bitkom

Position Paper

08. February 2024

Questionnaire for the report on the General Data Protection Regulation

1. General comments

a. What is your overall assessment (benefits/challenges, increase in trust and awareness, etc.) of the application of the GDPR since May 2018? Are there priority issues to be addressed?

Since May 2018, the implementation of the General Data Protection Regulation (GDPR) has significantly shaped the landscape of data protection practices across member federations. Bitkom appreciates the opportunity to engage in the public consultation for this year's report by the European Commission.

The GDPR has undeniably contributed to heightened awareness and improved hygiene in handling personal data. Enhanced emphasis on data protection has fostered a culture within enterprises, encouraging a proactive approach to compliance and an exploration of ways to meet requirements in a more transparent and compliant manner. Impact on businesses becomes visible in the incremental improvement of internal procedures for data discovery and audit trails, particularly in sectors with a high uptake of digital technologies. Significant investments have been directed toward GDPR compliance, especially by SMEs. This reflects the importance placed on adhering to the regulatory framework and improving the global flow of data. These data flows underpin the modern economy and are critical to protecting consumers wherever their data is located. However, as described below, the positive trend towards better data management practices requires the existing hurdles and issues of the GDPR to be improved with this review.

Moving forward, the priorities to address revolve around the practical implementation of GDPR principles. Innovation and emerging technologies stand out as key concerns of our members, with a need to strike a balance between data protection compliance and fostering innovation. Business suffers from potential obstacles that the GDPR may unintentionally create based on a lack of understanding of a specific market sector and an incomplete or one-sided balancing of relevant interests and fundamental rights. This situation blocks innovation, delays product developments, and creates an

immense bureaucratic overhead for businesses. Improvement can be reached by considering the role of the EDPB and the impact of its guidelines on the European industry. Ensuring consistency in applying the risk-based approach and proportionality principles, especially in international data transfers and data breaches, is essential. Improving transparency, communication, and simplifying data processing for corporate groups are avenues to explore for refining the GDPR's practical implementation. This can be achieved by a much stronger and earlier involvement of all relevant stakeholders when guidelines are intended to be developed to achieve a more balanced and society-wide accepted interpretation of GDPR. Concerns regarding a perceived zero-risk policy and inconsistent recommendations by some DPAs and the EDPB further highlight the need to align approaches with GDPR principles.

Specific concerns were expressed about certain national DPAs potentially exceeding their powers under the GDPR. This poses a risk to the balanced approach supporting innovation and economic growth in Europe. While the GDPR grants national authorities oversight, investigative, corrective, advisory, and enforcement powers, some interpret it expansively, going beyond EU legislators' intent. Such quasi-legislative actions without safeguards threaten to fragment GDPR interpretation, harming businesses and consumers across Europe. Bitkom urges the European Commission to clearly define national authorities' powers, ensuring discretion within a risk-based framework that protects privacy and supports innovation, avoiding unnecessary restrictions or lack of EU-wide consistency.

Bitkom members expressed additional concerns, emphasizing the importance of scrutinizing tools for international data transfers in accordance with the GDPR. These concerns encompass identified deficiencies that must be rectified to enable European companies to trust these tools without facing excessive compliance challenges. Some members also pointed out limitations on sharing customer data among pertinent group entities, causing frustration with customer expectations. To address these issues and align the tools with GDPR objectives, a comprehensive evaluation and potential enhancements are recommended, aiming to facilitate seamless cross-border data flows. Additionally, the pivotal role of anonymization in balancing privacy and the use of data for artificial intelligence is emphasized. Practical guidelines for standardized anonymization methods, privileges for processing pseudonymized data, and the exclusion of the process of rendering data anonymous as processing under Art. 4 Subsection 2 GDPR are considered essential solutions. Additional challenges persist in the coexistence of outdated sector-specific rules like the old ePrivacy Directive alongside GDPR. While GDPR provides a technology-neutral, risk-based framework, concerns exist about the comprehensive scope of the ePrivacy Regulation covering processing subject to the outdated ePrivacy Directive. Members suggest withdrawing the 2017 ePrivacy draft and repealing the ePrivacy Directive to align regulations more effectively and eliminate the need for sector-specific rules. Perspectives on Articles 82 and 83 of the GDPR are also crucial, advocating for the establishment of a clear threshold for non-material damage in individual and collective redress claims and a clear framework in the calculation of administrative fines. Common and clear standards are sought to ensure proportional sanctions, consistency with GDPR concepts among all members states, and avoidance of incentivizing investigations

based on turnover. A risk-based approach aligned with GDPR objectives would be emphasized and different fines for identical delinquency could be avoided.

Our assessment of the GDPR's application in the following questionnaire reveals a multifaceted landscape. While there is a consensus on the need for ongoing evaluation and improvement, the specific nuances of concerns and proposed solutions highlight the complexity of the data protection landscape in Europe. Addressing these priority issues will contribute to the continued effectiveness of the GDPR in balancing data protection and technological innovation.

2. Exercise of data subject rights

a. From the individuals' perspective: please provide information on the exercise of the data subject rights listed below, including on possible challenges (e.g. delays in controllers/processors reply, clarity of information, procedures for exercise of rights, restrictions on the basis of legislative measures, etc.). From the controllers and processors' perspective: please provide information on the compliance with the data subject rights listed below, including on possible challenges (e.g. manifestly unfounded or excessive requests, difficulty meeting deadlines, identification of data subjects, etc.).

-Information obligations, including the type and level of detail of the information to be provided (Articles 12 to 14)
-Access to data (Article 15)
-Rectification (Article 16)
-Erasure (Article 17)
-Data portability (Article 20)
-Right to object (Article 21)
-Meaningful explanation and human intervention in automated decision making (Article 22)

Where possible please provide a quantification and information on the evolution of the exercise of these rights since the entry into application of the GDPR.

