GIS Odyssey Journal

2022 • Volume 2 • Number 2

https://doi.org/10.57599/gisoj.2022.2.2.129

Piotr Drobek[1]

THE ROLE OF CODES OF CONDUCT IN THE EU DATA PROTECTION FRAMEWORK

Abstract: The paper presents the legal nature and functions of codes of conduct in EU data protection law. The General Data Protection Regulation (GDPR) contains much more extensive provisions on codes of conduct than previous Directive 95/46/EC, giving them a potentially much more significant role in the EU data protection regime. The GDPR specifies codes of conduct as co-regulatory instruments whose compliance by controllers and processors has significant legal consequences. They are primarily intended to facilitate compliance with the GDPR by controllers and processors from a specific sector or to perform similar processing operations. It is, therefore, essential to identify the legal nature of the codes of conduct, the legal consequences of adhering to them, and their function in the EU data protection model. The theoretical analysis of EU data protection codes of conduct considers legal and regulatory theory perspectives.

Keywords: accountability, data protection, GDPR, code of conduct, co-regulation

Received: 30 November 2022; accepted: 16 December 2022

[1] Cardinal Stefan Wyszyński University in Warsaw, Faculty of Law and Administration, Department of Informatics Law, ORCID ID: https://orcid.org/0000-0002-0178-851Xe, mail: p.drobek@uksw.edu.pl

Introduction

The General Data Protection Regulation (GDPR) was adopted in 2016 after four years of intensive legislative work. As an EU regulation, this legal act has been directly applicable in all EU member states since May 25, 2018. The reform of the personal data protection framework in the EU was carried out under the slogan of strengthening basic principles regarding data processing, strengthening the rights of data subjects, and adapting specific legislative solutions to the fast-moving environment of data processing. The purpose of the reform was to ensure the effectiveness of personal data protection law. The new regulations moved away from a descriptive specification of obligations favouring principle-based regulation. The accountability principle has become central to this new model of data protection. According to it, controllers must operationalise general data protection principles. The second key element is the risk-based approach permeating the GDPR. The regulatory model adopted by the EU justifies reaching out to regulatory theory scholarship. Often the process of adoption of the GDPR is framed as at least partly shifting from a traditional command-and-control model of regulation to meta-regulation (e.g. Gellert 2020). Meta-regulation approach can be understood as a situation in which regulators do not specify how the regulated organisations have to comply with standards but require them to create their own system of ensuring compliance and demonstrate it to regulators (Black, 2012). Meta-regulation expects that regulated organisations will identify risks, put in place an internal control system, and continuously evaluate the effectiveness of implemented solutions and improve them (Gilad, 2010). Karen Yeung and Lee A. Bygrave (2022) presented a more nuanced view of GDPR. According to them, the GDPR contains both legal norms specified in a traditional way (as a command and control), design regulation and meta-regulatory elements exemplified by codes of conduct. GDPR gives codes of conduct a potentially much more significant role in the EU data protection regime. It is, therefore, necessary to examine the legal nature of the codes of conduct and their function in the EU data protection model in light of the evolution of the legislation in this field.

Material and Methods

This paper presents the results of the research carried out using the desk research method involving analysis of EU and national legal acts, policy documents, including documents of the European Commission, reports on the implementation of the EU data protection legislation and opinions and Guidelines adopted by the Article 29 Working Party on data protection and European Data Protection Board. The available scientific literature on law and regulation relevant to analysing data protection codes of conduct was also examined.

Regulatory theory perspective

The codes of conduct under EU data protection law are often categorised as self-regulation (Góral & Makowski, 2018; Fajgielski, 2018) or enhanced self-regulation tools (Medzini, 2021). The regulation is generally understood as "any public means of control over an activity that is essentially lawful but which the state wishes to be undertaken subject to certain constraints" (Hodges, 2015). According to paragraph 3.2 of the Opinion of the European Economic and Social Committee on Self-regulation and co-regulation in the Community legislative framework, self-regulation "broadly denotes the adoption by economic operators of certain rules of conduct among themselves or in relation to third parties in the market and in society, adherence to which is agreed among themselves, without any external coercive mechanisms". Such voluntary and flexible rules are based on the identical interests of the actors in the given sector rather than on state coercion (Csink & Mayer, 2014). Examples of such regulations initiated and undertaken by those whose behaviour is to be regulated are unilateral codes of conduct, customer charter, negotiated code, and unilateral sector codes (Hodges, 2015).

European Economic and Social Committee, under paragraph 3.4 of its opinion mentioned above, indicated that the term co-regulation means "a form of regulation of stakeholders that is promoted, guided or controlled by a third party which is either an official body or an independent regulatory authority, normally with oversight and monitoring powers and in some cases with the power to impose sanctions" (2015). Unlike self-regulation, co-regulation involves some degree of direct government involvement (Hodges, 2015). However, even when regulation is required by law, it is usually enforced by the industry itself. Nonetheless, professional or state regulators accept codes of conduct as a result of cooperation (Csink & Mayer, 2014). Cooperation understood in this way does not mean that the data protection code of conduct is a kind of "contract" between its owners and DPA (Drobek, 2019).

