selbstregulierung
informationswirtschaft e.V.

GDPR's 5th Anniversary Resumée

A practical resumée from a co-regulatory perspective, reflecting Codes of Conduct and Monitoring Bodies in particular.

June 2023

Publisher

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. Claus-Dieter Ulmer

Geschäftsführer

Frank Ingenrieth

Disclaimer

Suggested Reference

In case you want to reference or quote this publication or any contents thereof, due referencing is expected. This publication could be referenced, e.g., with the following pattern: "SRIW - GDPR's 5th Anniversary Resumée - *ARTICLE-HEADLINE*, 2023., *p. NN*"

Table of Contents

Editorial

One of the most ambitious and prestigious legal projects in the internet world can party now it's 5th anniversary, the General Data Protection Regulation (GDPR). However, the GDPR also has been highly controversial as it affects potentially every kind of digital transaction and concerns not only EU wide data streams rather than also the international transfer of data to States outside the EU. On the other side, the GDPR introduced for the first time the concept of Codes of Conduct with an impact on supervisory activities as laid down in Articles 40 ss. GDPR. Even though this Article states that in principle liability and responsibility should not be touched by adhering to a Code of Conduct it also allows for some impact on the level of supervision – and by that means, probably also upon liability.

Hence, the role of the SRIW as the principal German organization for developing Codes of Conduct within the realm of the GDPR cannot be overweighed. The articles contained in this volume demonstrate very clearly the important role of Codes of Conduct for industry as well as for stakeholders and Data Protection Supervisory Authorities, starting with the Geodatenkodex (Code of Conduct for georeferenced streetside imagery), which draws once again attention as Google obviously started once again with its Street View project in Germany - a project which had raised serious concerns ten (10) years ago. By means of the Code of Conduct it is likely that these concerns can be overcome.

Even though Codes of Conduct play a prominent role in the GDPR they are also starting to get more attention in other areas, such as the struggle against fake news, fostered by the Digital Services Act, or in the upcoming regulation of Artificial Intelligence. Thus, the article on how Codes of Conduct are developed gives highly intriguing insights on references to other legal areas and disclose the complex relationships between those.

Prof. Dr. Gerald Spindler
Chair of the Advisory Board of Selbstregulierung Informationswirtschaft e.V. (SRIW)

Moreover, and up to now little used but with a high potential, Codes of Conduct can play an important role for third country transfer which is being explored in the related article. Here, the decisions of the CJEU establish the framework, thus, encouraging to develop tailor-made Codes of Conduct that may enable also in the third party transfer setting the justified “export” of personal data.

One of the success stories of the SRIW and the idea of Codes of Conduct is represented by the EU Cloud Code of Conduct, approved by the Belgian Data Protection Supervisory Authority and managed by a subsidiary of SRIW, SCOPE Europe. It is not overdoing to state that the final approval of this European wide Code of Conduct can serve as a blueprint for other Codes of Conduct that should be adopted in the future. However, how difficult it could turn out to get an unanimous approval by Data Protection Supervisory Authorities is reflected by the story being told by Bitkom on the effort to design a Code of Conduct for pseudonymization which obviously came to a halt due to differences in the stances of Data Protection Supervisory Authorities.

This short overview of practices how Codes of Conduct work and how they are designed and which kind of hurdles they have to overcome is being completed by perspectives given by prominent members of SRIW, besides Bitkom, eyeo and SAP.

All in all, it can be stated that the idea of Codes of Conduct plays an important role for the GDPR which should be fostered and enhanced by organizations, here in particular the SRIW. It will be intriguing to see what will happen in the next five (5) years to come.

About Prof. Dr. Gerald Spindler, University of Göttingen, Germany

Prof. Dr. Gerald Spindler, born 1960, studied Law and Economics in Frankfurt a.M., Hagen, Genf and Lausanne. He is a full tenured Professor for Civil Law, Commercial and Economic Law, Comparative Law, Multimedia- and Telecommunication Law at the University of Goettingen/Germany where he, among other topics, is mainly occupied with legal issues regarding E-commerce, i.e., Internet and Telecommunication Law. He has been elected as a full tenured Member of the German Academy of Sciences, Goettingen, 2004. Apart from teaching, various books (more than 20) and commentaries (annotated codes), more than 400 articles in law reviews, as well as expert legal opinions are published by Professor Spindler.

He has been elected as general rapporteur for the bi-annual German Law Conference regarding privacy and personality rights on the Internet (2012). He is editor of two of the most renowned German law reviews covering the whole area of cyberspace law and telecommunication law as well as co-editor of international journals on copyright law, also founder and editor of JIPITEC, an open access-based journal for intellectual property rights and E-Commerce which has won awards by research foundations.

The EU commissioned him with the review of the E-commerce-directive in 2007 (DG Internal Market); he is currently an expert for data economy for the single market (2017). He was also recently (June 2018) appointed as High Level Expert for legal issues of New Technologies, in particular artificial intelligency and liability.

Regarding Data Protection, Prof. Dr. Spindler was involved in the negotiations on the GDPR as an external consultant for the German government.

Report – General Observations, Experience and Recommendations

Codes of Conduct and Monitoring Bodies, in the context of Articles 40 and 41 GDPR, can be effective tools in addressing pressing challenges related to the uniform application of GDPR requirements and consistent enforcement.

selbstregulierung informationswirtschaft e.V.

SRIW recommends to further streamline the approval and implementation processes of GDPR Codes of Conduct. This can be achieved by reviewing the procedural requirements for obtaining approved Codes and accredited Monitoring Bodies. The existing legal framework and guidelines provided by the European Data Protection Board (EDPB) are considered suitable if consistently applied. Furthermore, clarification on how to determine the competent Data Protection Supervisory Authority is required when it comes to the approval process of transnational Codes of Conduct in accordance with Article 40.5 GDPR. Streamlining the procedural requirements of a Code of Conduct's approval and Monitoring Body's accreditation can facilitate realising the full potential of Codes of Conduct.

The Selbstregulierung Informationswirtschaft e.V. (SRIW)[1)] is a non-profit association that was established in 2011 as an umbrella organisation, supporting credible self-regulation and co-regulation in the information economy. Focusing on, but not limited to, data and consumer pro-tection, the SRIW takes a modern regulatory approach that aims to align regulatory requirements with market realities and industry practicalities while protecting consumers interests.

To this end, the SRIW is deeply involved in the development of projects which, through the effec-tive use of self-regulation and co-regulation - for example in the form of approved Codes of Conduct pursuant to Article 40 GDPR - remove structural obstacles and create advantages for companies compared to "classic" regulation.

In parallel, the SRIW provides opportunities for companies to actively participate and take proac-tive roles in potential regulatory initiatives. The numerous ongoing projects, increasing implemen-tation of co-regulatory approaches within current legislation, and the deepening debate all high-light the potential of self-regulation and co-regulation in various sectors and legal domains.

The SRIW has been able to gain valuable practical experience on the extent to which different solutions and processes are at all amenable to economic implementation and approved by the Data Protection Supervisory Authorities.

Moreover, the SRIW has established a subsidiary in Brussels called SCOPE Europe[2)]. SCOPE Europe plays a crucial role in strengthening the European perception

[1)] https://sriw.de
[2)] https://scope-europe.eu

of the approaches advocated by SRIW and also serves as an officially accredited Monitoring Body under GDPR by more than one Data Protection Supervisory Authority for more than one Code of Conduct[3)].

1. Introduction

As we successfully celebrated the 5th year anniversary of the entry into force of the General Data Protection Regulation (GDPR), and with the anticipated GDPR review scheduled for the first quarter of 2024, the SRIW is pleased to present this resumé. In this paper, we share our observations, experience, and recommendations on the implementation and enforcement of the GDPR, drawing from our expertise as an organization that specializes in the development and monitoring of Codes of Conduct pursuant to Articles 40 and 41 GDPR.

The GDPR, which came into effect on May 25th, 2018, has been a significant milestone in data protection and privacy regulation, providing enhanced rights and protections for individuals in the European Union (EU) with regard to the processing of their personal data. As an organization that actively contributes to the development of industry-driven standards through GDPR Codes of Conduct, we have gained valuable insights into the practical application and impact of the regulation.

With the European Commission's Digital Decade goals aimed at accelerating the digital transition in Europe, it is crucial to highlight the potential of GDPR Codes of Conduct in fostering the use of processing technologies in Europe while ensuring compliance with the stringent standards enshrined in European legislation. These Codes of Conduct, developed by industry stakeholders in collaboration with Data Protection Supervisory Authorities, provide practical guidance, promote accountability, and support compliance efforts, thereby contributing to a harmonized and consistent approach to data protection across industries and sectors.

In this paper, we discuss the challenges and successes in implementing GDPR Codes of Conduct, highlight their benefits and potential in promoting compliance and fostering innovation, and provide recommendations for the anticipated GDPR review in 2024. We believe that our insights will contribute to the ongoing discussions and efforts towards further strengthening the data protection landscape in the EU, aligning with the goals of the Digital Decade, and safeguarding the rights and freedoms of individuals in the ever-evolving digital world.

2. GDPR Codes of Conduct as tools supporting harmonization and consistent enforcement of GDPR

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

2.1. Sector-specific particularization and harmonization

As GDPR is written in a sector-agnostic manner in terms of processing activities, GDPR requires particularization. It is expected that such particularization of general legal terms will be addressed by guidelines of the European Data Protection Board (EDPB), court proceedings, industry good practices, academia, etc. Whilst Data Protection Supervisory

[3)] https://www.dataprotectionauthority.be/publications/decision-n-06-2021-of-20-may-2021.pdf; https://edpb.europa.eu/system/files/2023-03/document_4_data_pro_code_nl_sa.pdf

Authorities have progressed in reaching harmonization, it is essential to stress the potential that Codes of Conduct have in order to complement such efforts. This applies both to sectoral implementation but also specific processing activities across sectors; both will be addressed as "sector-specific implementation" in this article. Against this background, we want to stress that Codes of Conduct are by definition sector specific and are translating general GDPR obligations into specific means of implementation. Codes of Conduct are developed by industry stakeholders and provide sector-specific guidance on how to implement GDPR requirements in practical ways. In this regard, they can address the unique challenges, risks, and best practices associated with data processing in a particular industry, providing tailored guidance for compliance. Furthermore, they can provide a flexible and adaptable mechanism for addressing sector-specific implementation challenges, as they can be updated and revised over time to reflect changing technologies, business practices, and regulatory requirements. This allows for continuous improvement and refinement of industry-specific data protection practices, ensuring that they remain relevant and effective in a rapidly evolving digital landscape. Consequently, Codes of Conduct perfectly match the current needs when it comes to guiding sector implementation.

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

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

2.2. Codes of Conduct as tools supporting enforcement

First and foremost, it should be noted that for a Code of Conduct to be operational and to demonstrate compliance by adherence, pre-requisite is the monitoring of the adherence to a Code of Conduct's principles by an accredited Monitoring Body under Article 41 GDPR. For accreditation, monitoring bodies must meet the requirements defined by Article 41 GDPR, as well as those of the corresponding EDPB guidelines[4)] and national accreditation criteria[5)]. According to the former and latter, the key elements a monitoring body must possess to receive accreditation and become legally operational are:

(1) independence, **(2)** appropriate level of expertise and, **(3)** established procedures for assessing compliance and handling complaints.

