CONTRIBUTION FROM THE MULTISTAKEHOLDER EXPERT GROUP TO THE COMMISSION 2024 EVALUATION OF THE GENERAL DATA PROTECTION REGULATION (GDPR)

Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679

Report

10 June 2024

The Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679 has been established in 2017 to assist the Commission in identifying the potential challenges in the application of the General Data Protection Regulation (GDPR) from the perspective of different stakeholders, and to advise the Commission on how to address them. It also provides the Commission with advice to achieve an appropriate level of awareness about the new legislation among different stakeholders, including business and citizens. Finally, the group is tasked to provide the Commission with advice and expertise in relation to the preparation of delegated acts and, where appropriate and necessary, the early preparation of implementing acts to be adopted under the GDPR, before submission to the committee in accordance with Regulation (EU) n° 182/2011 also in the light of relevant studies.

This report of the Multistakeholder Expert Group does not reflect the opinion of the Commission nor one of its Services.

More information can be found here:
https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3537

REPORT – CONTRIBUTION FROM THE MULTISTAKEHOLDER EXPERT GROUP TO THE COMMISSION 2024 EVALUATION OF THE GDPR

On 19 September 2023 the Commission circulated to the members of the GDPR Multistakeholder Expert group a list of questions to gather feedback on their experience, and/or the experience of their own members, on the application of GDPR[1]. The deadline for responding was initially set at 18 November 2023, and was then extended until 22 November 2023.

The report is based on the contributions received by the Commission from the following members[2]:

Business:

- BusinessEurope
- Confederation of the European Data Protection Organisations (CEDPO)
- DIGITAL-EUROPE
- European Banking Federation (EBF)
- eCommerce Europe
- European Federation of Pharmaceutical Industries and Associations (EFPIA)
- European Telecommunications Network Operators' Association (ETNO) – GSMA Europe
- Federation of European Data and Marketing (FEDMA)
- Insurance Europe
- SMEunited

Civil society:

- Access Now Europe
- Bureau Européen des Unions de Consommateurs (BEUC)
- Privacy International
- Stiftung Digitale Chancen (Digital Opportunities Foundation)
- The Transatlantic Consumer Dialogue (TACD)
- Verbraucher-zentrale Bundesverband (Federation of German consumer organisations, VZBV)

Individual members (Professionals or Academics):

- Estelle Dehon (Professional)
- Gloria González Fuster (Academic)
- Christopher Kuner (Academic)
- Tanguy Van Overstraeten (Professional)

The questionnaire provided a list of questions on 14 main aspects of the GDPR, in particular: the exercise of data subjects' rights; use of representative actions under Article 80 GDPR; experience with Data Protection Authorities (DPAs); experience with accountability and the

[1] The questionnaire is published on the page of the group: Register of Commission expert groups and other similar entities (europa.eu).

[2] The information on members of the Multistakeholder Expert group is available on the page of the group: Register of Commission expert groups and other similar entities (europa.eu)
Additionally, a few comments were received from stakeholders not belonging to the Multistakeholder Expert group, which correspond to a large extent to the contributions received from the members.

risk-based approach; Data Protection Officers (DPOs); international transfers and the impact of the GDPR on the approach to innovation and to new technologies.

1. Overall assessment of the application of the GDPR

All individual members and civil society members underline positive developments such as the increase in data protection compliance and awareness of data protection rules and giving individuals greater control over their personal data through the enhancement of their data subject rights. Some of those members note that the GDPR is setting up a global privacy standard as regions worldwide are increasingly adopting the GDPR model, which benefits European companies and data subjects.

Similarly, most business members note positively the achievements of the GDPR in strengthening the data protection culture in the companies and fostering a collective consciousness about the value and protection of personal data. A member representing small and medium-sized enterprises (SMEs) reports that SMEs have done significant investments for GDPR compliance as they consider personal data as corporate assets and added value for the company's reputation. Business members stress the importance of preserving the risk-based approach as being one of the main benefits of the GDPR. Two civil society members consider that the risk-based approach lowers the level of compliance because companies provide a bare minimum compliance of their obligations stemming from the GDPR.

Furthermore, individual members acting as legal advisors and some business members acknowledge the role of the GDPR for harmonising the rules on data protection and helping the establishment of a single digital market within the EU based on one comprehensive data protection law.

On the other hand, all members point to a number of challenges that persist with the implementation of the GDPR. Despite that, most of the members consider that it is premature to revise the GDPR and the shortcomings could be addressed without opening the Regulation. Among the most noticeable challenges, several individual and business members regret that despite the attempts to ensure a consistent application of the Regulation, certain level of fragmentation remains due to inconsistencies in the interpretation of the GDPR by the Data Protection Authorities (DPAs) (e.g. in relation to the interpretation of the risk-based approach, the interpretation of the GDPR concerning research in health, the calculation of administrative fines under Article 83 GDPR) which leads to legal uncertainties. According to a business member representing the pharmaceutical sector such fragmentation hampers the development of scientific research in the EU.

Several members raise difficulties with the application of specific provisions of the GDPR. For instance, individual members express concerns about the application of the fundamental principles of data minimisation and storage limitation and the deployment of the GDPR compliance tools, i.e. codes of conduct and certifications. One individual member and one member representing consumers are concerned about the GDPR not delivering effective protection of personal data of minors. Several members mention challenges for SMEs, in particular as regards compliance costs and the fear of high sanctions by DPAs which can have a discouraging effect for innovating. A member representing SMEs calls for a specific regime with simplified rules for them.

Potential conflicting requirements due to the interplay between the GDPR and other regulations (e.g. in the banking sector the EU's anti-money laundering (AML) obligations and the revised Payment Services Directive (PSD2)[3]) or the requirement to retain personal data over longer periods of time for the implementation of 'the right to repair') are also a source of concerns for some business members. In the same vein, some business members consider that legal certainty with respect to rules that govern data sharing, for example through anonymisation and pseudonymisation techniques, will be key for the competitiveness of Europe's single market and industry. The non-adoption of the e-Privacy Regulation is regretted by some business and civil society members, respectively because the ePrivacy rules are not aligned with the GDPR and because the new rules are deemed essential to reinforce trust in online services. Another business member underlines the need for first gaining clarity on the impact of new laws under the Data Strategy covering both personal and non-personal data and the overall interplay with the GDPR.