Considering how codes of conduct are addressed in EU legislation, it should be noted that they are a co-regulation that aims to facilitate the application of laws. The same is true concerning the protection of personal data.

Evolution of the legal landscape

The General Data Protection Regulation (GDPR) introduces broader and more extensive provisions on codes of conduct than those previously provided in Directive 95/46/EC. They are in line with the European Commission's announcement of further support for self-regulatory initiatives and, in particular, the promotion of codes of conduct. As European Commission pointed out, such initiatives "can contribute to a better enforcement of data protection rules"(European Commission 2010). Directive 95/46/EC referred to codes of conduct in Article 27 in general terms. The Member States and the Commission were primarily to encourage trade associations and other bodies representing other categories of controllers to develop codes of conduct (Article 27(1)). These instruments were intended to contribute to properly implementing the data protection legislation taking into account the specific features of the various

sectors. Directive 95/46/EC referred separately to national and Community codes without indicating criteria to distinguish the two types from each other. A draft national code of conduct or a draft amendment or an extension to an existing code of conduct was to be submitted for an opinion to the national supervisory authority, which could assess whether the draft code complied with national data protection legislation implementing Directive 95/46/EC (Article 27(2)). With regard to the Community code of conduct, at the EU-level opinion was issued by the Article 29 Working Party on data protection (Article 29 Working Party), an independent advisory body composed of representatives of national supervisory authorities (Data Protection Authorities or DPAs) from the EU Member States, the European Data Protection Supervisor and the European Commission. In addition, a role was also envisioned for the European Commission in ensuring that approved Community codes were properly publicised (Article 27(3)).

According to the European Commission, the provisions mentioned above of Directive 95/46/EC "have rarely been used so far and are not considered satisfactory by private stakeholders" (European Commission 2010). Indeed, only a few community codes have been approved. In 2003 the Article 29 Working Party positively assessed the Community code of conduct on direct marketing submitted by the Federation of European Direct and Interactive Marketing (FEDMA) (WP 29 2003), and later in 2010, the On-line marketing Annex to this code (WP 29 2010). The Article 29 Working Party issued a working document on Recommended Practice 1774 – Protection for privacy and transborder data flows of personnel used in international air transport of passengers and of cargo submitted by the International Air Transportation Association (IATA), recognising that this is not a Community code of conduct in the meaning of art. 27 of Directive 95/46/EC (WP 29 2001). In other cases, the Article 29 Working Party did not approve the submitted codes (WP 29 2008, WP 29 2009, WP 29 2015, WP 29 2018).

In its first report on the implementation of Directive 95/46/EC in 2003, the European Commission expressed disappointment that so few organisations had submitted sectoral codes of conduct for approval at the community level (European Commission 2003). The industries, however, drew attention to the slowness of the proceedings and the minuteness of the Article 29 Working Party's analysis of the submitted Community codes (Kantar, 2010). Another problem was related to Article 27(3) of Directive 95/26/EC, which requires that Community Codes ensure compliance with national data protection laws. As a result, more than mere compliance with Directive 95/46/EC, due to differences in its implementation, was needed, and additional adaptation to the legal requirements of each member state was required. Christopher Kuner, addressing this problem, postulated that the Article 29 Working Party, in such a situation, "should not insist on the continued application of every provision of national law in addition to the code" (2007).

An interesting potential problem regarding the paragraph mentioned above of Article 27 was raised by Carl Vander Maelen (2020). He argued that this paragraph makes the submission of a Community code for review by the 29 Working Party optional. Consequently, given the risk of a negative opinion on the code, the provision

creates a free-rider scenario in which organisations that have not submitted their codes for opinion may be in a better position than organisations that have submitted their codes in good faith to the 29 Working Party.

There were many more codes of conduct in operation at the national level. However, researchers stressed the wide variation in national regulations on codes of conduct, their application in practice, and, consequently, the varying popularity of such tools in different countries (Robins et al., 2009). The nature and role of codes of conduct and their possible legal effects in data protection systems have been understood differently. For instance, in the Netherlands, "approval" of a code by a supervisory authority was not binding on the courts, while in Ireland or Greece, codes could be more formally incorporated into the legal system and become legally binding (LRDP KANTOR Ltd, 2010; Vander Maelen, 2022; Korff, 2003). In Poland, the Act 1997 did not directly refer to codes of conduct and thus did not provide any procedure for their approval. Despite this, the Polish supervisory authority took steps to initiate the preparation of codes of best practices and informally accepted them after early and often intensive consultations within its general competence. Such codes did not introduce any mechanisms for enforcing compliance with their provisions by those who adhered to them. It should be added that they had no binding force.