Talking from the perspective of our membership as controllers and processors, we underscore a prevalent issue concerning insufficient awareness among data subjects regarding the nuanced limitations of data protection rights outlined in the GDPR. These rights, far from being absolute, are intricately balanced against the rights of others. There's a noted misuse of GDPR rights, detached from their intended context of

safeguarding fundamental rights. Instead, they are wielded for general complaints about products or services, divorcing them from a clear connection to the processing of personal data. In addition to that, very often the right of access is exercised in an abusive manner by the data subject. For example, a customer dissatisfied with supplier's performance might request information about all stored data in order to raise pressure on the supplier into giving in to a legal dispute. Or a former employee who is disputing with his employer may ask for all e-mails or notices written in which the employee is mentioned during his time of employment. Often companies are also faced with access requests by data subjects in the context of litigation. These requests do not only cause significant additional expense for controllers but also collide with the purposes set out in recital 63 and undermine the burden of proof in civil litigation (by an almost unlimited "fishing for evidence"). Responses gleaned from members collective experiences reveals a disproportionate burden on controllers and processors, struggling to elucidate unclear requests—particularly those generated by automated tools designed for data subjects. The lack of practical guidance on resolving these tensions from the EDPB and DPA's, as well as detail on what is expected with respect to controls under the Accountability Principle (and understanding of how such expectations may change over time), makes it even harder for companies to reasonably anticipate or plan for compliance while bearing a disproportionate risk of turnover penalties should their good-faith solutions be deemed insufficient. For quantification, we noticed an increase of Art. 15 requests after the entry into force of the GDPR in 2018 and 2019. After a decrease in 2020 – 2022 we notice an increase again in 2022, which seems to be mainly triggered again by enterprises trying to make a business model out of encouraging data subjects to submit requests (e.g. https://itsmydata.de/startseite-en/). This trend continues recognizable in 2023.

Further details, showing the need for an effective and equitable implementation of data subject rights, are listed below:

Information Obligations (Articles 12 to 14)

The GDPR's stipulations regarding information obligations have presented challenges, especially concerning the extensive nature of information required under Art. 13 and Art. 14. The inconsistency in treating data that the data subject has made publicly available poses uncertainties. Further, the withdrawal of consent under Art. 7(3) affecting contractual obligations warrants clarification to avoid potential conflicts. Clarity on the scope of the controller's duty to provide a copy of personal data under Art. 15(3) is essential. The need for greater clarity in the context of information provision is underscored by the potential misuse of GDPR rights for purposes beyond data protection concerns.

Access to Data (Article 15)

The right to access data under Article 15 has posed challenges related to the identification of the data subject and the scope of the right. The need for clarification on the concept of "manifestly unfounded or excessive" requests (Art. 12(5)) is evident, along with the necessity to strike a balance between the right to access and the protection of personal data. Clarifying the Article 12(5) exception regarding pre-litigation scenarios and legal claims is crucial to avoid potential misuse.

Rectification (Article 16)
The right to rectification, while rarely exercised, demands attention. Challenges are mitigated by the ability of businesses to verify most personal data from independent sources. However, clarity on rectification requirements and processes remains necessary to streamline compliance.

Erasure (Article 17)
Erasure requests have witnessed an increase, accompanied by challenges such as insufficient awareness about data retention obligations and technical complexities in manual deletion. Guidance on erasing user-generated content and navigating the intersection with other data subjects' rights is essential.

Data Portability (Article 20)
Although rarely exercised, the right to data portability necessitates clear methodologies and agreed-upon formats. Guidance in various sectors is lacking, creating uncertainty for controllers and data subjects alike.

Right to Object (Article 21)
The right to object, while relatively infrequently exercised, presents challenges related to its use for marketing reasons and potential misuse to withdraw consent or express dissatisfaction with products or services. Further clarity on the legitimate grounds for objection is essential.

Meaningful Explanation and Human Intervention (Article 22)
The right to meaningful explanation and human intervention in automated decision-making, though rarely exercised, poses challenges in the context of increasing automation. Balancing this right with the protection of sensitive business information and trade secrets requires careful consideration.

b. Do you avail of / are you aware of tools or user-friendly procedures to facilitate the exercise of data subject rights?

Yes, online self-service tools and forms already play a pivotal role for our members, offering a secure and efficient means to handle data subject requests at scale. Such tools empower users to assert control over their accounts, allowing for the secure management, download, or deletion of their own account or associated content. This approach aligns with GDPR principles, promoting privacy by design and default, as well as data minimization. The absence of these user-friendly tools would not only jeopardize the efficiency of processing requests but also introduce significant risks. Unauthorized access by individuals other than the account holders could compromise data integrity and privacy. The use of online self-service tools emerges as a proactive measure to mitigate these risks.

However, it's essential to acknowledge the challenges outlined in the broader context of data access and portability rights. Developing systems to comply with these rights presents inherent complexities, ranging from cost considerations to the technical feasibility of providing comprehensive datasets. While these challenges are valid and pose potential strains on companies, the lack of practical guidance and detailed expectations from regulatory bodies complicates the path to compliance. In navigating this landscape, companies must strike a delicate balance between facilitating user-

friendly processes and addressing the technical and financial challenges associated with data subject rights. Proactive measures not only enhance GDPR compliance but also contribute to a more streamlined and efficient exercise of data subject rights. The overarching goal is to create an environment where data subjects can assert their rights with ease, while companies are enabled to navigate the intricate landscape of data protection with clarity and foresight.

c. Do you have experience in contacting representatives of controllers or processors not established in the EU?

N/A

d. Are there any particular challenges in relation to the exercise of data subject rights by children?

The exercise of data subject rights by children under the GDPR introduces challenges, particularly concerning the involvement of parents. While the GDPR grants children the right to assert their data subject rights, uncertainties persist regarding parental roles in this process.

Despite acknowledging children's agency, practical complexities arise in determining how parents can effectively exercise these rights on behalf of their children. Current DPA guidance emphasizes the role of parents in decision-making for their children's best interests. However, the practical implementation of parental involvement remains a challenging aspect for organizations. One additional concern arises in the context of consent, especially concerning tracking tools. The challenge lies in reliably verifying the age and legal capacity of the consenting individuals, raising questions about the legitimacy of consent. Ensuring that the person providing consent is of legal age becomes crucial, as it determines their capacity to make decisions in their own best interest. This complexity adds an extra layer of intricacy to the already challenging landscape of managing data subject rights for children.

To address these challenges, there is a need for flexibility within the GDPR framework, allowing organizations to navigate nuances in parental involvement in a case-by-case manner. Striking a balance between recognizing children's rights and considering parental responsibility is crucial, especially in contexts where consent complexities may compromise the validity of data processing involving children.

3. Application of the GDPR to SMEs

a. What are the lessons learned from the application of the GDPR to SMEs?