Several individual members ask for the rapid adoption of standard contractual clauses (SCCs) for data transfers to controllers and processors outside the EU whose processing is subject to the GDPR. Those members consider also that the issuance of some guidelines by the European Data Protection Board (EDPB) is too slow (e.g. delay with the development of revised guidelines on anonymisation and pseudonymisation), which leads to legal vacuums. The majority of the members find that, overall, there is room for improvement when it comes to the content of the EDPB guidelines. On one hand, individual members stress their complexity, and that they are sometimes in contradiction with national guidelines adopted by individual DPAs, which could create legal uncertainties. Those individual members call for more simplified and practical EDPB guidelines that address concrete issues for which stakeholders need most clarifications. On the other hand, some business members regret that EDPB and DPAs' guidelines are sometimes too strict as they do not apply consistently the risk-based approach and proportionality principles enshrined in the GDPR, and consequently reduce the margin of manoeuvre of controllers. In the same vein, one individual member acting as legal advisor and some business members underline the key role of the EDPB and DPAs for striking a fair balance between the right to data protection and other considerations, such as the freedom to conduct business. Members also call for the EDPB to increase its dialogue with stakeholders to learn about emerging issues and develop guidelines that are better aligned with the realities faced by businesses. Furthermore, several members stress that a number of notions still need to be clarified by guidelines (e.g. the concepts of "Data Protection Officer (DPO)" and "(compelling) legitimate interest").

Most of the civil society members and some individual members are worried about the effective enforcement of the GDPR, especially in cross-border cases. Some of the civil society members point to lack of coordination between DPAs and differences in national procedural laws which results in slow decisions. One member representing consumers deplores that many of the fines are being challenged in court by the companies involved and the proceedings are therefore likely to continue for several more years. Furthermore, some business members stress the importance of using the full range of corrective measures for enforcing the GDPR, not just fines.

[3] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, p. 35–127.

2. Impact of the GDPR on the exercise of data subjects' rights

Overall, members indicate that respectively the right of access (Article 15 GDPR) and the right to erasure (Article 17 GDPR) are the two most known and exercised data subject rights, while the other rights are much less used.

From the individuals' perspective, members find it difficult to provide a quantification and information on the evolution of the exercise of data subject rights since the entry into application of the GDPR. According to Access Now, there is a need for an IT system harmonised across the EU to help to monitor or to report on the evolution of data subject rights and trends.

One academic member and several civil society members (BEUC, Stiftung Digitale Chancen and Verbraucher-zentrale Bundesverband) report difficulties faced by data subjects for the exercise of their rights under the GDPR. An initial challenge is the lack of individuals' awareness about their data subject rights and how to exercise them in practice, as well as the lack of understanding of which data are processed, where and by whom.

Most of the business members see a certain degree of burden on the side of controllers for replying to requests for exercise of data subject rights and call for increasing the awareness on the limitations of the rights (which are not absolute) in order to reduce the burden on the controllers and the possible frustrations of the data subjects. Business members representing the insurance and marketing sector emphasise the challenge of retrieving the personal data in different systems and business processes, and identifying to whom the data was transferred; therefore, they call for a pragmatic approach to the handling of the data subjects' requests. Some business members report that meeting the deadline for replying to data subjects as well as identifying the individual who submits the requests have been other difficulties faced by controllers.

- *Information obligations (Articles 12 to 14)*

Some civil society members are concerned about how companies comply with their transparency obligations under the GDPR. Two of them report that many controllers still provide information required under Articles 13 or 14 GDPR in a manner that is incomprehensible to the average data subject, sometimes using vague or overcomplicated terms, which is considered not be in line with the GDPR. One civil society member notes that the lack of transparency remains among the key concerns EU consumers raise regarding the data processing by companies, which has also negatively impacted the online trust of consumers while another civil society member observes that the controller-processor relationship is not always clearly described in privacy policies.

On the other side, several business members call for consistent application of the risk-based approach to limit the scope of the information to be provided to the data subjects (e.g. sometimes it would be sufficient to disclose only the categories of recipients, instead of their complete identification). Some business members value the EDPB layered approach (i.e. providing information in different layers to facilitate the data subject's understanding of the information), which sometimes has become a commonly accepted standard for providing information to data subjects.

- *Access to data (Article 15)*

Most of the civil society members report the following problems: responses to access requests are often delayed, incomplete (the most basic information might be sometimes considered as "trade secrets" or just "confidential"), or even sometimes missing; the data received is sometimes not in a truly readable format; many GDPR complaints are related notably to companies' failures to reply to access request; the handling of such complaints by DPAs can be also slow and take up to several years.

Two civil society members observe that many companies, including in the aviation sector, charge a fee to consumers for the exercise of their rights.

From the point of view of business members, the right of access has been by far the most used right and at the same time the one that has posed most challenges for controllers. A member representing the insurance sector reports that in some companies and markets the quantity of requests for access has increased by a factor of 3 to 5, and sometimes even by a factor of 10. Another business member reports that there was a temporary rise of requests for access after the entry into application of the GDPR, since then the flow of requests has stabilised.

One member acting as legal advisor and several business members think that the right of access is too far-reaching, especially in case of excessive requests when the data subject asks access to all the personal data processed. For this reason, some of those members explain that the lack of the principle of proportionality for the handling of access requests is a significant issue. Members call therefore for more clarity on the scope applicability of the right of access, in particular in some specific contexts such as in an employment relationship or complaint management by Customer Support Centre.

Another concern expressed by one individual member acting as legal advisor and several business members is that the right of access is often being exercised in an abusive manner, which can impose a substantial burden on organisational resources. This is because the predominant motivating factor for the exercise of the right of access is not the protection of personal data, but instead other purposes such as the need to obtain information in an employment context, gather evidence for complaints or legal proceedings (something that could conflict with access to documents rules established in national civil procedures). Nonetheless, many of those members refer to the broad interpretation of the right of access endorsed by the CJEU in its ruling in Case C-307/22[4] and argue that this can result in significant burdens for controllers. In addition, some members call for more guidance on what constitutes an unfounded or excessive access request.

A member representing the insurance sector considers that there is still legal uncertainty over the interpretation of the right to obtain a copy and calls for clarification that this is not an independent claim in addition to Article 15(1) GDPR and in particular that copies of the documents in which the data are located do not have to be issued.

