Report on the General Data Protection Regulation

Comments and Responses by Selbstregulierung Informationswirtschaft

Call for Evidence by the European Commission

February 2024

selbstregulierung informationswirtschaft e.V.

Herausgeber

Selbstregulierung Informationswirtschaft e.V.
Großbeerenstraße 88
10963 Berlin
https://sriw.de

+49 (0)30 30878099-0
info@sriw.de

Amtsgericht Berlin Charlottenburg
Registernummer: VR 30983 B
USt-Nummer: DE301407624
Deutsche Bank AG
IBAN: DE33 1007 0000 0550 0590 00

Vorstandsvorsitz
Dr. Oliver Draf

Geschäftsführer
Frank Ingenrieth

Table of Contents

1. Executive Summary

This executive summary focuses on our observations and recommendations concerning the implementation of the General Data Protection Regulation in the light of Codes of Conduct. It underscores the need for clear guidance and support from the European Commission in implementing GDPR for a framework protecting data subjects in a phase of innovation, reflecting a nuanced understanding of operational practicalities, business reality and legal clarity, where the role of Codes of Conduct and Monitoring Bodies is encouraged.

1.1. General Remarks and Harmonization of GDPR

- GDPR's key element – harmonization – across the Europe Union has not yet been reached. Therefore, we stress out the necessity for enhanced support, clarification, and harmonization in the application of GDPR provisions, aiming to achieve a balanced and effective data protection framework that is adaptable to the evolving technological and societal landscape.
- We stress out that especially transnational Codes of Conduct may act as facilitator to harmonize GDPR's interpretation across Europe; likewise, Codes of Conduct may act as facilitator to determine sector-specific, effective yet efficient means to implement GDPR.
- We recommend the European Commission to strongly encourage the Member States to harmonize their interpretation and application of GDPR provisions, as well as to follow the EDPB in order to have a unified legal framework that balances innovation and data protection.
- Codes of Conduct inherently involve different stakeholders, experts and strive for a fair balance of interests. The approval process ensures that Codes of Conduct will not undermine GDPR's requirements. In cases of transnational Codes of Conduct, it promotes cross-European harmonization. It must be interpreted as the opportunity for the industry to implement GDPR closest to operational practice, eventually satisfying both the authorities, the industry and data subjects.
- Given the importance of and the impetus by EDPB's guidelines, it is recommended to enhance stakeholders' involvement and allow for direct legal remedies and protection against such guidelines. In practice, Guidelines appear having stronger impact on determining legality of processing personal data than GDPR's original provisions.
- It shall also be highlighted that in the process of balancing interests, GDPR must acknowledge several fundamental rights, freedoms and interests of data subjects, including those interests and rights deriving from various legal requirements and societal norms outside GDPR.

1.2. Codes of Conduct and GDPR Compliance

- We believe that the potential of Codes of Conduct has not yet been sufficiently utilised. Experience and reports indicate that industry is willing to establish more Codes of Conduct but faces overly complex processes, ambiguous or even overly rigorous expectations by supervisory authorities.
- We recommend the European Commission to actively support the development and approval of Codes of Conduct, highlighting their crucial role in providing clarity, enhancing data subject rights, and ensuring effective data protection tailored to different sectors and company sizes. The benefits and incentives for Codes of Conduct shall be enhanced, structurally and effectively.

- We stress out that Codes of Conduct will increase effectiveness and efficiency of GDPR enforcement and may take a key role in facilitate cross-European harmonization.
- We recommend clarifying that adherence to a Code of Conduct shall be per se considered as a positive factor.
- EDPB's guidelines require added value by particularizing GDPR, which eventually requires the exchange between different stakeholders. We recommend the European Commission to clarify that such exchange during the drafting of Codes of Conduct is privileged conditionally.

1.3. Approval of Codes of Conduct

- We recommend a clarification that Supervisory Authorities shall prima facie approve Codes of Conduct unless they positively conclude a conflict with GDPR; the principle of majority votes in the EDPB shall be emphasized.
- Data protection supervisory authorities shall be invited to acknowledge and in best cases reflect cross-regulatory requirements.
- We recommend for transnational Codes of Conduct to streamline the procedures reducing unnecessary formalities, limiting risks that initiatives are halted by ambiguities to determine the competent supervisory authority. If transnational Codes of Conduct are concerned, the process shall be streamlined, clarifying that any authority shall be deemed competent which has been selected by code-owners.
- We recommend allowing for an active involvement of code-owners in the approval-process– even at the level of the EDPB – ensuring a close and efficient exchange of arguments and mutual understanding of the processing context, business realities, interpretation of GDPR and non-negotiable essentials of protecting data subjects.
- Upraising interpretations requiring EDPB's involvement for any – even minor or editorial – update of a Code of Conduct appear excessive. Clarification is recommended limiting the EDPB's involvement to fundamental, material aspects. Operational questions, as they do not affect material matters, should be treated similarly.
- We stress out that corporate governance shall not be subject to the approval decision.
- We observe that the general validity mechanism as an implementing act as well as its related legal effects against the specific context of Codes of Conduct remains generally unclear. In this respect, we consider that general validity shall be granted in a timely manner to not unduly delay the process and to allow for the rapid adoption of these tools by the market. To this end, we recommend that the process between the EBPB and the European Commission will be further streamlined; or as evaluation may indicate, even delete the requirement of a general validity.

1.4. Monitoring Bodies and Accreditation

- A harmonisation of requirements is needed regarding the accreditation criteria for Monitoring Bodies. Currently accreditation criteria that a Monitoring Body must meet to be-come accredited are particularized by the national data protection supervisory authorities and thus differ at a national level. Deviations should only refer to Member State's administrative law.
- A mechanism that will support a consistent interpretation of accreditation criteria by data protection supervisory authorities is highly welcomed.

- To facilitate the accreditation of Monitoring Bodies, it would be very appreciated if the European Commission will clarify on the need of a fully harmonized approach in respect of Art. 41 (2). To facilitate transnational Codes of Conduct, overarching clarifications are highly recommended. E.g., in cases of transnational Codes of Conduct, it shall suffice to submit documents in English.

1.5. International Data Transfers

- As a specific aspect of third country transfers, we would like to point out that from our point of view the Guidelines for Codes of Conduct are mainly written from a controller's perspective. However, in practice processors play a significant role. Therefore, we stress out that Codes of Conduct should also be drafted from a processor's perspective, as, e.g., the related initiative of the EU Cloud Code of Conduct.
- Requirements in establishing such Codes of Conduct or Certifications as appropriate safeguards – materially and procedurally – shall be re-evaluated to facilitate their operationalisation.
- It is acknowledged that GDPR foresees different requirements understanding Codes of Conduct and Certifications applicable to different scenarios. However, if in practice, both mechanisms are approved without such differentiated approach, additional requirements to one or the other mechanisms shall be deleted.
- It is recommended to clarify that adequacy of data protection in a third country shall be understood as equivalency rather than identity.

1.6. Cross-Regulatory Compliance

- Potential challenges may arise in achieving alignment between the Data Act or other recent European Acts with GDPR. We recommend extending Art. 40.2 GDPR, stating that Codes of Conduct may act as cross-regulatory harmonization.

1.7. Data Subject Rights

- We noticed uncertainties in the application of Art. 21 GDPR and its relation to Art. 6.1 (f) GDPR. Codes of Conduct may provide clarity, for example by creating preliminary categories as to when a "particular situation" exists and therefore Art. 21 GDPR applies.
- Transparent information of data subjects is one key element of effective data protection. We recommend limiting transparency obligations to those elements eventually providing added value to data subjects. Conditional elements or alternatives shall be subject to sector-specific initiatives such as Codes of Conduct.

1.8. Impact on mSME

- Disproportionate operational burden seems placed on micro, small, and medium-sized enterprises by some interpretations of GDPR. We stress out that GDPR allows for distinct risk evaluations, considering elements such as economic powers, to what extent processing of personal data reflects core business activities or rather a enabling necessity for other activities We suggest that the European Commission clarifies the differentiation by company size, aiming to tailor requirements to avoid unnecessary burdens on smaller entities.
- We recommend the European Commission to facilitate the development of codes of conduct specifically addressing mSME. In specific industry sectors, codes of conduct could actively support mSME to comply with GDPR regulations. As codes of conduct will be drafted by regulatory experts, they will help mSME by several means, e.g., understanding how to best implement GDPR

requirements. This will provide enhanced clarity and have a positive effect on mSME by ensuring transparency and stability. Overcoming ambiguities and receiving pragmatic guidance by means of codes of conduct will benefit mSME economically, allowing them to focus on their main business activity.

1.9. Impact on Research and Development

- The importance of balancing data subject rights with the needs of processing entities is highlighted, suggesting that the European Commission gives impetus to research and development efforts that advance the public interest, even if performed by private entities, within the legal boundaries of GDPR. Codes of Conduct may act as a linking element in balancing concluding adequate protection of data subject's interests.

2. Introduction

We highly appreciate the opportunity to submit our first-hand experience in regards of the effective implementation of GDPR. Representing an entire European ecosystem in establishing self- and co-regulatory measures, such as Codes of Conduct pursuant Art. 40 GDPR, our submission will have a distinct focus and angle.