Remarkable that, according to industry representatives, supervisory authorities seemed less interested in reaching a consensus on data protection practices with the industry and more interested in unilaterally imposing their own set of rules. There was also pointed to insufficient resources devoted to promoting and assessing codes of conduct for some supervisory authorities (Robins et al., 2009). There has also been tension between organisations and supervisory authorities (Korff, 2003) related to tense expectations and, to some extent, mistrust.

GDPR, as previously announced by the European Commission, seeks to increase the role of codes of conduct in the new EU data protection architecture and also respond to the failure of the regulations contained in Directive 95/46/EC. The codes of conduct are regulated in Articles 40 and 41 of the GDPR. Other provisions of the regulation also refer to them. The personal scope of the codes has been expanded to include not only controllers but also processors. Their material scope has been tightened by indicating examples of areas of possible regulation, the roles of all actors involved have been clearly defined, and procedural issues have been provided for to the extent necessary. The EU legislator has placed a firm emphasis on ensuring the operation of effective compliance monitoring mechanisms, including the existence of accredited monitoring bodies. At the same time, the attempt to counteract the fragmentation of regulation through mechanisms for the approval of transnational codes and to ensure consistency with the requirements for accreditation of monitoring bodies should be emphasised.

According to Article 40 (1) GDPR, a wide range of actors like the EU Member States, the supervisory authorities, the EDPB and the European Commission are required to encourage the drawing up of codes of conduct intended to contribute to the proper application of GDPR, "taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises". Codes of

conduct, amendments or extensions to such codes may be prepared by associations and other bodies representing categories of controllers or processors. The purpose of the codes was defined as specifying the application of GDPR. Among the examples listed of possible areas to be covered by the codes are the following, such as with regard to:

- "fair and transparent processing;
- the legitimate interests pursued by controllers in specific contexts;
- the collection of personal data;
- the pseudonymisation of personal data;
- the information provided to the public and to data subjects;
- the exercise of the rights of data subjects;
- the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
- the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;
- the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;
- the transfer of personal data to third countries or international organisations; or
- out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79".

The draft code, amendment or extension must be submitted to the competent supervisory authority under Article 55 GDPR. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with and shall approve it if it finds that it provides sufficient appropriate safeguards (Article 40 (5)). Where a draft code of conduct relates to processing activities in several Member States, the competent supervisory authority shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the EDPB, which shall provide an opinion on whether the draft code, amendment or extension complies with GDPR or, where the is a tool for international transfers provides appropriate safeguards. Where the EDPB's opinion confirms that the draft code, amendment or extension complies with this GDPR or provides appropriate safeguards for international transfers, the EDPB shall submit its opinion to the Commission. According to Article 40 (9) GDPR, the European Commission may, by implementing acts, decide that such approved code of conduct, amendment or extension has general validity within the EU under the examination procedure set out in Article 93(2). The European Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity (Paragraph 9). Approved transnational codes of conduct having general validity may also be adhered to by controllers or processors that are not subject to GDPR in order to provide appropriate safeguards for personal data transfers to third countries or international organisations under the terms referred to in Article 46(2)(e). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards,

including with regard to the rights of data subjects (Paragraph 3). Except for codes covering the public sector, accredited monitoring bodies must monitor controllers' or processors' compliance with approved codes of conduct under Article 41 GDPR. The Monitoring bodies' competencies are without prejudice to the tasks and powers of the competent supervisory authorities.

In order to clarify the provisions in question, the European Data Protection Board adopted Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 Version 2.0. The guidelines clarify procedures and rules related to the submission, approval and publication of codes of conduct at national and European levels. They also specify the conditions that must be taken into account by supervisory authorities when assessing whether a submitted draft code of conduct is correct and whether it contributes to the effective application of the GDPR. At the same time, the guidelines clarify the conditions that must be met by monitoring bodies. In addition, the EDPB clarified that all previously approved codes of conduct must be reviewed and approved again under the GDPR. The EDPB adopted several opinions on the draft accreditation requirements for monitoring bodies submitted by national supervisory authorities (see more at: https://edpb.europa.eu). The primary role of the EDPB is to ensure consistent application of the GDPR. Therefore, these opinions contribute to a harmonised approach concerning drafting national accreditation requirements for monitoring bodies. As a result, at the national level, supervisory authorities have already approved various codes of conduct or are still in the evaluation process. Significantly, the EDPB has already given a positive opinion on two transnational codes on cloud services (2001a, 2001b). In this regard, it was hoped that this approval of the two codes could set the path for faster adoption of future codes in various fields, keeping in mind that a positive opinion is only the beginning of the path for the actual operation of these codes in real life (Vander Maelen, 2021). After more work, the EDPB adopted the European Data Protection Board Guidelines 04/2021 on Codes of Conduct as tools for transfers Version 2.0. These guidelines complement the previously mentioned EDPB guidelines on Codes of Conduct and Monitoring Bodies. They clarify the actors' roles in drawing codes of conduct intended to serve as a tool for data transfers to third countries. Such codes of conduct under Article 46 GDPR should address the core principles, rights and obligations under the GDPR and specific safeguards required in the data transfer context. The guidelines provide a checklist of elements to be included in a code of conduct intended for data transfers. The EDPB also indicated that depending on the original scope and content of the code of conduct, it may need to be amended to cover all of the above issues necessary for data transfers to third countries.

