

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

SCOPE Europe<sup>12)</sup> 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.



**SCOPE**  
EUROPE

Hereby, SCOPE Europe instantiated the next iteration and evolution of the activities which its primary, Selbstregulierung Informationswirtschaft e.V.<sup>13)</sup>, 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)<sup>14)</sup>, 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-

<sup>12)</sup> <https://scope-europe.eu>

<sup>13)</sup> <https://sriw.de>

<sup>14)</sup> <https://eucooc.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<sup>15)</sup>, 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 preferable, 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.

<sup>15)</sup> [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_201901\\_v2.0\\_codesofconduct\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf)



EDPB Guidelines<sup>16)</sup> 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.<sup>17)</sup> 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<sup>18)</sup>, 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.

<sup>16)</sup> [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_201901\\_v2.0\\_codesofconduct\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf)

<sup>17)</sup> See as starting point [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_201901\\_v2.0\\_codesofconduct\\_en.pdf](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.

<sup>18)</sup> <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.



**SCOPE**  
EUROPE