We acknowledge that the European Commission may not have foreseen this specific dimension in its request for consultation. However, we consider this dimension crucial in effectuating GDPR while remaining accessible for mSME.

Since its establishment, our ecosystem has provided its perspective by various consultations, statements and papers. Those specifically addressing GDPR shall be listed below. Some detailed analysis or argumentation were not fit for purpose of the provided questionnaire. Nonetheless, we would like to raise the European Commission's attention to any of such papers, if and to the extent that the European Commission wants to analyse certain scenarios in more detail.

- GDPR's 5th Anniversary Resumée – A practical resumée from a co-regulatory perspective, reflecting Codes of Conduct and Monitoring Bodies in particular[1]
- Five Years of GDPR – Key Challanges & Recommendations (Joint Comments by ESOMAR, SCOPE Europe, Selbstregulierung Informationswirtschaft and FEDMA)[2]
- European Commission's Initiative: Further specifying procedural rules relating to the enforcement of the General Data Protection Regulation[3]
- Guidelines 04/2022 on the calculation of administrative fines – Joint Comments by SRIW and SCOPE Europe[4]
- Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR – Joint comments by SRIW, SCOPE Europe and the EU Cloud CoC[5]
- Comments on EDPB public consultation R01/2020: 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection

[1] https://sriw.de/fileadmin/sriw/files/202306_SRIW_5th-Anniversary-GDPR_Resumee.pdf
[2] https://sriw.de/fileadmin/sriw/files/consultations/5_YEARS_OF_GDPR.pdf
[3] https://sriw.de/fileadmin/sriw/files/consultations/Joint_Comments-SRIW-SCOPE_Europe.pdf
[4] https://scope-europe.eu/fileadmin/scope/files/consultations/Comments_on_Guidelines_04_2022_on_the_calculation_of_administrative_fines.pdf
[5] https://scope-europe.eu/fileadmin/scope/files/consultations/202201_Comments_on_EDPB_Guidelines_05-2021.pdf

of personal data' – Joint comments by SRIW, SCOPE Europe, and the EU Cloud Code of Conduct[6]

- Feedback to the initiative "Report on the application of the General Data Protection Regulation", pursuant to Article 97 of the GDPR[7]
- Comments by SRIW on the German concept on determining administrative fines under GDPR [German] (*Stellungnahme des Selbstregulierung Informationswirtschaft e.V. zum "Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen"*)[8]
- EDPB Codes of Conduct Guidelines – Public Consultation: Comments submitted by SRIW e.V. and SCOPE Europe bvba/sprl on "Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, adopted on 12 February 2019"[9]
- Policy Brief: Enhancing Consumer Protection with Co-Regulation[10]
- EDPB Certification Guidelines – Public Consultation: Comments submitted by SCOPE Europe bvba/sprl[11]

3. About the authors

Selbstregulierung Informationswirtschaft e.V. (SRIW)[12] is a non-profit association with European focus.

Ever since its establishment in 2011 and as the primary of a pan-European ecosystem, SRIW assembled first-hand experiences in the establishment of trusted self- and co-regulatory instruments in the information economy. Additionally, the association benefits from its independent subsidiaries across Europe and its diverse and constantly growing membership.

The everyday business of the association centres on harmonising industry practices with social demands and political requirements. The mechanism considered fit for purpose is balanced and monitored self- and co-regulatory frameworks facilitating effective data and consumer protection. SRIW

---

[6] https://scope-europe.eu/fileadmin/scope/files/consultations/20201221_Consultation_EDPB_Recommendations_Supplementary_Measures.pdf
[7] https://scope-europe.eu/fileadmin/scope/files/consultations/202004_Consultation_GDPR_Review.pdf
[8] https://sriw.de/fileadmin/sriw/files/consultations/Konzept_zur_Bussgeldzumessung_DSK_Kommentierung_SRIW.pdf
[9] https://scope-europe.eu/fileadmin/scope/files/consultations/Consultation_EDPB_Codes_of_Conduct_SRIW_SCOPE_Europe.pdf
[10] https://scope-europe.eu/fileadmin/scope/files/Policy_Brief_Enhancing_Consumer_Protection_with_Co-Regulation_SCOPE_Europe.pdf
[11] https://scope-europe.eu/fileadmin/scope/files/consultations/Consultation_EDPB_Certification-Guidelines_SCOPE-EUROPE_SRIW.pdf
[12] https://sriw.de

strives to collect and amplify valuable experiences to improve the necessary and independent structures required for the development, approval and monitoring of Codes of Conduct. By actively connecting experts and bringing together interested stakeholders, SRIW serves as a forum for exchange and discussions, providing the impetus for kicking-off frontrunner initiatives.

The ecosystem includes SCOPE Europe srl[13], most probably Europe's leading independent Monitoring Body. SRIW's subsidiary became known in supporting the first officially approved transnational Code of Conduct, i.e. EU Data Protection Code of Conduct for Cloud Service Providers, and becoming the first ever accredited transnational Monitoring Body as well as the first Monitoring Body which was accredited by more than one data protection supervisory authority and for more than one Code of Conduct.[14]

Since 2021 SRIW is participating as partners in a research consortium related to the project "Cognitive Economy Intelligence Platform for the Resilience of Economic Ecosystems" (CoyPu)[15] funded by the Federal Ministry for Economic Affairs and Climate Protection of Germany. The project addresses the complex (economic) challenges in crisis situations. SRIW's research is related to the legal challenges, including those resulting from GDPR. Researchers of the publicly funded project – CoyPu – contributed to this consultation, foremost regarding questions 14.a and 14.b, i.e., Section 15.

Supported by:
Federal Ministry for Economic Affairs and Climate Action
on the basis of a decision by the German Bundestag

16

[13] https://scope-europe.eu
[14] https://www.dataprotectionauthority.be/publications/decision-n05-2021-of-20-may-2021.pdf; https://edpb.europa.eu/system/files/2023-03/document_4_data_pro_code_nl_sa.pdf
[15] https://coypu.org/
[16] Integrated due to the involvement of CoyPu in drafting this consultation and related legal requirements of publicly funded research projects; This integration shall, by no means, indicate that the consultation or any other statement therein reflects the official position of the Federal Ministry of Economic Affairs and Climate Protection.

4. Question 2.a General Comments – What is your overall assessment (benefits/challenges, increase in trust and awareness, etc.) of the application of the GDPR since May 2018? Are there priority issues to be addressed?

The General Data Protection Regulation succeeds the Data Protection Directive, the first European approach to harmonize different national approaches on the protection of personal data. Against this background, the GDPR was not developed against a blank page, but against decades of (national) experience. Experience which penetrated any dimensions, i.e., legislature, jurisprudence, authoritative interpretation and (enforcement) actions, consulting and – last but not least – implementation by business and data subjects.

Unfortunately, GDPR's key element – harmonization – across Europe has not yet been reached. One overarching intent of developing GDPR was an increased level of harmonization across Europe. The protection of personal data has been identified as a significant value, in its societal dimension and economic dimension. Consequently, a level playing field was supposed to be established, overcoming constraints and distortions resulting from different interpretations and implementation of the Directive. Acknowledging GDPR is still maturing, final text was published in 2016 already, marking almost eight years in 2024. Compared to decades of experience under previous legal regimes, eight years appear short. In these eight years, significant, if not almost tectonic, shifts have occurred, especially when compared to recent societal and technological developments.

Upcoming implementation and review of GDPR should focus on amplifying one of GDPR's main intents, i.e., harmonization and establishing a level playing field across Europe. Suitable approaches will be presented throughout the entire set of responses.

Despite a lack of harmonization, GDPR must be concluded impactful. Companies of all size and sector were pinpointed to the necessity of consistent and effective processes to adequately protect personal data. In this context GDPR built bridges between privacy experts and IT security experts. Processes must reflect the entire processing cycle, which starts by implementing data minimization as a core principle and ends by effective deletion. Personal data management has been identified a positive element in the value chain since awareness has risen about the various scenarios in which personal data is involved. Spread processing of personal data in internal and external systems, and required resources in responding to data subject rights requests start balance return on invests the better data is managed by design. A positive side-effect: Effectively managed personal data have a potential to reveal hidden values that can lift serious business advantages.

While harmonization and a one-size fits all approach supports foreseeability, GDPR must remain open and accessible for differentiation as needed. Harmonization and level-playing field is needed from a general enforcement, authoritative and territorial perspective consequently facilitating the European (Digital) Single Market. However, differentiation is required in sector-specific or processing-specific dimensions. Global statements that processing of (determined) personal data is deemed – per se – incompatible with GDPR, specific legal grounds shall be given precedence amongst other, neglecting the engraved balancing of interests, freedoms and fundamental rights of any involved parties tends to result in slowing down the positive effects of GDPR. In this vein, it shall also be highlighted that interpreting the term "reasonable" shall include economic possibilities of processing entities, to the extent a reflection is compatible with the associated risks for data subjects.