The codes of conduct were also referred to in the first evaluation of the application of the GDPR on the EU level. Multistakeholder Expert Group established by the European Commission confirmed that micro, small and medium-sized enterprises recognise the value of codes of conduct in helping them comply with the GDPR and recommended drawing up a test to assess whether the codes take into account the needs of SMEs (2019). The European Commission, in its Communication, among other things, focused on supporting the establishment of code(s) of conduct that would contribute to a more

consistent approach, especially in health scientific research area and make the cross-border processing of personal data easier in this field (2020).

The Concept of a Data Protection Code of Conduct

The EU law recognises codes of conduct in different areas (Kamara, 2020). The relatively large number of 7149 documents containing the phrase "code of conduct" in the EUR-lex search results might prove this view's accuracy. Still, such a quantitative analysis may lead to erroneous conclusions since even a cursory examination of the documents retrieved shows that the term is used inconsistently in very different contexts and has a distinct legal character. Furthermore, how codes of conduct are regulated varies from one piece of EU legislation to another. In most cases, these legal acts do not define the concept itself, of which the GDPR is just one example.

In contrast, Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market contains a code of conduct definition. According to Article 2(f), it is "an agreement or set of rules not imposed by law, regulation or administrative provision of a Member State which defines the behaviour of traders who undertake to be bound by the code concerning one or more particular commercial practices or business sectors". As we can see, the definition is embedded in the specifics of consumer protection law and can be helpful for this paper only to a limited extent, as data protection codes of conduct go beyond commercial practices or business sector activities. Nonetheless, the broader implication of this definition is that a code of conduct is a set of rules of behaviour that members who voluntarily join it undertake to follow.

It may also be helpful to refer to the existing body of academic work, bearing in mind that scholars do not understand this concept uniformly. However, we can identify some common definitional elements of the concept. The Black's Law Dictionary defines this term as "a written set of rules governing the behaviour of specified groups, such as lawyers, government employees, or corporate employees" (1999). Similarly, codes of conduct embody "a set of rules for employees, members, or member organisations to follow" (Bennet & Raab, 2006). Carl Vander Maelen proposed a more comprehensive operational definition reads as follows: "codes of conduct aim to stipulate the desirability of a certain conduct by States, international or non-governmental organisations or private associations and persons, with codes aimed at corporations specifically seeking to enhance the accountability of such corporate actors in the (international) marketplace by defining voluntary standards and principles to steer the behaviour of similar types of enterprises (i.e., a certain sector)" (2020).

Based on the previous findings, we can identify the following conceptual elements according to which a code of conduct:

(1) sets out expected rules of behaviour for its adherents, who undertake to be bound by them;

(2) targets a homogeneous group of businesses, other organisations, or specific sectors;

(3) is voluntary;

(4) can be adopted by different organisations or bodies as owners of the code;

(5) serves to increase the accountability of adherents and influence their behaviour.

The privacy and data protection literature broadly divides codes of conduct by their scope into five categories: organisational, sectoral, functional, technological, and professional (Bennet & Raab, 2006).

The organisational code is an instrument implemented within the structure of a given private or public organisation, especially in more complex organisations. Such a code will not be a code of conduct in the sense of Article 40 GDPR but rather as a type of data protection policy referred to in Article 24 GDPR or binding corporate rules. For clarity, let us refer to the definition of binding corporate rules provided in Article 4(20) GDPR. According to it, these are "personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity."

On the other hand, sectoral codes will undoubtedly be codes of conduct within the meaning of Article 40 GDPR. The EU data protection law will mainly consider such codes as codes of conduct. It is worth emphasising that the distinguishing feature of sectoral codes is "that there is a broad consonance of economic interest and function among organisations in the sector, and by extension, a similarity in the kinds of personal information processed (Bennett & Raab, 2006). The concept of codes of conduct under Article 40 of GDPR will also include another category of codes mentioned by both authors, namely functional codes, the scope of which covers homogeneous data processing practices without being limited to one sector (EDPB 2019). For example, such codes may focus on various sectors' marketing activities, HR, or children's data processing (EDPB 2022). Another category relates to technology. As Bennet and Raab pointed out, technology codes deal with privacy and data protection issues associated with using new technologies. In practice, such codes, while often referring to a specific technology, cover homogeneous data processing operations. Therefore, they may be difficult to distinguish from functional codes, and the scope of Article 40 GDPR may also cover such. The last category refers to codes developed by professional societies or associations for professionals directly involved in data processing operations, such as market researchers (Bennett & Raab, 2006). This category, under certain conditions, could also qualify as a code of conduct under Article 40 of the GDPR.