The implementation of the GDPR has underscored the fundamental nature of privacy as a universal right applicable to all, irrespective of an organization's size. It has accentuated the significance of upholding individual privacy and safeguarding their data. However, for SMEs, the compliance journey under the GDPR has been marked by a notable burden. The regulation, while reinforcing the importance of privacy, has

introduced intricate requirements, including data mapping, the appointment of DPOs, ensuring data portability, and specific contracting obligations. SMEs, like their larger counterparts, have had to make substantial investments in robust data security measures to fulfil these requirements, protecting customer data against potential breaches. This process proves particularly challenging considering their limited resources.

Moreover, the varied interpretations of GDPR across EU countries have added complexity to the compliance landscape, posing specific difficulties for SMEs that may lack the resources to navigate diverse legal landscapes. SMEs have found that legal certainty is often only achievable through collaborative efforts and resource pooling. By joining forces with other entities, SMEs can navigate the complex GDPR landscape more effectively, sharing insights and resources to overcome the hurdles posed by the regulation. The absence of standardized tools at the EU level compounds these challenges, making it harder for SMEs to streamline compliance efforts.

Based on the input from our members, streamlining compliance requirements for SMEs should be a key consideration in this review. Simplifying the process for small businesses, while maintaining essential consumer protections, would address these concerns and focus the update effort on a critical issue. Thereby, the regulatory playing field is leveled, ensuring that all businesses, regardless of their size, adhere to the same privacy standards. This approach fosters a more equitable digital ecosystem, promoting fair treatment and accountability across the spectrum of businesses.

b. Have the guidance and tools provided by data protection authorities and the EDPB in recent years assisted SMEs in their application of the GDPR (see also the EDPB data protection guide for small business)?

N/A

c. What additional tools would be helpful to assist SMEs in their application of the GDPR?

N/A

4. Use of representative actions under Article 80 GDPR

a. From the controllers and processors' perspective: are you aware of representative actions being filed against your organisation(s)?

The landscape of collective redress mechanisms is evolving, with an anticipated increase in the utilization of Art. 80 GDPR representative actions. This shift is fueled by the growing trend of treating litigation as a lucrative business model, causing major costs for accused businesses. It is crucial to strike a balance that prevents frivolous

claims, ensuring that litigation genuinely serves the purpose of safeguarding individuals' rights rather than being exploited for financial gain.

Historically, representative actions under Art. 80 have seen limited use, with only sporadic cases across the EU. However, the adoption of collective redress mechanisms in 2023 is expected to reshape this landscape, potentially leading to a more extensive application of Art. 80 in the coming years. The careful application of requirements for entities bringing such actions becomes paramount to prevent vexatious claims and to ensure that litigation genuinely empowers individuals to assert their rights.

The call for clarity on compensatory damages gains significance, especially in the context of a collective action ecosystem. Controllers face the looming threat of substantial exposure in opt-out actions, with a lack of clear guidelines on the calculation of damages adding complexity to the scenario. This clarity is essential to prevent excessive exposure for controllers and to maintain the genuine purpose of litigation in protecting individuals' rights.

Harmonization of domestic procedures emerges as a critical need to address inconsistencies between Member States. This harmonization aims to prevent duplicative actions and alleviate the administrative burden on local courts and companies. Ensuring a cohesive and equitable application of Art. 80 GDPR representative actions across the European landscape is essential for effective privacy protection and regulatory accountability.

b. For civil society organisations: have you filed representative actions in any Member State (please specify: complaint to DPA or to court, claim for compensation; and the type of GDPR infringement) and if yes, what was your experience? Do you intend to take actions under the Representative Actions Directive?

N/A

5. Experience with Data Protection Authorities (DPAs)

a. What is your experience in obtaining advice from DPAs?

Obtaining advice from DPAs has been a mixed experience, varying significantly across Member States and countries. Positive interactions and examples have been noted, with instances of effective communication, particularly via telephone channels, proving more fruitful than written correspondence. However, it is crucial to acknowledge that the availability of resources within DPAs can be a limiting factor, with shortages of employees reported in certain cases.

While positive experiences exist, challenges in obtaining tailored guidance persist. DPAs, facing constraints on resources, often hesitate to provide the nuanced advice

required due to the horizontal and principles-based nature of the GDPR. Specific areas of guidance could include providing additional affirmation that all basis for processing personal data should be treated equally (especially affirming the importance of legitimate interest) and updating the 2014 guidance from the Article 29 working party on the use of anonymous and pseudonymous data. The later would be particularly important in helping with the development of new technologies including generative AI. Some DPAs even exhibit delays in responding to inquiries or failing to respond at all. These delays are noted not only in individual inquiries but also in industry-level requests, such as those related to declarations of consent. Additionally, the approval processes for codes of conduct and binding corporate rules (BCRs) are reported to be lengthy and complex (see question 12).

The overburdening of DPAs with technical breach notifications and formal complaint-handling may contribute to this reluctance towards tailored guidance. Addressing these challenges necessitates a collaborative approach, with the EDPB encouraged to create a framework facilitating voluntary engagement between data controllers and DPAs. Latter should also play a more proactive role in engaging with other regulators, fostering clarity on their areas of competence to avoid conflicting rulings. Ensuring adequate resourcing of DPAs at Member State level are adequately resourced is considered essential to improve their effectiveness. In addition, a strong collaborative approach with early involvement of all relevant stakeholders would help to create a innovation-friendly environment.

Another dimension of the experience involves DPAs' reluctance to advise on complex matters in cross-border scenarios requiring GDPR interpretation. The cautious approach is attributed to the need to consider potential divergent views among DPAs. In the context of complaint resolution, companies seeking advice on issues such as complaint scope and alternative suggestions for amicable resolution have encountered varying degrees of guidance. While supervisory authorities are generally willing to discuss concerns related to the Amicable Resolution process, there is a call for more directional advice with robust reasoning.

b. How are the guidelines adopted so far by the EDPB supporting the practical application of the GDPR?

The guidelines issued by the EDPB play a crucial role in supporting the practical application of the GDPR. While they can potentially serve as valuable tools for implementation and compliance, several issues in the execution process warrant attention for improvement according to our members.