[4)] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf

[5)] e.g., https://edpb.europa.eu/system/files/2021-04/de_mb_german_accreditation_requc_en.pdf, https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinion_202002_be_requirementsmonitoringbodies_en.pdf, or https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinion_202018_on_the_nl_sa_accreditation_requirements_for_monitoring_body_en.pdf.

In this regard, it is essential to note that the established procedures for assessing compliance and handling complaints are mechanisms that support and complement the enforcement of GDPR additionally to the enforcement by Data Protection Supervisory Authorities.

2.2.1. General Oversight

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

In case of a non-conformity, the Monitoring Body must take appropriate measures against a processor or controller and decide on sanctions, which include at least suspension or exclusion from the Code of Conduct. The Monitoring Body must then notify the competent Data Protection Supervisory Authority of any action taken against the controller or processor. It is therefore important to emphasize that this is a mechanism that strengthens the remedy protecting the rights and freedoms of data subjects, as such monitoring complements the general oversight performed by Data Protection Supervisory Authorities.

2.2.2. Additional Oversight and Complaint Channel

Next to the general oversight, the monitoring of Codes of Conduct adds another safeguard for conformity. The obligatory element of integrating complaint mechanisms 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 apply appropriate sanctions and remedies.

2.2.3. Enabling focus of resources and continuous expert's exchange

Monitoring Bodies enable Data Protection Supervisory Authorities to focus their resources as needed, as the robust oversight of Monitoring Bodies required by GDPR support the enforcement for a certain sector. To remain efficient and effective Data Protection Supervisory Authorities may, as needed, adapt their focus in respect of enforcement actions. Given that a Monitoring Body acts as a liaison between the industry and the Data Protection Supervisory Authorities by several communication channels, such as informing the Data Protection Supervisory Authorities of an infringement of a Code of Conduct or by regular evaluation reports, expertise and first-hand experience can be exchanged to the benefit of any parties involved.

Against the background of a sector specific nature of Codes of Conduct, Monitoring Bodies will develop distinct expertise in a specific sector, allowing to adopt sophisticated and tailored decisions in regards of remedies, when needed. Understanding and acknowledging Monitoring Bodies' independence, Monitoring Bodies and related practices of imposed remedies and sanctions might become a trusted reference for Data Protection Supervisory Authorities, too. At a minimum, Monitoring Bodies can act as expert stakeholders for Data Protection Supervisory Authorities, likewise as a multiplier, practical translator but also reasonable challenger of Data Protection Supervisory Authorities' guidelines. This helps establishing a mechanism that streamlines information and supports the appropriate cross-border

enforcement of GDPR by Data Protection Supervisory Authorities, particularly in the context of transnational Codes of Conduct.

3. Challenges faced when it comes to the approval of Codes of Conduct and their operationalisation

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

3.1. Competent Data Protection Supervisory Authorities for transnational Codes of Conduct, streamline of procedural elements

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

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

3.2. Periods of authoritative actions and potentially prohibitive administrative fees

3.2.1. Periods of processing requests

Where GDPR provides for distinct periods of action, it would be beneficial to either define such periods more realistically, allowing Data Protection Supervisory Authorities to adequately conclude in such periods. We acknowledge that Codes of Conduct, in particular transnational Codes of Conduct, may address highly complex matters and may require extensive alignment. Likewise, it might help the adoption of Codes of Conduct that, in cases such deadlines are not met, a positive decision shall be considered as taken. If Data Protection Supervisory Authorities cannot unanimously or by majority determine that a Code of Conduct – or any other self- or co-regulatory measure – conflicts with GDPR, a Code of Conduct must be considered rather in accordance with GDPR.

In this context, we also want to raise awareness that GDPR's ambiguities and limited foreseeability of its enforcement may result in ostrich tactics by industry. Low adoption rates of most sophisticated interpretations appear less beneficial than high adoption rates of ambitious but still practical approaches. Especially in economically tense times, investments are used to be strictly evaluated. Therefore, rigorousness of enforcement of GDPR's interpretation must be aligned and balanced with actual enforcement actions. If the level playing field becomes out of balance, this might

cause industry to choses carefully its investments given that competitors might do the same. Whilst it is appreciated that there is and that there shall be a striving for the best protection of data subjects, GDPR clearly does not understand the protection of personal data without considering the individual contexts. GDPR rather positions the protection of personal data amidst several interests, freedoms, rights, and obligations by numerous stakeholders. Further adoptions of Codes of Conduct might build the bridge between stakeholders, allowing for higher implementation rates.

3.2.2. Potentially prohibitive administrative fees

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

3.3. Accreditation requirements for Monitoring Bodies

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

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

3.4. General validity mechanism for Codes of Conduct as tools for transfers

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 European Commission by way of implementing act.[6)]

We note that the general validity mechanism as an implementing act as well as its related legal effects

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

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

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

Data Protection for Streetside Imagery

Georeferenced, streetside imagery can be used for a variety of value-added services and purposes. In addition to purely commercial applications, a variety of social and non-profit applications have emerged since the introduction of this technology.

datenschutz kodex für geodatendienste

The diverse legal interpretations surrounding the data protection requirements for such services have created uncertainties, although their general permissibility is not disputed. To establish and foster legal certainty for service providers and users of such image material, the Geodatenkodex – Code of Conduct for georeferenced streetside imagery – ("the Code" or "Geodenkodex")[8] was developed.

The Code acknowledges the various interest of those concerned, including users and service providers. Those interests have been transferred into a balanced system of rights for the data subjects and obligations of the service providers, incorporating binding technical and organizational measures. In this way, the Code promotes the responsible and legally compliant design of geo-referenced, roadside imagery services and reconciles the needs of the market with the legal requirements.

1. Background

Georeferenced, streetside imagery services have become increasingly popular in recent years, offering a diverse range of value-added applications. These services involve capturing street-level images with geolocation data, enabling their utilization across commercial, social and non-profit sectors.

There is a huge variety of different services that utilize georeferenced, roadside imagery, ranging from public-availably imagery to closed-group availability. Publicly available imagery can be used to supplement existing map material with further information, such as the location of curb drops, wheelchair-accessible entrances to buildings, suitability of the ground for certain means of transport, or general obstacles. Closed-group availability can be used by municipalities and other organizations for surveying and planning activities, water runoff simulations, and infrastructure planning.

Appropriate imagery enables municipalities and municipal corporations to perform many of their tasks, such as evaluating conditions and information on the basis of a single data collection, more efficiently. Additionally, infrastructure planning based on such imagery is becoming increasingly important, for example in the area of broadband expansion.

However, there are also ambiguities across the European landscape raising concerns about privacy and data protection. The primary focus of the debate revolves around the collection and processing of personal data. While the general permissibility of these services is not disputed, the requirements for such services are often subject to divergent legal interpretations. Consequently, the use of georeferenced, roadside imagery services in Europe is subject to a range of legal and regulatory requirements, which also may vary by country.

[8] https://geodatenkodex.de

Ultimately, it is important for companies offering these services to comply with applicable laws and regulations to ensure the protection of individuals' privacy rights. As a result, there has been a growing need for a coherent and comprehensive Code of Conduct to ensure compliance with GDPR and other relevant regulations. The Geodatenkodex is answering this call for a trusted compliance tool and specifies requirements for the use of optical sensors on the roadside for the purpose of processing the captured data.

During the development process of the Code and the revision a few years later, together with main stakeholders of the industry, the working group encountered some impediments. To this end, the SRIW (Selbstregulierung Informationswirtschaft e.V.)[9] and its related working group would like to take the 5-Year General Data Protection Regulation Anniversary as an opportunity to outline a few of these obstacles, in order to raise expectations about how future steps can further strengthen the added value of the Code and pave the way for many other initiatives practically increasing data subjects rights.

2. Stakeholders and Formalities

2.1. Diverse Dialogue

In order to incorporate the interests of users and providers into an interests balanced, viable and industry-valuable Code of Conduct under GDPR, engaging with a broad range of stakeholders – such as Supervisory Authorities, municipalities and public administration, as well as related expert groups - during different stages in the development process is a necessity, but by no means something that can be achieved effortlessly. Deriving from the viewpoint of the development of Codes of Conduct, constant dialogue between regulators, service providers and consumers is the key to a successfully implemented and enforced regulation in general.

Against this background, it has been unexpected, especially as the Secretariat of the Geodatenkodex - bringing together all relevant stakeholders since the beginning of the discussions on a Code of Conduct for georeferenced streetside imagery and the development of a first version in 2011; and also having years of experience in developing and monitoring of co- and self-regulatory measures – that previous discussions were not actively followed-up by Data Protection Supervisory Authorities when being in the process of operationalizing new approaches and interpretations of legitimacy of streetside imagery services.

Furthermore, there is a sense of frustration regarding the preference of municipalities and public administrations (more precisely tenders) to rely on pre-GDPR non-Data Protection Supervisory Authorities' expert group guidelines instead of embracing the Geodatenkodex or reaching out for potentially needs of adjustments, in cases where the current version surprisingly may not be considered fit for purpose. It is worth mentioning that those guidelines apply rather to aerial photography – which require totally different evaluations – and are dated as of 2014 –therefore missing ten (10 years of jurisprudence – notably also the evolvement of GDPR.

Closer to the matter and legally more up-to-date is therefore the latest version of the Geodatenkodex (2.1)[10]. Revised in light of the General Data Protection Regulation, the updated version takes practical experience with the Geodatenkodex under the Data Protection Directive and its application since the General Data Protection Regulation came into force, as well as changed framework conditions due to new resolutions and guidelines of the German Data Protection Conference, the European Data Protection Board, and also decisions of the courts into account.

Beyond the actual development process of a Code of Conduct, Article 40 GDPR foresees the possibility to approve a Code of Conduct by Data Protection Super-

[9] https://sriw.de

[10] https://geodatenkodex.de/fileadmin/gdk/files/GDPR_Code_of_Conduct_for_Geodata_Services_v2-1-informal-EN-version.pdf

visory Authorities. Unclear responsibilities among national and European Data Protection Supervisory Authorities and inconsistent understandings regarding the formalities of the approval process are just a few of the challenges that need to be addressed in the future to ensure the effective implementation and enforcement of GDPR requirements through an approved Code of Conduct.

In this respect is shall be highlighted that – regardless of the initiatives intent to seek approval – given the various interpretations by Data Protection Supervisory Authorities of their own guidelines, it would be cumbersome to determine the competent Data Protection Supervisory Authority, either within Germany or within Europe.

2.2. Societal Benefits

The lack of a diverse dialogue and streamlined responsibilities and formalities within the Data Protection Supervisory Authorities result in diffuse actions which consequently result in overly cautious municipalities and the public administration, as they fear conflicting or constantly changing stands by Data Protection Supervisory Authorities.

In return, the reluctant involvement ensues in a lack of implementation of modern means of city planning, greenfield monitoring, streetside asset management, crises prevention (flood planning) but also emergency services (e.g. emergency response planning in regards of best ways to approach the scene, precautionary and continuous analysis of bottlenecks).