The protection of personal data – doubtlessly – is important and a serious societal value. Requesting adequate (reasonable) means for protection of personal data by anyone with commercial respectively professional interest in processing such data proves a logical consequence. However, interpretation and enforcement, eventually implementation of GDPR should acknowledge distinct risk evaluations, considering elements such as economic powers, to what extent processing of personal data reflects core business activities or rather an enabling necessity for other activities (e.g., in case of craftsmen), and size / prominence of companies to the extent such the latter might influence the probability of being subject of targeted attacks.

GDPR provides for effective mechanisms establishing the required differentiation without undermining GDPR's principles and adequate protection of data subjects. Those mechanisms are, e.g., Codes of Conduct as governed by Art. 40. The benefits and incentives for Codes of Conduct shall be enhanced, structurally and effectively.

Besides more detailed description on pressing needs in this respect, GDPR should be clarifying in the following elements:

- If no conflicts with GDPR can be determined, authorities shall approve a Code of Conduct; the principle of majority votes in the EDPB shall be emphasized.
- Unless adherence to a Code of Conduct has been communicated abusively, it shall be clarified that adherence must be considered as a *positive* factor.
- Active involvement of code-owner in the approval-process shall be emphasized – even at the level of the EDPB – ensuring a close and efficient exchange of arguments and mutual understanding of the processing context, business realities, interpretation of GDPR and non-negotiable essentials of protecting data subjects.

5. Question 3.a Exercise of data subject rights – From the controllers and processors' perspective: please provide information on the compliance with the data subject rights listed below, including on possible challenges (e.g. manifestly unfounded or excessive requests, difficulty meeting deadlines, identification of data subjects, etc.).

Generally, a more concise approach in interpreting data subject rights will be appreciated. In this vein, emphasis on the balancing of interests of multiple parties will be appreciated. Interpretation of GDPR tends overly weighting individual data subject's interests instead of balancing data subjects' interests from a general perspective, acknowledging that several data subjects may be concerned and, last but not least, that also processing entities have their legitimate (business) interests and legal obligations.

GDPR sensibly follows a generic and agnostic approach, while engraving the need to individually assess the requirements of a suitable implementation. Terminology allowing for context-specific detailing should be honoured. The process of detailing the understanding should involve relevant stakeholders as early as possible. Against this background, co-regulative measures, such as codes of conduct, are deemed a suitable leveraging factor. Where suitable, codes of conduct should be amplified in their potential.

5.1. Question 3.a.1 Exercise of data subject rights – Information obligations, including the type and level of detail of the information to be provided (Articles 12 to 14)

Upfront, transparent information of data subjects is one key element of effective data protection. Following explanation shall not question the added value of such information per se. However, two elements must be considered in this context:

- too much information or overly complex description may rather confuse than enabling data subject to act in an informed manner;
- consistency in content, including language, and structure ease comprehensibility.

5.1.1. Codes of Conduct as means to particularize interpretation and practical implementation

Interpretation of required information remain ambiguous, still. E.g., based on first-hand experience in the context of the Geodatenkodex (Code of Conduct for streetside imagery)[17], and the EU Cloud CoC[18] ambiguities have practical impact on the effectiveness of data protection and economic impact of GDPR implementation.

[17] https://geodatenkodex.de
[18] https://eucoc.cloud

A suitable solution may be Codes of Conduct, for which to approaches can be thought of

- a general Code of Conduct addressing data subject rights and related obligations on transparent information;
- sector-specific codes of conduct that inherently address transparency related elements that require clarification within the scope of such Code of Conduct.

Added value of a generic approach is deemed unlikely. A generic approach would have to address diverse requirements of several sectors whilst providing operational added value for implementation. GDPR lacks the operational detailing because GDPR sensibly acknowledges that different contexts may require different means of implementation. Therefore, reproducing a generic approach within a Code of Conduct will either result in an overly complex Code of Conduct with several conditional requirements, or stipulate rigorous undifferentiated requirements, resulting in probably unnecessary burdens for mSME.

Significant added value is foreseen in sector-specific codes of conduct, addressing transparency obligation within their scope. The distinct (processing) context of a Code of Conduct and potentially inherent balancing of interests allows for a tailor-made assessment on the required information, as well as means when and how such information must be provided. Such tailor-made approaches will – however – require an open mind set of all stakeholders involved, refraining from position which make any information listed in GDPR as mandatory, even if individual elements are explicitly referred to as conditional or equivalently suitable alternatives.

5.1.2. Elements of ambiguity which should either be clarified within GDPR or amplified as suitable and legitimate approaches if enclosed within Codes of Conduct

5.1.2.1. Conditional elements in Articles 13 and 14, respectively equivalent effective alternatives

Art. 13 and 14 mention elements either explicitly as conditional or as alternatives. E.g., Art 13.2 and Art. 14.2 GDPR refer to elements which shall only be subject to transparency notices, if “necessary to ensure fair and transparent processing”.

At least subject to a balancing and safeguards by codes of conduct conditional elements must be treated indeed conditional and – eventually – the possibility must remain that such conditional elements may be skipped in individual transparency information. This will help focussing the information on relevant and impactful aspects. Such focus underpins the seriousness and added value of well-drafted, transparency information. It is appreciated that a so-called layered approach has become accepted good practise. Such an approach helps preventing a fatigue by overwhelming amounts of information. Several elements of Art. 13.2 and 14.2 appear redundant or rather a matter of general

societal education, e.g., (b) to (d). It is hard to imagine cases where – if such information is provided additionally – data subjects will experience an increased protection of their freedoms and fundamental rights.

Emphasis must be given to the equivalence of alternatives, e.g., in Art. 13.1 (e) or Art. 14.1 (d). Processing activities and processing chains have become flexible, fast-evolving, and consequently increasingly complex. Considering categories of information sufficient will also support consistency across GDPR. The record of processing requires in any case only categories of some information, Art. 30.1 lit c and lit d. Thus, information within external transparency information shall not exceed the required information for internal documentation.

Acknowledging that rare individual scenarios may exist, where detailed information is essential, default scenarios will allow for a categorization of information. At a minimum, where additional safeguards by codes of conduct are provided, a general information should remain a possibility.

E.g., the individual, one may question the added value of the explicit listing of individual processors, compared to generic statements: Personal data will be processed with support of external storage and software providers. Which must be considered the expected default by data subjects in any case. Professionalised external services eventually increase the protection of data, and involvement of such professional services should not be made unnecessarily cumbersome. Especially, if the selection and management of such services is well-done, risks for data subjects reasonably and adequately prevented or limited. The same applies to categories of personal data: The explicit exhaustive list of data fields, such as “Street”, “Number”, “City”, “ZIP/Post Code”, “Country”, brings minimum added value compared to a reference to “Address Data”.

5.1.2.2. Applicability of Article 13 vs Article 14

In practice, the applicability of Art. 13 and Art. 14 remains ambiguous, especially considering the exempt in Art. 14.5.

It should be clarified that the phrasing of the English version of the GDPR reflects the intent perfectly; i.e., „where [...] collected **from** the data subject“ and „where [...] have not been obtained **from** the data subject“. Emphasis is on the origin, with a notion of (active) involvement of the data subject. A non-suitable differentiation are the *whereabouts* of the data subject. Especially the German translation “Erhebung bei (Engl: “collection at/close to” as well as “during/while/at the process of”)” results in confusing interpretations. Codes of conduct that refer to the original English intent shall not suffer from ambiguities of different language versions.

Art. 14 clearly intends limiting the operational burdens where relevant data (must/) will be collected without (active) involvement of data subject. This cumulates in Art. 14.5 GDPR. Clarification is necessary, that the provided examples in Art. 14.5 (b) are non-exhaustive and with no deliberate precedence. Especially in cases, where interests of data subjects are appropriately balanced and safeguard by means of a Code of Conduct, a rather extensive application of Art. 14.5 (b) should remain possible. This may be cases in which personal data of data subjects is collected *en passant* but were never in the focus of such collection; or where data does not identify data subjects but only includes information by which data subjects could be identified if the information would be analysed accordingly or upgraded with additional information.

5.1.2.3. Upholding GDPR core principles, such as data minimization

Generally, and in the light of 5.1.2.2, GDPR's core principles must be kept effective, also in the context of data subject rights and transparency obligation. The most effective protection is, where data is not processed at all. GDPR already engraves this principle, e.g., in Art. 11.1 GDPR.

Data subject rights may also be performed abusively, which is acknowledged by GDPR, e.g., in Art. 12.6 or Art. 12.5 GDPR. Art. 12.6 clarifies that doubts in respect of a data subject's identity shall be good reason for rejection of a data subject right request. Art. 12.5 clarifies that rejection may happen in cases where a request is manifestly unfounded or excessive.

Unfortunately, only Art. 12.6 refers back to Art. 11 GDPR explicitly but does not include Art. 12 to 14. This results in ambiguities if additional personal data must be processed only to allow for transparency pursuant Art. 12 to 14. Because Art. 11 determines a general principle, Art. 11 shall apply in any case, even without explicit references. At a minimum in cases where additional safeguards are provided by means of codes of conduct, it shall be clarified that processing of non-relevant information and unnecessary identification of data subjects shall not be required if the intent of Art. 12 to 14 will be reached by other means – e.g., generally publicly available information or by allowing for individual information requests.