Positively, EDPB guidelines offer a theoretical foundation, providing insights into the interpretation of GDPR. However, stakeholders express a need for more concrete and precise guidance that is adaptable to real-world situations, especially in the form of practical use cases. This would enhance the applicability of the guidelines, offering clearer insights into compliance requirements. There is a consensus among stakeholders that certain guidelines, particularly those related to international data transfers, right of data access, automated decision making, and data breaches, need refinement. Concerns have been raised about the consistent application of the risk-based approach and proportionality principles outlined in the GDPR. It's important to

note that, some guidelines might not withstand judicial scrutiny; however, due to a lack of resources, most companies cannot afford to pursue litigation.

Bitkom members particularly stressed the importance of EDPB efforts in creating a more integrated approach to industry feedback during public consultations to solve mentioned problems. They argue that industry input is not consistently considered when shaping guidelines. This leads to a potential dysfunctionality of guidelines, including an overly strict interpretation of GDPR, theoretical over-preparedness leading to watered-down guidance, non-practical advice that is challenging to implement, and guidelines anticipate the legislative processes without a legal basis.

The One Stop Shop (OSS) and Improve Procedural Rules play a crucial role in establishing consistency in guideline implementation. We advocate for the harmonization of OSS procedures, recognizing its significance as a critical tool in this regard. In alignment with the GDPR procedural rules, our support extends to specific changes aimed at strengthening the framework, including safeguarding the confidentiality of administrative files through an effective sanctions regime in cases of breaches, ensuring the right-to-be-heard with reasonable and proportionate timelines, promoting amicable settlements throughout cross-border procedures, and fostering outcome-based enforcement. To achieve this, we emphasize compelling complainants to exhaust industry complaint mechanisms and establishing mechanisms for amicable settlements at all procedural stages.

c. Are DPAs following up on each complaint submitted and providing information on the progress of the case?

There is a lack of transparency in the timelines set by DPAs for providing information and progress on a case. At present, there are no harmonized procedural rules requiring parties under investigation to be kept informed of progress. The timing seems to depend on the resources and workload of the DPA concerned at any given time. In our members experience is that in the past, there have been very long delays between the submission of responses and hearing back from DPAs, e.g. up to 1 year. However, in the last 6 months, we have seen an improvement in the speed with which DPAs are processing complaints and providing updates.

d. Are you aware of guidelines issued by national DPAs supplementing or conflicting with EDPB guidelines? (please explain)

Members recognized that there are partially different interpretations of EDPB guidelines across Europe, with some national DPAs issuing guidelines that may supplement or conflict with EDPB guidance. Clarification by the EDPB would be beneficial to ensure consistent interpretation and application of the GDPR.

6. Experience with accountability and the risk-based approach

a. What is your experience with the implementation of the principle of accountability?

A case-by-case assessment is needed to determine whether data processing that interferes with this right is lawful. For example, some DPAs have recently adopted a zero-risk policy for the transfer of personal data to third countries, which contradicts the GDPR's risk-based approach to justifying data transfers. Similarly, the EDPB has issued recommendations on appropriate additional safeguards under Art. 46(2) GDPR, which can be understood as a zero-risk approach. This is incompatible with the guiding principles of the GDPR. Therefore, the EDPB should correct the wording of these recommendations to clarify the standards to be applied under Art. 46 GDPR. Instead, we see efforts to work towards a complete reversal of the burden of proof in civil proceedings, including supporting case law.

More complexion is added through contradictory assessments in EDPB guidances, such as Scenarios 15 and 16 of EDPB Guidelines 01/2021 regarding Personal Data Breach Notification. In Scenario 15, the EDPB considers the case non-reportable to a DPA, as the recipients were contacted, likely resulting in the deletion of the mistakenly received emails. Conversely, in Scenario 16, where similar steps were taken to contact recipients, the EDPB deems the case reportable to the DPA, citing uncertainty about the potential posting of wrongfully received information on social networks. EDPB's Recommendations 01/2020, particularly Use Cases 6 and 1, show further adoption of zero-risk policies and pose significant challenges for SaaS providers. It argues that the current state of technology lacks effective measures to prevent unauthorized access by public authorities in certain scenarios. Given the evolving nature of technology, the publication three years ago, and the availability of alternative protections necessitates reconsideration. Clarification is needed from the European Court of Justice (ECJ) regarding its role in reducing administrative burdens. Additionally, a positive step would involve comparing EDPB guidance with additional DPA guidance published to ensure uniformity in risk approaches across the EU.

b. What is your experience with the scalability of obligations (e.g., appropriate technical and organisational measures to ensure the security of processing, Data Protection Impact Assessment for high risks, etc.)?

The experience with the scalability of obligations, such as appropriate technical and organizational measures and Data Protection Impact Assessments (DPIAs), reveals challenges in the application of a risk-based approach by DPAs. DPAs have been observed to reject the risk-based approach, especially concerning data transfers to third countries. Some have recognized additional measures going beyond the non-exhaustive list of technical, organizational, and contractual measures set forth in EDPB supplementary measures guidance. It is however unclear whether the supplementary

measures recognized by some DPAs would be directly applicable in all EU Member States.

A significant concern lies in DPAs and the EDPB adopting a zero-risk policy, which conflicts with the concept of appropriateness and inhibits a one-size-fits-all approach. This rigid stance poses challenges for the development and deployment of Privacy Enhancing Technologies (PETs) and Privacy-Preserving Machine Learning (PPML), hindering innovation and investment in this domain. Pseudonymous datasets with state-of-the-art technical and organization measures can support privacy- and confidentiality, and hence would merit further attention from EDPB and DPAs. The following points would lead to significant improvement and more security for our members and individuals:

- Practical guidelines on standardized anonymization methods should be established to ensure that data rendered anonymous under the GDPR remains outside its jurisdiction.
- Anonymizing personal data, making the data subject unidentifiable, should not be deemed as "processing" under Article 4 Subsection 2 GDPR, and no explicit legal basis should be required.
- Pseudonymized data should be considered anonymous if the re-identification key is not reasonably available, allowing the pooling of data for analysis, benefiting smaller entities with limited data.
- Using personal data for internal analytics and algorithmic model development is akin to processing data for statistical purposes, with potential GDPR easements, but it is crucial to distinguish its application on customers to mitigate impacts.
- The exemption in Article 22 Subsection 2 GDPR on automated decisions should not be overly strict in interpreting the "necessity" of such decisions.
- Article 22 GDPR, concerning automated decisions with legal or significant effects, should not apply to decisions merely replicating human decisions.
- Updating Working Party 05/2014 guidelines is necessary to establish a practical standard for anonymization guidance, promoting uniformity across EU Member States and departing from the requirement that anonymization occurs only when reidentification is impossible.