Municipalities and municipal companies could, for example, cost-efficiently evaluate several conditions and information on the basis of a single data collection, where otherwise a multitude of repeated and / or more immersive manual evaluations would be necessary on site.

Likewise the cautiousness is resulting in unnecessary high costs also in private businesses and even more processing or personal data (e.g. architects, city planners, heavy load transport planning, broadband and energy extension and maintenance planning).

In addition and in the interest of an inclusive society, georeferenced image material could also be used, for example, to supplement existing, classic map material with further information.

> *Including the location of curb drops, wheelchair-accessible entrances to buildings, the suitability of the ground for certain means of locomotion, or general obstacles; whether on the ground or through objects protruding from the path.*

The advantages of georeferenced imagery is definite and the added value of the Geodatenkodex unquestionable, but those described societal benefits are not yet available to its full potential, because of avoidable concerns and unclear and partially apparently excessive legal requirements given the Data Protection Supervisory Authorities' interpretations.

3. The Geodatenkodex

3.1. Balancing Interests

The Geodatenkodex was developed considering the different interests of the data subjects, as well as the users and service providers. It translates these mutual interests into a balanced system of rights of the data subjects and obligations of the service providers. Service providers who voluntarily submit their services to the Geodatenkodex and thereby join the independent monitoring and complaints mechanisms by the SRIW, ensuring that both the data protection interests of data subjects and the general information interests of the public are preserved. Additionally, it fulfils the overarching goal of a Code of Conduct, which is to make information easily access-

ible for those concerned, without any particular obstacles.

By taking this inclusive approach the Code overcomes ambiguities in regards of GDPR key elements, such as multi-purpose processing (pursuant to Article 6.1 f) GDPR), data minimization (Article 5.1 c) GDPR) and incorporating a suitable means to request blurring of personal data, but also fosters trust through a harmonized way of addressing various requirements under GDPR and its technical and organisational implementation.

3.2. Harmonizing the European Regulatory Landscape

As described above, the process of getting a Code of Conduct approved is hampered by several unclear formalities at this stage. But, if approved by Data Protection Supervisory Authorities, the Geodatenkodex has the potential to harmonize the approach to georeferenced, streetside imagery services across Europe. By establishing a unified set of guidelines and standards, the Geodatenkodex can foster consistency in the implementation and enforcement of GDPR requirements. Harmonization is essential for facilitating cross-border operations, providing clarity to service providers, and enhancing the protection of individuals data protection rights.

The approval of the Geodatenkodex can serve as a trusted anchor point for companies offering georeferenced, streetside imagery services. The Code provides a clear framework for compliance, ensuring that organizations adhere to the highest standards of data protection and privacy. This, in turn, would foster trust in the responsible use of geodata services, among different stakeholders, including consumers, businesses, and regulatory bodies.

Furthermore, a harmonized approach facilitated by an approved Code of Conduct would streamline regulatory processes. It would help reduce the burden on national Data Protection Supervisory Authorities by providing a consistent and recognized set of guidelines that companies can adhere to. This alignment would simplify compliance efforts and promote efficiency in regulatory oversight, ultimately benefiting both service providers and regulatory bodies.

3.3. Operationalization of Key Data Subject Rights

Touching upon another element of GDPR, it is essential to ensure that data subjects have a clear understanding of their rights and the circumstances under which these rights may be limited or denied. The Geodatenkodex presents an opportunity to provide clarity on the operationalization of those individual rights, which can help prevent disappointment, anger, and confusion among data subjects seeking to exercise their rights.

Currently, there can be instances where service providers claim that data subjects may perform one of their data subject rights, even with endorsement by Data Protection Supervisory Authorities, but in practice, the majority of requests by data subjects will be legitimately dismissed. This situation can lead to frustration and confusion. To avoid such scenarios, effective communication should be prioritized, ensuring that data subjects understand that their personal data processing remains legitimate unless specific conditions apply, which may de-facto result in no right of interference by data subjects in most common processing contexts.

This proactive approach can help manage expectations and prevent unnecessary disappointment or anger among data subjects. Information about the circumstances under which their rights may do apply and in which circumstances the performance of their rights will result in no changes, equips them to make informed decisions and navigate the data protection landscape more effectively.

Moreover, by emphasizing communication in a manner that highlights the legitimacy of data processing unless specific conditions apply, a more balanced and transparent approach can be achieved. This approach empowers data subjects to understand the rationale behind processing decisions, enabling them to accept legitimate processing while also asserting their rights when necessary.

4. Future Expectations

By communicating the following expectations, SRIW aims to, on the one hand, foster the Geodatenkodex as a comprehensive and trusted framework for georeferenced, streetside imagery services and on the other hand improve the dialogue with relevant stakeholders.

Considering the significant expertise and valuable contributions reflected in the Geodatenkodex, the SRIW expects to contribute to existing and future working groups. The resulting information exchange will remain key to maintain an up-to-date, broadly adopted and accepted standard such as the Geodatenkodex. Related extensive work and knowledge have been instrumental in shaping the Geodatenkodex to address the specific challenges and requirements of georeferenced, streetside imagery services. Already the previous versions of the Code have significantly impacted today's landscape of understanding and evaluation of processing streetside imagery, eventually directing heated debates in structured, analytical and objectives balancing of interests by any stakeholders involved.

Secondly, we anticipate a comprehensive evaluation of the Geodatenkodex in collaboration with key stakeholders. This evaluation process will provide an opportunity to assess the effectiveness of the Code, identify any areas that may require further adaptation or clarification, and ensure that it aligns with evolving market needs and legal frameworks. Feedback from stakeholders will play a crucial role in enhancing the Code's robustness and usability.

The initiative will further evaluate the required formalities to seek for an approval and resulting benefits. This involves presenting the Code to relevant authorities and organizations for review and endorsement. The SRIW expects the authoritative landscape to further streamline their interpretation of GDPR and subsequent guidelines, as well as the resulting formalities. In this respect it is also expected that is remains acknowledged by Data Protection Supervisory Authorities that GDPR reflect a European-wide regulation and that streetside imagery is processed in any member state. Against this background, it must be recognized that partially significantly diverging interpretation on legitimate processing must be resolved. Provided the uncertainties regarding the approval process will be resolved and benefits of proceeding accordingly, obtaining formal approval pursuant to Article 40 GDPR will validate the Code's compliance with legal and regulatory standards and foster broader acceptance and adoption within society of related services.

About the Authors / the Project

The Geodatenkodex – Code of Conduct for georeferenced streetside imagery – is the first Code of Conduct which was established under the umbrella of Selbstregulierung Informationswirtschaft e.V. (SRIW).

Since its earliest days, the initiative was striving for balancing interest of different stakeholders involved in the creation and processing of streetside imagery. Industry stakeholders acting as service provider itself or utilizing imagery provided by third-parties have been contributing to the material requirements.

As SRIW in its role as centralized contact for stakeholders, SRIW has been in direct contact numberous data subjects, users and providers. A significant shift in the preception of streetsided imagery can be noted. Stakeholders are invited to participate in the future development of the Geodatenkodex.

datenschutz
kodex für
geodatendienste

Developing Codes of Conduct – Potentials for and a Strong Need of Further Alignment of Regulatory Frameworks

Codes of Conduct under Article 40 GDPR act as a sandwich across regulations. Besides addressing dedicated data protection laws overarchingly, Codes of Conduct may also include sector-specific regulations, whereby they must comply with the monitoring requirements under Article 41 GDPR and its challenges, in addition to comprehensive requirements on competition and antitrust law. Cooperation amongst authorities of different expertise and stakeholders may avoid conflicts when interpreting the GDPR and facilitate improving cross-sectoral applicability. Due to remaining ambiguities and uncertainty, Codes of Conduct fall short of their potential.

selbstregulierung informationswirtschaft e.V.

1. Background

Since there is remaining and significant ambiguity in the area of data protection regulations, Codes of Conduct have been anchored in Article 40 of the GDPR. In this regard, the expectations of the Data Protection Supervisory Authorities for the functionality and implementability of the Codes of Conduct are quite high which is also reflected in the guidelines of the European Data Protection Board (EDPB)[11] and thus supports the high requirements of the Data Protection Supervisory Authorities. The GDPR itself can be seen as a lex specialis compared to other regulations but cannot overrule them.

This comment is not intended as comprehensive analysis of the interplay of any regulatory frameworks applicable to the development of Codes of Conduct. Nonetheless, it reflects initial experiences by initiatives and stakeholders strongly involved in the development of Codes of Conduct and related monitoring activities. Such experiences shall be presented as a high-level observation alongside conclusions where such experience may impact the operationalization of tools, seriously demanded by industry and regulators.

2. Mostly affected regulatory frameworks next to GDPR

2.1. Competition and Antitrust

Codes of conduct are deemed to particularize the GDPR by clarifying and enabling suitable industry implementation which inherently touches the exchange of different types of information by stakeholders. Consequently, compliance with competition and antitrust requirements must be observed and maintained.

In the following, the challenges regarding the requirements for drafting a Code of Conduct as well as monitoring against the background of compliance with competition and antitrust law are briefly presented.

2.1.1. Drafting a Code of Conduct

When drafting a Code of Conduct in accordance with Article 40 GDPR, many aspects must be considered, including the legal requirements outside the GDPR. As indicated above, EDPB's guidelines require added value by particularizing GDPR, which eventually requires the exchange between different stakeholders. A clarification by regulators, that such exchange during the drafting of Codes of Conduct is privileged conditionally, will be highly appreciated.

[11] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf

It should be noted that not any exchange of information is per se illegal, especially if it remains on a high level. To meet the requirements of the Data Protection Supervisory Authorities and the guidelines of the EDPB, however, Codes of Conduct may require granular provisions. The very existence of such granular provisions 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.

The lack of privileges for the drafting of Codes of Conduct plus the potentially conflicting expectations in the different legal frameworks, imposes additional burdens on those stakeholders willing to support GDPR's implementation and enforcement for the benefit of data subjects. 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. This might also be addressed by the implementation of due public consultations, allowing stakeholders who were not primarily involved to provide feedback. But even the application of such safeguards, does not undoubtedly prevent from different interpretations and subsequent action from competition and antitrust authorities.

It must be noted, that applying such a framework to the development of a Code of Conduct may eventually result in slower processes, or limited granularity of a Code of Conduct's requirements. The latter may, subsequently, face concerns by Data Protection Supervisory Authorities, requesting adaptations. Depending on the requests, in such a situation, the development of a Code of Conduct might be required to decide which legal framework shall have precedence, resulting in a fine-line to upkeep compliance with competition and antitrust law; a burden which is not comforting the development of such tools in general. Maintaining due sensitivity of Data Protection Supervisory Authorities on this matter as well as positively incorporated privileges in the regulatory frameworks will be highly appreciated.

2.1.2. Monitoring of a Code of Conduct

In addition to drafting the Code of Conduct, the monitoring of the Code of Conduct under Article 41 GDPR with regard to competition and antitrust law also plays a significant role. The monitoring becomes sensitive, as the Monitoring Body may – depending on a Code of Conduct's requirements – have access to very sensitive information as part of the review of an adherent company.

