ESOMAR

SCOPE EUROPE

selbstregulierung informationswirtschaft e.V.

FEDMA

Federation of European Data and Marketing

FIVE YEARS OF GDPR

KEY CHALLENGES & RECOMMENDATIONS

Publishers

ESOMAR	FEDMA AISBL	Selbstregulierung Informationswirtschaft e.V.	SCOPE Europe s.r.l.
Burgemeester Stramanweg 105 1101 AA Amsterdam https://esomar.org info@esomar.org	Avenue des Arts, 43 1040 Brussels https://www.fedma.org info@fedma.org	Großbeerenstraße 88 10963 Berlin https://sriw.de info@sriw.de	Rue de la Science 14 1040 Brussels https://scope-europe.eu info@scope-europe.eu
Register Number: 29952722795-07	Register Number: BE 0464157569	Register Number: VR 30983 B, Amtsgericht Charlottenburg	Register Number: BE 0671.468.741

1 KEY MESSAGES

1. **It is strongly recommended to set the risk-based approach as the decision-making compass in the interpretation and implementation of the GDPR by:**
   - Applying in a consistent manner the GDPR risk-based approach stemming from the general principle of proportionality.
   - Reconciliating the fundamental right of data protection with other fundamental rights and public policy objectives.
   - Fostering and promoting stakeholders' driven initiatives supporting the balancing involved in the processing of personal data with adequate protection of data subject rights.

2. **It is strongly recommended to promote the added value of Legitimate Interest for data subjects by:**
   - Promoting a more balanced narrative that does not set consent as the default legal basis with the highest level of effective data protection.
   - Incentivizing and clarifying reliance on legitimate interest subject to full compliance with the GDPR.
   - Enabling a constructive dialogue with relevant stakeholders for developing templates for legitimate interest balancing assessments (LIA) for different types of activities via Codes of Conduct and certifications.

3. **It is strongly recommended to encourage organizations to invest in pseudonymization and anonymization techniques by:**
   - Fostering a common approach to pseudonymization methodology across the EU through guidelines and Codes of Conduct.
   - Incentivizing companies in investing resources to process pseudonymous data.
   - Adopting a risk-based approach to the concept of anonymous data in light of existing international standards such as ISO/IEC 27559:2022.

4. **It is strongly recommended to ensure that the roles and responsibilities of controllers, processors and third parties are clear and proportionate by:**
   - Refraining from relying solely on simplistic examples and instead considering the complexity of data processing chains. Recognizing the complexity inherent in such endeavours is crucial for crafting effective policies that accommodate diverse (e.g., research) requirements.
   - Striking a balance regarding granularity requirements for Codes of Conduct. Given the inherent challenges in comprehensively describing all types of processing activities, such codes should prioritize overarching

principles and methodologies rather than attempting to provide excessively detailed guidance. This approach ensures that Codes of Conduct remain relevant and adaptable to various contexts, including research.

5. **It is strongly recommended to further streamline the approval and operationalization of GDPR Codes of Conduct:**

   - By reviewing the procedural requirements in receiving a Code of Conduct's approval and a Monitoring Body's accreditation.
     - Generally, the legal framework and EDPB's guidelines are considered suitable, if applied consistently. Specifically for transnational Codes of Conduct, it is recommended to ensure harmonized interpretation, because projects suffer delays, e.g., by means of consistently and mutually determining the competent data protection supervisory authorities.
     - Periods as indicated by GDPR are not yet met in practice. So, it is recommended to adapt such periods to more realistic timelines and to clarify that in case data protection supervisory authorities cannot by majority determine undisputable conflicts with GDPR, Codes of Conduct shall be deemed in accordance with GDPR.
   - In regards of third country transfers, a general validity by implementing act is required. It is strongly recommended to ensure that procedural efforts will be streamlined preventing any unreasonable delays in operationalizing such projects.
     - Safeguarding third country transfers is one of the key elements subject to legal, political and operational discussions.
     - Codes of Conduct may act as a safeguard provide that, next to the formalities to be met for transnational Codes of Conduct in any case, general validity will be granted.
     - Considering the procedural steps of deciding on an implementing act, it is strongly recommended to allow for a material assessment by the European Commission and the EDPB in parallel.

Table of Contents

2 INTRODUCTION

Since its entry into force on May 25th, 2018, the General Data Protection Regulation (GDPR) has emerged as a pivotal milestone in data protection and privacy regulation. Providing strengthened rights and safeguards for individuals within the European Union, the GDPR has shaped the processing of personal data and has fundamentally changed the way organisations must manage data. As we celebrate 5th year anniversary of its entry into force and as organizations that are involved in its implementation, ESOMAR, FEDMA, SCOPE Europe and SRIW ("**We**"), have come together to present collective observations and recommendations to further enhance the effectiveness and applicability of the GDPR.

This comprehensive paper comprises several chapters, each focusing on a key aspect of GDPR and providing valuable insights and suggestions to address pertinent challenges. The chapters cover a range of topics, including the risk-based approach, legal bases, privacy-enhancing technologies such as pseudonymisation and anonymisation, determination of controller, processor and third-party role, and the streamlining of the approval and operationalisation of Codes of Conduct.