Even if PETs and PPML may not be silver bullet solutions in all situations, Bitkom recommends further exploring these new solutions, and assessing where they can offer alternative solutions to e.g. anonymization techniques. This can foster innovation, including machine learning that is used to advance societal goals or to protect individuals' fundamental rights.

The treatment of IP addresses as personal data under GDPR poses another challenge, subjecting them to data transfer restrictions. The free flow of IP addresses is essential not only for the functioning of the global Internet, but also for advanced cybersecurity applications, which rely on IP addresses and other metadata from around the world. While destination countries with adequacy decisions, such as the EU-US Data Privacy

Framework, currently evade this issue, the potential invalidation of these decisions could lead to a situation where GDPR restricts the processing of IP addresses linked to EU residents in third countries or even prevents them from leaving the EU. Such an outcome could result in a fragmented European Internet, jeopardizing data privacy and isolating the EU from global marketplaces, information exchanges, and social media platforms. One viable solution may lie in reconsidering IP addresses as not always constituting "personal data" under GDPR, aligning with the ECJ's approach in Breyer v. Bundesrepublik Deutschland. This case clarified that dynamic IP addresses qualify as personal data only if they can be linked to an individual by the processor. However, some DPAs have rejected this relative approach, insisting that all IP addresses should be deemed personal data. Establishing guidelines or legal clarification for DPAs that acknowledge IP addresses as non-personal data when the data processor cannot tie them to a real person could enable an application of GDPR that both preserves the open Internet and better protects privacy online. An additional noteworthy observation is the lack of differentiation in the GDPR between business-to-business (B2B) and business-to-consumer (B2C) scenarios. Advocates suggest that an upstream risk-based approach, particularly for B2B situations, could streamline compliance, avoiding the need to fulfill consumer law requirements in the B2B realm. Long-term thinking is proposed, emphasizing the potential exclusion of certain data categories, such as employee data, through standardized European legislation.

7. Data protection officers (DPOs)

a. What is your experience in dealing with DPOs?

The experience in dealing with Data Protection Officers (DPOs) presents a multifaceted perspective. The requirement to appoint a DPO has been effective in ensuring that organizations that traditionally did not have staff responsible for data protection would integrate one into their structure to help assist with GDPR compliance. However, the role of DPOs is observed to be played inconsistently across industries, with varying emphasis on the independence of the role. Limited guidance from DPAs contributes to disparities in DPO practices across companies. DPAs should clarify that there is not a one size fits all solution to the DPO Role and should provide suitable deference in application of the requirement.

Additionally, concerns arise regarding the potential prescriptiveness of DPO appointments. The GDPR mandates a DPO to be "conflict-free," yet also "informed" and "appropriately qualified," creating tension in practice. This tension may lead to the appointment of less senior individuals with limited expertise, potentially impacting their ability to provide sophisticated insights into business practices.

From the SME perspective, there is a call for standardized processes at the EU level to reduce the administrative burden associated with the examination for DPO registration. The variability in the registration process, whether online or in writing, across different cases is noted, demanding substantial resources.

b. Are there enough skilled individuals to recruit as DPOs?

Due to the variety of legal requirements under Article 39 of the GDPR, it is difficult to find one individual with all the necessary skills. Instead, teams could be set up (e.g. Offices of DPOs) to achieve greater clarity in the division of responsibilities. Furthermore, members notice that there is a lack of academic qualifications for the role of DPO.

c. Are DPOs provided with sufficient resources to carry out their tasks efficiently?

As per answers above (7a and 7b), the expectations placed on DPOs require significant resources which are not available at times.

d. Are there any issues affecting the ability of DPOs to carry out their tasks in an independent manner (e.g., additional responsibilities, insufficient seniority, etc.)?

It remains unclear what the consequences might be for controllers should they not adhere to DPO advice. This creates uncertainty in the interactions and prevents more dynamic decision-making. Likewise, the issue of the DPO role's independence remains as a key one to address by DPAs. One possibility could be to stipulate that the DPO is a staff position so that the respective officer remains capable of acting independently.

8. Controller/processor relationship (Standard Contractual Clauses)

a. Have you made use of Standard Contractual Clauses adopted by the Commission on controller/processor relationship?

Yes. They are referred to in e.g. the standard data protection terms our members are using with their vendors.

b. If yes, please provide feedback on the Standard Contractual Clauses?

In the overall landscape, it becomes obvious that particularly SMEs are very willing to use the standard contract clauses. Larger companies with their own ecosystem of contract templates however insist on using their own templates. The Commission's model has not yet established itself as the market standard due to mentioned challenges.

Turning to joint controllership responsibilities under Article 26 Subsection 3 GDPR, a relevant factor for assessment should be the practical ability to influence arrangements. This recognizes the importance of practical influence in determining the responsibilities of joint controllers. Additionally, under Article 82 Subsection 3 GDPR, the issue of liability when processors engage further sub-processors is crucial.

Limiting the controller's liability in cases where the controller is not responsible for the event giving rise to the damage is a valid suggestion. This limitation aligns with the need for a fair distribution of liability in complex data processing chains involving sub-processors.

9. International transfers

a. For controllers and processors: Are you making use of the Standard Contractual Clauses for international transfers adopted by the Commission? If yes, what is your experience with using these clauses?

Yes, our members are making use of the SCCs for international transfers as required by the GDPR. While the intention of SCCs is to ensure safeguards, the administrative burden associated with them has been onerous for businesses. These practical issues with the SCCs raise several important considerations.

SCCs, while integral, now require an additional Transfer Impact Assessment (TIA), which presents challenges, given the diverse use cases. Conducting these assessments involves engaging external legal counsel due to the intricate legal considerations of the destination jurisdiction. Some importers (i.e. SMEs) may not have the resources to undertake this obligation. In addition, these increased efforts may not be sufficient to address in enough detail the entire legal framework of a territory. Despite striving to implement additional safeguards, challenges persist, and compliance with GDPR requirements remains a nuanced task, particularly for non-adequate jurisdictions other than the US, which is addressed by the EU-US Privacy Framework. The details of TIAs are not set forth in GDPR, yet the guidance from the EDPB remains impractical when considering the multitude of required use cases. Future guidance must consider what is practically feasible versus a best of all world's solution. Particularly when the requirement is not set forth in the GDPR itself it is inappropriate for the EDPB to "legislate" their preferred format.