5.2. Question 3.a.2 Exercise of data subject rights – Right to object (Article 21)

First, it should be emphasised that Art. 6.1 (f) GDPR provides a strong protection for data subjects Legal grounds enumerated in Art. 6 (1) GDPR are equivalently valid. Overly weighting Art. 6.1 (a) GDPR, i.e., consent, must be prevented. One might even argue that through the balancing of interest in Art. 6.1 (f) GDPR, especially in cases where it will be supported by means of codes of conduct, creates very strong and fair results for data subjects.

Art. 21 GDPR complements Art. 6.1 (f) GDPR. Art. 6.1 (f) GDPR which is an abstract-generic provision balancing interests overarchingly. Art. 21 GDPR allows for corrective measures (objection) for the data subject in individual cases. When evaluating Art. 21.1 GDPR, one should not disregard this interplay of two dimensions within GDPR.

These two dimensions in Art. 6.1 (f) and Art. 21.1 GDPR find their expression by mentioning a "particular situation" in Art. 21.1 GDPR. Although a processing of personal data can be permitted by Art. 6.1 (f) GDPR it can be inadmissible in individual cases.

The data subject has the right to object on grounds relating to his or her "particular situation", but these grounds are not defined in the provision. Although the recitals directly address the legitimate interest of the processor in accordance with Art. 6.1 (f) GDPR, there is no definition of the "particular situation", which leaves legal uncertainty.

We would invite the European Commission to re-iterate the addition "particular situation" in Art. 21.1 GDPR. It shall also be stressed that, even in cases where a particular situation can be determined, Art. 21.1 GDPR still foresees another layer of evaluation. Such evaluation then may determine that processing may continue.

In addition, in the specific case of Art. 21.6 GDPR, it would be appreciated if the research mentioned here were given a greater impetus when balancing the interests of the data subject and the processing entity. Highlight shall be given that serious progress – also in public interest – results from general research and development efforts by industry.

A Code of Conduct could provide clarity, for example by creating preliminary categories as to when a "particular situation" exists and therefore Art. 21 GDPR applies. Codes of Conduct may also add clarity on the second layer of evaluation determining in which cases the interest in continuing the processing prevails. In our view, a purposeful application of Art. 6.1 (f) GDPR in combination with a Code of Conduct that specifies the categories in Art. 21.1 GDPR offers more effective protection than consent.

Codes of Conduct can increase effectiveness and efficiency of GDPR enforcement and the protection of data subjects. Beyond that, a Code of Conduct offers the opportunity for the industry to implement GDPR closest to operational practice, eventually satisfying both the authorities, the industry and data subjects.

For more information on general challenges that come with developing a Code of Conduct, please, refer to section 12.

6. Question 4.a to c Application of the GDPR to SMEs – What are the lessons learned from the application of the GDPR to SMEs? Have the guidance and tools provided by data protection authorities and the EDPB in recent years assisted SMEs in their application of the GDPR (see also the EDPB data protection guide for small business)? What additional tools would be helpful to assist SMEs in their application of the GDPR?

As outlined in section 4, too, GDPR is considered providing positive impact. It is also acknowledged and appreciated that GDPR were drafted in an abstract manner. At the same time the abstract and one-size fits all approach – at first sight – creates burdens specifically for mSME. GDPR incorporates elements which allow for differentiation by company size. Clarification and emphasis that a differentiation has been intended by the European Commission will be appreciated. Approaches that appear suitable for large companies shall not automatically create reflexes requiring the same approaches from any other company size.

Additionally, it shall be stressed out that GDPR's several occasions of balancing interests and acknowledgment of context specific needs can be perfectly addressed by codes of conduct. In this vein, clarification is appreciated highlighting that added value and good solutions suffice, and must not be halted by seeking perfection.

7. Question 5.a to c Experience with Data Protection Authorities (DPAs) – What is your experience in obtaining advice from DPAs? How are the guidelines adopted so far by the EDPB supporting the practical application of the GDPR? Are you aware of guidelines issued by national DPAs supplementing or conflicting with EDPB guidelines? (please explain)

7.1. Establishing Guidelines and more effective stakeholder involvement

We came across guidelines issued from various bodies. It shall be highlighted that the existence of any such guidelines is principally appreciated. GDPR requires particularization and practical guidance. The good intention of drafting guidelines might even be facilitated if different stakeholders will be involved even more often and more effectively. The latter relates specifically to remain open in stakeholder dialogues, saying, that feedback should result – as needed – also in more fundamental adjustments rather than minor or even mere editorial changes.

7.2. Considering Codes of Conduct as effective alternative to guidelines

Amplification should be given to the potential of Codes of Conduct. Codes of Conduct inherently involve different stakeholders, experts and strive for a fair balance of interests. The approval process ensures that Codes of Conduct will not undermine GDPR's requirements. Especially in cases of

transnational Codes of Conduct, such approach will also support on core-intent of the GDPR, i.e., cross-European harmonization.

Because – in most cases – industry drives such initiatives, Codes of Conduct may also ease cross-regulatory alignment. Code of Conduct initiatives are perfect to facilitate such process, as sector-specific experts of different backgrounds – e.g., legal, operations, business, engineering – will be involved. As needed such initiatives may also reach out to different authorities in parallel to ensure a speedy development. Certainly, data protection supervisory authorities shall be invited and in best cases reflect cross-regulatory requirements already. However, it must be acknowledged that different authorities and public bodies were deliberately created to build specific expertise. Formal administrative assistance across authorities responsible for different regulations usually is slow and complex, as well as binding significant public resources. In regards of cross-regulatory alignment, please, also see Section 15.

It shall also be highlighted that in the process of balancing interests, GDPR must acknowledge several fundamental rights, freedoms and interests of data subjects, including those interests and rights deriving from various legal requirements and societal norms outside GDPR. In other words, there may be requirement stipulated by other regulatory frameworks or general societal expectation, that industry shall reach distinct goals and / or contribute to and facilitate in the protection or enhanced accessibility and usability of data subjects and their activities. Preventing a protective / supportive regime A by enforcing another protective / supportive regime B will become hardly arguable and defendable towards society. This principle shall apply generally, i.e., to the development of codes of conduct, the establishment of Guidelines and everyday application of GDPR.

7.3. Experience with Guidelines in the sphere of Article 40 and Article 41

7.3.1. General Findings

7.3.1.1. Material elements

In accompanying the development of Codes of Conduct pursuant to Art. 40 GDPR, guidelines ultimately slow down the process of developing Codes of Conduct unnecessarily.

Efforts should be increased to position data protection as compatible with innovation, data protection as providing flexible tools and means to realize its goal, and lastly being able to adapt in due time where necessary subsequent legal or operational developments. Approval processes and alignment processes of Codes of Conduct between industry and authorities were reported to be halted because in the respective scope of Code of Conduct neither EDPB nor national authorities have not yet drafted their initial guidelines. In other words, the potential of Codes of Conduct to pro-actively support

particularization and determine sector-specific guidelines by themselves seems unused. Codes of Conduct appear limited to areas in which data protection authorities already provided their own guidelines and detailing of GDPR's interpretation. This eventually doubles the resources needed to effectuate GDPR and potentially prevents positive impacts of GDPR, i.e., the protection of data subject. Likewise, such multiplication of resources spent increases the wrongful impression of data protection as hindering for innovation.

7.3.1.2. Available Legal Actions

In practice, guidelines have proven to have significant impact. Since Codes of Conduct yet appear limited to areas where authorities have positioned them upfront and the strong operational impact of guidelines, legal actions to review guidelines must be improved.

Authorities consider them as binding as GDPR itself. Statements were reported in which authorities would give guidelines precedence even in cases where lower courts already decided in conflict with such guidelines; only higher court rulings were deemed as indicator to re-evaluate the application of existing guidelines.

7.3.2. Article 40

Guidelines in developing Codes of Conduct were published. Guidelines established procedural elements which can be understood as not primarily required by GDPR, and thus negatively affect the effectiveness of the process.

More importantly, it shall be highlighted that application of GDPR and subsequent Guidelines should be streamlined. It has been reported that – despite unambiguous statements in the respective guidelines – Codes of Conduct initiative feel stuck because data protection authorities remain undetermined which authority shall be deemed the leading, i.e., competent authority. Understanding GDPR as regulation, imposing harmonized standards across Europe, different authorities shall not conclude differently in first place. Additionally, it should be clarified if and to what extent authorities shall claim fees to the approval process.

Especially if transnational Codes of Conduct are concerned, the process shall be streamlined, clarifying that any authority shall be deemed competent which has been selected by code-owners. Alternatively, a distinct channel to submit transnational Codes of Conduct shall be established. Additionally, it shall suffice to submit documents in English; sometimes authorities request (un-)official translations. Besides the resources needed to simply translate documents, the maintenance of several language versions also increases the risk of linguistic inconsistencies.

For more details on the practical experience in regards of Art. 40 GDPR, see also Section 12.

7.3.3. Article 41

More intensively, unnecessary operational burdens were recognized by applying the criteria for accreditation of Monitoring Bodies of different member states. Material added value remains highly limited resulting from the divergences across the member states. Individualized formal requirements appear reasonable but could be enhanced to facilitate transnational Codes of Conduct.

