CONTRIBUTION FROM THE MULTISTAKEHOLDER EXPERT GROUP TO THE STOCK-TAKING EXERCISE OF JUNE 2019 ON ONE YEAR OF GDPR APPLICATION

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

Report

13 June 2019

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:
http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&NewSearch=1&NewSearch=1

REPORT – CONTRIBUTION FROM THE MULTISTAKEHOLDER EXPERT GROUP TO THE STOCK-TAKING EXERCISE OF JUNE 2019 ON ONE YEAR OF GDPR APPLICATION

On 8 March 2019, 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 since 25 May 2018. The deadline for responding was initially set at 5 April 2019, and was then extended until 11 April 2019.

The Commission received contributions from the following members[1]:

Business:

- Confederation of the European Data Protection Organisations (CEDPO)
- European Banking Federation (EBF)
- DIGITAL-EUROPE
- E-Commerce Europe
- European Federation of Pharmaceutical Industries and Associations (EFPIA)
- European Telecommunications Network Operators' Association (ETNO) – GSMA Europe
- Federation of European Direct and Interactive Marketing (FEDMA)
- Insurance Europe
- SMEunited[2]

Civil society:

- Access Now Europe
- Bureau Européen des Unions de Consommateurs (BEUC)
- The Danish Consumer Council
- European Parents Association (EPA)
- Privacy International
- Stiftung Digitale Chancen (Digital Opportunities Foundation)
- Union Fédérale des Consommateurs - Que Choisir (UFC – Que Choisir)
- Verbraucherzentrale Bundesverband (Federation of German consumer organisations)

Individual members (Professionals or Academics)

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

The questionnaire (see in Annex) provided a list of questions on 11 main aspects of the GDPR, in particular: the exercise of data subjects' rights; consent; complaints and legal actions; use of representative actions under Article 80 GDPR; experience with Data

[1] The information on members of the Multistakeholder Expert group is available on the Commission Register of Expert groups, at:
http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&NewSearch=1&NewSearch=1
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.

[2] The contributions come from SMEunited member organisations in Austria, Belgium, Denmark, France, Germany, Greece, Italy, Poland, Spain and the Netherlands.

Protection Authorities (DPAs) and the one-stop-shop mechanism (OSS); experience with accountability and the risk-based approach; Data Protection Officers (DPOs); controller/processor relationship; the adaptation/further development of Standard Contractual Clauses (SCCs) for international transfers; and experience with the national legislation implementing the GDPR.

1. Main issues experienced by organisations in complying with the GDPR

Most organisations underline the considerable investments they have made in ensuring compliance with GDPR and the workload generated by GDPR accountability requirements. They report that most of their resources were devoted to documenting accountability, refreshing consent (where applicable), updating data protection information notices and contracts, implementing policies for dealing with data breaches, creating new internal business processes for handling data subjects' requests or validating new processing operations, internal awareness-raising and training. Many organisations welcomed the spur of GDPR in obtaining funding and management buy-in for finally updating IT systems that have for some time needed to be upgraded; in that way GDPR was often seen as effecting positive change. Small and medium- sized enterprises ('SMEs') report having spent considerable resources to adapt to GDPR obligations, such as documentation or establishing data processing policies, which they perceive as an increase in administrative duties. Many SMEs mention they had to seek advice from external consultants to understand the rules and set up systems to comply with the GDPR (including the implementation of technical and organisational measures), and that they usually lack the necessary human and economic resources to implement the obligations in GDPR.

Several organisations experienced difficulties in respect of the information technology systems they use. Those with old legacy information technology systems found it challenging to deal with data subjects' requests for access and erasure. Some organisations also indicate that making technical changes in legacy systems to implement data protection by design/by default, or for implementing the deletion of data in decentralised IT systems, is sometimes very difficult or too costly. Several organisations fear that DPAs would take a strict approach on the implementation of the risk-based approach; they underline that DPAs should be encouraged to be pragmatic in recognising the scale of the changes implemented and the impossibility to achieve perfection.

Some members indicate difficulties in applying the GDPR stemming from the way that certain provisions of GDPR are formulated (e.g. absence of a definition of 'risks' in relation to personal data breach notification, no definition of 'processing on a large scale', no minimum threshold for when to include a processing activity in the records, etc). Some members complain that the GDPR lacks exceptions for SMEs (e.g. in practice there is no real exception applied in relation to the obligation to maintain records of processing activities), and that the law in some Member States obliges them to appoint a Data Protection Officer also in situations not required by the GDPR (e.g. in Germany). SMEs value the importance of codes of conduct in helping them comply with the GDPR, and recommend the development of an SME-test by the European Data Protection Board (EDPB) for purpose of assessing whether codes of conduct submitted to DPAs sufficiently take account of the needs of micro, small and medium-sized enterprises. On the other hand, they report that certification mechanisms are not financially attractive to SMEs because of high costs for certification.

While the EDPB guidelines are generally welcomed, several members regret that it was not delivered earlier in the process. They note positively the achievements of the EDPB in

fostering a consistent application of the rules in the EU and encourage the Board to continue its work in preventing fragmentation. Several members would also welcome more guidance from EDPB on new complex principles and rules of GDPR, including on the safeguards to be applied in further processing for scientific purposes or on anonymisation (following a risk-based methodology). Furthermore, SMEs would welcome the development of concrete, simple and user friendly tools to help them apply the guidelines in practice.

Several members report that while there has been a high level of awareness of individuals about the GDPR, they did not always fully understand the impact of the GDPR; for example, there were misunderstandings leading to the assumption that it was always necessary to obtain their consent or that the right to erasure was absolute. Dealing with these misconceptions was sometimes time consuming.

Civil society organisations point out that the GDPR is a very positive development in the protection of consumers' fundamental rights and in building a fair digital society and a digital economy that consumers can trust. Data protection is now recognised as an important and serious issue. Civil society organisations have witnessed the first positive impacts of the GDPR, with individuals in the EU using their data protection rights and filing complaints to the national authorities, as well as data protection authorities starting to apply the first fines. However, they indicate that the impact the Regulation should have on business practices still has to fully materialise and that they see a need to move from the implementation to the enforcement stage. While they witness cases of businesses implementation of GDPR which led to more privacy protections for users as well as growth in revenue and better customer service, they observe that a large number of businesses and public entities are continuing with data practices that raise serious compliance concerns (e.g., lack of sufficient information in terms of use and data protection notices, consent that does not fulfil GDPR requirements, lack of facilitation of the exercise of rights, etc.). Enforcement of GDPR is also needed in their view in relation to the respect of transparency and consent obligations in cookie banners and tracking walls. In addition, civil society organisations mention difficulties in the application of GDPR as concerns children and requirements for parental consent. They expect to see more important decisions undertaken by the DPAs in the coming months, particularly in cross-border cases, which are likely to lead to important disputes and court proceedings in the coming years. They warn that it is therefore likely that many of the positive effects of the GDPR will not be visible at the time of evaluation.