Member companies now primarily rely on the EU-US DPF for data transfers from the EU to the US but continue incorporating the EU SCCs into their Data Processing Addendum as a backup option for customers. If the Data Privacy Framework were to be invalidated as the EU-US Privacy Shield was in the Schrems II decision, some DPAs would likely again take this as an opportunity to double down on their view that EU personal data cannot be processed in the US consistent with the GDPR. This interruption of international data flows and high level of legal uncertainty poses a risk of fines, even for organizations acting in good faith by using their own resources within the framework of the EU's adequacy decision.

While the reviewed 2021 SCCs ensure adequate safeguard for the transfer of data to non-adequate countries, challenges remain in the present in SCCs. Art. 14 SCCs requires an in-depth study of the legal framework that is applicable to the territory where the data importer is located. This triggers additional efforts in external resources (i.e. external counsel) to examine in detail such legislation. In absence of an

aligned threshold determining when a TIA will be satisfactory by a DPA, the abovementioned efforts may not be sufficient. Furthermore, the wording in Arts. 14 and 15 SCCs raise disputes in contract negotiations about who is responsible for conducting the TIA and whether the TIA needs to be shared with the other party.

Simplifying the administrative procedure for Binding Corporate Rules comparable to SCCs is suggested as one possibility to enhance accountability and transparency. A second suggestion is based on the notable challenge that arises from the need for companies to assess the privacy standards in the receiving jurisdiction themselves, relying on their resources. Instead, it should be the Commission itself to determine whether the local laws and customs of a third country represent an obstacle to the transfer of personal data. This would relieve companies from the burden of individual assessments and guarantee an equal footing on both sides of the transfer for data protection through the SCCs.

b. For controllers and processors: Are you using other tools for international data transfers (e.g., Binding Corporate Rules, tailor-made contractual clauses, derogations)? If yes, what is your experience with using these tools?

Yes, members highlighted successes with Processor Binding Corporate Rules, as approval processes and reviews by the EU supervisory authorities can be extensive. The publication of the EDPB's processor-BCR referential can help for further improvement of this tool.

c. Are there any countries, regional organisations, etc. with which the Commission should work in your view to facilitate safe data flows?

We welcome the adoption of the EU-US Privacy Framework and generally call on the EC to continue its work to develop new adequacy decisions that will allow for the lawful transfer of data outside the EU while respecting the privacy of citizens. Adequacy decisions are the most appropriate instrument for international data transfers, as they provide the most appropriate safeguards for both data controllers and data subjects. Existing Adequacy decisions should be continued to guarantee long-term stability. However, the overall list of countries covered by an adequacy decision is still quite limited and falls short of covering data transfers in an environment where global data flows are increasing daily. The EC should take note of this gap and speed up the process of adopting adequacy decisions for third countries and territories with adequate levels of protection.

The list below comprises countries, some with sunset clauses, that our members suggest could be evaluated for the implementation and continuation of adequacy decisions. It is not exhaustive, and the order does not indicate the countries' relevance to our members:

- Australia
- Indonesia

- Singapore
- India
- Ukraine
- South Africa
- Thailand
- Malaysia
- Hong Kong
- Taiwan
- Saudi Arabia
- Guatemala
- Turkey
- Madagascar
- Vietnam
- Philippines
- Nigeria
- UAE
- Kenya
- Senegal
- Colombia
- Mexico
- Brazil
- Peru
- Chile
- Ecuador
- UK
- US (a permanent solution that diminishes the risk of potential NOYB requests to annul the DPF or equivalent Adequacy decisions that may be approved in the future)

10. Have you experienced or observed any problems with the national legislation implementing the GDPR (e.g., divergences with the letter of GDPR, additional conditions, gold plating, etc.)?

For the effective functioning of the internal market and to avoid unnecessary burdens on businesses, it is essential that national legislation does not go beyond the scope of the GDPR and/or does not introduce additional requirements where there is no scope. However, our members highlighted divergence in the interpretation of rules among various national DPAs.

One divergence was highlighted in relation to Article 45/46 GDPR and particularly sensitive data according to Article 9 GDPR. With regard to the current opt-out procedures of the German government for organ donation and electronic patient records, the opt-out procedure should also be assessed as extremely critical. This is because patient data can be transferred to third countries, e.g. to pharmaceutical companies outside the EU.

11. Fragmentation/use of specification clauses

a. Please provide your views on the level of fragmentation in the application of the GDPR in the Member States (due to Member State implementation of the GDPR or the use of facultative specification clauses, such as Articles 8(1) and 9(4) GDPR).

The GDPR aimed to harmonize data protection rules across the European Union (EU), but it has fallen short of this objective due to significant fragmentation in Member States' implementations. This fragmentation becomes evident in various aspects, such as consent for the use of cookies, privacy impact assessments, the interpretation of legitimate interest, flexibility around the “age of consent” and the use of facial recognition technology. The divergence is particularly notable in areas where Member States have leeway, such as for processing biometric data based on substantial public interests or national security. Furthermore, the differing positions adopted by DPAs on specific requirements, such as the Guest Check-Out feature for online shopping, underscore the need for proactive efforts by the EDPB to drive true uniformity. Only with collaborative frameworks and mutual recognition of positions among DPAs, processes for organizations operating across diverse Member States can be efficiently streamlined.

b. Please specifically identify the area in which you consider there to be fragmentation and whether it is justified.

Fragmentation is observed in specific areas:

- Youth - Minimum Age Requirements for Consent: Discrepancies in minimum age requirements across Member States and varying interpretations by DPAs.
- Key Concepts and Controllership: Different interpretations on fundamental concepts like personal data, anonymization, special categories of data, controllership, and joint controllership.
- Interpretations of Legal Bases: Differing interpretations on the requirements, appropriateness, and lawfulness of specific legal bases, especially in specific contexts.
- Shift from Risk-Based to Zero-Tolerance Approach: Departure of DPAs from the risk-based approach towards a zero-tolerance approach, particularly in areas like anonymization, Technical and Organizational Measures (TOMs), and data transfers.

12. Codes of conduct, including as a tool for international transfers

a. Do you consider that adequate use is made of codes of conduct?

Codes of conduct, as envisioned by the GDPR, are considered a valuable tool by the industry, yet their potential remains largely untapped. While only a few codes of conduct have secured approval, both at the member state and EU-wide levels, our members welcome the idea embedded in the GDPR. The tool provides a constructive means for collaboration between industry players and DPAs, fostering mutual trust and understanding.