A harmonisation of requirements is indisputably needed regarding the accreditation criteria for Monitoring Bodies. It is appreciated that the EDPB aligned on a referential publication and defined a process, that any national criteria must remain compatible with such referential criteria. However, this approach still allows for accreditation requirements that a Monitoring Body must meet to become accredited applied by the national data protection supervisory authority which differ at a national level. Because the criteria are eventually developed by each member state. In case of member states organised and shaped by federalism – such as Germany – the application and interpretation of such requirements may differ between the federal states.

Also to facilitate the accessibility for mSME, the operational burdens for Monitoring Bodies should be limited to what is effectively necessary. In other words, any material requirements shall be determined once across Europe. Deviations should only refer to Member State's administrative law. However, to facilitate transnational Codes of Conduct, overarching clarifications are highly recommended. E.g., in cases of transnational Codes of Conduct, it shall suffice to submit documents in English; sometimes authorities request (un-)official translations. Besides the resources needed to simply translate documents, the maintenance of several language versions also increases the risk of linguistic inconsistencies.

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

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

For more details on the practical experience in regards of Art. 41 GDPR, see also Section 12

8. Question 6.b Experience with accountability and risk-based approach – What is your experience with the scalability of obligations (e.g., appropriate technical and organisational measures to ensure the security of processing, Data Protection Impact Assessment for high risks, etc.)?

The accountability and especially the risk-based approach reflects one dimension of balancing interests. One of the best means to balance interests is involving different stakeholders in the process of determining adequate measures. It is therefore recommended that the opportunities of Codes of Conduct will be highlighted in future. This requires a clarification that Codes of Conduct indeed are a tool fit for purpose in this sense. Additionally, it should be stressed out that Codes of Conduct shall respect the needs of mSME and therefore determining whether a Code of Conduct is compatible with GDPR must allow for effective, yet risk-adequate measures; in this context (resource) capabilities for multi-billion corporations may not be a perfect blueprint for mSME.

The risk-based approach is a key element in allowing for adjusting measures reasonably considering elements such as company sizes and economic realities. The latter supports GDPR's intent to remain accessibly for mSME and limiting operational burdens to the extent necessary, whilst upholding a robust protection of personal data.

9. Question 7.a and b Controller / processor relationship (SCC) – Have you made use of Standard Contractual Clauses adopted by the Commission on controller/processor relationship? If yes, please provide feedback on the Standard Contractual Clauses?

9.1. Streamlining Terminology and Scope of SCC vs SDPC

A more streamlined language and separation of intents will be appreciated. Standard Contractual Clauses refer to Art. 28.7 GDPR; Standard Data Protection Clauses refer to Art. 46.2 (e) GDPR.

- Standard Contractual Clauses, per definition, address the specific needs of a processor relationship. Third country transfers are not prima facie reflected by Standard Contractual Clauses.
- Standard Data Protection Clauses address the specific needs of third country transfers, establishing appropriate safeguards to the extent needed in the individual transfer.

The currently effective version of the of the European Commission's Standard Contractual Clauses – as they are deemed establishing an appropriate safeguard pursuant Art. 46 GDPR – is generally appreciated. Such appreciation specifically results from the fact that the draft addresses the different relationship between the parties and therefore cover highly relevant transfer scenarios in practise, which were not covered under the Directive version of the SCC.

However, it must be highlighted that the term SCC is confusing in practice. It must also be highlighted that the current effective version of the SCC combines general requirements under Art. 28 GDPR and additional elements only necessary to define appropriate safeguards pursuant Art. 46 GDPR. This results in operational ambiguities or contractual complexities in cases where the parties like to govern Art. 28 GDPR related elements differently but need to sign the SCC in an unmodified manner to build upon the provided legal effect.

9.2. Remaining uncertainty due to annexes of SCC

The current version of SCC addresses most relevant transfer scenarios for the first time. This added value cannot be overestimated. Likewise, the SCC remain flexible for several sectors and processing activities, as well as for different processing contexts, such as the affected third countries. In this respect, flexibility upholds a relevant degree of legal uncertainty. The annexes determine the key elements, such as the categories of personal data, the processing purposes, and the required technical and organisational measures. The burden of assessing the adequacy of such information remains with the parties signing the individual SCC. This includes a thorough Transfer Impact Assessment.

SCC may prove the most flexible mechanisms, which will always require abovementioned flexibility and remaining legal uncertainty. For those who in need of more detailed and specified mechanisms, Art. 46 GDPR provides suitable tools, such as Codes of Conduct. A lighthouse initiative to be mentioned is certainly the Third Country Initiative of the EU Cloud Code of Conduct.[19]

9.3. Empasis on multitude of suitable safeguards

Emphasis shall be given to the multitude of appropriate safeguards pursuant Art. 46 GDPR and the equivalence of their legal effects. It should also be highlighted and clarified that each of the mechanisms pursuant Art. 46 GDPR may have their unique approach. Unnecessarily replicating one approach in several mechanisms with different headlines will conflict the original intent of redundancy and alternatives. Recent years have proven that controllers and processors must not rely on only one safeguarding mechanism. Adequacy decisions or other safeguards can be declared void subsequent

[19] https://eucoc.cloud/3rdcountryinitiative

court decisions. The operational impact can be severe if controllers and processors have not established alternatives. If alternatives are designed too similar to each other, this will create a risk of overspilling effects, saying, that instead of one mechanism all mechanisms will be voided. Authorities and the European Commission, therefore, shall recommend and facilitate operational variety. Variety may relate to the parties involved (processors or controllers), alternatives in scopes, e.g., focussing on elements of contractual, technical or organisational nature.

10. Question 8.b International transfers – For controllers and processors: Are you using other tools for international data transfers (e.g., Binding Corporate Rules, tailor-made contractual clauses, derogations)? If yes, what is your experience with using these tools? Are there any countries, regional organisations, etc. with which the Commission should work in your view to facilitate safe data flows?

10.1. General Remarks

We would like to draw the European Commission's attention to Codes of Conduct pursuant to Art. 40 GDPR and Certifications pursuant to Art. 42 GDPR as safeguards for international data transfers. Requirements in establishing such alternatives – materially and procedurally – shall be re-evaluated to facilitate their operationalisation. E.g., the involvement of the European Commission next to the EDPB for Codes of Conduct may be redesigned if not even concluded unnecessary. In the same vein, GDPR's requirements in the context of determining safeguards for Third Country Transfers for adequacy or equivalence must not be understood as identity; different law regimes will never be identical; but their effects may equally and adequately protective. Initiatives such as the European Councils Convention 108[20] shall be highlighted.

Third Country Transfers are often safeguarded by redundant mechanisms, such as adequacy decisions pursuant to Art. 45 GDPR, standard contractual clauses pursuant to Art. 46.2 (c) GDPR and binding corporate rules pursuant to Art. 47 GDPR. The scope of application of those three current main solutions may appear limited or requiring high individual expenses. Furthermore – and most important – the jurisdiction in recent years has shown that adequacy decisions and standard contractual clauses bear the risk of only serving as short-term safeguards, resulting in a lack of legal certainty for processors and controllers.

[20] https://www.coe.int/en/web/data-protection/convention108-and-protocol

In practice, more tailormade solutions as (additional) alternatives are therefore required for sectors that rely on third country transfers to continue their business activities in Europe. Such solutions could be Codes of Conduct and Certifications as suggested by Art. 46.2 (e) and (f) GDPR.

10.2. Details on different requirements for Codes of Conduct and Certifications

Unquestionably the requirements to be met by any solution should be generally comparable, as the object of protection remains identical. Nonetheless, particularities of each mechanism should be endorsed allowing for effective but also efficient solutions. Currently, non-necessary differences might exist, as GDPR – and subsequent guidelines[21] – foresee differences between Codes of Conduct and Certifications. E.g. Codes of Conduct require a general validity involving the European Commission (see Art. 40.3 GDPR, Art. 40.5 to 40.9 GDPR), whereas Certifications do not require such additional step (see Art. 42.3 and 42.5 GDPR).

Differences in the approach could be argued in the different approaches of Codes of Conduct and Certifications. Certifications were understood as the verification of a distinct implementation of a processing activity. In other words, changes in the implementation, be it technical or organisational, will require a re-certification. Additionally, certifications focus on a processing (activity); entire products or companies therefore were considered unsuited targets of evaluation, unless several certifications will be combined and maintained. In contrast, Codes of Conduct allow for more general approaches, including management programmes resulting into a foreseeability of implemented technical and organisation measures fit for purpose and conformant with the requirements and principles determined by the respective Code of Conduct.

Codes of Conduct may upgrade their scopes to a fine granularity almost equivalent to a certification, the abovementioned interpretation would not allow certifications to refrain from their required granularity and define rather high-level objectives.

Recent practical examples passing the authorities approval question the original intent of GDPR distinguishing between codes of Conduct and Certifications. Either, the differentiator between both mechanisms must be clarified. Alternatively, the playing field must be levelled by harmonising the requirements for Codes of Conduct and Certifications.