This collaborative paper aims to contribute to the ongoing dialogue surrounding GDPR implementation. By offering a range of observations and recommendations, we strive to enhance data protection practices, foster compliance, and support the continued success of the GDPR.

Through this paper, we invite policymakers, DPAs, and stakeholders to engage in constructive discussions and collaborate towards further improving the GDPR's implementation, ensuring the privacy and rights of individuals are safeguarded while balancing it with other fundamental rights.

3 ABOUT THE AUTHORS

3.1 ESOMAR

ESOMAR champions the research, insights, and analytics sector worldwide. Founded in 1947, the global membership association is a network reaching over 50,000 professionals and 750+ companies in 130+ countries. We support our global community through raising ethical standards, facilitating education, advocating with legislators, sharing best practices, promoting evidence-based solutions for decision-makers, and ensuring the values of honesty, transparency, and objectivity are applied to all data sources.

3.2 FEDERATION OF EUROPEAN DATA AND MARKETING (FEDMA)

The Federation of European Data and Marketing (FEDMA) is a Brussels-based trade association representing the interests of the data and marketing industry from across Europe. Its members use data for effective marketing and improved customer experience through all communications channels. FEDMA operates mainly through the participation of its network of national Data Marketing Associations (DMAs) across Europe and significant companies in the sector's value-chain, ranging from postal operators, marketing services providers, to database marketing companies, consultancies, etc.). FEDMA also holds the secretariat of the Global Data and Marketing Alliance (GDMA), a global organisation that represents, supports, and unites the world's largest network of Data Marketing Associations and influencers.

3.3 Selbstregulierung Informationswirtschaft e.V. (SRIW) and SCOPE Europe:

SRIW is a non-profit association supporting the co and self-regulation of the information economy. It acts as a think tank to discuss and debate key issues in digital policy and provides an umbrella organisation supporting credible and effective self- and co-regulation of the information economy.

SCOPE Europe is a subsidiary of SRIW. Located in Brussels, it continues and complements the portfolio of SRIW in Europe. SCOPE Europe gathered expertise in levelling industry and data subject needs and interests to credible but also rigorous provisions and controls. SCOPE Europe has been the first accredited Monitoring Body under the GDPR since May 2021 related to a transnational Code of Conduct, i.e., EU Data Protection Code of Conduct for Cloud Service Providers. Since February 2023 SCOPE Europe is the first ever Monitoring Body under GDPR which has been accredited for more than one Code of Conduct and by more than one data protection supervisory authority.

SRIW and SCOPE Europe are calling for suitable regulatory methods to foster innovation and drive the digital transition while promoting corporate responsibility, particularly in the fields of data and consumer protection. To achieve this overarching objective, SRIW and SCOPE Europe work to enhance transparency and strengthen best practices in data protection by mobilizing and supporting the industry to engage in voluntary, yet binding commitments underpinned by appropriate remedies and sanctions.

4 GDPR RISK-BASED APPROACH: Setting the risk-based approach as the decision-making compass in the interpretation and implementation of the GDPR

Five years after the entry into force of the GDPR, organisations view the EU data protection framework as a guarantee of trust for the data subjects whose data is processed. Compliance with the GDPR is therefore seen as a potential competitive advantage even *vis-à-vis* non-EEA-based organisations. As such, over the past five years, organisations have made significant investments to ensure compliance with the GDPR, especially in data collection and management systems, data governance, IT infrastructures, human resources (DPOs, legal experts, privacy engineers), tools and processes to handle data subjects' requests and Privacy Enhancing Technologies (PETs),

In practice, however, many organisations easily face significant hurdles in complying with the GDPR, which may at first sight raise internal economic concerns regarding related benefits of a trustworthy relationship with data subjects, whilst understanding that compliance with applicable laws must never be questioned. In particular, the divergent interpretation of the GDPR by national Data Protection Authorities (DPAs) is perceived as the main impediment and source of legal uncertainty, preventing organisations in different sectors from benefitting from the data economy while ensuring the protection of individuals' personal data.

Many DPAs have fallen short in applying the risk-based approach of the GDPR to the modern data economy. Reflected in a number of provisions (e.g. Art 24 on accountability, Art. 25 on the principles of privacy by design and privacy by default, Articles. 33 and 34 on governing the management of a data breach, Article 32 on security, etc.) the GDPR's risk-based approach means that data controllers are encouraged to implement protective measures corresponding to the level of risk of their data processing activities, taking into account the likelihood and severity of the risk on the rights and freedoms of individuals. However, in practice, the GDPR is generally interpreted in a conservative and one size-fits-all manner by a number of Data Protection Authorities (DPAs), even when the risk of the processing is purely theorical and trivial, thus creating many tensions and disruptions.

This is, for instance, reflected in the interpretation by the Dutch DPA that the Legitimate Interest legal basis[1] cannot be relied upon for commercial interests, or the French CNIL's position that when relying on consent through contractual commitments of partners, the controller is under the obligation to audit such partners, including in controller to controller or joint controller relationships.[2] In doing so, there is a general perception that regulators prioritize the sole objective of personal data protection over other public policy objectives, including the protection of other fundamental rights as per Recital 4 GDPR such as the Freedom to conduct a business (Art.16 CFR). These regulators are doing so regardless of the actual level of risk for the rights and freedoms of individuals the data processing activities at stake,

[1] European Commission, 6 March 2020, Letter of the European Commission to the Dutch DPA regarding the interpretation of the Legitimate Interest legal basis.
[2] Mind Media, 21 March 2023, Amende de 60 millions d'euros par la Cnil : Criteo dénonce une position "anti-publicité en ligne".

whereas the GDPR provides that they have to be "determined by reference to the nature, scope, context and purposes of the processing".