However, challenges persist in realizing the full potential of codes of conduct. The EDPB and DPAs are noted for interpreting the GDPR in a manner that some perceive as conflicting with the clear wording of Article 41. This misalignment, especially regarding the monitoring of codes of conduct, needs clarification and practical support from the EDPB. Encouragingly, Article 40 and 41 of the GDPR should be further promoted to facilitate the development and application of codes of conduct, with the EDPB playing a supportive role through practical interpretations.

Despite the mentioned hurdles and current limited usage, there is an expressed intention among some industry players to increase their reliance on codes of conduct in the future. Adequate support is crucial for organizations to develop effective codes of conduct, and current challenges indicate underutilization and ineffectiveness in their implementation.

b. Have you encountered challenges in the development of codes of conduct, or in their approval process?

The development and approval of codes of conduct, as envisioned by the GDPR, present significant challenges, impeding their widespread adoption and effectiveness.

One notable challenge is the prolonged approval process and the limited adoption of endorsed codes of conduct at the EU level. Codes of Conduct can take years to be drafted and approved due to the complex requirements to be met and therefore may discourage stakeholders in launching initiatives in general. National DPAs in member states may interpret the requirements differently, leading to varying and, at times, conflicting expectations. Some authorities impose additional requirements that extend beyond the EDPB guidelines. Consequently, obtaining approval for codes of conduct becomes a protracted and complex endeavor, with the process lasting several years in some cases. To address this, the European Commission must take a proactive stance in promoting the development of industry-wide codes of conduct, especially those covering international data transfers. Alternatively, the Commission should acknowledge that codes of conduct may not be accepted unless they surpass GDPR requirements—an impractical expectation for the industry.

Seals and marks could enhance clarity on the use of cookies and related technologies, particularly concerning their legitimate purposes in enabling specific requested services. Such developments would benefit consumers, businesses, and regulators by providing clarity on obligations, improving overall compliance and enforcement efficiency, and easing the burden on small businesses.

c. What supports would assist you in developing codes of conduct? Please clearly distinguish in your reply when Codes are used for international transfers.

In general, strong regulatory guidance and official, timely approval of codes of conduct are essential to incentivize their development. Codes of conduct play a pivotal role in providing legal certainty for users and aiding supervisory authorities in their work. Regulatory support and streamlined approval processes would encourage industries to actively engage in developing codes of conduct, fostering a collaborative approach to compliance and data protection. These measures are critical for realizing the intended benefits of codes of conduct under the GDPR.

More specifically, for codes of conduct related to international transfers, one major obstacle is the stringent requirements set by the EDPB. The EDPB's Guidelines 1/2019 stipulate that the establishment of a private monitoring body is a prerequisite for approving any code of conduct. However, Article 41 of the GDPR provides flexibility by framing the establishment of a monitoring body as optional. This discrepancy creates uncertainty and may impede the development of codes of conduct, particularly those aimed at facilitating international transfers. To address this, initiatives should be considered to make monitoring bodies optional, aligning with the objective of encouraging code development outlined in Article 40(1) of the GDPR.

13. Certification, including as a tool for international transfers

a. Do you consider that adequate use is made of certifications?

The GDPR allows for recognized certification mechanisms, coupled with binding obligations, to enforce the appropriate safeguards. We believe that certification is an adaptable and flexible approach, which allows different systems to be respected while achieving a high level of data protection standards. Any certification program will require robust oversight and regulatory trust. However, these mechanisms have not been widely adopted at EU level. To date, there is only one recognized GDPR certification (the European Data Protection Seal). Increased development of certifications should be done in consultation with the EDPB and promoted as widely as possible.

b. Have you encountered challenges in the development of certification criteria, or in their approval process?

N/A

c. What supports would assist you in developing certification criteria? Please clearly distinguish in your reply when certification is used for international transfers.

N/A

14. GDPR and innovation / new technologies

a. What is the overall impact of the GDPR on the approach to innovation and to new technologies?

Article 1(3) of the GDPR emphasizes the importance of allowing the free flow of data. However, the current implementation doesn't always align with this principle, primarily due to the lack of a consistently applied risk-based approach.

Mainly, better regulation necessitates harmonization. The GDPR, while designed to be future proof, faces challenges in accommodating emerging technologies like artificial intelligence, biotechnology, and blockchain that offer substantial opportunities for industries to enhance their products and services. The overlap with sector-specific legislation, such as the e-Privacy Regulation, Digital Markets Act, Cloud Act, ISO 27001 et seq. and AI Act, introduces complexities and uncertainties at the intersection of these frameworks. The GDPR's risk-based approach holds the potential to make it adaptable to evolving technologies. However, the GDPR, and its associated guidelines, sometimes fall short of fully embracing this approach, posing unintended obstacles to innovative practices. To gain success, guidance and collaboration are needed by the Commission, the EDPB and other relevant regulators to provide workable and scalable

guidance in this space to economic operators and legislative proposals from the Commission must carefully consider potential areas of contradiction and overlap.

b. Please provide your views on the interaction between the GDPR and new initiatives under the Data Strategy (e.g., Data Act, Data Governance Act, European Health Data Space etc.)

The intricate interplay between the GDPR and the evolving legislative landscape introduced by new initiatives such as the Data Act, Digital Services Act, Digital Markets Act, and the AI Act, add layers of complexity to the existing framework. Understanding the implications of these acts and their interactions with the foundational principles of the GDPR is crucial for navigating the evolving data governance landscape in the European Union.

For instance, novel data initiatives, especially those driving innovation and research, may encounter challenges within the GDPR's regulatory framework. Balancing the imperative to encourage innovation with the need to uphold GDPR's privacy and consent principles poses a delicate challenge. To address this, the EDPB could play a pivotal role by providing clearer guidelines or introducing amendments that strike a harmonious balance. Exploring areas such as anonymization techniques, Privacy-Enhancing Technologies (PETs), and the use of artificial intelligence within the bounds of GDPR principles would contribute to a more cohesive regulatory environment. It is furthermore essential that data protection regulations be enshrined in data protection laws, particularly the GDPR, rather than scattered across sector-specific legislation. To ensure legally sound data processing, it is imperative to establish well-defined standards for anonymizing personal data.

