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