Business members representing the banking and insurance sector express concerns with the

[4] Case C-307/22, *FT v DW,* ECLI:EU:C:2023:811.

prescriptive approach adopted in the EDPB guidelines on the right of access, something which risks jeopardising the flexibility of controllers and can result in a more burdensome handling of access requests without any clear benefits for the data subjects. Furthermore, one of those members calls for taking into account sector specific obligations (e.g. AML purposes) and stress that sharing of personal data processed for these specific purposes poses serious risks to banks.

- *Rectification (Article 16)*

According to members representing consumers, the data subjects need to be aware of the categories of their data that are being concretely processed and for which legal basis in order to be able to properly exercise their other rights (notably the right to rectification, the right to erasure and the right to object). One of them explains that when it comes to more complex processing activities, the lack of transparency of the controllers can make it very hard or even impossible for the data subjects to determine if the data is incorrect or incomplete.

The majority of business members report limited or no use of the right to rectification.

- *Erasure (Article 17)*

Civil society members refer to the following issues regarding the implementation of Article 17 GDPR: a reluctance of controllers to erase the personal data from their systems justified by the necessity to continue processing the data for the "public interest" or for the purposes of archiving or research; the fact that the automated technical setup of companies' practices of sharing personal data makes it practically impossible for a consumer to request erasure from all parties which have received the data; the absence of guarantee that pseudonymised data and advertising profiles are also deleted; the fact that companies come up with arguments for not deleting the data (e.g. the need to keep the data as proof in case of eventual litigations) or make the erasure process complicated.

Some business members report that the exercise of the right to erasure has been increasing. According to a business member representing the banking sector, the right to erasure is the second most popular right, which is often invoked when a credit application is rejected. Some business members point to technical challenges for the implementation of deletion requirements (which can take costs and time) and call for alternative safeguards in case of lack of technical feasibility. Furthermore, a member representing SMEs reports that the right to erasure is sometimes problematic for retailers where the personal data to be erased is needed for court cases or for building customer relationships.

- *Data portability (Article 20)*

Civil society members report that the right to data portability is not much used in practice. The reasons advanced include: the fact that this right is widely unknown among data subjects and not supported by controllers (with most service providers not having procedures for data porting in place); and the absence of standardisation of data formats (the GDPR only provides that the data transmitted has to be in "structured, commonly used and machine-readable format").

Some business members also report that the right to data portability is very rarely exercised.

One business member explains that it is a challenge to separate the data that can be ported from the data that must not be ported for reasons affecting the rights and freedoms of others. A business member representing the insurance sector expects the number of portability requests to increase once the Commission proposal for a framework for financial data access is adopted. According to that member, it is important that inferred and derived data is not included in data-sharing obligations, for competition reasons.

- *Right to object (Article 21)*

One civil society member reports frequent complaints from data subjects on the difficulty to exercise the right to object, notably due to the assessment of what can qualify as grounds relating to the data subject's particular situation that justify the right to object.

According to some business members, the right to object is relatively rarely exercised, most often with the aim to object to processing of personal data for marketing purposes. Another business member calls for an increased clarity regarding the applicability of the right to object, in particular how to conduct the balancing of conflicting rights in case when the controller needs to assess whether its compelling legitimate grounds for the processing override the interests, rights and freedoms of the data subject.

- *Automated decision making (Article 22)*

Some civil society members note low level of knowledge and awareness of data subjects about this right that can be explained by a lack of transparency and meaningful explanation provided by controllers (some of them deny that they are conducting automated decision-making or fail to provide any information on the existence of automated decision-making).

A business member indicates that in the banking sector the final decision concerning the data subject in potentially impactful processes, such as the decision to report suspicious transactions to competent authorities in the context of AML legislation, involves human intervention. That member raises questions about the interplay between Article 22 GDPR and the new AI Act and calls for clarity for businesses. Another business member points to competition issues in the exercise of this right in case where the data subject is considered to be the competitor of the controller. In this scenario, explanation of automation could reveal sensitive information of the business of the controller and the exercise of this right has to be balanced with the right to protection of property and trade secrets. A member representing the insurance sector argues that the restrictive interpretations of the exceptions in Article 22(2) and (4) GDPR by DPAs cause significant problems in practice and that there should be a clarification that Article 22 GDPR provides a right of the data subject and is not a prohibition.

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

Most of the individual members report that they avail of or are aware of tools or user-friendly procedures to facilitate the exercise of data subject rights. One academic member considers that existing tools should be improved as they are not beneficial for data subjects because of their ambiguity and uncertainty (e.g. delete my account button or the existence of many interfaces of the system of the organisation). Another individual member mentions the existence of several tools to redact documents relying on existing technologies and the on-

going experiments in AI tools to process emails, although not still accurate enough.

Several business and civil society members also refer to a number of concrete tools or user-friendly procedures that are already available, including in the consumers' context, such as standardised templates for exercising data subject rights that can help to verify the legitimacy of data subject requests. One civil society member considers that more should be done to promote the development of such tools.

On the other side, other business and civil society members report that they are not aware of tools or user-friendly procedures to facilitate the exercise of data subject rights.

Experience in contacting representatives of controllers or processors not established in the EU

Overall, members report limited or no experience in contacting representatives of controllers or processors not established in the EU. One civil society member reports that the representatives are either not appointed or are small external service companies that have no meaningful relationship with the controller while another civil society member observes that too many companies assume that they do not have to comply with the GDPR because they are based outside of the EU.

Particular challenges in relation to the exercise of data subject rights by children

Two individual members, together with some business members and civil society members report challenges in relation to the exercise of data subject rights by children, notably that children do not fully understand their rights, lack digital literacy skills and are subject to undue influence, as well as difficulties for the online age verification (most services do not (and cannot) differentiate between adults and children) and different age limits established across the EU which creates a level of fragmentation. Some members doubt also whether the parental consent for children under a certain age gives priority to the best interest of the child and whether parents should be enabled to exercise rights on behalf of their children.

3. Application of the GDPR to SMEs

Lessons learned from the application of the GDPR to SMEs

One individual member acting as legal advisor observes positive consequences from the application of the GDPR to SMEs, notably that the regulation pushed SMEs to adopt data protection practices and that SMEs are capable to adapt to the regulation more quickly and easier compared to large organisations. An academic member reports that SMEs suffered lack of resources to devote to compliance and at the same time they may not trust the advice they receive from external GDPR experts. That member underlines also that the common challenges faced by SMEs is to understand what changes and processes they need to put in place to be compliant.