Additionally, initiatives promoting data sharing for the public good, such as in healthcare research, may come into conflict with GDPR's principles of data minimization and purpose limitation. Encouraging the creation of regulatory sandboxes, where controlled environments facilitate testing data-sharing initiatives, emerges as a potential avenue to strike a balance between fostering innovation for societal benefit and adhering to GDPR principles.

In the subsequent sections, we will look into selected legislative acts, examining their nuances and evaluating their impact on the evolving landscape of data protection and innovation within the European Union.

Data Act

Interactions between the GDPR and the Data Act introduce complexities and potential misalignments that warrant careful consideration. Overlap is introduced with the Data Act's applicability to both personal and non-personal data, leading to potential issues in enforcement and penalties. The dual enforcement regimes and (potentially) distinct national supervisory authorities for the Data Act and GDPR create challenges, likely resulting in inconsistent enforcement practices across the single market. The relationship and hierarchy between GDPR fines and penalties mandated by Member States under the Data Act remain unclear.

Examples for not entirely resolved overlaps include:

Article 4 (1) Data Act obliges data holders under certain conditions to make data and relevant metadata (including personal data) accessible to the user. Article 20 GDPR grants data subjects the right to data portability which includes a similar (but very different in detail) right for access to personal data. In practice, the data holder respectively controller will need to know under which legal framework (both?) the data access request is made by the user respectively data subject if this is not clearly indicated in such request.

Article 6 (1) Data Act obliges a third party that has received the data from a user to delete the data made available to it pursuant to Article 5 Data Act when it is no longer necessary for the agreed purpose. If the third party has the agreement of the user, non-personal data can be retained for other purposes. However, it is unclear to what extent a third party may retain personal data if the user has given explicit consent.

Article 6 (2)(b) sets out a clear obligation for a third party to use the data it receives for the profiling of natural persons only if necessary for the provision of a service. The text does not allow for profiling for other purposes (than the provision of a service) even with the explicit consent of the user.

Article 32 (1) Data Act obliges providers of data processing services to take "all adequate technical, organizational and legal measures" to protect non-personal data from international and third-country access and transfer conflicting with EU or national law. Against this background, providers of data processing services acting as a processor under GDPR must not / cannot always know if a *specific* piece of data processed in their service is personal or non-personal and may thus have difficulties deciding which measures (Article 31 (1) Data Act) and/or appropriate safeguards (Article 46 (1) GDPR) to apply as well as which vetting process to follow when receiving a data access / transfer request.

Balancing these mentioned intricacies calls for a nuanced approach to ensure both regulatory frameworks can coexist effectively.

DSA/DMA

Both the DSA and the DMA introduce obligations that build directly on the definitions in the GDPR (such as 'profiling' in the DSA and 'special category data' in both the DSA and the DMA) – the unpredictable interpretation of these definitions under the GDPR is likely to lead to similar legal uncertainty in the application and interpretation of the DSA and the DMA.

As a specific example, recital 50 DSA states Notice & Action mechanisms "should allow, but not require, the identification of the individual or the entity submitting a notice". On the other hand, Art. 16(2)(c) DSA states hosting service providers shall enable and facilitate the submission of notices containing "the name and email address of the individual or entity submitting the notice". It will be important to understand how Recital 50 and Art 16(2)(c) DSA will interplay. In particular, if a Hosting provider can oblige a recipient of a service to provide his/her name and email when submitting a notice & action, and if affirmative, how will this interplay with the principle of minimization enshrined in Art. 5 GDPR.

AI Act

The AI Act introduces roles and definitions that may create inconsistencies with the GDPR. The ambiguous interpretation of these roles, particularly whether providers under the AI Act will be considered data controllers under the GDPR, poses a risk of legal uncertainty.

Tensions arise in the broader context of AI systems and fundamental GDPR principles. The data minimization and purpose limitation principles in the GDPR may clash with AI's inherent need for large datasets. The more information that is ingested in the models, the more accurate the AI system will be. This could raise conflict with minimization. It will be therefore important to understand how the principle of minimization will interact with the obligation to ensure training, validation and testing data sets remain representative, free of errors and complete (Art. 10 AI Act). Additional transparency challenges emerge due to the complexity of AI systems, making it difficult to provide detailed information to data subjects. Accuracy requirements may conflict with AI systems being trained on data from a specific point in time, and the practical aspects of anonymization in AI systems need recognition.

Moreover, biometrics and the definition of "biometric data" are subjects of concern. The lack of alignment between the AI Act and the GDPR on this front may lead to legal uncertainty, especially as jurisprudence develops around this term. Similarly, the legal basis for processing special categories of data (SCD) under Article 10 of the AI Act in relation to Article 9 GDPR remains unclear. Art. 10(5) AI Act allows for the processing of special categories of data (as defined in the GDPR) by providers of high-risk AI systems when it is “strictly necessary for the purposes of ensuring bias monitoring, detection and correction”. Art. 10(5) AI Act however says this processing is “subject to appropriate safeguards for the fundamental freedoms of natural persons”. It will be important to understand whether this provision will create a specific and additional Art. 9 GDPR condition for processing (unlikely) or whether providers of high-risk AI systems must rely on an Art. 9(2) GDPR condition to process special categories of data for the above purpose (most likely). In the case of the latter, it will be important to understand what Art. 9(2) GDPR condition will be considered appropriate by the DPAs for this purpose.

In view of the current discussions within the German supervisory authorities on the responsibilities for supervision under the AI Act, it is important that Member States, within the EDPB network, quickly clarify how supervision of AI could take place and what consistency mechanisms can be applied. It is crucial that DPAs in the Member States develop a clear interpretation, in particular regarding the processing of personal data in the context of AI. In doing so, DPAs will remain competent for the part of AI that concerns the processing of personal data. An early definition of the supervisory mechanisms will ensure the effective implementation of the AI Act and strengthen consistency across the EDPB network.

While the AI Act aims to complement GDPR protections, addressing these concerns is vital to maintaining legal clarity and coherence between the two frameworks. Efforts should focus on harmonizing definitions, roles, and legal bases to ensure a consistent and transparent regulatory environment for AI technologies.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Tabea Wilke | Head of Data Protection and Security
T +49 30 27576-161 | t.wilke@bitkom.org

Felix Kuhlenkamp | Policy Officer for Cybersecurity
T +49 30 27576-279 | f.kuhlenkamp@bitkom.org

Responsible Bitkom committee
Working Group Data Privacy