Based on an analysis of the GDPR provisions on codes of conduct in terms of their scope of application and function, we can provide the following typology of data protection codes of conduct:

- National codes applicable in one Member State;
- Transnational codes;
- Transnational codes having general validity;
- Transnational Codes have general validity applicable to international transfers.

Nevertheless, first and foremost, we should divide codes into national and transnational. The EDPB has clarified that a transnational code refers to data processing activities in more than one Member State (2019) in contrast to a national code, which relates to processing activities in only one Member State. One should emphasise that cross-border processing under Article 4(23) is unnecessary for a code to be considered transnational (EDPB 2019). It will be sufficient for such a code to cover processing operations carried out by entities in the separate Member States.

The European Commission may make a transnational code universally valid within the EU through an implementing act. Adopting such an implementing act by the European Commission is a prerequisite for the code of conduct to be used for data transfers to third countries under Article 46 of the GDPR.

Although codes of conduct are often equated exclusively with the private sector, the GDPR does not limit the application of codes of conduct to that sector. However, Article 41 GDPR distinguishes public sector codes of conduct from private sector codes by excluding, in the former case, provisions for monitoring bodies of codes of conduct. This exclusion does not in any way weaken the requirement to implement effective monitoring mechanisms for such kinds of codes. However, it raises the problem of ensuring effective compliance monitoring mechanisms. According to the EDPB, effective monitoring can be achieved by adapting existing audit requirements to include code monitoring (2019). Mixed codes covering controllers and processors from the public and private sectors should also be mentioned.

Functions of codes of conduct. In relating the above features to data protection codes of conduct, it is worth referring to Peter Hustinx. He distinguished four purposes for developing data protection codes of conduct in different countries: to avoid legislation, anticipate legislation, implement legislation, and supplement it (Hustinx, 1991). In light of the GDPR, data protection codes of conduct are primarily developed for the third purpose mentioned above and much less for the fourth purpose. For these reasons, Urszula Góral and Paweł Makowski rightly argued that codes of conduct are sets of guidelines and instructions aimed at clarifying provisions of the GDPR (2018). According to Article 40 of GDPR, the primary purpose of codes of conduct is to facilitate compliance with the GDPR. To this end, the codes should concretise and operationalise the general principles of personal data protection for a specific industry or a particular type of processing operation. A data protection code of conduct is "a detailed description of what is the most appropriate, legal and ethical set of behaviors of a sector." Therefore it can "operate as a rulebook for controllers and processors who design and implement GDPR compliant data processing activities which give operational meaning to the principles of data protection set out in European and national law" (EDPB 2019). In this sense, we should view data protection codes of conduct as implementation or compliance tools that in no way replace or modify the provisions of the GDPR (Drobek, 2019). In particular, such codes can tailor the general obligations of controllers and processors to the risk of violation of the rights or freedoms of natural persons that sector-specific processing may entail.

Codes of conduct can provide controllers and processors with a greater degree of autonomy to establish standards and best practices for protecting personal data in the sector covered by the code, as well as increase legal certainty regarding solutions to problems identified in the sector. Codes of conduct also serve to build trust among data subjects.

In addition, codes of conduct may provide adequate safeguards in relation to data transfers to importers in third countries under Article 46(2)(e).

Codes of conduct may also serve as a means to facilitate the demonstration of compliance with the provisions of GDPR, as explicitly indicated by Article 24(3). In particular, this concerns under Article 32(3) GDPR, the demonstration of compliance with data security obligations or under Article 28(5) GDPR, the demonstration of sufficient guarantees by the processor. According to Article 35(8) GDPR, controllers or processors, in assessing the impact of the processing operations, in particular for a data protection impact assessment, must consider approved codes of conduct.

Pursuant to Article 83(2)(j) GDPR, when deciding whether to impose an administrative, financial penalty and determining the amount of the penalty, the supervisory authority will pay attention to the application of approved codes of conduct. It should be noted that, depending on the circumstances and behaviour of the controller or processor, this may reduce or increase their liability in this respect.

