in the first GDPR multi stakeholder report in 2020 (see page 29, 31, 32) with a call for more exchanges between industry and data protection authorities on technological aspects.

There are important risks of tension between the GDPR (based on the principle of data minimisation and data deletion) and the data strategy of the EU that relies on data sharing and reuse. DPAs have also had strict interpretations of the GDPR, considering that the processing of large amounts of data for business purposes is inherently bad, whereas the Data Governance Act (DGA), Data Act and data spaces are intended to create value and innovation around data and to confirm data's economic dimension. Unfortunately, DPAs are far from acknowledging this. In addition, there are no guidelines or rules governing the articulation of the different texts with the GDPR, aside from the traditional "without prejudice to". The definition of what constitutes non-personal data that falls outside of the scope of the GDPR is left to the DPAs themselves. An EU harmonised definition of non-personal data would be welcomed.

About the European Tech Alliance

EUTA represents leading European tech companies that provide innovative products and services to 500 million users[1]. Our 29 EUTA member companies from 16 European countries are popular and have earned the trust of consumers. As companies born and bred in Europe, for whom the EU is a crucial market, we have a deep commitment to European citizens and values.

With the right conditions, our companies can strengthen Europe's resilience and technological autonomy, protect and empower users online, and promote Europe's values of transparency, rule of law and innovation to the rest of the world.

Our members

Adevinta, AirHelp, allegro, appJobber, bol., Bolt, Booking.com, Cdiscount, CRITEO, DAILYMOTION, deliveroo, Delivery Hero, dreamstime, eMAG, FREENOW The Mobility Super App, Glovo, meetic, MIRAKL, Proton, Schibsted, SEZNAM.CZ, Spotify, stripe, tomtom, trivago, Trustpilot, Vinted, Wolt, zalando

Visit us at www.eutechalliance.eu.

[1] It reflects users, consumers and business customers from EUTA member companies, per year. It includes overlaps but illustrates the reach and impact of our services.