Business members raise several issues concerning the application of the GDPR to SMEs. This includes, in particular, high compliance cost which are due to some extent to the complexity of the regulation and the need to rely on external help if SMEs do not have appropriate in-house data protection expertise. Several business members underline the need for more practical guidance tailored for SMEs.

One member representing SMEs regrets that the derogation provided to SMEs under Article 30(5) GDPR from the obligation to maintain a record of processing activities does not apply in practice (since it is limited to occasional processing) and should be amended. More generally, that member argues to lower the GDPR requirements for SMEs. Another business member calls for SMEs to be able to provide simplified Data Protection Impact Assessments (DPIAs).

One member acting as legal advisor points to divergence in regulatory scrutiny between large organisations and SMEs. In the view of that member, to ensure fairness and promoting responsible business conduct across all sectors, the GDPR and penalties for breaches of the GDPR have to be applied consistently, irrespective of company' size, considering that some SMEs can have a substantial impact on personal data.

Guidance and tools provided by Data Protection Authorities and the EDPB in recent years

Some business members report that the level of support provided by DPAs varies greatly from one Member State to another.

Two individual members acting as legal advisors recognise that SMEs have benefited from guidance and tools from the DPAs and the EDPB, especially sector-specific guidance. One of these two members regrets, however, that the guidance provided can be lengthy and complex and requires certain degree of knowledge about the GDPR which SMEs do not necessarily have.

Similar findings were observed by several business members which consider the EDPB guidelines sometimes useful, but often also too theoretical, superficial and legalistic, and not grasping the reality of the economy, especially as SMEs have very diverging national business realities. As a consequence, SMEs which do not necessarily have in-house data protection legal experts have difficulties to comprehend the guidelines. Some business members suggest concrete solutions, such as to establish a permanent advisory committee or a specific service inside the DPAs for SMEs and to provide for more targeted guidelines, no one-size-fits-all solutions. Finally, several members regret the fact that the national and the EDPB guidelines are sometimes not aligned.

Additional tools that would be helpful to assist SMEs in their application of the GDPR

Several individual members and business members underline that SMEs are in general interested in receiving additional help to assist them with the implementation of the GDPR, such as templates (e.g. for conducting data protection impact assessments), risk assessment software, helpline or AI driven chatbot and practical guidance, in particular on the types of technical and organisational measures needed as well as tools which assist with the encryption, anonymisation and deletion of data, guidelines on concrete topics such as new technologies (e.g. biometrics), security solutions and data subject request management tools.

4. Use of representative actions under Article 80 GDPR

From the controllers and processors' perspective

Two individual members acting as legal advisors argue that Article 80 GDPR has not been implemented consistently while the use of representative actions is set to increase due to the rise of collective redress mechanisms and more generally litigations; hence those members see

a need for further clarification and harmonisation of the application of Article 80 GDPR. They point to a degree of uncertainty for the application of Article 80 GDPR due to open questions concerning the right to receive compensation for damages under Article 82 GDPR and the approach to the notion of damage taken by the EU Court of Justice in the case C-300/21[5].

From the few business members which address this question, one business member reports mixed feedback on the use of representative actions under Article 80 GDPR, expressing concerns about the potential financial impact on SMEs if a mass claim for even smaller amounts, such as 50 EUR, gets approved. Another business member indicates also that the use of representative actions is expected to increase, and preventing duplicative actions will be key to avoid burdens on local courts and companies alike.

For civil society organisations

Most of the civil society members have experience with representative actions under Article 80(1) GDPR[6]. However, those civil society members refer to limitations of their capacity to bring forward actions under Article 80(2) GDPR to address systemic failures in the implementation of the GDPR; this is due to the fact that most Member States did not use the possibility to legislate under Article 80(2) GDPR.

Looking forward, those civil society members hope that the Representative Actions Directive[7] could resolve the difficulties encountered with the use of Article 80 GDPR.

One member representing consumers notes that a representative action for compensation under Article 82 GDPR may require massive resources which consumer organisations often do not have and calls therefore for the support of national and EU programmes to provide funding to such organisations to act. Another civil society member considers that taking representative actions on Article 82 GDPR is risky because of uncertainties regarding the compensation of non-material damages under Article 82(1) GDPR, and advocates for full harmonisation of compensation under Article 82 GDPR.

5. Experience with Data Protection Authorities

Experience in obtaining advice from Data Protection Authorities

The majority of individual members report challenges in the interaction with DPAs. They refer to shortcomings in the ways DPAs comply with their obligation to facilitate the lodging of data subjects' complaints, the slowness of DPAs to respond, difficulties to obtain in-depth or confirmative advice from DPAs, tendencies of DPAs to refuse to give advice in parallel to an ongoing investigation and lack of sufficient transparency (e.g. in relation to access to the files) during the investigation of the complaints.

[5] Case C-300/21, *UI v Österreichische Post AG*, ECLI:EU:C:2023:370.
[6] Privacy International, BEUC, Verbraucher-zentrale Bundesverband and TACD refer to concrete representative actions that they have launched in the consumer context pursuant to Article 80(1) GDPR.
[7] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, OJ L 409, 4.12.2020, p. 1–27.

Overall, the feedback from business members is mixed. They mention that the level of availability and expertise of DPAs varies considerably; that some DPAs are not open to engage in constructive dialogue with the industry and are slow and reluctant to provide binding replies, or too restrictive when providing advice or even refuse to respond to enquiries. By contrast, other DPAs are seen as more available, rapid and precise in answering inquiries. Consequently, business members consider that there is still room for improvement for DPAs. Some business members suggest that additional training for DPAs on new and emerging technologies could be beneficial.

A member representing consumers notes that DPAs are generally perceived as helpful and they regard consumer organisations as valuable sources of information and insight in their work, particularly when producing guidelines. On the other side, another member representing consumers submits that DPAs should refrain from providing specific advice to a controller (as this is not foreseen in the GDPR), since that advice puts the DPA in a predicament when later confronted with a complaint against that controller.