Functions of codes of conduct

In relating the above features to data protection codes of conduct, it is worth referring to Peter Hustinx. He distinguished four purposes of developing data protection codes of conduct in different countries: to avoid legislation, anticipate legislation, implement legislation, and supplement it (Hustinx, 1991). In light of the GDPR, data protection codes of conduct are primarily developed for the third purpose mentioned above and much less for the fourth purpose. For these reasons, Urszula Góral and Paweł Makowski rightly argued that codes of conduct are sets of guidelines and instructions aimed at clarifying provisions of the GDPR (2018). According to Article 40 GDPR, the primary purpose of codes of conduct is to facilitate compliance with the GDPR. To this end, the codes should concretize and operationalize the general principles of personal data protection to a specific industry or a particular type of processing operation. A data protection code of conduct is “a detailed description of what is the most appropriate, legal and ethical set of behaviors of a sector. "Therefore it can "operate as a rulebook for controllers and processors who design and implement GDPR compliant data processing activities which give operational meaning to the principles of data protection set out in European and national law" (EDPB 2019). In this sense, we should view data protection codes of conduct as implementation or compliance tools that in no way replace or modify the provisions of the GDPR (Drobek, 2019). In particular, such codes can tailor the general obligations of controllers and processors to the risk of violation of the rights or freedoms of natural persons that sector-specific processing may entail.

Codes of conduct can provide controllers and processors with a greater degree of autonomy to establish standards and best practices for the protection of personal data in the sector covered by the code, as well as increase legal certainty with regard to solutions to problems identified in the sector. Codes of conduct also serve to build trust among data subjects.

In addition, codes of conduct may serve to provide adequate safeguards in relation to transfers of data to importers in third countries under Article 46(2)(e).

Codes of conduct may also serve as a means to facilitate the demonstration of compliance with the provisions of GDPR, as explicitly indicated by its Article 24(3). In particular, this concerns under Article 32(3) GDPR the demonstration of compliance with data security obligations or under Article 28(5) GDPR the demonstration of sufficient guarantees by the processor. According to Article 35(8) GDPR, controllers or processors in assessing the impact of the processing operations, in particular for the purposes of a data protection impact assessment, must take into due account approved codes of conduct.

Pursuant to Article 83(2)(j) GDPR, when deciding whether to impose an administrative financial penalty and determining the amount of the penalty, the supervisory authority will pay attention to the application of approved codes of conduct. It should be noted that, depending on the circumstances and behaviour of the controller or processor, this may reduce or increase their liability in this respect.

Legal nature of the codes of conduct

Data protection codes of conduct are often included in the broad category of soft law as opposed to hard law (Fischer, 2018; Góral & Makowski, 2018; Gaeta, 2019). It should be stressed that soft law is intensively developed and plays an important role in the EU regulatory framework (Stefan, 2012). This progressive development of EU soft law does not diminish all concerns regarding, among other things, the legitimacy, nature and legal effect of such acts. It has recently been particularly demonstrated by the actions undertaken at the EU level concerning the Covid-19 pandemic (e.g. Stefan, 2020). It should be added that the legal nature of soft law within the EU law system does not mean it has no legal effect. Moreover, in fact, the codes of conduct created under the GDPR produce the legal effects provided for in this regulation and the obligations imposed in them can be legally enforced.

However, soft law is not a sufficiently precise term to describe the codes of conduct. First of all, it is questionable whether they should be regarded as law. It is assumed that codes of conduct do not generally constitute binding acts of law (Fajgielski, 2018). They are only self-binding for entities that have voluntarily agreed to apply them directly or indirectly, and they could even be considered so-called "tools of self-discipline" (Gaeta, 2019). One can say that codes of conduct can constitute a source of civil law obligations imposed on their adherents, as they can be regarded as an advanced form of contract between the signatories (stakeholders) creating them.

Consequently, codes of conduct shall be binding in the first instance on those who have subscribed to the code voluntarily (Drobek, 2019). Codes of conduct may also indirectly affect the understanding of the content of the obligations imposed on controllers or processors by the GDPR in the industry concerned, but who have not adhered to such a code. They also bind the supervisory authorities that have approved these codes. Supranational codes that require an opinion from the European Data Protection Board bind this body and its members (national supervisory authorities). Doubts have been raised about the legal force of supranational codes, for which, according to Article 40(9) GDPR, the European Commission may decide that they have general validity within the Union.

As a rule, codes of conduct are not sources of generally applicable law but constitute a source of civil law obligations imposed on their signatories, as they can be regarded as an advanced form of contract between the signatories (members of the code) (European Economic and Social Committee 2015). Consequently, a breach of the obligations imposed on the signatories to a code of conduct will give rise to liability under the terms of the code, which should provide for appropriate sanctions in the event of non-compliance with its provisions. Codes of conduct are intended to facilitate compliance with the provisions of GDPR by clarifying them and considering the specificities of a particular sector. In such a situation, a breach of the code of conduct may be treated as a breach of GDPR and give rise to administrative liability under the general rules. However, if the code of conduct introduces a higher standard of personal data protection than that provided in generally applicable data protection legislation, its breach will give rise to liability on the principles set out in the code.