This comes without saying, that the risk-based approach requires solid contextual evaluation and implementation. Understanding the complexity of applicable regulatory frameworks and business models, risk-based approaches should not invite for unduly limiting the protection of data subject's freedoms and fundamental rights. Where the application and results of a risk-based approach address the fine gradient of suitability and compliance, industry and DPAs should foster their engagement in collaboratively clarifying GDPR's interpretation across EU/EEA, either by consulted guidelines or by mechanisms such as codes of conduct.

Recommendations

EU policymakers and DPAs should:

- **Apply in a consistent manner the GDPR risk-based approach stemming from the general principle of proportionality.**
- **Reconciliate the fundamental right of data protection with other fundamental rights and public policy objectives.**
- **Foster and promote stakeholders' driven initiatives supporting the balancing involved in the processing of personal data with adequate protection of data subject rights.**

5 GDPR LEGAL BASES: Promoting the added value of Legitimate Interest for data subjects

The GDPR provides organisations with a range of legal bases for processing and organisations can choose a basis that is appropriate to their particular processing activity. All legal bases for processing are on equal footing with one another, meaning that there is no "default" legal basis, no hierarchy between them, and none should be privileged over the other. However, many organisations in different sectors point out a significant degree of uncertainty and misconceptions about legitimate interest, often resulting in an over-reliance on consent.

Such over-reliance on consent stems from an interpretation by some Data Protection Authorities (DPAs) which privileges consent over legitimate interest, portraying the former as a processing ground that gives individuals more control and provides for more legal certainty even where consent is less suitable to the processing at hand and results in lower privacy outcomes when compared to legitimate interest.

Referring to consent as primary legal basis disregards the fact that individuals increasingly express "consent fatigue" as they are constantly asked to make meaningful decisions at speed, multiple times during the day on the basis of information often related to complex processing scenarios. In other words, the consent ground puts all the responsibility and onus on the data subjects who are expected to endlessly conduct a balancing test themselves. In parallel, though the current narrative unfairly portrays legitimate interest as the lesser ground with a potential adverse impact on data subjects, it overlooks the benefits of this legal basis. In contrast to consent, legitimate interest shifts the responsibility on data controllers to make the balancing test while still providing data subjects with the necessary information and the indisputable right to opt-out as all GDPR provisions continue to bind the data controller. In other words, relying on the legitimate interest legal basis is not a blank check given to the controller as, in addition to complying with the GDPR, it has to perform a formal legitimate interest assessment (LIA) balancing its own legitimate interest versus individual interest and identifying possible mitigation measures.

Despite some of the clear benefits of legitimate interest compared to consent, uncertainty over the use of legitimate interest can negatively affect revenue opportunities, research and innovation, which ultimately limits the use of legitimate interest and consequently high level of the protection of data subjects.

This is for example reflected in the ongoing debate on direct mail in Germany where there is a lack of consensus among DPAs on the appropriate legal basis for address data trading. Currently based on legitimate interest which gives the specific right of the recipients concerned to object to such data processing under Article 21 (2) GDPR, address data trading enables companies to reach out to new potential customers. However, as some DPAs in Germany (e.g. Baden-Württemberg, Berlin) hold that such processing can only take place with the prior consent of the respective recipients, some companies refrain from taking the risk of being sanctioned, thus curbing new customer promotion. On the opposite side of the spectrum, the Austrian DPA approved a Code of Conduct under Art.40 GDPR for the Austrian direct marketing industry allowing the transmission and use of list data based on legitimate interest.

However, even where organisations rely on consent as the default option because of uncertainty over the legitimate interest legal basis, they still face significant issues and implementation costs in complying with the requirements for consent. Some of these challenges include:

- Setting up systems for tracing and time-stamping consent in order to provide proof that consent was lawfully collected;
- Providing, as data processors, comprehensive lists of data controllers to obtain informed consent, where the data processors rely on data providers on behalf of the controllers;
- Obtaining consent by telephone because of the need to record customer identification which customers perceive as intrusive;
- Assessing to what extent a consent request must be specific such as whether separate marketing campaigns addressed to the same data subject require separate consent.

Finally, organisations are also disincentivized in using legitimate interest as a legal basis due to the need of carrying out legitimate interest balancing assessments (LIA) which are not tailored to their processing activities or sector, often resulting in time-consuming procedures. As such, a constructive dialogue between DPAs and interested stakeholders should incentivize the adoption of Codes of Conduct and certifications to provide templates LIA for different types of activities enabling organisations to easily assess whether they have a legitimate interest, the evidence they need to provide, and the parameters for not extending that legitimate interest further than is intended.

Besides supporting the development of suitable tests to determine the adequate balancing of interest on a case-by-case scenario, Codes of Conduct may also significantly foster GDPR implementation and interpretation across EU/EEA. As transnational Code of Conduct they involve the EDPB as highest representation of all European DPAs, whilst they allow for more specific, sector-tailored balancing of interests. Such approaches may especially be deemed beneficial in cases where otherwise a case-by-case determination - even by approved templates - may face concerns whether data subjects' interests will be reflected properly.