Several members note that a number of challenges for the proper implementation of GDPR lie with the Member States. On the one hand, they are responsible for the resources of the DPAs, which play an essential role in the enforcement of GDPR. On the other hand, the implementation of the GDPR in national laws has raised some difficulties. Further details are provided in section 10.

Some members also report concerns on the fact that the ePrivacy Regulation is not yet adopted, which leads to legal uncertainty for telecom operators and online services on the application of the law and on the scope of the future additional requirements with which they will need to adapt. One member suggests that the GDPR evaluation could be an opportunity to cover aspects related to ePrivacy. Consumers' organisations emphasise that the GDPR and the proposed ePrivacy Regulation constitute important building blocks for restoring the confidence of consumers in the digital economy, which is a basic condition for realising the full potential of digitisation.

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

Implementation of the information obligations

Many members (CEDPO, DIGITALEUROPE, EBF, Ecommerce Europe, Insurance Europe, as well as several individual members) indicate that organisations have undertaken extensive efforts in order to implement the GDPR's transparency and information requirements. This has included reviewing and updating the information they make available about their data processing practices as well as the mechanisms they use to communicate such information to data subjects. Several SMEunited members report that the number of micro and small businesses that publish the information on the company website has generally increased; however, they would like the information obligations to follow the risk-based approach, in particular for low-risk data processing activities. Members report that the implementation of the GDPR has led to a significant increase in the amount of information controllers include in their data protection information notices to data subjects.

Difficulties have been raised as to how detailed the provided information must be. On the one hand the controller should use "clear and plain language", on the other hand data processes are often highly technical and very complex. Companies and organisations therefore find it unclear how to inform about such data processes in an easily comprehensible way. Several members report that the EDPB guidelines on transparency provide recommendations that make it difficult in being both concise and comprehensive. For example, they indicate that the guidelines suggest that every recipient is named, or every country to which personal data is transferred is named. It can be difficult for organisations to collate all this information and keep it updated. In addition, some members doubt whether this information is always useful or meaningful to data subjects. One member underlines that it is important for DPAs to maintain the right balance and respect the risk-based approach of the GDPR, also in respect of the application of the information requirements.

Moreover, **several members express concerns on the way to provide the information,** including the way to use the layered approach, following recent decisions and/or documents from national DPAs. Furthermore, specific sectors (e.g. insurance) mention difficulties in complying with transparency requirements vis-à-vis data subjects that are not part of the contract.

Consumers organisations as well as two individual members indicate that **there are serious shortcomings in the application of the GDPR most notably regarding compliance by data controllers with their information obligations**. They underline that this is also confirmed by actions undertaken by different DPAs in that respect. They observe that it is still possible to find websites targeting the European market completely lacking a data protection notice or not making it visible, or with data protection notices not updated to recent legal developments. They note that although many data controllers have modified their information practices as a reaction to the GDPR, these changes are not enough yet as individuals still do not really understand the use of their data by data controllers and the consequences for their data protection. They underline that companies still have a very legalistic approach, taking data protection notices as a legal compliance exercise, and that information is still often quite complex, difficult to understand or incomplete[3].

Consumers organisations further observe that the content of data protection notices is often not clear on aspects such as whether the processing falls within the scope of GDPR, the provision of additional information (such as the right to withdraw consent where consent has

[3] A recent study funded by BEUC undertook an analysis of the privacy policies of 14 popular online services. The results of the study showed that none of the privacy policies was fully compliant with the GDPR. Study available at: https://www.beuc.eu/publications/beuc-x-2018-066_claudette_meets_gdpr_report.pdf

been asked, the safeguards applicable in relation to automated-decision making), or on how to exercise the rights. They point to issues of intelligibility and accessibility, in particular where information is provided following the structure of Articles 13 and 14 without cross-references to other relevant pieces of information[4]. Furthermore, consumers' organisations report issues with the way in which a few major digital players present information and choices to individuals in order to nudge them towards privacy intrusive options[5].

Exercise of data subjects' rights

Most members report a significant increase in requests to exercise data subjects' rights directly after 25 May 2018 in both private and public sector. In several sectors (e.g. banks and telecom), however, they experienced a temporary rise of requests directly after 25 May 2018, which have since then slowed down.

For most members, the majority of the requests concerned **access to personal data**. By contrast, Ecommerce reports that in its sector the vast majority of the requests concerned **erasure**. The increase of access requests is mainly attributed to factors such as the fact that access requests are free, that GDPR specifically provides that requests submitted electronically must be accepted, and the publicity around GDPR. They observe that requests for access have started to include all the various elements of the right of access, such as asking about the source of the personal data and recipients of the personal data and whether any of the personal data is transferred outside the EEA.

Several members report that there has also been an increase in **requests to exercise the rights of rectification and erasure**, although this varies according to sector. For example, DIGITALEUROPE, Ecommerce Europe, EFPIA and Insurance Europe also report an increase on the exercise of the right to erasure. FEDMA and some banks experienced an increase of requests for rectification and erasure. ETNO-GSMA and FEDMA also noted an increase in the exercise of the right to erasure and of **the right to object**, including objections to commercial communications. Several members also mention requests concerning the **withdrawal of consent**.

Most members report having received no request or no noticeable increase in **requests for meaningful explanation and human intervention in automated-decision making**. One individual member however indicates that often data subjects are not informed about the possibility to request access to meaningful information about the logic involved in automated decision making, which may affect the exercise of this right.

Concerning the exercise of the right to **data portability**, most members did not receive any request or no noticeable increase. Insurance Europe indicates that few insurance companies reported having received data portability requests with regard to claims history statements in motor insurance. One individual member and a consumer organisation note that this right is not enough explained to individuals; for instance the information provided on this right in

[4] In 2018, the Digital World Market Watch published a study about the compliance of eight social network apps with the GDPR, in particular regarding the provision of transparent information and the implementation of appropriate measures for ensuring data protection by default and by design. As concerns transparency requirements, the study showed that while information was given for purposes and legal bases, however seven out of eight providers did not correlate this information. This means that users could not see what data is collected, on what legal basis, for what purpose. Summary of the study available in English at: https://www.marktwaechter.de/sites/default/files/downloads/social_media_and_the_gdpr.pdf

[5] See for example Norwegian Consumer Council reports 'Deceived by Design', available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018- 06-27-deceived-by-design-final.pdf and 'Every step you take, How deceptive design lets Google track users 24/7', available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf

privacy policies is occasionally partial and sometimes missing. They underline that it is therefore difficult for data subjects to exercise it and to understand its usefulness. Members also mention that several data portability tools have been developed to assist individuals with the exercise of this right: for example the "Data Portability Cooperation" in the telecom sector launched by Telefónica, Deutsche Telekom, KPN and Orange in February 2018; the Google's Data Transfer Project, involving Microsoft, Facebook and Twitter[6]; and a new business model created by a digital marketing company to exercise the right to data portability on behalf of individuals having mandated it.