The criteria for the accreditation of a Monitoring Body are comprehensively regulated in Article 41 GDPR. In addition to independence and the necessary expertise, they also require procedures and structures with which the Monitoring Body investigates complaints about violations of provisions in the Code of Conduct. Some Member State's accreditation criteria for the Monitoring Body apparently uses language that appears borderline when it requires the Monitoring Body to make the files of a complaint accessible to any adherent companies.

Generally, the necessity appears questionable, as depending on the issue of the complaint. There may be no learning or added values for any other party than the ones involved. More particularly, an non-redacted copy of such files may include business sensitive information. The Monitoring Body is legally prohibited to share such information. Already the fact that the complaint was filed, might qualify as protected, sensitive information and must therefore not be shared with others.

It is expected that Data Protection Supervisory Authorities will continue reviewing their guidelines and criteria alongside the expertise of other authorities, safeguard-

ing that Monitoring Bodies are not directly or indirectly requested to act in conflict with other regulations to comply with Data Protection Supervisory Authorities' interpretation of GDPR, remaining the burden of resolving such conflicts with the Monitoring Body.

2.2. Business activities acts

In addition to the requirements of competition and antitrust law, other regulatory frameworks must also be considered. Member states often foresee that entities who are acting as a business will have to register their business activities. In this regard, Data Protection Supervisory Authorities apparently prefer that the registered business activities already and explicitly reference the drafting of GDPR Codes of Conduct or related monitoring activities. The public administration respectively related authorities which are responsible for the processing of such registration, tend to refer to the GDPR requirements "approval" or "accreditation"; subsequently, the submission of proofs that approval or accreditation has been granted prior the registration of the business activity is requested.

This represents a chicken egg issue. The business activity to support stakeholders in drafting Codes of Conduct (prior their approval), as well as the preparatory work of designing and performing the accreditation process itself (i.e., prior accreditation) may already be the business activity.

The chicken-egg issue resolves easily, if reference to the term Code of Conduct or Monitoring Body would not result in reflexive concerns. It will be appreciated if the Data Protection Supervisory Authorities and other authorities involved in the process of registering the business activities will allow for a differentiated approach along the different steps throughout the process of a code's approval or a Monitoring Body's accreditation.

In this context, it is important to highlight that the intended activity of being a Monitoring Body pursuant Article 41, generically, does not require any accreditation. Pursuant Article 41 GDPR, only the performance of monitoring activities for a specific Code of Conduct, requires accreditation. Consequently, any preliminary activities under the vein of filing an accreditation request, should be possible to be registered. Only the registration of performance of monitoring activities related to a specific GDPR Code of Conduct, can be subject to the condition of prior accreditation. In no case, however, a condition of the approval appears suitable, because the approval refers to the document (Code of Conduct) but not any entity which registers its activities.

It will be highly appreciated if both, public administration responsible for the processing of business activities, will remain open-minded to the complexities in the field of Codes of Conduct. Likewise, to the extent Data Protection Supervisory Authorities will be involved from other public administrations / authorities, consideration of the abovementioned possibilities for differentiation and awareness of other legal frameworks applicable next to GDPR will certainly foster the adoption of Codes of Conduct in general.

2.3. Other sector specific laws

Interaction with other sector specific laws may relate to formalities, as above, but also relate to the material provisions and material need for Codes of Conduct. E.g., GDPR interacts with several sector specific regulations, such as telecommunications, media, energy, etc. Each of such regulations may also include specific provisions regarding the required processing and retention of personal data.

These sector specific laws result from different legal provisions. On the one hand, such sector specific laws result from EU Directives which needed to be

translated in the law of the member states, so that the GDPR must be acknowledged in any case; on the other hand, such sector specific laws result from other EU Regulations. Alongside, there are non-harmonized sectors, to which only national Member State laws apply; the latter should be aligned with GDPR by principle, but unfortunately may remain ambiguous.

In this regard, Codes of Conduct may help to align the interpretation of different sector specific regulations, where the applicable legal framework remains high level and not directly conflicting. In this respect the overarching intent of Codes of Conduct, i.e., particularizing the implementation of GDPR, is directly addressed. Where the applicable legal framework may be explicitly conflicting with GDPR, Codes of Conduct most likely will not be able to resolve the situation. In these cases, it is probably and most suitably the regulator that should resolve the identified conflicts.

Consequently, Data Protection Supervisory Authorities should foster the drafting of Codes of Conduct – national and transnational – 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 context and acknowledging that – especially in cases of potentially unresolvable conflicts – it shall be highlighted that pragmatic approaches are always in the best interest of data subjects and consequently often preferably compared to rather formalist approaches. In situations where stakeholders remain in limbo to potentially conflict with one or the other legal requirements, data subjects will not benefit from upholding the conflict until the regulator officially resolves the situation. Without pragmatic approaches, that indicate options for stakeholders to comply at a best-efforts principle, this will only result in resignation. Consequently the de facto protection remains unnecessarily limited, whereas pragmatic approaches may keep implementors motivated and thus keep the level of protection as high as possible given the conflicting scenario.

3. Expectations

Against the background of the above explanations, it would be desirable for Data Protection Supervisory Authorities to maintain and further establish a solid awareness of any other regulations which apply alongside the GDPR. Furthermore, streamlined collaboration between the different authorities involved will certainly limit situations in which code-owners or Monitoring Bodies are required to take impossible actions. Additionally, a clarification across the applicable regulations, where needed, that the preparation of Codes of Conduct as well as monitoring of such is a privileged activity is welcomed and considered a critical element to significantly raise the adoption of such tools in future.

About the Authors

The SRIW (Selbstregulierung Informationswirtschaft e.V.) is a non-profit association that was established in 2011 as an umbrella organisation, supporting credible self-regulation and co-regulation in the information economy. Focusing on, but not limited to, data and consumer protection, the SRIW takes a modern regulatory approach that aims to align regulatory requirements with market realities and industry practicalities while protecting consumers interests.
The SRIW has been able to gain valuable practical experience on the extent to which different solutions and processes are at all amenable to economic implementation and approved by the Data Protection Supervisory Authorities.

Developing Codes of Conduct and Monitoring at Scale – First Practical Experience

SCOPE Europe[12] has been established in 2017 to promote and facilitate two key elements in the context of GDPR Codes of Conduct:

1) *the drafting and maintenance,*
2) *the independent monitoring.*

Hereby, SCOPE Europe instantiated the next iteration and evolution of the activities which its primary, Selbstregulierung Informationswirtschaft e.V.[13], has paved the way for.

In general, Codes of Conduct prove to be an effective tool. SCOPE Europe also recognizes that the developing and monitoring can follow distinct patterns. Additionally, SCOPE Europe recognized that negotiations related to the approval (material requirements) and the accreditation (monitoring of such requirements) follow common systematics. Therefore, developing and monitoring Codes of Conduct provide opportunities for scaling. However, practical experience suggests that stronger alignment across Europe is appreciated to further limit rather formalist differences with limited added value resulting in partially disproportionate additional efforts.

1. Background

Codes of Conduct allow the particularization of GDPR requirements addressing specific needs of distinct sectors and / or processing activities. Thus, Codes of Conduct support legal certainty related to the interpretation of GDPR and may initiate and establish a process of harmonization.

Pre-GDPR the requirements for added value of Codes of Conduct have been highly debated, partially resulting in opinions that each Code of Conduct must (significantly) go beyond the existing legal requirements. GDPR has clarified that a particularization is sufficient, in other words, Codes of Conduct do not have to extend the legal requirements; nonetheless they must contribute to the practical implementation and interpretation of GDPR requirements. Practical experience by SCOPE Europe, as it were part of the negotiations of the first fully operational transnational Code of Conduct (the EU Code of Conduct for Cloud Services Providers, EU Cloud CoC)[14], Data Protection Supervisory Authorities are taking a very conservative position: it has even been recognized critically, if a Code of Conduct goes beyond the legal requirements.

SCOPE Europe appreciates this development that particularization shall suffice, in principle, because voluntary tools and initiatives such as Codes of Conduct require significant efforts and resources by interested stakeholders. Insisting on extending the legal requirements – logically – is considered a dis-

12) https://scope-europe.eu
13) https://sriw.de
14) https://eucoc.cloud

advantage and the opposite of an incentive to participate. Nonetheless, evolving interlinks of GDPR with other legal frameworks may make it handy for stakeholders to – carefully and reasonably – include provisions that might be considered an extension of the direct requirements of GDPR. Opinions that might be interpreted as prohibiting an extended level of protection by Codes of Conduct appear counterindicative.

2. Key elements of a Code of Conduct

Given the Guidelines on the development of Codes of Conduct[15], there are several key elements that must be addressed. Without considering any and all of such elements necessary, the existing checklist certainly supports the development of Codes of Conduct. On the other hand, practical experience has shown, that additional elements can prove handy.

Guidelines and practical experience provide that certain aspects must be addressed in the process of developing a Code of Conduct. Addressing aspects is not equal to including the if and how in the actual text of a Code of Conduct for any instance. Guidelines and – for practical reasons – the actual request for approval require supporting documentation. For the purposes of clarity of the actual text of a Code of Conduct it is recommended to limit the text to those aspects which are necessary for the compliance with and implementation of the Code of Conduct. Mere formal and procedural aspects should be addressed solely in the supporting documents.

This comes along with the possibility that a Code of Conduct can comprise of several documents and Annexes. It is understood that one document with several chapters might appear preferrable, but this would also require increased version numbers for any changes, even if they do not relate to the material requirements of a Code of Conduct. Changed version numbers might create confusions if material requirements were adapted, and it may also affect the lifecycles of valid adherences to a Code of Conduct. Against the background that Codes of Conduct often will address professionals, the interlink of several documents must be considered a well-known practise anyway.

In any case, the development and maintenance of several Codes of Conduct by identical code-owners or with the support of specialised providers, will ease the processes enormously. Especially in areas where the Code of Conduct – or its Annexes - does not govern specific requirements of GDPR implementation but rather addresses administrative elements, such as its governance, optimizations can easily be spread across all such “interlinked” Codes of Conduct. In this vein, Codes of Conduct may be understood as a conjunction of several building blocks, which altogether form a sound framework.

This may also speed-up the approval process and helps the negotiations. Data Protection Supervisory Authorities will know significant parts of a Code of Conduct and may focus their assessment on the actual material requirements. Likewise, evolving notions and interpretations on the required level of detail by a Code of Conduct, good practices in phrasing provisions etc. can be recognized and implemented smoothly in any future developments. Altogether, the development process will speed-up and becomes more foreseeable.

3. Monitoring of Codes of Conduct with equivalent procedures

Similar to the approach of developing a Codes of Conduct, Monitoring Bodies must establish a code-specific monitoring framework and associated procedures.

[15] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf

EDPB Guidelines[16] impose key aspects of what shall be addressed in such a framework. Similar to the submission for an approval of a Code of Conduct, also the submission of a request for accreditation requires supporting documentation in practise. Likewise, the same logics apply. The constantly growing experience in drafting such supporting documentation facilitates future requests.