Recommendations

EU policymakers and DPAs should:

- **Promote a more balanced narrative that does not set consent as the default legal basis with the highest level of effective data protection.**
- **Incentivise and clarify reliance on legitimate interest subject to full compliance with the GDPR.**
- **Enable a constructive dialogue with relevant stakeholders for developing templates for legitimate interest balancing assessments (LIA) for different types of activities via Codes of Conduct and certifications.**

6 PRIVACY ENHANCING TECHNOLOGIES (PETs): Encouraging organizations to invest in pseudonymization and anonymization techniques

Since the entry into force of the GDPR, Privacy Enhancing Technologies (PETs) has been another area increasingly explored by organisations in different sectors to mitigate privacy risks while harnessing the value of data. Provided as an example of an appropriate data protection safeguard by the GDPR, pseudonymization is, for instance, a foundational PET technique to mitigate privacy risks by replacing private identifiers with fake identifiers or pseudonyms to hide key identifiable information. Pseudonymisation thus enables organisations to single out individual behaviour without directly identifying the individuals. However, though this technique has become a helpful tool for organisations to protect data subject's personal data and optimise their processing activities, there remain both operational and legal challenges.

Specifically, the strict requirements of the GDPR, regardless of the type of processing of pseudonymised data, along with the lack of common pseudonymisation criteria for specific types and risks of category of personal data as well as the correspondent types of pseudonyms to use represents a barrier for smaller organisations to adopt this technical solution. Additionally, the lack of officially recognized/approved pseudonymisation criteria has also raised challenges from a compliance perspective whereby certain DPAs do not recognize some pseudonymised data processing as such and look at the data processed by these companies as purely personal data of an identified individual. As a result of these challenges, organisations in different sectors have less incentives to invest resources in processing pseudonymised data, leading to a significant drawback in the relationship with their customers. In this context, initiatives such as the draft GDPR Code of Conduct[3] on Pseudonymisation which would establish an EU-wide management system for pseudonymisation with general pseudonymisation requirements recognized by DPAs across the EU are very much welcome. More specifically, the code aims at stipulating requirements for controllers/processors to enhance transparency in decision-making and to help manage the pseudonymisation process by assigning responsibilities. As it is drafted to be a transnational Code of Conduct that presupposes the involvement of the EDPB as highest representation of all European DPA, the approval of such Code of Conduct could provide the sought clarification and harmonization on suitable pseudonymisation criteria on EU level.

In parallel, organisations also stress the need for processing anonymous data under a risk-based approach, more focused on transparency and accountability rather than zero-risk unlinkability. In the Data and Marketing Industry, for example, anonymous data is used to identify trends within a group of targets - even without having specific information on the individual level – to tailor a specific campaign which is still relevant to the consumer. However, there is a lack of consensus on what constitutes anonymous data with the Working Party 29's Opinion on Anonymisation Techniques as well as from some DPAs holding that the only remaining solution to obtain GDPR-compliant anonymizations is to

[3] SCOPE Europe presents on "Advancing Pseudonymisation with a Universal Code of Conduct" at Bitkom's Privacy Conference 2021

effectively delete the original dataset. As the concept of 'personal data' is bound to expand even further and as a result to apply to an exponentially growing range of situations, this zero-risk approach seems unfeasible for most data controllers and would in many cases contravene other legal provisions.

While recognizing the unfeasibility of a zero-risk approach and the controller's obligation to use state-of-the-art techniques, we wish to emphasize how the accountability for any advanced reverse engineering and re-identification activities shall lie with the entity that engages in such endeavours, rather than the business that initially implemented the anonymization technique.

Though court cases such as Breyer[4] seem to point to a more risk-based approach, it remains unclear how to operationalise the requirement that the risk of re-identification must be insignificant. The more recent judgement by the General Court of the EU in SRB v EDPS[5] could already provide more legal certainty, holding that pseudonymized data transmitted to a data recipient will not be considered personal data if the data recipient does not have any additional information enabling it to re-identify the data subjects and has no legal means available to access such information. Though a case-by-case assessment will always be necessary, this judgement may incentivize marketers to invest more in pseudonymised data and foster third party's data sharing while ensuring that individuals' personal data is protected.

This approach could equally incentivize researchers by providing legal certainty regarding the nature of the data shared within the data chain, when the data recipient does not have access to the decryption key.

Additionally, future guidance for anonymization and/or constructing a risk-based test should balance the need for concrete, clear, and precise recommendations and the necessity of exercising some margin of discretion by the controller in applying those recommendations. This is, for instance, reflected in the recently adopted ISO Standard on data de-identification which, rather than adopting an impossible zero-risk approach, provides a framework to identify various risks and mitigate (instead of nullifying) them across the lifecycle of deidentified data.

Recommendations

EU policymakers and DPAs should:

- **Foster a common approach to pseudonymization methodology across the EU through guidelines and Codes of Conduct.**
- **Incentivize companies in investing resources to process pseudonymous data.**
- **Adopt a risk-based approach to the concept of anonymous data in light of existing international standards such as ISO/IEC 27559:2022.**

[4] Judgement of 19 October 2016, *Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.
[5] Judgement of 26 April 2023, *SRB v EDPS*, ECLI:EU:T:2023:219.