As indicated earlier, codes of conduct are, by their very nature, voluntary. However, this does not exclude a situation where the code becomes de facto mandatory as an indirect result of belonging to a professional or industry organisation that has adopted the code as binding on its members.

Conclusions

The GDPR gives a more significant role to codes of conduct than in the previous EU data protection regime. The GDPR explicitly identifies codes of conduct as co-regulatory instruments. Their compliance with which controllers and processors have significant legal consequences but also provides an essential layer of cooperation between controllers, processors and supervisory authorities. However, the codes of conduct must not lower the level of protection from what is guaranteed by the data protection legislation, including GDPR and sector-specific laws.

At this still preliminary stage of application of the GDPR, it can be said that there is already an adequate formal framework for the preparation and approval of codes of conduct, as well as for the accreditation of monitoring bodies; there are also already the first approved codes on the EU and national level. However, it is too early to comprehensively assess their functioning, as there needs to be more experience with their practical operation.

References

Act (1997). Act of 29 August 1997 on the Protection of Personal Data, unified text: Journal of Laws of 2014, item 1182 with amendments.

Bennet C., Raab C. (2006). The Governance of Privacy. Policy Instruments in Global Perspective. The MIT Press, Cambridge, London, pp. 155–158.

Black J. (2012). Paradoxes and Failures: New Governance, Technics and the Financial Crisis. Modern Law Review, vol. 76, no. 4., pp. 1037–1063.

Black's Law Dictionary (1999). West Group, St. Paul, p. 250.

Csink L., Mayer A. (2014). How to Regulate: The Role of Self-Regulation and Co-Regulation. Hungarian Yearbook of International Law and European Law, vol. 3, pp. 403–420.

Opinion of the European Economic and Social Committee on Self-regulation and co-regulation in the Community legislative framework (2015/C 291/05).

Directive 95/46/EC, 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281/31.

Directive 2005/29/EC, 2005. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), Official Journal L 149/22.

Drobek P. (2019). Opracowywanie i zatwierdzanie kodeksów postępowania oraz warunki i tryb akredytacji podmiotu monitorującego jego przestrzeganie (*Drawing up and approving codes of conduct, as well as the conditions and procedure for accreditation of monitoring bodies*). In: D. Lubasz (ed.), Ustawa o ochronie danych Osobowych. Komentarz (*Personal Data Protection Act. A Commentary*). Wolters Kluwer, Warszawa, pp. 179–204.

EUR-Lex. https://eur-lex.europa.eu/homepage.html [access: 24.11.2022].

European Commission (2003). Report from the Commission. First report on the implementation of the Data Protection Directive (95/46/EC) COM(2003) 265 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0265&qid=1669466237911&from=PL [access: 24.11.2022].

European Commission (2010). Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union (COM/2010/0609 final) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52010DC0609&qid=1669720186919 [access: 24.11.2022].

European Commission (2020). Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation (COM/2020/264 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1669720562137&uri=CELEX%3A52020DC0264 [access: 24.11.2022].

EDPB (2019). Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 Version 2.0 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf [access: 24.11.2022].

EDPB (2021a). European Data Protection Board 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. https://edpb.europa.eu/system/files/202105/edpb_opinion_202116_eucloudcode_en.pdf [access: 24.11.2022].

EDPB (2021b). European Data Protection Board Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE). https://edpb.europa.eu/system/files/202105/edpb_opinion_202117_cispecode_en_0.pdf [access: 24.11.2022].

EDPB (2022). European Data Protection Board Guidelines 04/2021 on Codes of Conduct as tools for transfers Version 2.0. https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf [access: 24.11.2022].

European Economic and Social Committee (2015). Opinion on Self-regulation and co-regulation in the Community legislative framework, Official Journal C 291/05.

Fajgielski P. (2018). Art. 40 Kodeksy postępowania (*Article 40 Codes of conduct*). In: P. Fajgielski. Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz (*General Data Protection Regulation. Personal Data Protection Act. A Commentary)*. Wolters Kluwer, Warszawa, p. 250.

Fischer B. (2018). Art. 40 Kodeksy postępowania (*Article 40 Codes of conduct*). In: M. Sakowska-Baryła (ed.), Ogólne rozporządzenie o ochronie danych osobowych. Komentarz (*General Data Protection Regulation. A Commentary*). C.H. Beck, Warszawa.

Gaeta M. (2019). Hard Law and Soft Law on Data Protection: What a DPO Should Know to Better Perform His Or Her Tasks. European Journal of Privacy Law & Technologies, vol. 2019, no. 2, pp. 61–78.

GDPR, 2016. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation. Official Journal L 119/1.

Gellert R. (2020). The risk-based approach to data protection. Oxford University Press, Oxford.

Gilad S. (2010). It runs in the family: Meta-regulation and its siblings. Regulation & Governance, vol. 4., no.4, pp. 485–506.