Usefulness of guidelines adopted by the European Data Protection Board

Many members acknowledge that the EDPB guidelines are helpful (especially the guidelines on personal data breach notification, consent, cookies and sector-specific guidelines) as they play a key role for a harmonised interpretation of the GDPR. Some civil society members deplore that the EDPB guidelines are not considered as binding and plead for an open process for NGOs to input in their drafting.

Many members find that there is room for improvement. Some academic and business members regret that the EDPB is slow in issuing the announced guidelines, while the utility of the input received during the public consultation is unclear. Some members suggest the EDPB and DPAs to proactively engage with stakeholders (including DPOs) in an early stage of the process for the development of guidelines to better understand market dynamics and business practices.

One academic member points to issues concerning the quality of the EDPB guidelines, notably that the legal reasoning therein can sometimes be questioned when guidelines state broad conclusions without providing full explanations and supporting sources (in particular concerning issues of EU law, for which an independent outside review is recommended). Several business members regret that the EDPB guidelines are either overly strict or prescriptive in the interpretation of the GDPR and not applying consistently the risk-based approach and proportionality principles enshrined in the GDPR (e.g. EDPB guidelines on the right of access) or not in-depth enough in the provision of concrete advice, which diminish their added value for the practical implementation of the GDPR. Furthermore, some members consider that the guidelines do not sufficiently take into account the interplay with other legislations to avoid conflicting requirements and lack of consideration for industry use cases.

Overall, many members call for timely and practical EDPB guidelines to be published as announced in the annual EDPB program and to provide concrete solutions to real situations. Concretely as possible improvements, members suggest EDPB guidelines to focus on more case studies and illustrative examples, to be more concise and to cover more essential subjects (e.g. pseudonymisation and anonymisation, the legitimate interests' legal bases and scientific

research), to avoid opting for the strictest interpretation of the GDPR, disregarding the difficulties faced by businesses in the application of the GDPR and to avoid creating additional requirements that go beyond the GDPR.

Some members call for DPAs not to issue national guidelines that contradict EDPB guidelines, as this hampers the consistent application and enforcement of the GDPR, and to promote EDPB guidelines at national level, in particular towards SMEs.

Some business members encourage an inter-regulatory cooperation between on one side the EDPB and DPAs, and on the other sectoral regulators (e.g. banking and pharma authorities) to produce some general data protection guidance pertaining to industry specifics: for example, more regulatory sandboxes to accompany companies to identify sector specific solution. Another business member calls the EDPB to provide clarification on the interaction between the GDPR and new regulations with data protection implications, such as the Digital Markets Act (DMA)[8], the Digital Services Act (DSA)[9], the Data Act[10], the Artificial Intelligence (AI) Act[11] and the NIS 2 Directive[12].

DPAs following up on each complaint submitted and providing information on the progress of the case

Overall, members report that the experience in the handling of complaints by DPAs has been mixed, as some DPAs are highly responsive, while others do not provide information about the progress of a complaint procedure or do it with considerable delays.

According to some business members this backlog could be due to lack of resources or to the divergent procedural rules that exist among Member State authorities. Another constraint identified by several members is the absence of internal or legal deadlines for handling complaints, which can lead to inconsistent processing times. Moreover, the prioritisation of cases at a national level, often influenced by the limited budget and resources allocated to DPAs, further compounds the issue.

One civil society member refers to the different approaches between DPAs on what handling a complaint actually means under Article 78(2) GDPR, with some DPAs aiming to issue a decision for each admissible complaint, while other DPAs having recourse to amicable solutions; sometimes DPAs decide to handle only certain complaints or to turn complaint procedures into *ex officio* investigations, thereby excluding complainants. Another issue

[8] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, p. 1–66.
[9] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1–102.
[10] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 2023/2854, 22.12.2023.
[11] COM/2021/206 final.
[12] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, p. 80–152.

brought up by this member is the lack of uniform approach by the Member States on the publication of decisions by the DPAs.

Guidelines issued by national Data Protection Authorities

A business member representing the insurance sector notes positively that its members report a number of useful guidelines at national level that have supplemented the EDPB guidelines (e.g. on topics such as the handling of ID cards or COVID-19 vaccinations).

Several individual, business and civil society members refer to concrete guidelines issued by national DPAs conflicting with EDPB guidelines or creating fragmentation (e.g. on the requirements for a DPIA, on cookie banners, on legitimate interests and on the validity of consent in pay or consent models).

Furthermore, one individual member acting as legal advisor thinks that consistency issues arise also from the potential conflicts or overlaps of the GDPR with other regulations (e.g. financial institutions, which are subject to both AML rules and the GDPR).

6. Experience with accountability and the risk-based approach

Experience with the principle of accountability

In the views of several individual and business members, the principle of accountability should provide flexibility for organisations rather than leading to administrative burden for organisations. Some business members consider that there is a high level of discretion in the practical application of the principle of accountability, and that EDPB guidelines are overly prescriptive on how to implement certain GDPR obligations. They argue that it undermines this principle because little margin of manoeuvre is left for controllers to attain the same goal by using compliance mechanisms that are more appropriate for the sector.

At the same time, some civil society members express support for the accountability principle which requires organisations to firstly respect the data subject rights and makes them directly accountable if they breach those rights.

Experience with the scalability of obligations

In general, individual members acting as legal advisors and business members value the risk-based approach of the GDPR as a guiding principle allowing for flexibility and scalability of the obligations, especially in terms of the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (Article 32 GDPR). One business member reports that obligations stemming from the GDPR are still unclear and too rigid for many SMEs, while other members are concerned that the overly stringent and prescriptive approach adopted in the EDPB and DPAs guidelines pose challenges to the risk-based approach and call for a more nuanced approach towards scalable obligations. Scientific research and data transfers are two areas where the importance of the risk-based approach is highlighted by business member representing the pharma and the insurance sectors. Business Europe considers also that the expectations of the level of compliance have to be higher with respect to heavily regulated institutions, such as banks, as opposed to small businesses.

By contrast, some civil society members express concerns about the risk-based approach which they find non-adequate to protect fundamental rights. They stress that fundamental rights are non-negotiable, must be respected regardless of a risk level associated with external factors, and that it should not be a pretext for a controller to waive certain obligations.

7. Data Protection Officers

Experience in dealing with a Data Protection Officer

Several members report a generally positive experience and highlight the crucial role that especially in-house DPOs can play for a company's compliance efforts on all levels. However, another business member representing SMEs report that the experience in dealing with DPOs is not always positive, as sometimes DPOs may censor all processing activities and do not provide their advisory role.