7 CONTROLLERS, PROCESSORS, AND THIRD PARTIES: Ensuring clear roles and proportionate responsibilities

The determination and attribution of the controller, processor, or third-party role has practical implications for the parties involved in complex data processing activities, e.g. a research data chain. Through the attribution of the role, the liability and responsibility for safeguarding the processing of personal data changes as does the ability to exercise control over and determine further uses of the personal data.

Under the GDPR, the attribution of this role is depending on the factual involvement of the parties in the processing activities which is then left to the appreciation of the parties involved. It is up to them to determine to what extent they are involved, resulting in any of the classifications and subsequently designating themselves accordingly and ensure that this designation is respected by the other parties in the data chain.

In the context of this controller, processor and third-party debate, the dichotomy of controller and processor is not always clear cut nor should regulators conclude too easily in their guidance with the risk of creating legal uncertainty.

This is, for example, reflected in the opinion of some German DPAs (e.g. Baden-Württemberg, Berlin) according to which the use of third-party data from list owner of third-party addresses for postal promotion leads to a joint-controllership. The lack of consensus in Germany over this issue is pushing companies to shield themselves from any infringement risk and extend the controllership down the value chain. Yet, as some companies cannot afford the potential costs stemming from the liability risk associated to the joint controllership, they sometimes refuse taking the joint controllership, leading to a loss of potential revenue.

As such, rather than imposing a one-size-fits-all approach in determining controllers, processors, and joint controllership relationships solely based on the nature of the processing, we believe a case-by-case assessment is necessary, taking into account the nature of the partnership, the degree of instruction, and the personal data flow, to determine ultimately who is controller, processor, or third party distinct from the commercial relationship which is bringing the parties together.

In the data, research and insights environment, for example, where clients commission research agencies to support them to resolve, through an independent evidence-base, concrete business or strategic questions, the complexity of research data chains and the processing activities that they entail highlight the difficulties of applying the GDPR concepts in a data-rich world. As such, these “research projects” are often deconstructed into different singular activities and then grouped in phases as this can be much more effective in resolving uncertainties in the role attribution.

The determination will then depend highly on the level of specificity of the client brief given to the supplier and the level of specification that comes from it. A consumer brand or government body which asks an agency to understand how to

improve its advertising effectiveness without specifying to the agency how it should derive its recommendations is more likely to not be deemed a controller compared to a consumer brand which specifies to an agency that it is looking to conduct a study with 1000 individuals belonging to a specific demographic.

Another notable example can be found in the case of 'blinded surveys'. In this scenario it is recommended that participants are informed at the beginning of the interview about the delayed disclosure of the client's identity until the conclusion of the survey. This precautionary measure aims to prevent potential response bias that could arise from upfront disclosure of this information, e.g. when the client's identity is immediately communicated to the research participant in compliance with GDPR's transparency requirements.

We therefore underscore that it is important that regulators do not automatically associate the commercial relationship with the data processing relationship, and to consider the extent by which the vagueness of a client request impacts the role that they play within a data chain.

Relying on the nature of the partnership, the degree of instruction, and the personal data flow may thus prove more effective for all parties involved in the data processing activity as well as to ensure effective communication to the data subjects rather than adopting an approach that artificially simplifies the processing activity.

Acknowledging the abovementioned complexities, it shall be highlighted that industry stakeholders would appreciate enhanced legal certainties and collaboration with supervisory authorities to resolve pressing challenges of complex processing chains. Such collaboration and continuous exchange may, besides others, be addressed by the development of codes of conduct. Given the complexities and the pressing need by the industry, one should imagine iterative developments, where initial solutions resolve high-level principles, which may be further particularized in future, as needed. Refraining from too granular provision will allow for stronger harmonization across the sectors and in the general application of GDPR, will accelerate the implementation of and adoption of such code of conduct and eventually provide a generally optimized level of protection of data subjects.

Recommendations

EU policymakers and DPAs should:

- **Refrain from relying solely on simplistic examples and instead consider the complexity of data processing chains. Recognizing the complexity inherent in such endeavors is crucial for crafting effective policies that accommodate diverse (e.g. research) requirements.**
- **Strike a balance regarding granularity requirements for Codes of Conduct. Given the inherent challenges in comprehensively describing all types of processing activities, such codes should prioritize overarching principles and methodologies rather than attempting to provide excessively detailed guidance. This approach ensures that Codes of Conduct remain relevant and adaptable to various contexts, including research.**

8 Article 40 GDPR CODES OF CONDUCT: Further streamlining their approval and operationalization

As we mark the fifth anniversary of GDPR's entry into force, it is fair to say that it was drafted as a future-proof regulation that has inspired the global privacy regulatory environment. This was reflected when regulators put forward a toolbox to support GDPR implementation which has been instrumental in promoting a harmonized approach to data protection across various sectors and industries. One of the tools within this toolbox are Article 40 Codes of Conduct, which have been developed by industry stakeholders in collaboration with data protection authorities. These codes provide practical guidance, promote accountability, and support compliance efforts, thereby contributing to a consistent and harmonized approach to data protection. The EU Cloud Code of Conduct is a great example of a code of conduct that has been developed to ensure compliance with GDPR in the cloud sector. It has successfully harmonized the concerns and interest of users, providers, and competent authorities, delivering a unique compliance mechanism capable of protecting the rights of hundreds of millions of European citizens. At a national level, the recently revised Code of Conduct on the processing of personal data for advertising activities by the Spanish self-regulatory and supervisory body for the advertising industry, AUTOCONTROL, is another example of how a code of conduct can clarify the application of the GDPR in a specific sector, and it can also help data subjects to exert their rights. The revised Code provides, indeed, for an online out-of-court dispute settlement mechanism for resolving data protection disputes between adhering entities and data subjects.