Difficulties in the application of the data subjects' rights

So far no insurmountable difficulties were detected in the application of the rights from the side of data controllers.

Business members report, however, that due to the increase in the number of requests to exercise their rights from data subjects, there may be some challenges in meeting the deadlines; in particular it is not just that the number of requests is higher, but that the requests are more wide ranging. They indicate that responding to requests for access within the prescribed deadline can also be time-consuming when dealing with unstructured electronic information or multiple IT systems in large organisations or decentralised management mode. Micro and small enterprises could experience difficulties in managing requests in the absence of adequate IT tools. Some members indicate that a challenge has been to ensure consistent training of front-line customer service teams on GDPR and the handling of data subjects' requests. Other common challenges reported relate to the lack of sufficient information provided in the request (such as absence of indication of which right is exercised or the scope of the request, lack of relevant identification of the individual, no clear explanation of what information is being sought in the context of an access request, no indication of the restriction requested or of the third party to whom to port the data).

On the exercise of the right of access, several members mention cases where individuals not only ask for information about and copies of their personal data, but also request copies of the original documents on which these data are based, which in their view is not prescribed in Article 15 GDPR. They further indicate that the exercise of access rights in the context of employer - (ex)employee relationship can be difficult and time-consuming, for example when individuals want to obtain all emails where they are mentioned or copies of CCTV footage.

Several members mention the issue of how to verify, in a proportionate manner, that the data subject exercising his or her rights is the person to whom the personal data relate as an area where further guidance from the DPAs would be helpful. They indicate that clarifications would also be welcomed as regards age verification for the processing of children data. Some organisations recognise that there is still room for improvement to facilitate the exercise of data subjects' rights, for instance in providing data subjects with user-friendly tools that ensure their identification, or in handling fully automated requests.

Some business members report that there have been few instances of malicious use of the rights, such as massive campaigns of requests for access to data sent to email addresses of DPOs from unknown organisations or bots, or requests made using the new 'rights access Apps' to organisations without any relationship with the individuals filing the requests. In addition, they mention instances where data subjects are taking advantage of the GDPR process to advance complaints that should be dealt with as part of the customer care process.

Consumers and civil society organisations consider that controllers still have some work to

[6] https://datatransferproject.dev/

do in implementing their obligations to facilitate the exercise of the rights. In their view, it often takes a very long time for consumer requests to be answered by companies and by the DPAs. They underline that individuals have difficulties in exercising their rights when it is not clear who is processing their data (e.g. processing by data broker and ad tech companies) and in the absence of clear contact address where to address the request (they indicate that an email address, while not mandated by GDPR, would be helpful). There are difficulties reported concerning the application of the right of access and the right to data portability[7], or the handling of requests for deletion. Furthermore, they point to situations where some controllers render such exercise highly difficult, notably by failing to provide enough useful information and guidance, and also by not putting in place procedures that could be regarded data-subject-friendly or at least not placing an excessive, insurmountable burden on data subjects wishing to exercise their rights.

Dealing with manifestly unfounded or excessive data subjects' requests

Several members indicate that there is no guidance yet at either national level or EU level about what an "unfounded or excessive" request is pursuant to Article 12(5) GDPR, and that controllers would highly value guidance from EDPB in this area. For many members, the current view is that meeting access requests although excessive is easier than trying to prove the request was excessive. Some organisations indicate having rejected requests as unfounded where individuals exercising the rights failed to provide information for their identification. Examples of possible 'unfounded' or 'excessive' requests provided by members include searching for personal data in un-structured electronic information systems or in back-up tapes, or making requests via a template for the sole purpose of causing harm to the controller by making the controller undertake a lot of work responding to the requests.

3. Impact of Article 7(4) GDPR regarding the conditions for valid consent

Several members report that there have been miscommunications leading individuals to believe that the consent was required for every data processing.

Shifting from consent to other legal basis

Several organisations report not having switched the legal basis of their existing processing operations to another legal ground. However, with respect to future processing, they mention that there has been a significant shift in the approach towards consent since the entry into application of the GDPR. Many organisations indicate that they would now choose where possible to rely on another legal basis for their processing, such as performance of a contract or a (balanced) legitimate interest. For these organisations, consent is used for specific types of processing where no other legal basis is available, for example sending of direct marketing. They explain that this is partly because of the additional requirements for a valid consent but also because of the threat of withdrawal. Several organisations underline that

[7] In 2018, the Digital World Market Watch published a second study related to the compliance of eight social network apps with the rights of access and data portability. The study showed that none of the providers provided adequate and complete information about the stored data. The providers often referred in standardised form to general help areas, web forms or data protection declarations. As a result, the lack of sound information also makes it difficult for individuals to exercise other rights such as the rights to rectification, restriction or erasure of certain data. As regards data portability requests, the data sets were available in very different file formats and could usually not be opened with standard software. In addition, the individual file and folder names and the content of the files were mostly in English. As a result, the data is hardly verifiable by individuals. This means that they cannot make an informed decision about whether the data is correct and which data should be transferred when switching to the new provider. Study available (in German only) at: https://www.marktwaechter.de/sites/default/files/downloads/bericht_dsgvo_ii.pdf

consent standards should remain practical otherwise that may lead to removing consent as a viable legal ground on which to process personal data.

Civil society and consumers organisations however note that practices in the online environment still do not fulfil all the requirements set out in the GDPR for obtaining valid consent. They underline that many companies continue to track users online and through their devices without valid consent in the meaning of the GDPR; they mention as example that cookie banners found on websites often give ambiguous information and force users to consent to the processing of their data and the sharing of such data with unspecified third parties for targeted advertising purposes if they want to access the website, or indicate that consent is "given'' by simply browsing on the site. They expect some clarifications will be brought on this issue by the EU Court of Justice in the case *Planet 49*[8]. They warn that a number of digital players are relying on specific designs to discourage users from choosing the more privacy-friendly settings or to force consent[9].