Considering the accreditation requirements across Europe, such requirements are, in principle, aligned.[17] It is highly appreciated and recommended to resolve current rather formal differences, though. Accreditation requirements generally relate to key elements such as independence, transparency, expertise. Areas, which will require similar, if not even identical, implementation for any Code of Conduct. Practical experience has proven, that adaptations to reflect specific needs of several Codes of Conduct are limited and let core-procedures untouched. E.g., SCOPE Europe is accredited Monitoring Body for the EU Cloud CoC, which is a transnational Code of Conduct. In the meanwhile, SCOPE Europe is also accredited Monitoring Body for the Data Pro Code[18], a national Code of Conduct in the Netherlands. Core procedures remained untouched, while code-specific elements could be addressed in dedicated procedures. The concept of building blocks allows SCOPE Europe to adapt to new Codes of Conduct in relatively short time. On the other hand, Data Protection Supervisory Authorities might also process accreditations more easily given the building block approach, as a significant share of the relevant documents will not change.

4. Expectations

SCOPE Europe has made good experience alongside the approval and accreditation processes. SCOPE Europe acknowledges that processes let room for optimization but as SCOPE Europe often acts a frontrunner, it is expected that there are no blueprints for any possible scenario, yet. In this vein, though, SCOPE Europe likes to repeat its recommendations, that collaboration between the Data Protection Supervisory Authorities should be strengthened. Likewise, differences in the formalities in different Member States should be limited to the extent legally necessary. For the purposes of efficiency, it seems also reasonable that Data Protection Supervisory Authorities endorse building block approaches and subsequently also consider accepted building blocks by other Supervisory Authorities as generally suitable. Undoubtedly, also core-building blocks will require updates, from time to time, but it appears more beneficial to the empowerment of data protection, if the (limited) resources will be focussed on the material and individual elements, rather than repetitively assess the same (administrative) documents and provisions.

[16] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf

[17] See as starting point https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf. Additionally, the EDPB has taken several opinions on related decisions by the competent Data Protection Supervisory Authorities regarding their national accreditation criteria.

[18] https://scope-europe.eu/data-pro-code

About the Author

SCOPE Europe s.r.l. (SCOPE Europe) is an organisation supporting the self-regulation and co-regulation of the information economy. Located in Brussels, it continues and complements in Europe the portfolio of its primary, the non-profit association Selbstregulierung Informationswirtschaft e.V. (SRIW). It acts as a think tank to discuss and debate key issues in digital policy and provides an umbrella organisation supporting credible and effective self- and co-regulation of the information economy.

SCOPE Europe gathered expertise in levelling industry and data subject needs and interests to credible but also rigorous provisions and controls. SCOPE Europe has been the first accredited Monitoring Body under the European General Data Protection Regulation (GDPR) since May 2021 related to a transnational Code of Conduct, i.e., EU Data Protection Code of Conduct for Cloud Service Providers also known as the EU Cloud Code of Conduct. Since February 2023 SCOPE Europe is the first ever Monitoring Body under GDPR which has been accredited for more than one Code of Conduct and by more than one Data Protection Supervisory Authority.

Third Country Transfers – Potentials and Level Playing Field for Codes of Conduct

The adequate protection of data subjects when personal data is transferred to a Third Country must be maintained. Court decisions and GDPR provisions consider data subjects subject to additional risks, acknowledging such risk will be dependent on the Third Country. In the absence of adequate safeguards, also due to recent jurisdiction, some Third Country Transfers are significantly challenged currently.

This contradicts and prevents businesses' cross border activities in a globalized world and makes Third Country Transfers a highly debated topic. Against this background the industry has a strong need for safeguards putting Third Country Transfers on a solid legal ground. Due to the need for individual assessment of each transfer, all-in-one solutions will prove highly complex, overly burdensome, because the risks supposedly being addressed are potentially not applicable, and thus limitedly suitable to serve as safeguards. Instead, there is a need for tailored, yet cost efficient and therefore not individual-driven safeguards. As such, Codes of Conduct and Certifications lend themselves as solutions, but whose requirements to receive an approval should be equalized as both seem to converge in scope in practice. It can be noted that the industry is already working on its own solutions.

It is desirable that regulators perceive the needs of the industry and do not immediately cut their efforts considering that solutions will be developed further on an ongoing basis.

selbstregulierung
informationswirtschaft e.V.

1. Background

Third Country Transfers have been given more attention for some time now due to geopolitical tensions and growing sensitivity for personal data. The origins of the debate as to whether and under which conditions personal data may be transferred to Third Countries were related to authority and governmental access to personal data of European citizens by non-European authorities/governments without safeguards such as (prior) judicial review by European courts. Subsequently the ECJU decided upon adequacy decisions regarding the US with the result of twice voiding them. At the present time the discussions about Third Country Transfers become potentially counter indicative to the intensified need for digitalism and related cloudfirst strategies as well as overly simplified though addressing highly complex scenarios and eventually extending and shifting applicability of precedence to even further use cases due to a lack of legal certainty. The following article deals with the necessity of bringing these discussions to operationalizable solutions and the requirements for such.

2. Due protection of Data subjects

Undisputedly data subjects must remain protected regardless of the location of processing. Considering this, undermining applicable regulatory frameworks by reallocation of activities is undoubtedly to be prevented. The dilemma to be faced in this respect is that there is no undermining led by businesses, as the associated risks result from authorities' and governmental access. It is to be noted and taken into account that undue surveillance does hardly stop at territorial borders.

3. Need for adequate mechanisms adapting to transfer related risks

When assessing whether a Third Country Transfer may take place, it is necessary to refrain from mixing up of general risk associated with a certain sector, processing activity or outsourcing in general. Instead an individual analysis of Third Country specific risks is required which should be freed from political dimensions, as those should not be resolved neither by data subjects nor by businesses but rather by those stakeholders who are destined to do so.

In such an analysis the general legal risks respectively risk clusters and related measures are to be assessed rather than focussing on territories, as the legal framework (either literally or in its application) may constantly change. Ambiguities and the unfortunate mixup of several dimensions bring any existing mechanisms as safeguards for Third Country Transfers at risk. Third Country Transfers therefore are often safeguarded by redundant mechanisms, such as adequacy decisions pursuant to Article 45 GDPR, standard contractual clauses pursuant to Article 46.2 (c) GDPR and binding corporate rules pursuant to Article 47 GDPR.

As those three current main solutions sometimes require high individual expenses and their scope of application is limited, in practice, more tailormade solutions – as additional – alternatives appear needed. Such solutions could be Codes of Conduct pursuant to Article 40 GDPR ("Code of Conduct") and Certifications pursuant to Article 42 GDPR ("Certifications") as suggested by Article 46.2 (e) and (f) GDPR. However, the practical relevance of both measures crucially depends on what legal requirements are posed on them.

4. Level playing field

GDPR's requirement in the context of safeguards for Third Country Transfers for equivalency is not to be understood as identity. 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. In relation to Codes of Conduct and Certifications those principles are not always consistently followed, as GDPR – and subsequent guidelines[19] – foresee differences between Codes of Conduct and Certifications; e.g. pursuant to Article 40.3 GDPR in conjunction with Article 40.5 to 40.9 GDPR Codes of Conduct require a general validity (including the involvement of the European Commission), whereas Certifications do not require such additional step (see Article 42.3 and 42.5 GDPR).

This may result from the fact that Certifications address a specific "processing" rather than a company or product in its entirety. Thus, the certified specific technical implementation in its specific version might allow for such a deviation. Practically, Certifications appear less bound to this level of detail, considering recently published schema. Schemas appear targeting a large range of different processing operations and providing rather for a management system as specific technical and organizational measures are only to be applied if an evaluation process has

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

shown that particular data are processed. In this sense, the differences in formalities should not result in significant mistreatment.

Saying, where Codes of Conduct and Certifications practically become almost identical from a material point of view, GDPR's requirements imposed on them should be equal – either equally simple or equally complex.

5. Expectations of the industry

Apart from the requirements defined by law and political stakeholders, also the industry makes demands on safeguards for Third Country Transfers. The industry expects that solutions to be developed will provide an additional level of legal certainty.

Certainly such solutions never will be a carte-blanche, but adhering to a Code of Conduct / Certification should indeed allow for positive statements that adequate supplementary measures are implemented. Where distinct measures cannot be determined it shall be clarified that following a defined methodology to assess Third Country Transfers and subsequently implement measures accordingly will suffice, even if – on a case by case basis – the measures will prove inadequate in future.

On the contrary, where there is any notion that implemented measures were intentionally or gross negligently determined wrongfully or where the defined assessment logic is not applied / documented, the benefits of legal certainty and protection should not apply either.

Solution-oriented initiatives from the industry exist, seeking for support and cooperation with authorities. One of them is the Third Country Initiative[20] of the General Assembly of the EU Cloud Code of Conduct ("EU Cloud CoC" or "Code")[21]. The EU Cloud CoC is a Code of Conduct managed by SCOPE Europe[22], which covers the requirements of the GDPR regarding cloud services and was approved by the Belgian data protection authority in May 2021 after a positive opinion of the EDPB[23]. The General Assembly of the EU Cloud CoC is currently working on a draft of an effective but accessible safeguard for Third Country Transfers by means of a separate on-top module to the Code.

Another example for an initiative from the industry is the Transfer Impact Assessment Tool ("BiTIAT") published by Bitkom[24] which is a software providing Bitkom members with a framework for conducting transfer impact assessments for international data transfers to the US, Brazil, India, Australia and Colombia by standardizing the analysis of the Third Country and the respective data transfer and also the necessary documentation. The software also suggests additional safeguards.[25]

In the context of current efforts of the industry it is expected that Data Protection Supervisory Authorities do not require more from them as what is being managed by public stakeholders themselves. Saying, current ambiguity and uncertainty create an ostrich approach, especially by SMEs.

Acknowledging and endorsing that data subjects shall be protected adequately at all time, pragmatic

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

[21] https://eucoc.cloud/en/home

[22] SCOPE Europe b.v.b.a/s.p.r.l. was founded in February 2017 as a subsidiary of Selbstregulierung Informationswirtschaft e.V. (Self-Regulation Information Economy). It is an association supporting the co-regulation of the by acting as a think tank to discuss and debate key issues in digital policy and providing an umbrella organisation for a range of co-regulatory measures in the digital industry. In May 2021 SCOPE Europe became the first Monitoring Body to be accredited under the GDPR pursuant Article 41. More information can be found here: https://scope-europe.eu/en/home

[23] Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe, 19.05.2021, at: https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202116_eucloudcode_en.pdf

[24] https://www.bitkom.org

[25] https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Transfer-Impact-Assessment-TIA

approaches are appreciated, as well as openness to stakeholders' suggestions, which may allow for dynamic yet effective solutions. In this regard it is to be taken into account that a general resignation eventually provides less protection, as a general endorsement and implementation of good measures, even if such measures are allegedly perfect.

An area as complex as Third Country Transfers, as continuously evolving as legal frameworks, should rather seek for best effort solutions, and continuous improvement, acknowledging that true perfection does not exist. One should not limit the good for the sake of the (potentially never operationalised) better.

selbstregulierung
informationswirtschaft e.V.