By fostering the use of processing technologies while ensuring compliance with the stringent standards enshrined in European legislation, GDPR Codes of Conduct can help accelerate the digital transition in Europe, which aligns with the European Commission's Digital Decade goals. Therefore, as organizations that have been involved in the development of such tools, it is essential to highlight the benefits and potential of GDPR Codes of Conduct in promoting compliance and fostering innovation, while also addressing the challenges faced in their approval and operationalisation. Finally, in preparation for the expected GDPR review in 2024, it is critical to offer recommendations with respect to the procedural elements related to their adoption.

8.1 GDPR codes of conduct as tools supporting harmonization and consistent enforcement of GDPR

Codes of Conduct and Monitoring Bodies, in the context of Articles 40 and 41 GDPR, can be effective tools in addressing pressing challenges related to the uniform application of GDPR requirements and consistent enforcement, especially when those bear a transnational scope, i.e., covering processing activities across several member states. These mechanisms can contribute to the success of GDPR by promoting uniformity and consistency in the implementation of GDPR across different jurisdictions and sectors.

8.1.1 Sector-specific particularization and harmonization

As GDPR is written in a sector-agnostic manner in terms of processing activities, GDPR requires particularization. It is expected that such particularization of general legal terms will be addressed by guidelines of the European Data Protection Board, court proceedings, industry good practices, academia, etc. Whilst data protection supervisory authorities have progressed in reaching harmonization, it is essential to stress the potential that codes of conduct have to complement such efforts. This applies both to sectoral implementation but also specific processing activities of the same stakeholder. Against this background, transnational Codes of Conduct are by definition sector specific and are translating general GDPR obligations into specific means of implementation. That means, they can be sector-specific in terms of the specific industry sector covered (i.e., a code of conduct focusing on the automotive sector) as well as specific in terms of the common processing activities covered (for example, a code of conduct developed by different industry sectors but covering common processing activities such as pseudonymisation). Therefore, as Codes of Conduct are developed by industry stakeholders they can provide sector-specific guidance on how to implement GDPR requirements in practical ways. In this regard, they can address the unique challenges, risks, and best practices associated with data processing in a particular industry/processing activity, providing tailored guidance for compliance. Furthermore, they can provide a flexible and adaptable mechanism for addressing sector-specific implementation challenges, as they can be updated and revised over time to reflect changing technologies, business practices, and regulatory requirements. This allows for continuous improvement and refinement of industry-specific data protection practices, ensuring that they remain relevant and effective in a rapidly evolving digital landscape. Consequently, Codes of Conduct perfectly match the current needs when it comes to guiding sector implementation.

In addition, transnational Codes of Conduct undergo a rigorous process of scrutiny by data protection supervisory authorities, including the EDPB (comprised of all EU national data protection authorities), which ensures that 1) they harmonize the interpretation of GDPR among supervisory authorities, 2) do not conflict with GDPR's requirements and, 3) they provide added value as required under GDPR. Therefore, they help achieving harmonization and consistency in the interpretation and application of GDPR across different supervisory authorities and member states. This potential of harmonization inherent to the mechanisms, such as Codes of Conduct, specifically benefits code members which are micro, small and medium-sized businesses ("**SMEs**"). Such SMEs may not have the inhouse resources or scale to liaise with multiple data protection supervisory authorities across multiple member states. Therefore, they promote a unified understanding of GDPR obligations and facilitate consistent enforcement, reducing fragmentation and divergent interpretations among different jurisdictions.

Alongside, the approval procedure supports data protection supervisory authorities to understand the specificities of the affected sector and thus contributes to GDPR's uniformity in its entirety, as the take-aways of the approval of a Code of Conduct can be leveraged in any future actions by the data protection supervisory authorities.

8.1.2 Codes of conduct as tools supporting enforcement

First and foremost, it should be noted that for a Code of Conduct to be operational and to demonstrate compliance by adherence to an approved Code of Conduct, pre-requisite is the monitoring of the adherence to its principles by an accredited Monitoring Body under Article 41 GDPR. For accreditation, monitoring bodies must meet the requirements defined by Art. 41 GDPR, as well as those of the corresponding EDPB guidelines and national accreditation criteria. Accordingly, the key elements a monitoring body must possess in order to receive accreditation and become legally operational are: 1) independence, 2) appropriate level of expertise and 3) established procedures for assessing compliance and handling complaints. In this regard, it is essential to note that the established procedures and for assessing compliance and handling complaints are mechanisms that support and complement the enforcement of GDPR by supervisory authorities.