Consent by children

Several members, in particular civil society and consumers organisations, express concerns on the application of parental consent requirements under the GDPR. They note that information provided to data subjects about who can consent – whether minors can consent or it must be their holders of parental responsibility - is often unclear. In their view, this may have the consequence of denying services to children and keeping children away from the Internet until they have attained a certain age, which is not the purpose pursued by GDPR. Public bodies and charities working with children who usually obtained parental consent for processing children data indicate that they are shifting their approach by either allowing children to consent themselves where possible or relying on a different legal basis than consent. Consumers' organisations working with children's welfare organisations are concerned about digital platforms choosing other legal bases than consent depending on the national legislation in the respective countries (in particular choosing the contract legal basis under Article 6(1)(b) GDPR depending on the age of children for entering into a contract applicable in the national law). They warn that such practices circumvent the obligations pursuant to Article 8 GDPR and will lead to a fragmentation across Europe that was not intended by the GDPR.

Explicit consent for the processing of health data

The finance/insurance industry mentions specific difficulties on requesting explicit consent for processing health related data in insurance contracts where the processing of such data is necessary to be able to execute the contract correctly. Different justifications under Article 9 GDPR are being used across Member States for processing health data in an insurance context. This is also related to the fact that each Member State can rule out the exception of explicit consent, but this is not the case in every Member States. They suggest that a more European and harmonised approach for such cases would be useful. Insurance Europe and SMEunited member BIPAR[10] mention that insurance undertakings and intermediaries are facing difficulties in obtaining consent from data subjects that are not directly part of a contract with the insurance company or intermediary, and divergences of approaches between Member States on the legal basis for processing health data in a reinsurance context and for fraud prevention/detection purposes.

[8] Case C-673/17, *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, ECLI:EU:C:2019:246.
[9] See report by the Norwegian Consumer Council, 'Deceived by Design', *ibid*.
[10] European Federation of Insurance Intermediaries.

Dealing with tied consent

Several members underline that the question of the scope of Article 7(4) GDPR is of great importance. They note that the issue of tied consent directly questions some organisations' business model, including in the area of online marketing. One business member argues that the application of Article 7(4) GDPR should reflect the risk-based approach of the GDPR and it should be possible in certain circumstances for the controller to overturn the presumption in Article 7(4)[11]. One SMEunited member reports that micro and small enterprises have not yet reached an adequate awareness of the need for free consent and what are the consequences of a processing based on tied consent. Several controllers still have difficulties understanding how to obtain fully valid consent, and often confuse specific data protection consent and contract. They also struggle in tracking valid consent and collecting all necessary information to prove that all validity conditions are satisfied.

Consumer organisations indicate that a number of companies have switched the legal ground for processing from consent to the legal ground "performance of a contract" although the processing is not necessary for the performance the contract, thereby circumventing Article 7(4) GDPR. There are concerns about forced consent or contractual bundling of consent as a practice in the tech industry, which is the basis for the complaints against Facebook, Google, WhatsApp and Instagram filed by NOYB.eu in May 2018.

4. Complaints and legal actions under GDPR / Use of representative actions under Article 80 GDPR[12]

Complaints to Data Protection Authorities

Most members report an increase in the number of complaints submitted to DPAs. However not all sectors are equally affected; for instance DIGITALEUROPE members have experienced such an increase concerning complaints to DPAs, whereas EBF, Insurance Europe, GSMA-ETNO did not detect a significant increase of complaints to DPAs against their members' organisations.

Several members reported complaints related to transparency obligations, consent, request for identification by the controller before responding to a data subject's request, and the exercise of data subjects' rights in particular the right of access.

Court actions

Most business members indicate that there was either no court actions or no significant increase in the number of court actions against their members' organisations caused by the GDPR. DIGITALEUROPE members have in some cases challenged DPA decisions to courts. One individual member acting as a legal advisor reports an increase in the number of persons seeking to bring court actions to enforce their data subjects' rights.

Use of representative actions under Article 80 GDPR

Civil society and consumers organisations report that not-for-profit organisations entitled to enforce data subjects' rights under Article 80 of the GDPR have started to make use of the

[11] Reference is made to the AG Opinion in the case C-673/17, Planet 49, in particular paragraphs 98 and 99, *ibid*.

[12] Questions on complaints and legal actions under point 4 of the questionnaire were mainly answered by business members and individual members, while consumers and civil society organisations reported about complaints and legal actions under point 5 of the questionnaire. For legibility, the replies to the two sets of questions have been merged together.

possibility to bring representative actions for infringements of the GDPR. One member underlines that in many cases, these NGOs, or at least part of their staff, were already involved in data-protection-related advocacy or litigation prior to the GDPR. In other cases, action has been undertaken with the help of or by organisations with experience in consumer protection.

Civil society and consumers organisations indicate that the majority of these actions were launched based on a mandate from the affected individuals, considering that only few Member States have used the possibility to allow for non-mandated representative action on the basis of Article 80(2) of the GDPR[13].

Representative actions have taken the form of complaints to DPAs as well as requests for injunctions and claims for compensation in court. A consumer organisation in Germany (Verbraucher-zentrale Bundesverband) reports that several letters for "cease and desist" were sent by consumers' organisations to organisations such as Facebook, Google, Twitter. The letters dealt primarily with the legal basis for direct advertising, tracking and profiling; conditions for consent; custom audiences and further data transfer to third parties without consent; rights of data subjects and transparency.

Members report that NOYB.eu and la Quadrature du Net were among the first NGOs to file complaints on 25 May 2018 with several DPAs across the EU against the major digital players (Google, Amazon, Facebook, Apple, Microsoft), mostly around the issue of consent. BEUC indicated that a coordinated GDPR enforcement action against Google was launched at the end of November 2018, which entailed the filing of complaints with the DPAs in Norway, Sweden, The Netherlands, Slovenia, Greece, Czech Republic and Poland for infringements of the GDPR in relation to the processing of location data[14]. Privacy International reports having filed complaints in November 2018 with the DPAs in France, Ireland and the UK against seven data brokers and credit reference agencies on the ground that their use of personal data in particular for profiling does not have a legal basis and fails to meet, among others, the requirements of transparency, fairness, data minimisation, purpose limitation and accuracy[15]. Access Now reports that in December 2018 and January 2019, Open Rights Group, Panoptykon Foundation and their partners filed complaints related to the functioning of the online behavioural advertising ecosystem.

Several civil society and consumer organisations mention considering filing representative actions before courts to exercise the right to receive compensation on behalf of data subjects.