[21] https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf

11. Question 12.a Codes of conduct, including as a tool for international transfers – Do you consider that adequate use is made of codes of conduct?

Generally, Codes of Conduct are useful and effective to harmonize the needs of a specific sector with the rights of data subjects. Codes of Conduct provide companies with operational understanding in complying with the comprehensive requirements of the GDPR and provide and additional pilar in enforcing GDPR and monitoring industry's implementation, next to the remaining powers of supervisory authorities.

We believe that the potential of Codes of Conduct has not yet been sufficiently utilised. The number of Codes of Conduct which were approved is comparatively low. Experience and reports indicate that industry is willing to establish more Codes of Conduct but faces complex processes, ambiguous or even overly rigorous expectations by supervisory authorities. Codes of Conduct, as continuously evolving as frameworks, and involved stakeholders should seek for best effort solutions, and continuous improvement, emphasizing and amplifying a benefit of a co-regulatory mechanism: flexibility and speed. Processes must also be streamlined and optimized in respect of transnational Codes of Conduct. Focus on national Codes of Conduct jeopardizes the potential of Codes of Conduct as effective tool for cross-European harmonization of the implementation and interpretation of GDPR.

Where Third Country transfers are concerned, further clarifications are sought with respect to the procedural aspects relating to the general validity mechanism for Codes of Conduct acting as a transfer safeguard under Chapter V GDPR. Codes of Conduct acting as a Chapter V safeguard require, additionally to (1) the positive opinion of the EDPB and (2) the approval by the competent data protection supervisory authority, to be granted (3) general validity by the Commission by way of implementing act.[22]

We observe that the general validity mechanism as an implementing act as well as its related legal effects against the specific context of Codes of Conduct remains generally unclear. Clarification is sought on what is the procedure for a Code of Conduct to be granted general validity, besides the notification of the opinion of the EDPB to the European Commission, as well as on the related timeframes. In this respect, we consider that general validity shall be granted in a timely manner to not unduly delay the process and to allow for the rapid adoption of these tools by the market. To this end, we recommend that the process between the EBPB and the European Commission be further

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

streamlined. E.g., the substantive assessment of the code by both institutions should, to some extent, be carried out simultaneously and thus at an earlier stage than described in Annex 1 of the related EDPB guidelines. Notwithstanding and in fully appreciation of the powers of the European Commission, procedures by the European Commission should not – by any means – foresee any timelines that exceed the suitable blueprint provided by Art. 40 GDPR related to the processes to be performed by the EDPB, i.e., a default period of eight weeks plus an optional extension in case of need, e.g., due to complexity of the case. Against this background, also refer to Section 10; re-evaluating the interplay of Articles 40 to 42 may conclude that the general validity and related involvement of the European Commission is not necessary.

The challenges we see are briefly explained in more detail in Section 12.

12. Question 12.b Codes of conduct, including as a tool for international transfers – Have you encountered challenges in the development of codes of conduct, or in their approval process?

12.1. Development

Based on our experience with the development of national and transnational Codes of Conduct we would highly welcome further clarification on how the competent data protection authority is determined for the approval of such codes. Especially if transnational Codes of Conduct are concerned, the process shall be streamlined, clarifying that any authority shall be deemed competent which has been selected by code-owners. Alternatively, a distinct channel to submit transnational Codes of Conduct shall be established (see Section 7.3.2). Furthermore, also in this context, we would like to draw the European Commission's attention to the need for alignment of bodies issuing guidelines on Codes of Conduct (see Section 7.3) as a multitude of and divergences between documents creates unclarity with regard to expectations.

When drafting a Code of Conduct in accordance with Art. 40 GDPR, also the legal requirements outside the GDPR must be considered. EDPB's guidelines require added value by particularizing GDPR, which eventually requires the exchange between different stakeholders. Preventing different interpretations one legitimate exchange and alignment as well subsequent action from competition and antitrust authorities could increase the successful drafting process of a Code of Conduct. We would like to invite the European Commission to clarify that exchange and alignment during the drafting of Codes of Conduct is privileged conditionally. We want to highlight that not any exchange of information is per se illegal, especially if it remains on a high level. We see the aspect that Codes of Conduct may require granular provisions to meet the requirements of the Supervisory authorities and the guidelines of the EDPB. Expected, granular provisions within a Code of Conduct may - de facto - result in concerns by

competition and antitrust authorities, presuming that such provisions were developed subsequent undue exchange of information between relevant stakeholders. Certainly, requirements from a competition and antitrust perspective can be addressed, e.g., by means of good governance, or by means of ensuring that material requirements remain reasonable, in accordance with the law and implementable without undue advantages or disadvantages of individual stakeholders.

An improvement of the conditions for the drafting of Codes of Conduct plus an improvement of the potentially conflicting expectations in the different legal frameworks will prevent additional burdens on those stakeholders willing to support GDPR's implementation and enforcement for the benefit of data subjects.

As a specific aspect of third country transfers, we would like to point out that from our point of view the Guidelines for Codes of Conduct are mainly written from the controller perspective. However, the processor perspective also plays a significant role, especially for third country transfers.

Furthermore, the guidelines determine Codes of Conduct as Third Country Transfer safeguard as contractual element. Codes of Conduct are an independent tool and should be able to determine their best approaches. Extending the approach to other elements than contractual provision may even result in an improved level of protection compared to other mechanisms. We would like to encourage the European Commission to emphasise that each appropriate safeguard pursuant Art. 46 GDPR may have its unique approach. For details, also refer to Section 9.3.

12.2. Approval

As organizations involved in the approval process of several Codes of Conduct, we have encountered varying interpretations by data protection supervisory authorities when it comes to factors that determine their competence. As a result, approval processes for Codes of Conduct have been delayed, and in some cases suspended, because data protection authorities could not mutually resolve their competence. As a result of these procedural obstacles, the complementary enforcement potential that Codes of Conduct offer has not been realised. We highly appreciate the guidelines developed and published by the data protection supervisory authorities, and generally do not request any clarifications that go beyond such guidelines. Nonetheless, a closer or rather harmonized application, though, would benefit the development of Codes of Conduct, significantly. Especially in cases of transnational Codes of Conduct, that will apply to any of the member states, the competency should not be considered an obstacle. Clarifying that any authority shall be deemed competent which has been selected by code-owners. alternatively, a distinct channel to submit transnational Codes of Conduct, is deemed an appropriate solution (see Section 7.3.2). A harmonized interpretation of GDPR is sufficiently safeguarded by the EDPB's mandatory involvement.

Additionally, in practice, initiatives apparently face challenges related to a) the simple formatting and structuring a Code of Conduct and b) corporate governance related matters. Generally, it should be the free choice of Code-Owners to determine the best structure and format of a Code of Conduct, including decisions whether information will be published in one or several documents, and whether information will be published in layered, constantly detail adding approach by utilizing annexes. In the same vein, the corporate governance of Code-Owners, i.e., how documents are maintained internally, adds no added value from a GDPR's perspective. Therefore, such governance related questions shall not be part of the approval processes.

12.3. Maintaining a Code of Conduct (Updating, Modifying, Adapting)

In principle, we believe that transnational Codes of Conduct offer the most added value in the long term due to their additional harmonisation effects. Changes to a Code of Conduct, whether for clarification or editorial purposes, are necessary and must not result in disproportionate procedural requirements.

In cases of transnational Codes of Conduct clarification is necessary that involving the EDPB where only minor changes shall apply, is not necessary. Involving the EDPB in accordance with Art. 40 (7) GDPR serves to harmonise the interpretation and application of GDPR across Europe. It shall prevent different interpretations of the GDPR by various supervisory authorities, potentially resulting in a race to the bottom. We generally welcome such a safeguarding approach.

Upraising interpretations requiring EDPB's involvement for any – even the slightest – update of a Code of Conduct appear excessive. The non-necessity of EDPB's involvement results already from the current legal provisions. Currently, the EDPB merely provides a non-binding opinion. The opinion follows the procedure of the consistency mechanism, which allows for majority votes. The opinion by the EDPB, eventually, is not legally binding to the competent supervisory authority. It is legally feasible for the competent supervisory authority to deviate from the opinion of the EDPB, in any direction. The aforementioned underpins the main intent of the EDPB's involvement: i.e., exchange of arguments and subsequently harmonizing GDPR's interpretation in a common and broadly adaptable fashion. Individual, deviating positions – either by means of extreme rigor or extreme laissez fair – shall not impact the added value of operational Codes of Conduct as they may act as significant multiplicators.

- The following scenarios must be distinguished: Editorial changes, without impact of the original material provision of a Code of Conduct
- Operational and governance related updates
- Material updates to a Code of Conduct

Mere editorial, maybe even simple orthographic, do not indicate risks for a harmonized interpretation of GDPR. Added value in involving every supervisory authority in such changes appears hardly recognizable, if not even inexistent.

Regarding operational and governance related updates reference shall be made to Section 12.2. Because corporate governance shall not be subject to the approval decision, changes must not involve the EDPB. This shall not prevent Code-Owners from notifying the Competent Authority of any updated documents ensuring that versions of a Code of Conduct, as published by an initiative and authorities, remain in synch. Operational questions, as they do not affect material matters, should be treated similarly. In rare cases, where operations may indirectly affect material provisions, please, refer to the statement below in this respect.