Given that data protection supervisory authorities face challenges in being provided with sufficient resources to monitor and perform their enforcement on all sections of the market, the added value of the compulsory monitoring including effective complaint mechanisms offered by Codes of Conduct must be considered a value itself. Such monitoring must include procedures and structures for both, continuous oversight and dealing with complaints addressing potential non-conformities with a Code of Conduct's requirements. Requirements of a code as well as the mechanisms regarding oversight and complaints must be transparent to relevant stakeholders, such as data subjects.

In case of a non-conformity, the Monitoring Body must take appropriate measures against a processor or controller and decide on sanctions, which include at least suspension or exclusion from the code. The Monitoring Body must then notify the competent data protection supervisory authority of any action against the controller or processor. It is therefore important to emphasize that this is a mechanism that strengthens the remedy protecting the rights and freedoms of data subjects. Next to the general oversight, the monitoring of Codes of Conduct adds another safeguard for conformity. The obligatory element of integrating complaint mechanism makes available to relevant stakeholders, such as data subjects, an additional leeway to report potential infringements. In case such reports prove justified, the Monitoring Bodies will adopt appropriate sanctions and remedies. As such, monitoring complements the general oversight performed by data protection supervisory authorities.

Finally, Monitoring bodies enable data protection authorities to focus their resources as needed, as the robust oversight of Monitoring Bodies required by GDPR support the enforcement for a certain sector. To remain efficient and effective, authorities may, as needed, adapt their focus in respect of enforcement actions. Given that a monitoring body acts as a liaison between the industry and the data protection authorities by several communication channels, such as informing the authorities of an infringement of a Code of Conduct or regular evaluation reports, expertise and first-hand experience can be exchanged to the benefit of any parties involved. Against the background of a sector specific nature of Codes of Conduct, Monitoring Bodies will develop distinct expertise in a specific sector, allowing to adopt sophisticated and tailored decision in regards of remedies, when needed. Understanding and acknowledging Monitoring Bodies' independence, Monitoring Bodies and related practices of imposed remedies and sanctions might become a trusted reference for data protection supervisory authorities, too. At a minimum, Monitoring Bodies can act as expert

stakeholders for data protection supervisory authorities, likewise as a multiplier and practical translator of data protection supervisory authorities' guidelines. This helps establishing a mechanism that streamlines information and supports the appropriate cross-border enforcement of GDPR by data protection supervisory authorities, particularly in the context of transnational Codes of Conduct.

8.2 Challenges faced when it comes to the approval of Codes of Conduct and their operationalization

Given that those tools provide a significant added value when it comes to supporting GDPR harmonization and enforcement, it is essential to emphasize that the operationalization of such tools is still facing procedural obstacles. Further streamlining of approval and accreditation procedures under Article 40 and 41 GDPR is highly welcomed in that area and recommended to be taken into consideration in the in view of the 2024 GDPR review.

8.2.1 Competent data protection authorities for transnational Codes of Conduct, streamline of procedural elements

Further clarification on how to determine the competent data protection supervisory authority is required when it comes to the approval process of transnational Codes of Conduct in accordance with Article 40.5 GDPR. As organizations involved in the approval process of several Codes of Conduct, we have encountered varying interpretations by data protection supervisory authorities when it comes to factors that determine their competence. As a result, approval processes for Codes of Conduct have been delayed, and in some cases suspended, because data protection authorities could not mutually resolve their competence. As a result of these procedural obstacles, the complementary enforcement potential that these Codes of Conduct have to offer has not been realised.

We highly appreciate the guidelines developed and published by the data protection supervisory authorities, and generally do not request any clarifications that go beyond such guidelines. Nonetheless, a closer or rather harmonized application, though, would benefit the development of Codes of Conduct, significantly. Especially in cases of transnational Codes of Conduct, that will apply to any of the member states, the competency should not be considered an obstacle. A harmonized interpretation of GDPR is sufficiently safeguarded by the EDPB's mandatory involvement.

8.2.2 Periods of authoritative actions relating to Codes of Conduct

Where GDPR provides for distinct periods of action relating to the approval of Codes of Conduct, it would be beneficial to define such periods more realistically, allowing data protection supervisory authorities to adequately conclude in such periods. It is acknowledged that Codes of Conduct, especially in cases of transnational Codes of Conduct, may address highly complex matters and may require extensive alignment. Likewise, it might help the adoption of Codes of Conduct that, in cases such deadlines are not met, a positive decision shall be considered as taken. If authorities cannot by majority determine that a Code of Conduct – or any other self- or co-regulatory measure – conflicts with GDPR, a Code of Conduct must be considered rather in accordance with GDPR.

In this context, we also want to raise awareness that GDPR's ambiguities and limited foreseeability of its enforcement industry may result in ostrich tactics. Low adoption rates of most sophisticated interpretations appear less beneficial than high adoption rates of ambitious but still practical approaches. Especially in economically tense times, investments are used to be strictly evaluated. Therefore, rigorousness of enforcement of GDPR's interpretation must be aligned and balanced with actual enforcement actions. If the level playing field becomes out of balance, this might cause industry to choose carefully its investments given that competitors might do the same. Whilst it is appreciated that there is and that there shall be a striving for the best protection of data subjects, GDPR clearly does not understand the protection of personal data without considering the individual contexts. GDPR rather positions the protection of personal data amidst several interests, freedoms, rights, and obligations by numerous stakeholders. Further adoptions of Codes of Conduct might build the bridge between stakeholders, allowing for higher implementation rates.