Civil society and consumers organisations consider all these actions as particularly important to help bring GDPR protections into reality for individuals, and as a means to contribute to the development of guidance and jurisprudence ensuring harmonised implementation of the law across the EU.

Challenges in the effective use of representative actions

[13] However, non-mandated representative action may be allowed based on other EU or national law.

[14] The consumer organisations participating in the action were: Forbrukerrådet (Norway), Consumentenbond (The Netherlands), Ekpizo (Greece), dTest (Czech Republic), Zveza Potrošnikov Slovenije (Slovenia), Federacja Konsumentów (Poland) and Sveriges Konsumenter (Sweden). See also the press release, available at https://www.beuc.eu/press-media/news-events/gdpr-complaints-against-google's-deceptive-practices-track-user-location and a Q&A document, available at https://www.beuc.eu/documents/files/Google_complaint_geo-location_tracking_FAQ.pdf

[15] Privacy International mentioned that these submissions were made as a civil society organisation, rather than on behalf of an individual under Article 80(1) GDPR, to reflect the systematic nature of the issues. They note that as the nationals laws in these countries do not allow the possibility to act without a mandate, this leaves it to the discretion of the DPAs as to whether they take forward their requests.

Civil society and consumers organisations, as well as one individual member, underline that procedural hurdles remain in place for NGOs to bring complaints, in particular when cross-border in nature. In their view, this is partly due to the fact that many Member States have not made use of Article 80(2) of the GDPR, which would allow NGOs to bring forward collective complaints without having to be directly mandated by individuals. They warn that access to remedy and the enforcement of rights might be unequal across the EU depending on whether or not Member States have put this possibility in place and on the extent in which non-mandated representative action is allowed based on other legislation. In addition, an individual member stresses the possible lack of awareness of individuals on the existence of such representative actions.

5. Experience with Data Protection Authorities and the one-stop-shop mechanism

Experience in the dealings with Data Protection Authorities

Most members report broadly positive interactions with DPAs, which are overall constructive and solution-oriented. They value the helpful guidance and practical advice provided by DPAs, though they note that the amount and practicality of guidance materials available varies depending on country. Many members noted significant delays for DPAs in responding to requests due to the increase of queries received by DPAs and other priorities. CEDPO considers that in most countries the timeframe to receive guidance from DPAs is too long. Solutions to address this issue have included the establishment by the French organisation of DPOs of a single point of contact with the French DPA that streamlines and summarises concerns of its members. There are also concerns that DPAs do not have enough resources, including staff, in order to timely fulfil their tasks and efficiently enforce the GDPR.

Guidelines issued by EDPB and by national DPAs

Members generally welcome the **EDPB guidelines.** Some members complain that the recommendations in the guidelines sometimes go further than the letter of the GDPR. There are also complaints that the guidelines are not always easy to apply or practical. Some members also consider that the EDPB does not sufficiently take into account the feedback received during public consultation. SMEunited expresses the need for SMEs to be provided with more concrete guidance and tools, such as templates, to help them apply the GDPR in practice (for instance on the identification of the legal basis for processing, transparency requirements, etc.).

Some members point to the uncertainties generated by **inconsistencies in the application of GDPR by DPAs** (e.g., differences between DPAs on the lists requiring a Data Protection Impact Assessment, on methodologies on how to conduct a DPIA, on the data breach notification risk assessment threshold or notification criteria, on the appointment of DPOs and the communication of their contact details), and encourage the European Commission to pay attention to developments at national level. There are difficulties caused by variations in the advice given by DPAs from the 16 Länder in Germany and from the DPA at federal level[16]. On certain matters, such as Data Protection Impact Assessment lists, several members would see considerable benefit in the EDPB producing a single consolidated list of high risk processing requiring a Data Protection Impact Assessment, instead of having each national

[16] For example, accountants providing payroll services are considered as processors by the DPA of North Rhine-Westphalia but as controllers in Bavaria; some regional DPAs only accept natural persons as DPOs while others have no problems with legal entities as DPOs.

DPA producing its own list. Overall, members stress the **importance of preventing fragmentation in the approach taken on the interpretation of the GDPR by DPAs**.

The one-stop-shop and the new cooperation mechanisms

Concerning the one-stop-shop, those organisations that have a main establishment in the EU and therefore benefit from the one-stop-shop report that this new system contributes to deal more efficiently with pan-EU issues. However they indicate that it is too early to say how well this new system is working. On the other hand, there are organisations that have a corporate structure that does not allow them to benefit from the one-stop-shop due to its relatively restrictive requirements.

One individual member regrets the lack of information provided by DPAs to complainants in the handling of complaints, in particular in cases where cooperation mechanisms apply. Civil society and consumers' organisations expressed the view that guidance from DPAs on the functioning of the EDPB and the new one-stop-shop mechanism would be welcomed as this new system has yet to be fully tested.

The designation of a representative of controllers or processors not established in the EU

No business member organisation reported experience with the designation of a representative for controllers and processors not established in the EU pursuant to Article 27 GDPR.

An individual member acting as a legal advisor mentions having dealt with cases of appointment of another group company as a representative of a controller established outside the EU. In such cases, the intra-group designation of a representative was found to be fairly straightforward, through a simple letter of appointment. The member indicated that the need for an EU representative is likely to be greatest amongst recalcitrant controllers and processors, who may well not appoint an EU representative at all.

6. Experience with accountability and the risk-based approach

Experience with accountability

Most members indicate that organisations have devoted considerable effort in implementing processes to demonstrate compliance with GDPR. Several members point that although the initial workload to implement accountability is high, it ultimately contributes to improved data management, with more structure being implemented within companies to ensure that the processes work well together. For DIGITALEUROPE overall the feedback was positive since these efforts have improved companies' internal performance. One member indicated being in the process of updating to the GDPR its Code of conduct developed under the previous data protection regime. Marketers have overall positively embraced GDPR on the view that compliance is likely to improve customer sentiment towards brands in the long term and are using it as an opportunity to make data protection a brand asset[17].

However, some organisations have experienced difficulties, in particular SMEs and public bodies. Despite the risk-based approach in GDPR, SME organisations are of the view that implementing the principle of accountability in small-sized companies is sometimes difficult; maintaining accountability requires an increase in human resources within the company or

[17] The FEDMA UK member finalised a study on the industry perspective on data protection. The full study is available at: https://dma.org.uk/uploads/misc/data-privacy---an-industry-perspective-2018-final.pdf

from external consultants as well as a volume of work to implement compliance mechanisms and maintain the GDPR-awareness of employees. Ecommerce Europe and SMEunited indicate that the administrative burden for documentation has increased significantly and the requirements in relation to the documentation are not explicit, neither regarding the content nor regarding the level of detail or the form. They also point to difficulties with the application of the data protection rules on aspects such as retention periods and international transfers.