About the Authors

The SRIW (Selbstregulierung Informationswirtschaft e.V.) is a non-profit association that was established in 2011 as an umbrella organisation, supporting credible self-regulation and co-regulation in the information economy. Focusing on, but not limited to, data and consumer pro-tection, the SRIW takes a modern regulatory approach that aims to align regulatory requirements with market realities and industry practicalities while protecting consumers interests.

The SRIW has been able to gain valuable practical experience on the extent to which different solutions and processes are at all amenable to economic implementation and approved by the Data Protection Supervisory Authorities.

Moreover, the SRIW has established a subsidiary in Brussels called SCOPE Europe . SCOPE Europe plays a crucial role in strengthening the European perception of the approaches advocat-ed by SRIW and also serves as an officially accredited Monitoring Body under GDPR by more than one Data Protection Supervisory Authority for more than one Code of Conduct.

First Operational Transnational Code of Conduct – Deriving Good Practices from Real Life Lighthouses

Being the first requires patience, but also provides opportunities to pave the ground for future initiatives: The EU Code of Conduct for Cloud Service Providers (EU Cloud CoC)[26] – the first transnational fully operational Code of Conduct under GDPR – foresees several principles, which might be considered good practices as of today. In other instances, real life experience by the EU Cloud CoC indicate what adapted approaches will likely become good practices in future.

Codes of Conduct require good and transparent governance, to ensure fair and balanced requirements. Codes of Conduct should also strictly distinguish between their material requirements and their administrative, i.e., governance, related elements. Whilst the accreditation of a Code of Conduct's Monitoring Body or even several Monitoring Bodies will require the establishment of a suitable framework in any case, core principles of the expected monitoring framework should already be set by the Code of Conduct itself.

To remain future proof a modular approach is recommended, as such an approach easily allows the extension by the provision for any future particularities in the context of a Code of Conduct's scope. Likewise, it may be suitable to foresee mechanisms that enable interlinks between several Codes of Conduct or other established standards and certifications.

1. Background

The origins of EU Cloud CoC's initiative date back to the days when the European Data Protection Directive was still in effect. Consequently, the efforts spent by the initiative were disproportionally high until the European Data Protection Board (EDPB) decided on its positive opinion[27] and subsequently the competent Data Protection Supervisory Authority published the official approval[28]. De facto, the EU Cloud CoC its contents and approach needed to be rethought several times during its development, as first the applicable legal framework changed, and later the EDPB's Guidelines particularized the expectations by Data Protection Supervisory Authorities.

Considering the experience of today, the EU Cloud CoC certainly could be developed faster. Nonetheless, the repeated challenge and need to adapt to a changing legal framework genuinely forced the EU Cloud CoC to implement approaches which may be considered as general good practice, today.

2. Flexibility is key; Evolving and Optimizing is the very fundament.

Considering the increasing complexity of the sector, which is addressed by a Code of Conduct, it is important to ensure that whatever provisions a Code of Conduct may foresee these remain easily and broadly adoptable. The following aspects appear most significant.

[26] https://eucoc.cloud
[27] https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202116_eucloudcode_en.pdf
[28] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf

2.1. Building upon the existing

As GDPR – even five years after it became effective – must still be considered a new legal framework there are still countless new and unresolved legal and practical questions. Some of them may have no related good practices at all; some others have already very supportive and broadly adopted good practices.

In case of the latter, a Code of Conduct must not design its requirements from scratch and in ignorance of any existing good practices. Codes of Conduct should rather endorse existing good practices.

Building upon existing practices will boost the adoption rate, as companies can utilize their investments of the past. Similarly, companies will easily understand a Code of Conduct's requirements and spend their limited resources most efficiently. There will also be more interest in further evolving internal practices if any such optimization will pay in for several compliance goals and good practices, as the return on invest increases. Eventually, the protection of data subjects is genuinely strengthened by intrinsic motivation.

Existing good practices may be loose but broadly adopted practices as they reflect customer needs, but they may also be codified in existing standards, certifications or even other GDPR Codes of Conduct. Integrating and mapping those existing approaches will also allow a Code of Conduct to focus on those elements, which require particularization and/or clarification under GDPR.

However, it should be noted that defining one or several existing standards, certifications or alike as mandatory should be avoided. On the one hand, any such requirement may unduly limit the accessibility especially for small and medium sized enterprises (SME). On the other hand, any such obligatory relation to a third-party framework may negatively affect innovative approaches and makes the Code of Conduct dependent on the continuous improvement by such third-party framework. Where a third-party framework will not evolve and adapt to recent developments, a Code of Conduct may end up trapped. Instead, it is recommended to refer to existing standards, certifications and alike as reference by which conformity will be presumed. However, companies must be provided with possibilities to implement alternative but yet similarly effective approaches, or even implement approaches that do better than existing good practices. [29)]

2.2. Remain principle-based, where possible

Related to the scope of a Code of Conduct, its level of particularization will differ. As current Codes of Conduct are still paving the way for such tools, it is not expected that Codes of Conduct will address very specific technical, or organisational means of implementation. However, where a sectoral need exist, Codes of Conduct might also define very distinct means of implementation.

Nonetheless, the majority of Codes of Conduct will most likely address sector-specific but still high-level needs. In this context, it is recommended that Codes of Conduct will be drafted in a principle-based fashion. The principle and expected result should be clearly defined, whereas the individual technical and/or organisational means of implementation are not finally determined. In such a way, Codes of Conduct foresee measurable respectively verifiable requirements, while they accept innovation and practical diversity.

However, Codes of Conduct do well in incorporating guidance and good practise examples alongside such principles. Such a combination ensures that any determination of conformity is based on solid and transparent grounds. Companies remain flexible

[29)] e.g., see Annex A of the EU Cloud CoC, https://eucoc.cloud/get-the-code

in their individual approaches, whilst Monitoring Bodies and stakeholders in general are provided with a substantial referential threshold.

2.3. Modularity

Understanding the need of a principle-based approach, processing activities within a sector and related legal and practical needs will continuously evolve. It is worth noting that not any of such needs will affect any stakeholder within a sector. Most likely, any sector can be subdivided into sub-sectors or processing activities only provided or affecting a subset of stakeholders.

In this vein, integrating any such particularities in one and the same Code of Conduct resulted in an unnecessarily complex set of conditional requirements. Such a complexity will most likely and adversely affect the adoption rate. Instead, it is recommended that a Code of Conduct foresees the extension by modules. A modular approach has several advantages compared to yet another independent Code of Conduct. Modules inherit the requirements of its related core Code of Conduct. Therefore, any evolution of the core will automatically and positively affect its modules. Vice versa, experiences by modules may also result in evolutions of the core as requirements originally drafted for a module might be integrated into the core, in future.

3. Integrating Good Governance and Monitoring Principles

At a minimum as relevant for the success of a Code of Conduct are its good governance and monitoring principles.

3.1. Good Governance

It is recommended that Codes of Conduct foresee a transparent and fair governance structure, by which it is safeguarded that relevant stakeholder's interests will be reflected and that requirements of antitrust and competition law will be respected.

Even though for the publication of a Code of Conduct it may appear handy to integrate such administrative respective governance related matters in one document, it seems more suitable to separate material and governance related elements. Such a separation will allow for an asynchronous evolution of the individual elements without confusing stakeholders that modifications in one section automatically comes along with modifications in the other section. The impression of the latter, e.g., can result from an iterative version numbering of the overarching file and none or only limitedly communicated changelogs.

3.2. Monitoring Principles

It is acknowledged that the independence of a Monitoring Body under Article 41 will require a certain degree of flexibility of such Monitoring Body to design its procedures and general monitoring framework.

However, it may also support a Monitoring Body's position towards stakeholders if key elements were already provided by the Code of Conduct. E.g., if key elements are principally defined, these elements cannot be subject to any individual negotiations. Likewise, several Monitoring Bodies cannot engage in a race to the bottom, to economically undercut their respective proposals, because the Code of Conduct will not provide for leeway to strike-out core activities from their daily operations.

Likewise, it will ensure foreseeability for stakeholders on the elements of a monitoring framework. The less a Code of Conduct provides, the more remains subject to the interpretation of the Monitoring Body and its related competent Data Protection Supervisory Authority to determine a suitable monitoring framework. The more details a Code of Conduct

incorporates the stronger a Monitoring Body can also defend its approaches towards the competent Data Protection Supervisory Authority, as the Monitoring Body will have to comply with the approved requirements of the Code of Conduct.

4. Key take-aways

Acting as a front-runner can be burdensome. Nonetheless, acting as a lighthouse and frontrunner also enables initiatives to come up with innovative approaches, as there is no blueprint to rest oneself.

The EU Cloud CoC needed to adapt several times to evolving conditions. Hereby, the EU Cloud CoC genuinely chose approaches which could be referred to a good practice for the development of Codes of Conduct in general, today. One of the approaches is certainly the modularity. The EU Cloud CoC will use such approach in near future, of which on module will address third country transfers.[30)]

EU CLOUD COC

About the Authors / the Project

Run by industry stakeholders, the EU Cloud Code of Conduct is an EDPB endorsed and legally operational transnational Code of Conduct that provides explicit guidance for cloud service providers to effectively incorporate the obligations specified in Article 28 GDPR. Successfully going through the EU Cloud CoC assessment serves as proof of compliance towards Data Protection Supervisory Authorities and cloud users.

This compliance tool was designed to accommodate businesses of various sizes, operating within different cloud service layers (XaaS).

What sets the EU Cloud CoC apart from other compliance solutions is the rigorous monitoring framework. SCOPE Europe is the independent monitoring body that oversees the assessment on a yearly basis. The primary objective of the EU Cloud CoC is to harmonize the implementation of GDPR requirements. So far, the EU Cloud CoC already represents the vast majority of the (European) cloud market, establishing itself as a benchmark for transparent services.

[30)] Please, note the Third Country Initiative by the EU Cloud CoC, https://eucoc.cloud/3rdcountryinitiative

GDPR 5th Anniversary – Past Challenges and Future Expectations

About the Author

SAP is one of the world's leading producers of software for the management of business processes, developing solutions that facilitate effective data processing and information flow across organizations. As the market leader in enterprise application software, SAP is helping companies of all sizes and in all industries run better by redefining ERP and creating networks of intelligent enterprises that provide transparency, resiliency, and sustainability across supply chains. SAP's end-to-end suite of applications and services enables our customers to operate profitably, adapt continuously, and make a difference worldwide. Interviewed was Mathias Cellarius, Head of SAP Data Protection & Export Control at SAP.

1. Introduction

In light of the 5th General Data Protection Regulation (GDPR) anniversary SAP, a member of Selbstregulierung Informationswirtschaft e.V. (SRIW), is sharing its experience with GDPR compliance challenges, how to overcome them as well as expectations on future GDPR improvement, with a specific perspective on codes of conduct.

1.1. The EU is celebrating the 5th anniversary of the GDPR. Should SAP celebrate, too?

The GDPR has been a great achievement by the European legislator. Since GDPR, we have a common set of rules across all Member States and the associated countries of the European Economic Area on how personal data may be processed. These rules are the basis for a free flow of data across the continent. This is a huge benefit for any company that is active or has business partners in more than one country, like SAP – which certainly makes us celebrate, too.