8.2.3 Potentially prohibitive administrative fees

A more streamlined process would also allow for better argumentation from interested stakeholders to invest in Codes of Conduct. Especially, where authorities request specific administrative fees for the processing of approvals and accreditations – which may to the knowledge of the author's be up to 50,000.00 EUR per procedure – interested stakeholders require foreseeability of the procedures, especially in regards of timelines. We acknowledge that data protection supervisory authorities may impose fees to the processing of approval or accreditation requests. Nonetheless, the current situation in which investors are lacking foreseeability and processes may take rather years than weeks, these fees might be considered rather a mean to prevent submissions than a reasonable compensation of additional efforts by such authorities. Such an impression is contraindicative to the authorities' obligation to encourage the development of Codes of Conduct.

8.2.4 Accreditation requirements for Monitoring Bodies

The accreditation requirements that a Monitoring Body must meet to become accredited are especially challenging when a Monitoring Body is to be accredited against more than one Code of Conduct in different member states and thus needs to address specific procedural elements that are similar in their goal but may vary in their actual detailed requirements. This in turn causes significant delays in the operationalization of Codes of Conduct because Monitoring Bodies must make significant efforts to adapt to different configurations that achieve in a different way the same goals for each member state. In this respect, a mechanism that will support a consistent interpretation of those accreditation requirements by data protection supervisory authorities is highly welcomed. We acknowledge that different member states may require modifications regarding their national, e.g., administrative, laws. But besides such formalities, we do not see any reason why material requirements should be different, especially referring to GDPR as being a regulation.

Any additional efforts in addressing deviations, limit the scalability of monitoring services, which negatively affects the accessibility for SMEs– which are specifically mentioned to be considered in drawing up Codes of Conduct.

8.2.5 General validity mechanism for Codes of Conduct as tools for transfer

Keeping in mind the 2024 GDPR review, further clarifications are sought with respect to the procedural aspects relating to the general validity mechanism for Codes of Conduct acting as a transfer safeguard under Chapter V GDPR. Codes of Conduct acting as a Chapter V safeguard require, additionally to (1) the positive opinion of the EDPB and (2) the approval by the competent data protection supervisory authority, to be granted (3) general validity by the Commission by way of implementing act[6].

We note that the general validity mechanism as an implementing act as well as its related legal effects against the specific context of Codes of Conduct remains generally unclear. Clarification is sought on what is the procedure for a Code of Conduct to be granted general validity, besides the notification of the opinion of the EDPB to the European Commission, as well as on the related timeframes. In this respect, we consider that general validity shall be granted in a timely manner to not unduly delay the process and to allow for the rapid adoption of these tools by the market. To this end, we recommend that the process between the EBPB and the European Commission be further streamlined. E.g., the substantive assessment of the code by both institutions should, to some extent, be carried out simultaneously and thus at an earlier stage than described in Annex 1 of the related EDPB guidelines[7]. Notwithstanding and in fully appreciation of the powers of the European Commission, procedures by the European Commission should not – by any means – foresee any timelines that exceed the suitable blueprint provided by Article 40 GDPR related to the processes to be performed by the EDPB, i.e., a default period of eight weeks plus an optional extension in case of need, e.g., due to complexity of the case.

Recommendations

EU policymakers and DPAs should:

1. **Review the procedural requirements in receiving a Code of Conduct's approval and a Monitoring Body's accreditation.**

- Generally, the legal framework and EDPB's guidelines are considered suitable, if applied consistently. Specifically for transnational Codes of Conduct, it is recommended to ensure harmonized interpretation, because projects suffer delays, e.g., by means of consistently and mutually determining the competent data protection supervisory authorities.
- Periods as indicated by GDPR are not yet met in practice. So, it is recommended to adapt such periods to more realistic timelines and to clarify that in case data protection supervisory authorities cannot by majority determine undisputable conflicts with GDPR, Codes of Conduct shall be deemed in accordance with GDPR.

[6] See Articles 40.3 and 40.9 GDPR and EDPB-Guidelines 04/2021 on Codes of Conduct as tools for transfers tools, https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf
[7] EDPB-Guidelines 04/2021 on Codes of Conduct as tools for transfers tools, https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf

- Limit deviations in regards of the accreditation criteria for Monitoring Bodies to the minimum needed, e.g., by different administrative member state laws. Any material deviation creates unnecessary obstacles to Monitoring Bodies, which seek to pro-vide their services in several member states, limiting the scalability of their services, which is a key element in ensuring that adherence to Codes of Conduct remains accessible to micro, small and medium sized enterprises.

2. **In regards of third country transfers, a general validity by implementing act is required. It is strongly recommended to ensure that procedural efforts will be streamlined preventing any unreasonable delays in operationalizing such projects.**

- Safeguarding third country transfers is one of the key elements subject to legal, political and operational discussions.
- Codes of Conduct may act as a safeguard provide that, next to the formalities to be met for transnational Codes of Conduct in any case, general validity will be granted.
- Considering the procedural steps of deciding on an implementing act, it is strongly recommended to allow for a material assessment by the European Commission and the EDPB in parallel.

***