One individual member reports that the public sector has some difficulties with, in particular, keeping records in relation to information sharing. That member expresses concerns from local authorities that there is another layer of bureaucracy being introduced that will make data sharing difficult.

Furthermore, consumer and civil associations report difficulties on their own compliance with GDPR as well as uncertainties on how to ensure compliance with GDPR for the processing of children data which affects to some extent the activities they carry out towards children.

Experience with the risk-based approach

Members generally report an overall positive experience with the application of the risk-based approach. Awareness of the need for accountability via a Data Protection Impact Assessment (DPIA) is growing, however several businesses, including SMEs, underline resource constraints limiting the rate at which organisations are able to process DPIAs. Several members express the view that it remains unclear for which processing a DPIA has to be made, and that regulatory guidance and national DPIA lists established by DPAs in respect of applicable thresholds when to conduct data protection impact assessments were not always helpful. In doubt, they mention that they carry out DPIAs for all types of processing, although this places an administrative burden on companies, which they do not see as necessarily improving the protection of personal data. Furthermore, due to different guidelines and lists published by DPAs at national level, companies that conduct their business in several countries must comply with different set of rules, which they claim is ineffective and burdensome. Ecommerce Europe voices a fear from its members that risk-based decision-making will not be honoured by the DPAs; this results in the implementation of a conservative risk-adverse approach. Members would welcome a pragmatic approach from the DPAs on the measures implemented by organisations following the risk-based approach.

Impact of GDPR on innovation

Many members express the view that the exact impact of the GDPR on future innovation is hard to estimate at present. Several tools and approaches, including data protection impact assessment and data protection by design, can help the development of innovation that is data protection friendly. Several members, however, warn that the GDPR requirements and the risk of incurring high administrative sanctions may negatively impact innovation if applied in a very strict manner. Such impact may be greater for organisations that do not have a data protection culture or SMEs. Others indicate that, despite initial fears, most businesses seem to have adjusted well to the introduction of GDPR and these fears do not appear to have materialised thus far.

Amongst the challenges, EBF and Insurance Europe indicate that a strict interpretation of article 22 GDPR (on automated individual decision-making, including profiling) could hinder the design of innovative products. This is particularly the case as concerns the interpretation of the conditions to use automated-individual decision-making where this is necessary for the performance of the contract, and the high threshold for obtaining valid consent under Articles 22(2)(c) and (4) GDPR.

Several members consider that the application of GDPR to new technologies such as blockchain, big data or artificial intelligence raises questions, which, if left unresolved may impact their development. They would welcome concrete guidance and a pragmatic approach from the EDPB on these matters, including on the implementation of the principles of data minimisation and purpose limitation in data-driven businesses. The initiative of the UK DPA (ICO) of creating a regulatory sandbox to support the use of innovative products and services that are in the public interest was mentioned as a useful tool to assist in developing a shared understanding of what compliance in innovative areas looks like[18].

A member representing the pharmaceutical sector mentioned that the impact of GDPR will depend on the interpretation of key provisions relating to scientific research and processing of health data and whether there will be divergence in the Member States' implementation of key concepts such as the safeguards required under Article 89 GDPR for the processing of health data.

Adjusting IT and data management systems to the new requirements

For many organisations, substantial investments were necessary to upgrade and operationalise software and IT systems to address the inventory, data management, carry out Data Protection Impact Assessments, implement data retention policies (e.g. automated archiving, digital deletion), centralise processes to address individuals' rights, and to introduce new security measures. Additional legal and information security resources were required, in many instances with recourse to external resources for additional support. Many business members indicate that a large part of the investments were also related to human resources and training of staff.

Concerning the extent to which organisations could rely on existing data management systems, this varies according to sectors and organisations. Insurance companies mentioned that they mostly relied and adapted accordingly existing technical and organisational measures. Ecommerce Europe indicates that the vast majority of its members in Germany needed to establish a completely new data management system, while in some other Member States they could rely to some extent on existing technical and organisational measures. DIGITALEUROPE and GSMA-ETNO report that their members had already robust technical and organisational measures, which did not make it necessary for them to establish new data management systems.

Impact of the measures implemented by organisations on individuals' awareness and trust

For several organisations the real impact of the measures they implemented to comply with GDPR upon customers' trust is still unknown to its full extent. Both business associations and consumer associations have witnessed an increased awareness from individuals on their right to data protection, which might result from public awareness campaigns and media interest rather than due to the concrete technical and organisational measures implemented by organisations. Ecommerce Europe mentions that some customers have asked companies how they have organised their technical and organisational measures, which was not the case prior to GDPR.

7. Data Protection Officers

Circumstances for appointing a Data Protection Officer

[18] https://ico.org.uk/about-the-ico/news-and-events/blog-ico-regulatory-sandbox/

Companies/organisations have appointed a mandatory DPO where required pursuant to Article 37(1) GDPR (e.g. banks, public bodies) or pursuant to Member State law (e.g. Germany). Several businesses have also appointed a DPO on a voluntary basis. Business associations have usually not appointed a DPO for their activities (however, several insurance associations as well as consumer organisations, such as UFC Que Choisir and Ekpizo, have appointed a DPO on their own initiative). In groups of companies, the designation of a DPO can be accompanied by the establishment of a data protection channel of correspondents.

SMEs pursuant to Article 37 (1) GDPR often do not have to designate a DPO. However in some Member States, SMEs may be under the legal obligation to designate a DPO (e.g. in Germany they must appoint a DPO where they constantly employ as a rule at least 10 persons dealing with the automated processing of personal data).

In the pharmaceutical sector, most companies members of EFPIA designated a mandatory DPO pursuant to Article 37(1) GDPR, although companies that only conduct small clinical trials (e.g., less than 100 patients) may not. However, they mention that health authorities tend to presume that a DPO will be appointed, ignoring the threshold requirements in the GDPR. EFPIA expresses the view that increased coordination among DPAs and health authorities across the EU would be welcome to resolve such issues in a harmonised way.

Experience with the role and performance of Data Protection Officers

Several members report that in countries where the designation of a DPO was already an obligation under national law before the entry into application of the GDPR, the experiences are good. Several organisations that needed to newly appoint a DPO have positive feedback regarding the role and performance of the DPO. DPOs are viewed by many members as a good institution for implementing data protection requirements within an organisation as well as a reliable point of contact for data subjects and DPAs, which benefits compliance and awareness in a company. Consumers' organisations view DPOs as an important building block in strengthening corporate accountability.