Individual members and one civil society member report several issues concerning the function of an internal DPO, in particular the lack of independence, resources and senior support of internal DPOs to enable them to carry out their function properly. External DPOs would have less of issues about independence but would have less knowledge and understanding about the functioning of the organisation. According to one member acting as legal advisor, the situation of DPOs is better in large companies, where the DPO office is made up of several individuals with a blend of different experience that enables them to carry out their tasks more effectively. One civil society member regrets that DPOs have not taken a role that is as significant as the legislator foresaw.

Some business members report issues as regards the obligation to designate a DPO. For instance, one business member representing SMEs reports that this is unclear from the perspective of SMEs and calls for guidelines to precisely define when smaller companies do not have to appoint a DPO. A business member points out that the notion of "processing on a large scale of special categories of data" triggering the appointment of a DPO (Article 37(1)(c) GDPR) is unclear and interpreted overly broadly by DPAs. In the view of that member, the lack of clarity on the trigger, even in very precise contexts, such as clinical trials or pharmacovigilance, can create legal uncertainty.

A business member representing DPOs reports issues which are due in particular to the lack of support of DPOs from those senior decision makers who still struggle to understand the value of the compliance work carried out for their business; moreover, the GDPR can still be viewed as a business-blocker rather than an as an essential and natural component of good business planning, practice and implementation. It indicates that DPIAs continue to be a point of friction with some data controllers, e.g. because those try to minimise the significance of the risk involved in projects to avoid conducting a DPIA or force DPOs to effectively complete DPIAs by themselves despite Article 39(1)(c) GDPR which makes it clear that the DPO's role in a DPIA is advisory only.

Sufficient skilled individuals to recruit as DPOs

The opinions of the individual, business and civil society members converge on this matter as they see a risk of a shortage of qualified and adequately trained candidates for the DPO position

(in particular when the DPO need to have also understanding of a specific sector), while the existing offer for DPO training tends to be very fragmented in terms of content, intensity and quality. One civil society is of the view that many DPOs have no profound legal or technical background.

Several members call therefore the EDPB or the Commission to promote high standards for harmonised DPO training, to ensure that certifications issued in one Member State are recognised in others, or event to establish an EU-wide certification of DPOs.

Resources provided to the Data Protection Officers

The predominant views of individual and business members are that in general DPOs are still not provided with sufficient resources to carry out their tasks efficiently. According to some members, this depends on the size of the organisation, the sector of activity and the complexity of the data processing activities involved: usually public authorities, as well as large and tech companies, and sectors such as banking, insurance, health care and e-commerce provide sufficient resources to their DPOs; by contrast, SMEs and NGOs struggle to allocate sufficient resources to their DPOs or can invest in their training.

Issues affecting the ability of DPOs to carry out their tasks in an independent manner

Two individual members acting as legal advisor and one civil society member point to the following issues affecting the ability of DPOs to carry out their tasks in an independent manner: allocating additional responsibilities to DPOs, their insufficient seniority, lack of sufficient support from senior management, lack of protection from retaliation, insufficient resources, conflicts of interests if the DPO is required to carry out all tasks needed to make the controller compliant with GDPR and at the same time to monitor and oversee the controller's compliance. Several business members point also to the issue of combining the role of DPOs with other responsibilities which poses a risk of independence.

One business member representing DPOs mentions the insufficient seniority of DPOs as a persisting issue, especially when controllers may choose to appoint a more junior person who lacks the experience and confidence to challenge decisions at the senior management or board level. It considers also that there is a lack of understanding of what a DPO's statutory independence means. Some data controllers view it as a threat as they feel that the DPO is by their nature not a contributing factor to the business's aims.

8. The controller/processor relationship (Standard Contractual Clauses)

Use of the Standard Contractual Clauses adopted by the Commission on controller/processor relationship[13]

One individual member acting as legal advisor report that the SCCs are used by organisations, while two other individual members indicate that they are rarely used or not used as a whole,

[13] Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, OJ L 199, 7.6.2021, p. 18–30.

but they are sometimes considered by organisations for the negotiation of their own contractual agreements pursuant to Article 28 GDPR. The latter two individual members consider that organisations prefer to use their own templates for contractual agreements that can be tailored to their specific needs.

Business members report that the SCCs are not equally used by companies, and they have not established a standard for the market. Members explain that some companies use them without encountering particular issues, while other (mostly larger) companies (e.g. in the banking and insurance sectors) do not usually use them because they prefer to use their own clauses, or they simply take elements from the SCCs and apply them to their existing clauses. One business member representing SMEs reports that many SMEs adopt these SCCs as a basis for including further clauses, with the aim of protecting particular interests, rather than implementing the provisions of Article 28(3) GDPR.

Feedback on the Standard Contractual Clauses

Some individual members report that the Commission's SCCs lack sufficient flexibility for businesses. A member representing the insurance sector mentions the need to further clarify the status of joint controllership (to better distinguish it from that of a processor) and the right to audit of the joint controller, as well as the nature of liability (separate, joint or solidary). Another business member mentions that it would be very helpful to develop some specific provisions about AI in the SSC for the private sector, while another business member explains that a common point of debate and disagreement in the negotiations with customers and suppliers for the establishment of the SCC is whether it is allowed to limit the financial responsibilities between a controller and a processor.

9. International transfers

Several members indicate that they consider adequacy decisions adopted by the European Commission to be the most straightforward transfer instruments. They welcome the recent adoption of the adequacy decision for the EU-US Data Privacy Framework and expressed support for engaging with third countries to achieve new decisions. Members refer to a number of countries in Asia, Africa and Latin America as important actors to work with, because there is a large volume of cross-border data flows to those countries or because of (recently adopted) modern data protection laws and the existence of independent Data Protection Authorities. As regards possible new adequacy decisions, one member also suggested that the preparatory process would benefit from increased transparency, and another member underlined the importance of further clarifying the different steps of the assessment.