Material changes undoubtedly require an authority's involvement and approval decision to take legal effect. The question remains, to what extent the EDPB shall be involved. If the material adaptations are minor or within the margin of discussion that took place during the EDPB's opinion in the past, another involvement appears not necessary. If the competent authority concludes that the adaptations would not result in any diverging opinion of the EDPB, procedures should remain efficient, and the competent authority should conclude autonomously. The same applies if the material adaptations reflect subsequent guidelines of the EDPB or recent court decisions, saying, areas in which there is no risk of a non-harmonized interpretation. On the contrary, in cases, where adaptations are significant or potentially conflicting with previous opinions of the EDPB or not covered by the arguments exchanged in any previous EDPB's opinion, the EDPB shall be involved. Such a differentiated approach maintains the intent and essential involvement whilst allowing for pragmatic and efficient progression of Codes of Conduct.

Involving the EDPB unnecessarily results in a considerable delay. Such delay jeopardizes a key advantage of Codes of Conduct. Anxiety of unnecessarily complex procedures may also result in hesitance of code-owners to update their Codes of Conduct, even though minor clarifying updates may have significant impact on a Code of Conduct's adoption, which eventually increase the protection of data subjects.

We would appreciate if the European Commission could provide clarification to this regard.

12.4. The Monitoring

In addition to drafting the Code of Conduct, the monitoring of the Code under Art. 41 GDPR plays a significant role.

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

To facilitate the accreditation of Monitoring Bodies, it would be very appreciated if the European Commission will clarify on the need of a fully harmonized approach in respect of Art. 41 (2) GDPR. To facilitate transnational Codes of Conduct, overarching clarifications are highly recommended. E.g., in cases of transnational Codes of Conduct, it shall suffice to submit documents in English. See also Section 7.3.3.

12.5. Liability Cap

Monitoring Services result in a transparency for interested stakeholders. Depending on the individual design, the tasks and duties may vary. In any case, a Monitoring Body shall maintain a register of those entities or services, which adhere to a Code of Conduct. In this respect, the Monitoring Body makes a public statement which may be deemed a competitively relevant statement.

It is not yet clear to what extent the Monitoring Body will be liable for any such statement, if a third party – who has no contractual relation with such Monitoring Body – takes a decision based on the information mandatorily published by the Monitoring Body. In other fields of law, e.g., for auditors, the law provides a privileged liability cap. It is strongly recommended that the European Commission clarifies on the application of such liability for Monitoring Bodies. Such a clarification will also support the require independence of Monitoring Bodies and accessibility for mSME, as Monitoring Bodies were able to reasonably foresee their economic risks.

13. Question 12.c Codes of conduct, including as a tool for international transfers – What supports would assist you in developing codes of conduct?

We suggest that supervisory authorities should foster the development of Codes of Conduct – national, transnational and international – to streamline the protection of personal data across the regulations, acknowledging that there might be another perspective from other regulatory background that must be taken into consideration. In this respect it shall also be highlighted that it may reflect a significant added value of the application of GDPR and facilitate its implementation where a Code of Conduct maps GDPR requirements with other legal requirements of a particular sector. This may relate to retention periods, to contractually mandatory information but also the determination of legitimate interests and the subsequent balancing of interests. If a specific sector is required to process certain information or if applicable laws recommend a certain sector to process specific information, this shall be deemed a strong indication that such processing is legitimate under GDPR, and therefore in the context of a Code of Conduct, even if the sector-specific lacks an explicit reference to GDPR.

Moreover, we would like to invite the European Commission to foster the continuous review of the EDPB's and the supervisory authorities' guidelines and criteria, safeguarding that Monitoring Bodies are not directly or indirectly requested to act in conflict with other regulations to comply with supervisory authorities' interpretation of GDPR, remaining the burden of resolving such conflicts with the Monitoring Body.

Please refer also to Sections 11 and 12.

14. Question 13.a and b Certification, including as a tool for international transfers – Do you consider that adequate use is made of certifications? Have you encountered challenges in the development of certification criteria, or in their approval process?

Regarding tools to prove GDPR compliance we would like to refrain from limiting the scope on Certifications pursuant to Art. 42 GDPR and emphasize the existence of Codes of Conduct pursuant to Art. 40 GDPR especially highlighting their advantages.

Codes of Conduct, especially when those bear a transnational scope, i.e., covering processing activities across several member states, can effectively support addressing pressing challenges such as the uniform application of GDPR requirements and consistent enforcement.

As GDPR is written in a sector-agnostic manner in terms of processing activities, GDPR requires particularization. It is expected that such particularization of general legal terms, such as "appropriate" to name likely the most common example, will be addressed by guidelines of the EDPB, court proceedings, industry good practices, academia, etc. Whilst data protection supervisory authorities have

progressed in reaching harmonization, there are still opportunities in regards of further improvements. This applies both to sectoral implementation but also specific processing activities of the same stakeholder. Against this background, we want to stress that transnational Codes of Conduct are, by definition, sector-specific and are translating general GDPR obligations into specific means of implementation. Consequently, Codes of Conduct perfectly match the current needs. This potential of harmonization inherent to the mechanisms, such as Codes of Conduct, specifically benefits code members which are micro, small and medium-sized businesses ("mSMEs"). Such mSMEs may not have the inhouse resources or scale to liaise with multiple data protection supervisory authorities across multiple member states. Additionally, as transnational Codes of Conduct have passed a substantial process of scrutiny before the data protection supervisory authorities, including the EDPB, it is ensured that Codes of Conduct will not conflict with GDPR's requirements and that Codes of Conduct provide an added value.

Next to the general oversight, the monitoring of Codes of Conduct adds another safeguard for conformity. The obligatory element of integrating complaint mechanism makes available to relevant stakeholders, such as data subjects, an additional leeway to report potential infringements. In case such reports prove justified, the Monitoring Bodies will adopt appropriate sanctions and remedies.

For the presented benefits of Codes of Conduct in favour of GDPR implementation and enforcement to unfold in practice, appropriate requirements and incentives are needed to promote the development of this compliance tool. Those requirements should be particularly harmonised with those for Certifications as Certifications and Codes of Conduct seem to materially assimilate. We would therefore like to point the European Commission to Section 10, specifically 10.2.

15. Question 14.a and 14.b GDPR and innovation / new technologies – What is the overall impact of the GDPR on the approach to innovation and to new technologies? Please provide your views on the interaction between the GDPR and new initiatives under the Data Strategy (e.g., Data Act, Data Governance Act, European Health Data Space etc.)

The European Commission has started drafting new legislation or completed related initiatives recently. Legislation determines its scope, and especially legislation post-GDPR clarifies that any such new legislation shall not supersede or precede GDPR. Potential challenges in the evolving landscape were subject to a research project partnered by SRIW, i.e., CoyPu. Therefore, the following statements were significantly supported by and drafted under the responsibility of such research project. Nonetheless, as suitable solutions relate to Codes of Conduct, SRIW has added relevant remarks, as needed.

This section delves into the interaction between the GDPR and new initiatives under the Data strategy, notably the Data Act and the Data Governance Act. In this context we will shed light on the potential incompatibilities and challenges among these laws or legislative proposals.

15.1. Data Act

Potential challenges may arise in achieving alignment between the Data Act with the GDPR, particularly with respect to the following aspects:

15.1.1. Article 4 of the Data Act

According to Art. 4 Data Act, data holders are required to provide users, upon request, with data generated by products, encompassing both non-personal and personal data. Given that a significant share of product-generated data might be personal, the challenge remains on determining the legal basis for granting users access under Art. 6 GDPR; where sensitive data might be affected, Art. 9 GDPR must be respected, too. It is important to note that the GDPR takes precedence over the Data Act (Art. 1 (5) Data Act, recital 7) and remains applicable.

While this poses no issue in most scenarios, the legitimacy of data access remains ambiguous in rare instances. The legislation is unclear on whether GDPR and Data Act applies to the personal data of family members, particularly if they are registered users of a smart home gadget. Data holders might disclose personal data of family members based on the household exemption in the GDPR (Art. 2.2 (c) GDPR), yet the Data Act fails to address this specific scenario. Additionally, the Data Act does not specify whether data holders can grant access to data when the users are legal entities. It is recommended to clarify the household exemption on such modern scenarios. Even under GDPR the boundaries of the household exemption became challenged. At a minimum, it should remain possible to clarify the application and legitimacy of providing access, suitable limiting provided information et al by means of Codes of Conduct.

The Data Act states that valid legal grounds pursuant to Art. 6 GDPR are required in this case (Art. 4.12 Data Act). In addition to consent, such legal grounds will primarily be the performance of the contract in accordance with Art. 6.1 (b) GDPR (recital 34 sentence 8 Data Act). In order to refer to legitimate interests, users must weigh their legitimate interests against the interests of the data subjects. Data Act does not specify any admissible case groups for this task of weighing interests, which depends heavily on the individual case, nor does it provide any other guidance. Codes of Conduct should be treated as a suitable mechanism to harmonize the application of both regulations, including specifying a suitable balancing of interests.