However, CEPDO and DIGITALEUROPE express the view that the market for experienced DPOs is still immature and there are still too few experts in the field taking into account the actual needs of organisations. CEDPO raises concerns around the many training courses that have emerged that would allegedly allow non-experts to become DPO in a very short time period, which seriously harm the data protection profession. In their view, there are individuals acting as DPOs who do not have the requisite expertise.

CEDPO warns that many organisations and the public sector in general are not devoting sufficient resources to select experts and to put the DPOs in the appropriate conditions to conduct their work.

In the light of the increased complexity of data protection law accompanied by a severe sanctions' regime, there is a tendency towards shifting most of the data protection workload to the legal department whilst the DPO remains responsible for the minimum set of obligations as specified in the GDPR.

8. The controller/processor relationship

Several members argue that the characterisation of controller and processor is still not clear. They see a "trend" in the market after the European Court of Justice decision on Facebook where in some instances former processors now want to become controllers or joint

controllers[19]. Differences on roles are less clear for companies and therefore contracts governing the respective responsibilities of business partners in a processing are complex to negotiate. They mention that the contractual assignment of the controller/processor role is sometimes left upon the will of the strongest company in the market, rather than on who decides on the purposes. In addition, they note that the scope of who falls within the definition of a processor is not always clear; for example some vendors maintaining and supporting software refuse the adaptation of their contracts according to Article 28 GDPR arguing that their tasks do not include processing of personal data. Several members (e.g. SMEunited) welcome the stakeholder event organised by EDPB on the notions of controller and processor and stand ready to provide further contribution. They would welcome further clarifications by EDPB on these notions including further examples of the determination of controller / processor (e.g. in particular in relation to specialist service providers where they process personal data in accordance with their regulatory and/or professional obligations, such as intermediaries in insurance or banking sectors).

Experience with the adaptation of controller/processor contracts

Business members report that, where needed, the (re)negotiation of controller-processor contracts is often a time-consuming and lengthy process. The effectiveness in the adaptation of contracts depends on the level of understanding of the GDPR by the contracting parties. Some organisations (both controller and processors) have used this as an opportunity to either include provisions that go beyond those required under Article 28, to include additional commercial provisions or to change the liability position of each party. Business members mention the following difficulties:

- Controllers trying to add clauses about financial indemnification on which Article 28 is silent on;
- Controllers trying to transfer their obligations to processors, such as carrying out a DPIA, data breach notification to the DPA or the data subject, information to the data subject, including by transferring the risk of administrative fines to processors;
- Processor's obligations about breach notification, in particular when the processor obligation is triggered and what the notification should be;
- Processors facilitation of data subject rights, in particular whether processors can charge for facilitating those rights;
- Processors seeking indemnities from controllers in relation to any GDPR liability the processor might incur;
- Processors trying to restrict their obligations to cooperate with audits or inspections;
- For some telecom operators, the negotiation is around disagreement on security measures, period of data breach notifications, duty of cooperation, liability allocation, indemnification, audit rights, and sub-processors.

The interplay between the main contract and the data processing agreement is also a source of uncertainty, leading to renegotiations regarding aspects such as liability or termination of contract.

On the necessity to adopt Standard Contractual Clauses under Article 28(7) GDPR

[19] See judgment of the Court of justice of 5 June 2018 in Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388. See also AG Opinion delivered on 19 December 2018 in Case C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.*, ECLI:EU:C:2018:1039.

Several members including CEPDO, several members of Ecommerce Europe, ETNO-GSMA and consumers organisations recommend the adoption of standard contractual clauses for processor contracts. ETNO-GSMA and some members of Insurance Europe indicate that the adoption of standard contractual clauses could facilitate contract negotiations, bring clarifications on specific matters such as liability, and would overall improve compliance and harmonisation. Some members of SMEunited, Ecommerce Europe, CEDPO, EFPIA and Insurance Europe argue that standard clauses could especially benefit SMEs who do not have the resources to negotiate individual contracts with each of their data processing party.

Other members would support the creation of standard clauses provided they are not compulsory (individual member acting as legal advisor) or instead the development of a non-mandatory template of minimum requirements for data processing agreements that companies would be free to refer to (EBF). Other members do not see the need for the adoption of such standard clauses (e.g. DIGITALEUROPE and some members of Insurance Europe), and argue that the organisations that have already revised their agreements are not going to re-open them. Furthermore, they question to what extent all aspects of Article 28 GDPR can be standardised; for example, regarding the technical and organisational measures to be applied, the need for individual descriptions will remain (Ecommerce Europe).

One individual member expresses the view that if standard contractual clauses were to be adopted on this matter, account should be taken that this is an area where the negotiating position of the parties will not be equal, in order to include a number of possible clauses which can be chosen to best fit the commercial relationship between the parties. Otherwise, the standard clause would need to provide an appropriate commercial balance between the parties. Other members (including one individual member and EFPIA) recommend that standard contractual clauses should be considered for specific processing situations, e.g. for use in standard data processing, for use in public cloud, etc.

Content of possible standard contractual clauses under Article 28 GDPR

Several members (Ecommerce Europe, ETNO-GSMA) are of the view that the content of any such standard contractual clauses should identify what is really required under Article 28 GDPR. One member (Insurance Europe) argues that they should only contain elements that are listed in points 3 and 4 of Article 28 GDPR, while others see usefulness in clarifying certain aspects of the processor duty of cooperation (e.g. processors duty of cooperation in case of data subjects requests in the light of Articles 15 to 22 GDPR).

Ecommerce Europe is of the view that standard contractual clauses should provide variations to reflect different possible relationships with a service provider (controller/processor, controller/controller, or joint controllers). One member (Insurance Europe) recommends that they are adapted to the different levels of risk stemming from the processing.

It is proposed that the standard contractual clauses should include several provisions dealing amongst others, with auditing, liability allocation, the duty of cooperation of the processor, the processor's obligations in respect of data subjects' rights (in particular rectification and erasure), personal data breach (e.g. deadline for notification), and clear rules on return of the personal data upon termination of the contract (destroying vs. returning). Some members would value that the standard clauses clarify the obligation for the processor to be subjected to controls or audits requested by any data protection authority, and whether they allow for general authorisation to sub-processing and general audit rights. Several members also would

like clarifications on whether processors can charge controllers for the performance of functions which, by virtue of the language of the GDPR, appear to be mandatory (e.g. assisting with compliance with data subject rights; DPIAs; giving audit access; breach notification, etc).