With respect to other transfer tools, the feedback received from members, especially those representing industry, confirms that Standard Contractual Clauses (SCCs) remain the most used for data transfers outside the EU. Members generally welcome the modernised SCCs (adopted in 2021) and underline their clear structure and usefulness for companies. At the same time, several members stressed that the obligation to carry out so-called "transfer impact assessments" (TIAs) is burdensome, costly and time-consuming. They call for additional guidance (e.g. on the responsibilities of involved parties and the level of detail required) and tools to help companies carry out TIAs (e.g. templates, general country-assessments, risk catalogues). Some members also indicate that putting in place supplementary measures such as

encryption can be highly complex and costly. More generally, some members stress the importance of the EU's engagement with international partners to address issues concerning government access to data, which cannot be resolved by contractual instruments.

A few members refer to difficulties to negotiate and/or operationalise SCCs with large providers. Several members also explain that it can be time consuming to regularly update the SCCs (including because of the level of detail required in the annexes), for instance in case of changes in the roles of the parties. As regards specific provisions of the SCCs, a few members refer to practical difficulties in implementing the requirements for onward transfers, indicating that it may be difficult to check and enforce compliance down a processing chain. In this respect, one member indicates that the use of the docking clause is not yet so frequent. Several members suggest that the use of Module 4 of the SCCs (transfers from processors to controllers) may need some clarification on the obligations of the respective parties, including because controllers acting as data importers are often directly subject to the GDPR. One member highlights that it may be difficult in practice for individuals to obtain a signed copy of SCCs used by a controller by exercising the right foreseen in the clauses.

Looking forward, a few members call for a swift adoption of SCCs for data transfers to controllers and processors outside the EU whose processing is subject to the GDPR. In addition, several members encourage further "bridging" with transfer tools of other countries/regions, referring to the recent adoption of the EU-ASEAN Guide on model clauses as a positive example.

Several members indicate that binding corporate rules (BCRs) are considered by many companies as a useful compliance tool and trustworthy transfer instrument. However, they explain that the development of BCRs generally already requires a certain level of maturity, and that the approval process may be lengthy.

Finally, some members consider that the requirements for relying on derogations for data transfers are interpreted too restrictively, reducing their practical relevance (e.g. as regards the possibility to rely on consent of the data subject).

10. National legislation implementing the GDPR

The majority of the individual members indicate problems with the national legislation implementing the GDPR, including restrictions adopted by Member States pursuant to Article 23 GDPR and divergences between public and private bodies (e.g. Greek national data protection law) and more restrictive provisions than the GDPR (e.g. French health data processing law).

Some business members also refer to Member States where the national legislation implementing the GDPR is in their views not aligned with the spirit of the GDPR and with other sectorial legislation (e.g. in relation to the understanding of the controller-processor relationship). Some business members stress that the national legislation should not go further than the margins left to Member States under the specification clauses provided by the GDPR.

Civil society members point to differences concerning the conditions to lodge complaints on the basis of Article 77 GDPR (e.g., filing a complaint via email is not admissible, and no online form is available), broad restrictions on the GDPR rights and obligations without meeting the conditions of Article 23(2) GDPR.

11. Fragmentation/use of specification clauses

The level of fragmentation in the application of the GDPR in the Member States

All individual members and several business members think that there is a certain level of fragmentation due to the Member States' implementation of the GDPR or the use of facultative specification clauses. The level of such fragmentation is assessed by the members differently, some of them consider it as noticeable while others find it difficult to assess. One academic member stresses that the specification clauses in the GDPR giving rise to such fragmentation do not equal complete freedom for Member States to regulate.

The area in which there is fragmentation and is it justified

Several members report that Member States have used the specification clauses available under the GDPR to create specific national rules on a number of aspects.

The majority of individual members and some business members point to minimum age for child's consent (Article 8(1) GDPR) as one area where the existing fragmentation is not justified and leads to additional complexity for businesses. Another cause of unjustified and problematic fragmentation reported by some individual and business members is the introduction by Member States of further conditions, including limitations, with regards to the processing of genetic data, biometric data or data concerning health (Article 9(4) GDPR). A member representing the insurance sector explains that this fragmentation is problematic for the processing of health data for the conclusion and performance of insurance contracts. According to a business member representing the pharmaceutical sector the fragmentation in the area of research with health data (in particular clinical trials) is due principally to diverging interpretations of key aspects of the GDPR by DPAs, rather than to extensive use of facultative specification clauses by Member States. That member regrets that DPAs are unable to overcome those differences, despite the GDPR mechanisms in place to ensure consistency, and argues that this situation is very burdensome for the pharmaceutical sector and slows down scientific research.

Furthermore, some individual and business members refer to significant discrepancies in the processing of personal data relating to criminal convictions and offences (Article 10 GDPR), which could be problematic in certain regulated sectors (e.g. AML rules in the financial industry or in the employment context).

Other areas in which individual and business members consider there to be fragmented approach across Member States include: motivation by DPAs for the imposition of administrative fines (Article 83 GDPR); national lists with the kind of processing operations subject to the requirement for a DPIA (Article 35(4) GDPR) and the modalities for the notification of data breach by the controller (Article 33(1) GDPR) as there exist different template forms and different conditions for the reporting. As a solution for the last two issues, individual members call for the creation of a standard pan-EU form for a DPIA and a central portal that could be used by controllers to report a breach.

One academic member and some civil society members point to unjustified differences and fragmentation in national practices for handling of complaints. This concerns issues encountered by individuals when exercising the right to lodge a complaint with a DPA, something that has been researched in an academic study[14]. One civil society organisation gives as an example the implementation of Article 85 GDPR which appear to be in tension with the GDPR in some Member States.

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

Adequate use of codes of conduct

Most of the comments received from individual and business members indicate that sector-specific codes of conduct, including as a tool for international transfers, could be a very useful compliance tool (especially for SMEs as they could benefit from easier, quicker, and more cost-effective solution) and should be therefore promoted. However, members argue that the efforts for their development are disproportionate, which is why codes are currently not used or rarely used. Several members are aware of the two trans-national codes of conduct operating in the cloud sector.

Challenges in the development of codes of conduct, or in their approval process

As challenges in the development of codes, members mention difficulties to agree on the application of GDPR provisions to specific sectors and to adapt the codes to the specificities of national markets and laws. Furthermore, several members stress the requirements which they consider as too heavy (e.g. the requirement for setting up an accredited monitoring body before the code is approved) and say that some DPAs impose even further requirements that go beyond the EDPB guidelines on codes and monitoring bodies. Business and civil society members point to the too long approval process: often it takes a couple of years for a code to be approved, which discourages their development.