Therefore, it is crucial the Data Act will clarify the legal basis for allowing users to access data, as stated in Art. 4 Data Act, especially when it comes to personal data created by products. Moreover, the law should clearly state if data holders can give access to data when users are legal entities. In the meantime, where no changes to the Data Act will be possible, GDPR should include suitable clarifications, e.g., by extending Art. 40.2 GDPR, stating that Codes of Conduct may act as cross-regulatory harmonization.

15.1.2. Article 5 Data Act

According to Art. 5 Data Act, data holders must also grant third parties' access to data if requested by users or authorised third parties. This right complements the right to data portability under Art. 20 GDPR, which is expressively not superseded (Art. 1.5 sentence 3, recital 31 sentence 15 Data Act).

In contrast with the GDPR, Data Act provides for the sharing of data directly with third parties. Uncertainty remains on account of standards applicable to share such information legitimately. In the meantime, where no changes to the Data Act will be possible, GDPR should include suitable clarifications, e.g., by extending Art. 40.2 GDPR, stating that Codes of Conduct may act as cross-regulatory harmonization.

15.1.3. Article 6 (2) b Data Act

Regarding profiling, the Data Act imposes limitations on the use of profiling of natural persons unless it is necessary to provide the service.

The GDPR imposes strict conditions for the lawful use of profiling requiring clear legal bases such as explicit consent from the data subject, the necessity of processing for the performance of a contract, compliance with a legal obligation, protection of vital interests, the performance of a task carried out in the public interest or the exercise of official authority, or legitimate interests pursued by the data controller or a third party.

The Data Act introduces a constraint on profiling, specifying that it should only occur "unless necessary to provide the service requested by the user." This inclusion of the criterion of "necessity" raises concerns about its compatibility with the GDPR, which establishes specific and restricted legal bases for profiling. The term "necessity" in the Data Act is broad and may not precisely align with the GDPR's probably rather narrow conditions.

Hence, it is crucial for the Data Act to precisely define and align the criteria of "necessity" with the clearly defined and specific conditions outlined in the GDPR for lawful profiling. In the meantime, where no changes to the Data Act will be possible, GDPR should include suitable clarifications, e.g.,

by extending Art. 40.2 GDPR, stating that Codes of Conduct may act as cross-regulatory harmonization.

15.1.4. Article 3 Data Act

According to Art. 3 Data Act, users must be provided with certain information before concluding a purchase or rental agreement. This information includes, in particular, the type and scope of product-generated data, how users can access these data and for what purpose data holders will use the product-generated data (Art. 3.2 Data Act). Art. 3 Data Act apparently applies in addition to the obligations to provide information under Art. 13, 14 GDPR (recital 24 sentence 7 Data Act).

The lack of coordination between the two information catalogues could lead to consumers being even more overwhelmed by a large amount of information. Please, refer to Section 5.1.2, in particular 5.1.2.1. In the meantime, where no changes to the Data Act will be possible, GDPR should include suitable clarifications, e.g., by extending Art. 40.2 GDPR, stating that Codes of Conduct may act as cross-regulatory harmonization. Especially, as Codes of Conduct can define proper blueprints on how information required by both regulatory frameworks can be provided in a transparent, short but yet effective manner.

15.1.5. Article 14 and 15 Data Act

According to Art. 14 Data Act public bodies and institutions can access data on exceptional need. Such access also concerns personal data. Such exceptional need might exceed the case of a public emergency and establishes a legal basis for authority which, yet, could not obtain the data in any other way. This approach appears extremely broad and threatening towards core legal principals protecting European citizens. Consequently, requirements of GDPR may foresee that any such access must not be granted. The conflict of laws is already foreseeable and should be resolved by the legislator, by clarifying the definition of the term "exceptional need" and specifying the institutions that will have access to the data. In the meantime, where no changes to the Data Act will be possible, GDPR should include suitable clarifications, e.g., by extending Art. 40.2 GDPR, stating that Codes of Conduct may act as cross-regulatory harmonization.

15.2. Data Governance Act

15.2.1. Article 22 (3) Data Governance Act

The DGA introduces a unified form of consent for altruism concerning data. According to Art. 22.3 DGA, consent must enable data subjects to give and withdraw consent to specific data processing operations in accordance with the requirements of the GDPR. However, the DGA does not specify whether this consent mechanism should be considered as an additional requirement for legitimate

data exchange and the processing of personal data or become an alternative consent model (lex specialis) when data is used for general interest purposes.

It is important to note, that unlike the DGA, the GDPR has specific and detailed requirements for the consent in data processing Art. 4.11, Art. 7 GDPR.

The DGA should explicitly clarify whether the unified form of consent introduced applies as an additional requirement for legitimate data exchange or serves as an alternative consent model for general interest purposes. In the meantime, where no changes to the DGA will be possible, GDPR should include suitable clarifications, e.g., by extending Art. 40.2 GDPR, stating that Codes of Conduct may act as cross-regulatory harmonization.

Furthermore Art. 5.1 (b) GDPR establishes the principle of limiting the purpose to protect data subjects, imposing restrictions on the use of data by controllers. Personal data must be collected for specific purposes and must not be further processed in a manner incompatible with such pre-determined purposes. Re-processing for other purposes is possible if the data subject consents again or if the subsequent purposes are compatible with the already applied purposes, required a compatibility assessment based on various circumstances.

The DGA introduces a mechanism for reusing “protected public sector data”. Moreover, such reuse is also possible for personal data. This overlap with the GDPR raises concerns, as the DGA allows data intermediaries to determine the purpose of data exchange and personal data reuse the same GDPR guarantees, thereby conflicting with the intended protection of GDPR. This might result in ambiguous transparency information of less determined purposes prior processing, in order to comply with any of the applicable regulations.

One more aspect to highlight is the new definition of “permission of data holder”. DGA defines a “data holder” as a legal person or data subject with the right to access to or share certain personal or non-personal data under its control. This notion raises challenges, as there is a potential for conflicts in interpreting “permission” under DGA and “consent” under GDPR. Both may become competing concepts. This cumulates to a challenge for legitimate processing, because the concept of “permission” does not fulfil the criteria of the GDPR to qualify as a legal basis under Art. 6.1 (c) and (e) GDPR.

In the meantime, where no changes to the DGA will be possible, GDPR should include suitable clarifications, e.g., by extending Art. 40.2 GDPR, stating that Codes of Conduct may act as cross-regulatory harmonization.

15.2.2. Distinction between personal and non-personal data

The DGA does not specifically address mixed datasets – those containing both personal and non-personal data. While the DGA lacks clear regulations for handling such mixed datasets, it is noted that the EU Regulation on the Free Flow of Non-Personal Data states that it applies to the non-personal part of a mixed dataset. However, if personal and non-personal data are inseparably linked, the DGA is supposed to not prejudice the application of the GDPR.

Because the DGA does not include specific rules for mixed data, the handling of mixed datasets is not clearly regulated. This could lead to uncertainties, especially regarding the precedence of the GDPR in cases of conflicts with the DGA. In the meantime, where no changes to the DGA will be possible, GDPR should include suitable clarifications, e.g., by extending Art. 40.2 GDPR, stating that Codes of Conduct may act as cross-regulatory harmonization.

15.2.3. Concept of “general interest”

The DGA aims to establish a mechanism for the development of the EU data space to enhance control over generated data for individuals and businesses. Central to this is the role of third party “data sharing service providers” intended to facilitate access to and control over data. These service providers are obligated to ensure that data sharing aligns with the general interest, encompassing considerations related to data protection.

However, the definition of “general interest” is unclear, potentially causing issues, especially in evaluating and implementing data exchange. Despite Recital 45 of the DGA providing examples shaping the term “general interest”, the term remains a vague legal term that requires interpretation. While the DGA promotes neutrality, it faces challenges due to the absence of clear criteria for determining a "general interest," especially when conflicting general interests arise.

Additionally, a notable concern relates to the prohibition of agreements on the reuse of "protected data" held by public entities. Such restrictions, which may grant exclusive rights or limit access for alternative purposes, pose potential obstacles to innovation and collaboration. In the meantime, where no changes to the DGA will be possible, GDPR should include suitable clarifications, e.g., by extending Art. 40.2 GDPR, stating that Codes of Conduct may act as cross-regulatory harmonization.

selbstregulierung
informationswirtschaft e.V.

Über den SRIW

Der SRIW e.V. wurde 2011 als unabhängige, private Aufsichtsstelle branchenspezifischer Verhaltensregeln gegründet. Oberste Prämisse seit Gründung war und ist es, die notwendigen, unabhängigen Strukturen bereitzustellen, um branchenspezifische Verhaltensregeln zu etablieren und zu verwalten sowie deren glaubwürdige und wirksame Überwachung, inklusive eines Beschwerdemanagements, zu gewährleisten. Seither ist der SRIW erfolgreich an der Entwicklung von Verhaltensregeln, unter anderem im Bereich Datenschutz, beteiligt und engagiert sich auch in anderen Formen rund um das Thema *modern-regulation*.