Several members (Ecommerce Europe, ETNO-GSMA) see a need to develop new standard contractual clauses for the processor/sub-processor relationship or at least to clarify in standard contractual clauses the sub-processor objection rights, the direct monitoring rights with regard to sub-processor, as well as who bares the obligation to bind the sub-processor (the processor or the controller).

Some members underline that it may be difficult to come up with one single set of generic clauses that reflect all scenarios and therefore recommend a flexible structure of the clauses. The clauses should be able to be used in a number of different ways (e.g. as a standalone agreement or by integrating some of its wording into a contract). However other members recommend not adopting a separate set of clauses specifically for purpose of Article 28(7) GDPR and to make use of and adapt the already existing standard contractual clauses for international controller to processor transfers, which are well known and broadly accepted (DIGITAL EUROPE, ETNO-GSMA). Ecommerce Europe mentions that it would be useful if these standard contractual clauses could be set up as 'master processing agreements' under which additional processing activities could be added as necessary without having to negotiate separate agreements. Several members warn that the clauses should not be too rigid or extensive. Some of the details relating to the clauses will be fact specific, for example the security measures used by the supplier, and will have to be further specified in a separate Annex (like for the current international standard contractual clauses).

9. Adaptation/further development of Standard Contractual Clauses (SCCs) for international transfers

Most members concur that the current SCCs serve their purpose and are widely used for the transfer of personal data outside the EU. They are generally well-known and accepted by stakeholders, with very few exceptions. However, while some members have not encountered problems on a structural basis with the current SCCs (EBF) and do not see a need to update them (ETNO-GSMA, Stiftung Digitale Chancen), most members consider that a number of areas could be further improved. Many see a need to make the SCCs easier to use, or more flexible (for instance, in order to cater for complex global data processing situations involving several data importers and exporters, or varying degrees of risks), and they would like to see more clarity on specific aspects in relation to the use of SCCs (e.g. the treatment of sensitive data, onward transfers, situations of joint-controllership). Having multiple sets of SCCs has also been mentioned as a factor creating confusion. One member (CEDPO) would welcome sector-specific clauses.

The majority of members think that the existing SCCs should be adapted to better reflect the GDPR and in particular in order to take into account the requirements of Art. 28 (on the controller-processor relationship), while allowing some flexibility to reflect the specific circumstances and relationship between the parties. However, others do not think that a combination with SCCs for Art. 28 would be necessary.

They also agree on the importance of having processor to sub-processor clauses, as well as for other situations currently not covered: e.g. joint-controllership; EEA-processor to non-EEA-controller (if it is considered that the latter scenario involves an international transfer).

Areas identified as requiring further clarification include inter alia: relations with sub-contractors and collaboration to demonstrate compliance; auditing requirements (possibility to simplify burdens on processors being audited by several controllers, e.g. through certificates); data breach and reporting obligations; management, functions and identification of DPO; data-subject's rights; information obligations (Art. 13 and 14 GDPR), liabilities and indemnities. A few members indicated that additional mandatory principles (accountability, privacy by design and by default) should be explicitly referenced.

The continued availability of SCCs as a means to justify the transfer of personal data outside of the EU is considered essential for several stakeholders and some members expressed concerns that the SCCs might be invalidated by the European Court of Justice. One member suggested further strengthening the control mechanisms for data exports as a possible improvement in order to protect SCCs better against challenges on their validity (as in the Schrems II case). According to one member (EFPIA), while it is too early to say if adaptations are required in light of Schrems II, the SCC should enable disclosures where they take place in highly regulated fields and in accordance with standardized practices and safeguards that apply reciprocally across many jurisdictions. Others suggested the inclusion of additional protections, such as a unilateral right to terminate the SCCs if intelligence surveillance is demonstrated, coupled with a right to demand return of the data. According to one member (AccessNow), data protection authorities should ensure greater scrutiny and increased control of the implementation of SCCs, including through proactive investigations and checks. According to the same member it could also be further clarified that, if a third country government is violating fundamental rights, it is a duty of the relevant data protection authority to make full use of its powers to suspend transfers. This member highlighted the importance of DPA guidance both for the GDPR update and for any possible amendments in relation to the Schrems II case. It also suggested that for increased transparency for the users and in line with information rights under the GDPR, SCCs should be made available publicly and not just provided to the data subject on request.

Another member (Insurance Europe) suggested the involvement of the DPA of the importing country and other safeguards like "collective controls" and the use of certificates. It also suggested that the EDPB's concerns raised in the context of the second review of the Privacy Shield should be duly taken into account while developing updated SCCs.

In general, the need for legal certainty and predictability is mentioned as vital for international data transfers and therefore any possible modification/update of the SCCs should take into consideration the large amount of already signed contracts.

10. Experience with the national legislation implementing the GDPR in the Member States

Members point to issues in some Member States regarding the use of the specification clauses in GDPR and to provisions of national laws implementing the GDPR that would not be in compliance with the GDPR. They also raise concerns on the resources allocated to the DPAs.

Use of the specification clauses in GDPR by Member States

Several members report that Member States have widely used the specification clauses available under the GDPR to create specific national rules on a number of aspects. They mention that several Member States have adopted national laws providing specifications for the processing of special categories of personal data under Article 9 GDPR, which they argue creates fragmentation in the implementation of the GDPR. Several members observe that the use of the specification clauses in GDPR by Member States has created considerable hurdles for companies operating cross-border (e.g. in the area of health).

National laws implementing the GDPR not in line with the GDPR

Civil society organisations raise concerns on the fact that, one year after the entry into application of the GDPR, three Member States still have to adapt their national legislation to align it with the GDPR. Furthermore, they argue that in several Member States the national law that was adopted is not in line with the spirit of the GDPR. Their concerns relate essentially to the implementation by Member States of derogations to data subjects' rights, and to the provisions of national laws in areas where Member States may derogate to specific GDPR provisions, where necessary and proportionate to reconcile it with other fundamental rights and freedoms.

As regards the implementation of derogations to the data subjects' rights by Member States, civil society organisations expressed their views that this includes for example a wide interpretation of what exemptions are permissible under Article 23 GDPR.

As regards the provisions of national laws providing broad derogations from the GDPR, civil society organisations mention issues concerning the reconciliation of the right to data protection with the right to freedom of expression and information, as well as the processing of personal data in the political context.

DPAs' resources

Another concern expressed by the members relates to the effective resources available to DPAs for the performance of their tasks and the necessity for Member States to increase the funding and staffing of their data protection authorities. Members agree that recent data from the EDPB show that in some Member States, financial and human resources are significantly insufficient. As a result, they warn that data protection authorities might not be able properly and effectively perform their tasks, in particular if the number of complaints continues to grow.