Góral U., Makowski P. (2018). Art. 40. In: E. Bielak-Jomaa, D. Lubasz (ed.), RODO. Ogólne Rozporządzenie o ochronie danych. Komentarz *(GDPR. General Data Protection Regulation. A Commentary)*. Wolters Kluwer, Warszawa, pp. 819–820.

Hodges C. (2015). Law and Corporate Behaviour. Integrating Theories of Regulation, Enforcement, Compliance and Ethics. Hart Publishing, Oxford and Portland, pp. 1–2 and 466.

Hustinx P. (1991). The Role of Self-Regulation in the Scheme of Data Protection. Paper presented to the 13th Conference of Data Protection Commissioners, Strasbourg, cited by Bennet C. Raab C. (2006). The Governance of Privacy. Policy Instruments in Global Perspective. The MIT Press, Cambridge, London, p. 152.

Kamara I. (2020). Article 40 Codes of conduct. In: C. Kuner, L.A. Bygrave, C. Docksey (ed.), The EU General Data Protection Regulation (GDPR). A Commentary. Oxford University Press, Oxford, pp. 718–723.

Korff D.(2003). EC Study on Implementation of Data Protection Directive 95/46/EC (2002). Available at SSRN: https://ssrn.com/abstract=1287667 or http://dx.doi.org/10.2139/ssrn.1287667 [access: 24.11.2022], pp. 185–188.

Kuner C. (2007). European Data Protection Law. Corporate Compliance and Regulation. Oxford University Press, Oxford, pp. 46–48.

LRDP KANTOR Ltd (2010). Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments. Final Report. https://op.europa.eu/en/publication-detail/-/publication/9c7a02b9-ecba-405e-8d93-a1a8989f128b [access: 24.11.2022], p. 52.

Medzini R. (2021). Governing the shadow of hierarchy: enhanced self-regulation in European data protection codes and certifications. Internet Policy Review, vol. 10, no. 3. https://doi.org/10.14763/2021.3.1577.

Multistakeholder Expert Group (2019). Contribution from the Multistakeholder Expert Group to the stock-taking exercise of june 2019 on one year of GDPR application. https://ec.europa.eu/info/sites/default/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf, p. 4.

Robinson N., Graux H., Botterman M.,Valeri L. (2009). Review of the European Data Protection Directive. Sponsored by the Information Commissioner's Office. RAND Corporation, Santa Monica, p. 37. https://www.rand.org/pubs/technical_reports/TR710.html [access: 24.11.2022].

Stefan O. (2012). European Union Soft Law: New Developments concerning the Divide between Legally Binding Force and Legal Effects. Modern Law Review, vol. 75, no. 5, pp. 879–893.

Stefan O. (2020). The Future of EU Soft Law: Research and Policy Agenda for the Aftermath of Covid-19. Journal of International and Comparative Law, vol. 7, no. 2, pp. 329–350.

Vander Malen C. (2020). Codes of (Mis)Conduct? An Appraisal of Articles 40–41 GDPR in View of the 1995 Data Protection Directive and Its Shortcomings. European Data Protection Law Review, vol. 6, no. 2, pp. 231–242.

Vander Malen C. (2021). First or Many? First GDPR Transnational Code of Conduct Officially Approved After EDPB Opinions 16/2021 and 17/2021. European Data Protection Law Review, vol. 7, no. 2, pp. 228–231.

WP 29 (1998), Article 29 Working Party Working Document: Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country? https://ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/1998/wp7_en.pdf [access: 24.11.2022].

WP 29 (2001). Article 29 Working Party Working Document on IATA Recommended Practice 1774 Protection for privacy and transborder data flows of personal data used in international air transport of passengers and of cargo. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp49_en.pdf [access: 24.11.2022].

WP 29 (2003), Article 29 Working Party Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp77_en.pdf [access: 24.11.2022].

WP 29 (2008), Article 29 Working Party Opinion 3/2008 on the World Anti-Doping Code Draft International Standard for the Protection of Privacy. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp156_en.pdf [access: 24.11.2022].

WP 29 (2009), Article 29 Working Party Second opinion 4/2009 on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp162_en.pdf [access: 24.11.2022].

WP 29 (2010), Article 29 Working Party Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp174_en.pdf [access: 24.11.2022].

WP 29 (2015), Article 29 Working Party Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf [access: 24.11.2022].

WP 29 (2018), Article 29 Working Party letter to CISPE. file:///C:/Users/68366/Downloads/wp29_letter_to_cispe_final_ifp_9DD8DA13-948C-4F0E-50D80A5D97A2BB3E_49993.pdf [access: 24.11.2022].

Yeung K., Bygrave L. (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. Regulation & Governance, vol. 16, no. 1, pp. 137–155. https://doi.org/10.1111/rego.12401.