A business member representing the pharmaceutical sector refers concretely to a draft transnational code developed by the sector for the processing of health data in the context of clinical trials. That member regrets the lack of communication and engagement of the lead DPA, its decision to slow down the review of the draft code while waiting for the adoption of EDPB guidelines on scientific research, as well as the lack of interaction with the EDPB during the process for the approval of the code. In the same vein, a civil society member regrets that representatives of civil society, such as consumer protection organisations, are not involved in the development of codes and that the enforcement of codes is often weak or non-existent.

Supports for developing codes of conduct

To support the development of codes, some individual and business members find it necessary to provide transparency in the process and set up clear timelines for codes' approvals as well as to ensure that the EDPB is more open to interact with the industry, especially for codes in more technical areas. A business member representing the pharmaceutical sector calls for the Commission to reflect on ways to overcome a blockage in the decision-making process for the approval of codes. Another business member representing SMEs mentions the need for codes

[14] THE RIGHT TO LODGE A DATA PROTECTION COMPLAINT: OK, BUT THEN WHAT? An empirical study of current practices under the GDPR

to take into account the specific needs of SMEs, as well as templates and standard tracks to be followed for facilitating codes' approval.

13. Certification, including as a tool for international transfers

Adequate use of certifications

Similarly to the observation above on codes of conduct, several individual and business members regret that certifications, including as a tool for international transfers, are not widely used because the process for their development and approval has been complicated and slower than expected.

According to one individual member acting as legal advisor, companies' interest in certifications is decreasing due to the costs associated for obtaining certifications, the overall complexity of the certification process and the lack of legal certainty since certification only serves as a mitigating factor in terms of compliance, rather than providing a legal guarantee.

Challenges in the development of certification criteria, or in their approval process

In the view of one business member, certifications would be successful if there is a uniform cross-national understanding of the GDPR.

Supports for developing certification criteria

Some members call for a clearer timeline for the review and approval of certifications.

14. GDPR and innovation / new technologies

Overall impact of the GDPR on the approach to innovation and to new technologies

There are diverging opinions among members on the overall impact of the GDPR on the approach to innovation and to new technologies.

On the one hand, several civil society members note positively that the GDPR is beneficial to innovation by enabling privacy-friendly European solutions to be embedded in new technologies. In the same line, several individual and business members consider that the impact of the GDPR has been, broadly speaking, positive since companies tend to embed the GDPR rules and principles (such the principle of privacy by design and by default, and security of processing) in the development and implementation of new technologies, which is as a prerequisite for the trust and uptake of such technologies. In the views of some business members, the risk-based and technology neutral approach of the regulation has to be preserved as it is designed to be future-proof and adaptable to emerging technologies and evolving realities. However, certain concerns remain due to the tension between the GDPR and the use of emerging technologies (such as AI applications, biotechnologies and blockchain) and need to be addressed in specific guidelines with sector specific examples. From the business point of view, companies need legal certainty so that they can continue to invest in innovative data protection solutions.

On the other hand, some individual and business members report that the GDPR is seen as a block against innovation and technologies. Those members explain that the fundamental principles under the GDPR (such as purpose limitation and data minimisation), coupled with an overly restrictive interpretation by the EDPB of GDPR concepts (such as anonymisation, contract legal basis under Article 6(1)(b) GDPR and automated decision-making under Article 22 GDPR) could pose an obstacle to innovation in Europe. This concerns in particular AI training, which requires using and working on sets of data (including special categories of data) with unspecified purposes, reuse of data and combining the data with other data or sources. Furthermore, some business members are concerned that SMEs' fear for administrative fines could hamper their uptake of new technologies.

As solution to address the above-mentioned issues, those members call for the respect of the GDPR principle of technological neutrality and for the necessity to strike a balance between data protection and technological innovation. Furthermore, those members suggest the Commission should work closely with the EDPB to provide necessary clarifications (e.g. on the controller-processor relationship in more complex multi-party arrangements, such as Generative AI and white-label solutions) to enable businesses to benefit from new technologies.

On another note, a member representing consumers is concerned about the digital advertising market in Europe and calls for the Commission to propose a new regulation that prohibits tracking and profiling of consumers for advertising purposes. That member regrets that manufacturers are excluded from the GDPR and suggests the development of specific rules targeting manufacturers of products that are used to process personal data.

Interaction between the GDPR and new initiatives under the Data Strategy

Several members consider that the interaction between the GDPR and new initiatives under the Data Strategy raises questions.

More concretely, some individual and business members see a risk of fragmented enforcement of these new initiatives and recommend further defining the specific powers of the new regulatory bodies designed to ensure the compliance with the new initiatives to avoid a conflict with the competences of the DPAs and a risk of parallel proceedings.

Some members are concerned about the multiplication of new rules under the Data Strategy applying to data processing and the risk of inconsistencies with the obligations stemming from the GDPR and unclarities as to the lawful grounds for processing (most specifically, possible tensions surrounding the use of consent) as well as the relations between data subjects and new actors that are supposed to help them to exercise their rights. For instance, they ask for further clarification on the interaction of the requirement for DPIAs under the GDPR with the requirement for Fundamental Rights Impact Assessments (FRIAs) under the AI act. Those members call for strengthening the cooperation between DPAs and other competent regulatory authorities to ensure the coherence in the implementation of the new rules (especially concerning issues linked to data anonymisation, data retention and processing of special categories of data). Furthermore, some members point to issues such as lack of common

standards for anonymising and pseudonimising personal data (referring to the European Court of Justice decisions in the cases C-582/14[15] and T-557/20[16]).

A member representing the pharmaceutical sector is concerned that the GDPR may become an obstacle to the secondary use of health data in the context of the Commission's proposal for the European Health Data Space (EHDS). From the consumers' point of view, one civil society member expresses concerns that the EHDS proposal is watering down the level of protection afforded to the processing of health data under Article 9 GDPR as the EHDS introduces a new set of applicable rules.

A business member (CEDPO) is concerned that the new initiatives under the Data Strategy may generate disproportionate burden and responsibilities on DPOs.

[15] Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.
[16] Case T-557/20, *Single Resolution Board (SRB) v European Data Protection Supervisor (EDPS)*, ECLI:EU:T:2023:219.