1.2. SAP is a global company. Given your experience and in your opinion, is the GDPR a global success?

The GDPR has set a global trend. Since the GDPR came into force, we have seen similar data protection laws in many countries around the world that have adopted the principles set out in this regulation. The GDPR has also spearheaded significant changes in the overall governance, awareness, and strategic decision-making regarding the use of personal data globally. The risk of incurring e.g. hefty fines has made companies manage risks relating to privacy and security more proactively.

The global impact is even amplified. Since only countries that meet the GDPR requirements can engage in cross border data flows with the EU, the GDPR prioritizes the right to privacy and personal data protection in those countries as well. For these reasons, the GDPR can be considered a global success.

1.3. Going back five years, what were the biggest challenges in implementing the GDPR for service providers? What challenges did SAP encounter specifically?

One of the major challenges certainly lies in the different requirements that a company must implement in various functions when collecting, processing and storing personal data. The GDPR is strongly focused on the protection of personal data and the data subject. Service providers must ensure that they have robust security measures in place for protecting the personal data they are processing or storing. To do so, they must implement appropriate technical and organisational measures such as encryption, access controls and regular security assessments. Meeting these requirements can be challenging, especially for providers that process significant amounts of data or operate in different jurisdictions.

Taking SAP as an example: SAP is a complex and permanently changing enterprise with suppliers, partners and customers around the world. Implementing comprehensive legal requirements to existing processes and products requires intensive stock taking, good planning and project management across the company.

In addition, the GDPR requires the implementation of certain principles applicable to SAP, whether SAP acts as a controller that collects and processes personal data for its own purposes or whether SAP acts as a cloud provider processing personal data of SAP customers. In order to implement these requirements, we work with many data protection and privacy professionals in the SAP entities across the globe and in various Lines of Business. This is a community of highly skilled and motivated colleagues. We cannot thank these colleagues enough for the work they do every day.

1.4. Why is GDPR compliance important for service providers and what is SAP's approach at ensuring trusted compliance?

Compliance goes beyond avoiding fines, it helps achieve overall business objectives. For example, a strong compliance management system makes the company attractive for investors. Further, if we want to retain our customers' loyalty and trust, we must offer Cloud services that enable them to be compliant with GDPR and other data protection and privacy requirements. GDPR compliance can provide a competitive advantage.

Complexities as mentioned before may also be a challenge. Challenges often result from ambiguities within the law and its application by different authorities across all member states. One way to successfully to address such challenges and to comply with GDPR are Codes of Conduct, pursuant to Article 40. These Codes of Conduct can provide practical guidance on how to handle personal data, promote accountability, and enhance transparency in data processing practices.

On the one hand SAP has been one of the first companies to have a certified data protection management system, managed by DPEC. On the other hand, we would like to emphasis, that our team was deeply involved in creating the EU Cloud Code of Conduct (EU Cloud CoC)[31], a standard approved by the European Data Protection Authorities and monitored by an accredited Monitoring Body, i.e., SCOPE Europe[32], by which Cloud providers can demonstrate the compliance of their Cloud services with the GDPR and overcome the challenges I mentioned before.

Our team works with SAP's Cloud Lines of Business at implementing the EU Cloud CoC. This is an important asset for our customers, too. In our experience, such a Code of Conduct does not only help service providers to substantiate compliance with the GDPR,

[31] https://eucoc.cloud
[32] https://scope-europe.eu

but also harmonises the protection of personal data across borders.

Therefore, we encourage Data Protection Supervisory Authorities to promote the development of Codes of Conduct, at both the national and transnational level, to standardise the protection of personal data in all relevant regulations.

1.5. Do you consider the GDPR future proof, specifically with respect to the use of artificial intelligence? Are changes to the GDPR needed?

The GDPR's risk-based approach is technology neutral and puts the rights of the individual, the human being, at the center of its rules. For example, the transparency requirement imposes standards on how personal data must be collected and processed and how a system produces certain results with such data affecting an individual's rights. Similarly, the rules on automated decision making require that, if a decision produces legal effects that significantly impact an individual (e.g., during the hiring process), such decision may not be solely based on automated means.

The rules of the GDPR remain highly relevant with respect to today's cutting-edge technologies. This doesn't mean that there's no room for improvement. The EU Commission recognizes this and is constantly monitoring the scope and implementation of the GDPR in close contact with stakeholders from all parts of our society. I can attest to this as I am a member of a multi-stakeholder expert group established by the Commission. The Commission has also announced its plans to conduct a deep dive revision in 2024.

The agnostic approach by the GDPR makes it very future proof, by principle. Challenges that come along with high dynamism in economy and society since the first drafts of the GDPR can be addressed by two main pillars. From a regulator's perspective following the review set by 2024; from a stakeholders perspective, saying industry, by co-regulatory measures such as codes of conduct.

1.6. Last question: What is your birthday wish for the GDPR? (Expectations)

The GDPR has set a benchmark for the processing of personal data beyond Europe. Data processing must always be to the benefit of individuals.

At the same time, we must foster an approach with innovation, technology, business and European competitiveness in mind while putting the necessary controls and balances in place to ensure that society will not be put at crossroads. Especially in the context of the current debate on Artificial Intelligence (AI) we must ensure that the debate isn't becoming too polarized, with each side dismissing the concerns of the other. An automatic negative connotation versus new technologies would be detrimental and only lead to us consuming services and solutions that are offered from other parts of the world. As little as we like the idea of having machines make decisions on our behalf, we must ensure we take conscious decisions on the right balance for the future of Europe.

We are not suggesting that we should be subjecting key issues around our human individuality and dignity to automated, algorithmic decision-making. Clearly, the individual is at the center of society and critical decisions must always remain under the control of a human being. However, in a world ruled by economic principles, our European values will only be able to prevail if we manage to translate them into clear and easy to follow rules that people understand and accept and that our businesses can easily implement and comply with rather than being stalled by fears of new technologies!

My wish is that this central focus on preserving the individuals' rights will continue to grow and evolve, under the GDPR and other data protection and privacy laws, while giving new technologies opportunity to further develop. The future of GDPR should ideally be both: human-centric and technology friendly.

A Blueprint for Future Tech Regulation

About the Author

eyeo is dedicated to empowering a balanced and sustainable online value exchange for users, browsers, advertisers and publishers. By building, monetizing, and distributing ad-filtering technologies, we create solutions that allow all members of the online ecosystem to prosper. Our ad-filtering technology powers some of the largest ad blockers on the market, like Adblock Plus and AdBlock, and is distributed through partnerships to millions of devices. We currently have 250 million global ad-filtering users who consent to Acceptable Ads, an independently derived ad standard that determines whether an ad is acceptable and nonintrusive. To learn more, go to www.eyeo.com

1. Background

Co-regulatory tools, like Codes of Conduct under GDPR, can become a successful, future-proof playbook for regulating emerging technologies and privacy while balancing legal requirements with a practical, sector-specific application of the law. With more Codes of Conduct being approved, European Small and Medium Sized Enterprises ("SMEs") will benefit.

2. 5 Years of GDPR: Take-Aways

With GDPR turning five, it is a good time to take a look back at how Codes of Conduct have been implemented since 2018, what this means for European SMEs, and what predictions can be intuited for the future. For eyeo, as a German, mid-sized company with 300+ employees and headquarters in Cologne, it comes down to four main take-aways:

First, Codes of Conduct are among the most relevant frameworks for SMEs to underline their compliance efforts with GDPR. The particular mention of "specific needs of micro, small and medium-sized enterprises" in Article 40.1 GDPR underlines the intention, desire and mandate of the regulator to have a tool in place that caters to the needs of smaller organizations and entities. This seems especially relevant in the technology sector, which is prone to an imbalanced playing field between very large and powerful platforms and smaller, often European, start-ups and scale-ups. The adoption we have seen so far of transnational and national Codes of Conduct pursuant to Articles 40, 41 GDPR gives hope that more and more SMEs will benefit from these schemes. Future approvals of Codes of Conduct related to different sectors and different processing activities will underline these efforts.

Second, we have experienced an increased importance of technological solutions that incorporate privacy and data protection fundamentals in their systems, often referred to as privacy-enhancing technologies or privacy tech. Such solutions, like differential privacy, data masking techniques or federated learning, can play a crucial role in creating a more private, user-centric web. Especially in the field of online advertising, we see many promising privacy-enhancing technologies that aim to replace the status quo of targeted advertising as we know it today by, for instance, creating cookie-free, privacy-enhanced models based on interest-based advertising. However, these emerging privacy tech solutions generally lack proof of their compliance to the legal requirements of GDPR. Hence, we see a strong potential for Codes of Conduct to become the appropriate tool to underline how privacy tech solutions meet the requirements of GDPR; for instance, in the field of pseudonymization, anonymization, or other privacy-by-design frameworks.

Third, we believe Codes of Conduct are an important puzzle piece when it comes to emerging technologies and how privacy requirements can be met going forward. GDPR's fifth birthday is a good point in time to think about how technological advancements have changed since the regulation was adopted in 2018: disruptive technological advancements, for example in the fields of generative artificial intelligence, facial recognition, or machine learning, underline how new inventions - which we did not foresee or factor in five years ago - significantly affect the data protection regimes in Europe today. In this context, Codes of Conduct can flank regulatory oversight by establishing new co-regulatory frameworks for emerging technologies.

Fourth, and finally, we at eyeo believe in balance. It is at the core of our products, which are dedicated to empowering an equitable and sustainable online value exchange for users, browsers, advertisers and publishers. Similarly, a Code of Conduct is a co-regulatory framework that incorporates balance between the clear regulatory requirements - as given by the law itself and ensured during the approval procedures of the supervisory authorities - and the actual practical use cases and data processing environments of organizations which prepare a particular Code of Conduct. Going forward, we believe this balanced approach can ensure that the requirements of GDPR are reflected, while allowing a sustainable and sector-specific application of GDPR for organizations adherent to Codes of Conduct.

The Necessity and Potential of Privacy Codes of Conduct for a Functioning Data Protection Framework – A case study

About the Author

Bitkom represents more than 2,100 companies of the digital economy. Through IT- and communication services only, our members generate a domestic turnover of 190 billion Euros per year, including 50 billion Euros in exports. Members of Bitkom employ more than 2 million people in Germany. Among the members are more than 1,000 small and medium-sized businesses, over 500 startups and nearly all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the sectors of digital media or are in other ways affiliated to the digital economy. 80 percent of the companies' headquarters are located in Germany with an additional 8 percent each in the EU and the USA, as well as 4 percent in other regions. Bitkom supports the digital transformation of the German economy and advocates a broad participation in the digital progression of society. The aim is to establish Germany as globally leading location of the digital economy.

Codes of Conduct are an important part of the framework of the GDPR and one element to facilitate and demonstrate compliance with the legislation. They can also serve as guidelines, to promote best practices and improve legal certainty for controllers on how to implement the GDPR´s requirements while at the same time lessen the burden the Data Protection Authorities have to carry. Seemingly a win – win -win, right?

Five years after the GDPR entered into force, however, there are too few Codes of Conduct available in the market. And while industry stakeholders and Data Protection Supervisory Authorities are always claiming to promote the concept, especially the recent Guideline on administrative fines, lacking funding and personnel for the Data Protection Supervisory Authorities, unclear competences and lengthy negotiations and procedures before a Codes of Conduct can be approved are hindering the development and launch of much needed Codes of Conduct.

In our view, especially EU-wide Codes of Conduct should be supported and promoted more prominently and the conditions for the approval of such Codes of Conduct should be streamlined to achieve more scale and more consistent protection across Europe. Seeing that one of the major unkept promises of the GDPR is harmonization[33] due to different interpretation of the GDPR rules (and, of course, a lot of member states laws that were kept in place), Codes of Conduct could help streamline interpretation and implementation of rules. This in turn would increase legal certainty, free up time, money and data protection experts in Europe to concentrate on much more important and pressing tasks regarding Europe's privacy framework.

This article and case study focuses on the experiences while developing the Code of Conduct for Pseudonymization ("The Code") – a project that was introduced as an idea from the German Digitalgipfel in 2019 and developed into a Code of Conduct by

[33] https://www.bitkom.org/EN/List-and-detailpages/Press/Five-years-GDPR

GDD and Bitkom in cooperation with Selbstregulierung Informationswirtschaft and the SCOPE Europe.[34)]

1. Drafting the Code

1.1. The Code's origins

The idea to start a project for developing a draft for a GDPR Code of Conduct for Pseudonymization was formed as part of the German Digitalgipfel in 2019 in the Focus Group Data Protection.[35)]

All members of the focus group agreed that pseudonymization contributes to ensuring that users' personal rights are protected and GDPR compliance is achieved. But the techniques and management systems to operationalize pseudonymization were still elusive. Transparent guidelines for controllers and operators on how to implement pseudonymization were therefore one of the cornerstones of the draft.[36)]

1.2. The Code's objectives

The objective of the draft Code was to formulate, in accordance with Article 40.2 (d) GDPR, concrete rules of conduct for data protection-compliant pseudonymization. Pseudonymization was chosen as the subject matter due to its immense potential for the protection of users' data and the importance for data protection compliant processing, as the concept protects data subjects from unintentional identification and is an implementation of the data minimization principle. It also is one of the technical and organizational measures in accordance with Articles 25 and 32 GDPR. Additionally, it influences the lawfulness of the processing of personal data, as Article 6.4 (e) GDPR shows. It thus fulfils both a protective as well as an enabling function.

Pseudonymization is characterised by the fact that personal data is processed in such a way that the data can no longer be attributed to a specific person without additional information (see Article 4 No. 7 GDPR). The GDPR does not contain, however, any technical or organizational information or guideline on how a pseudonym can be created, nor does it provide information on possible protection measures with regard to the pseudonym created. For this purpose, this Code needed to define both procedural and organizational and technical requirements.

1.3. Industry Leads the Code's Finalization

Following the Digitalgipfel in 2019, the GDD ("Gesellschaft für Datenschutz und Datensicherheit e.V.")[37)] and Bitkom e.V.[38)] have developed the Code based on the preparatory work of the expert group bringing together several experts from different sectors, data protection specialists and specialists on monitoring from SCOPE Europe.

Members of the team that developed the Code included organisations from various sectors which process – among other types of personal data - pseudonymised data on a regular basis. Such sectors included health, telecommunications, finance or advertising. At the same time, GDD and Bitkom included processors according to Art. 4.8 GDPR which are processing pseudonymised data on behalf of Controllers as well as vendors developing software to pseudonymised personal data.

This inclusive approach guaranteed that different business models and processing techniques and necessities were properly addressed so that the Code can ve used by a wide variety of organizations while also formulating balanced requirements that took practical issues into account. It was also designed for

[34)] https://www.bitkom.org/sites/main/files/2020-08/20200825_mitteilung-und-status-quo-coc_pseudonymisierung.pdf

[35)] The Focus Group consists of a variety of data protection stakeholders, including Data Protection Supervisory Authorities, public authorities, as well as private companies and associations from the private sector.

[36)] https://www.bitkom.org/sites/main/files/2019-12/20191210-coc-pseudonymisierung-digitalgipfel-2019.pdf

[37)] https://gdd.de

[38)] https://bitkom.org

EU-wide adoption, because one of the underlying goals was and is the harmonization of GDPR's requirements related to pseudonymization to improve user's trust and give organizations more legal certainty.

2. The Code's concept

The Code is a transnational Code of Conduct, meaning that it addresses processing activities in more than one Member State. Likewise, the Code was also developed to cover processing activities regarding data subjects from different Member States. In fact, it is expected, that the Code will be applicable to processing activities and benefit, respectively data subjects, in any Member State.

The Code's approach is intentionally broad. This was discussed at length in the working group that developed the Code and was also subject to some discussions with different Data Protection Supervisory Authorities in the development process. The experts of the group agreed that pseudonymization is a key strategy of the GDPR to facilitate data processing and/or to protect data subjects. Limiting the Code to only one Member State or any limited selection of Member States would unnecessarily, and adversely restrict the Code's positive impacts and hinder the harmonizing effect.

The Code is also intentionally wide regarding its material scope and applies to controllers and processors, regardless of their industry or sector, provided they pseudonymize personal data themselves in accordance with the requirements of the GDPR or provided they are responsible for the pseudonymization process. This broad understanding of a sector is generally supported by the GDPR and, e.g., explicitly mentioned in the European Data Protection Board's Guidelines on Codes of Conduct as a tool for transfers.[39)]

The Code provides a comprehensive approach and much needed clarifications by defining a verifiable management process that covers the whole cycle of data processing. The Code enforces a documented balancing of interests and decision making based on a pre-determined checklist of relevant matters and aspects. As the Code takes a management process approach, it is neutral to the specific context or sector of the pseudonymization process.

At the same time, pseudonymization is applied in uncounted contexts, of which several are subject to additional regulations. Whilst detailed provisions per-context might - at first sight - appear more appropriate, research and discussions with relevant stakeholders have proven the need for an understanding of general requirements: As long as general requirements and interpretation of pseudonymization are not developed, any interest in defining context-specific, further-detailed requirements is exponentially decreasing. Recent work on developing a Code of Conduct for Anonymization has proven the same: As long as no "baseline" is established, sector specific Codes of Conduct are nearly impossible to develop, both in general and more specifically in a way that allows for later - much needed - interoperability with other sector-specific Codes of Conduct on the same or related aspects.[40)]

To take the requirements and technical specificities of sectors into account, GDD and Bitkom agreed to constantly review the application of the Code, likewise by opertional feedback as well as public, political, judicial, authoritative, and academic discussions and developments. Where necessary, both organizations are considering to extend the Code in future.

3. Status quo and current issues

The draft work for the Code was concluded in 2021 and since then GDD, Bitkom and SCOPE Europe were

[39)] EDPB Guidelines 04/2021, para. 6, in their version of July 7th, 2021.

[40)] On the Anonymization of data, see the preparatory work done by the Expert Group of Stiftung Datenschutz, that also formulated a baseline: https://stiftungdatenschutz.org/praxisthemen/anonymisierung

in contact with representatives of Data Protection Supervisory Authorities regarding the formal process to launch the Code.

There are several aspects to be considered in determining the competent Data Protection Supervisory Authority.

Besides others, competence may relate to the residence of the Monitoring Body. GDD and bitkom, both being registered in Germany, have analysed the market of suitable Monitoring Bodies in Germany, concluding that - back in 2021 - there is no suitable Monitoring Body in Germany – especiella due to the international scope and overarching nature of the Code. The decision to appoint SCOPE Europe as the Monitoring Body took that international view and application into account. SCOPE Europe has already received an accreditation for a transnational Code of Conduct, thus proven to have the expertise and generally required set-up to monitor a transnational Code of Conduct. Likewise it is considered supportive for a transnational Code of Conduct to be related to Brussels, as Brussels is considered Europe's headquarter. SCOPE Europe is also used to international Customers/Code-signatories, which are also expected for this Code. To ensure that the approval and the accreditation process do not fall apart, GDD and Bitkom wanted to submit the Code to the Autorité de protection des données as competent supervisory authority.

The expertise of the Data Protection Supervisory Authority is also considered a relevant factor. The Autorité de protection des données has proven expertise in handling transnational Codes of Conduct as well as handling Codes of Conduct addressing a complex matter. Therefore, Bitkom as well as GDD concluded that the Autorité de protection des données should be the competent Data Protection Supervisory Authority for the approval of the Code.

Considering the European Data Protection Board's guidelines, the compentency of the Data Protection Supervisory Authority appears sufficiently and unambigously argued. However, dissent was apparently formed between the different Data Protection Supervisory Authorities after the Autorité de protection des données started the consultation process within the European Data Protection Board, bringing the whole project to a temporary halt in 2022.

4. Expectations and Greater Picture

Seeing how few Codes of Conduct were approved in the more than five years since the GDPR entered into force, how important the Code would be for practitioners and how relevant a uniform interpretation of the GDPR is, it is more than a little incomprehensible why Data Protection Supervisory Authorities are hindering the efforts of launching new Codes of Conduct in the EU. All Data Protection Supervisory Authorities should collaborate to strengthen this important instrument and foster a system for GDPR implementation and enforcement in the EU that includes Codes of Conduct – rather than pushing them out of the market.

It is essential to underline the added value of complementary enforcement mechanisms, such as those established by Codes of Conduct and Monitoring Bodies. The Code for Pseudonymization, as well as all other Codes with a transnational scope, cover processing activities across several member states and can effectively support the uniform application of GDPR requirements and consistent enforcement.

In light of the growing regulatory landscape that Data Protection Supervisory Authorities will have to supervise or be consulted about when personal data is being processed (e.g. EU Data Act, Digital Services Act, AI Act etc.), such additional enforcement and oversight mechanisms will have to be strengthened

to support the Data Protection Supervisory Authorities in their tasks and streamline their processes. Codes of Conduct have several advantages for GDPR enforcement and provide legal certainty for controllers and processors. They also strongly support harmonization across Europe, by allowing for particularizing ambiguous interpretations in sector-specific manners. The enforcement of Codes of Conduct complements the public actions and may significantly increase GDPR compliant yet practical implementations. Another added value is the compulsory oversight by independent Monitoring Bodies that allows for additional robust enforcement. Required continuous communication between Monitoring Bodies and Data Protection Supervisory Authorities may establish exchange of first-hand experiences, fostering consistent, robust yet practical application of the law.

The next five years of GDPR implementation should therefore include some action in this regard: Firstly, strengthening the development and launch of Codes of Conduct by supporting them EU-wide without tussle for competences as long as the legal requirements for choosing a competent authority are met, and secondly, recognizing Codes of Conduct effectively in the administering of fines[41)].

[41)] Current Guidelines on the administration of fines can be misleading and suggest an interpretation, that a breach of a Code of Conduct can lead to increased fines. The exact opposite should be clearly stipulated in the official Guidelines of the EDPB: Adherence to a Code should generally be considered as a mitigation factor.

selbstregulierung
informationswirtschaft e.V.