Guidelines 04/2021 on codes of conduct as tools for transfers: Comments on public consultation

Joint comments by SCOPE Europe and the EU Cloud Code of Conduct

October 2021

1 About the authors

Headquartered in Brussels, SCOPE Europe is an organisation supporting credible and effective co-regulation of the information economy. It acts as a think tank to debate key issues in digital policy and provides an **umbrella organisation for a range of co-regulatory measures in the digital industry.** SCOPE Europe was founded in February 2017 as a subsidiary of the German non-profit-organization SRIW e.V. (*Selbstregulierung Informationswirtschaft - Self-Regulation Information Economy*) and acts as the **secretariat and accredited Monitoring Body** of the EU Data Protection Code of Conduct for Cloud Service Providers (the "**EU Cloud Code of Conduct**") pursuant to **Article 41 GDPR**.

SCOPE Europe is calling for **suitable regulatory methods to foster innovation and drive the digital transition while promoting corporate social responsibility**, particularly in the fields of data and consumer protection. To achieve this overarching objective, SCOPE Europe works to **enhance transparency** and **strengthen best practices in digital security** by mobilizing and supporting the industry to engage in binding voluntary commitments underpinned by appropriate sanctions.

The **EU Cloud Code of Conduct**[1] is a widely adopted code of conduct pursuant to **Article 40 GDPR**. **The EU Cloud Code of Conduct concretizes the legal requirements of Article 28 GDPR** – and all relevant related Articles of the GDPR – for practical implementation within the cloud market. Notwithstanding this wide applicability, **requirements under the EU Cloud Code of Conduct apply to all types of personal data**, **including those of sensitive nature.** In May 2021, following a unanimous positive opinion by the European Data Protection Board (the "**EDPB**"), **the EU Cloud Code of Conduct became the first tool of its kind to receive official approval by Data Protection Authorities to ensure and prove GDPR compliance for all service types of cloud computing.** Today, the Code has an extraordinary market reach, consisting in a vital instrument to solidify and generalize the commitment to European data protection standards, besides fostering international alignment conforming to GDPR.

The **EU Cloud Code of Conduct General Assembly** by launching the Third Country Transfers Initiative started developing an **on top-module** to the EU Cloud Code of Conduct for transferring personal data outside of the EU in line with **Article 46 GDPR**. In this context, the EDPB's "Guidelines 04/2021 on codes of conduct as tools for transfers" (the "**Guidelines**") constitute essential guidance for the development of robust privacy standard at the European level. Therefore, SCOPE Europe, and the EU

[1] https://eucoc.cloud

Cloud Code of Conduct (we) appreciate the opportunity to share our perspectives in the context of the public consultation and based on our experience, we provide the following comments.

2 Preliminary note

We would like to thank the EDPB for granting stakeholders the opportunity to provide their feedback on new guidance as well as for past projects. Consultations are crucial to implement the goals of the European Union's 'Better Regulation' strategy. Furthermore, they are essential to achieve alignment and adoptability of the tools supporting the implementation of the GDPR, especially in the context of the development of codes of conduct.

The comments that will follow have been drafted from our viewpoint as an organisation that specialises in the development and monitoring of codes of conduct based on Articles 40 and 41 GDPR, and our role in the EU Cloud Code of Conduct as mentioned above. As a result, the following comments are highly focused on our expertise within the ecosphere of third country transfers. Our feedback should be read in this light, and notwithstanding broader comments by other stakeholders.

Our comments follow a twofold structure. Firstly, we will begin with high-level overall observations. Secondly, we will provide more detailed remarks that centre around specific concepts/requirements of the Guidelines.

3 Remarks and observations

3.1 General remarks

The guidelines are highly appreciated and appropriately complement the **Guidelines 1/2019 on codes of conduct and supervisory bodies under Regulation 2016/679**[2] regarding the specifics of international data flows. **Their purpose and necessity are outlined**, as they aim to "*specify the application of Article 40-3 of the GDPR relating to codes of conduct as appropriate safeguards for transfers of personal data to third countries in accordance with Article 46-2-e) of the GDPR*", but also provide clarification on the expected content, adoption procedure and involved actors.

As a general remark, the concepts and processes described by these Guidelines are highly welcome. **The scope and purpose are delineated, and the guidance provided can clearly foster the development of codes of conduct as transfer tools and thus the practical implementation of Article 40-3**

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

GDPR within the market. As a result of the concretization of these guidelines, we believe that codes of conduct as tools of transfers will have the unparalleled potential to guarantee the enforcement of European Standards while guaranteeing the very operability of essential services that are responsible for orchestrating innovation and growth across our entire economy, such as the Cloud.

The guidance is helpful for stakeholders to understand the requirements that codes of conducts as tools for transfers must meet as well as specify the approval process. We highly welcome that the Guidelines leave room for flexibility especially with regard to the **cross-sectoral perspective** which in particular enables stakeholders to shape a robust standard without restricting innovation. Furthermore, it is appreciated that **the Guidelines enumerate examples** which enable future code owners to gain a clear idea on how those requirements can be implemented.

Especially from a **Monitoring Body's perspective**, we welcome that **the specificities of codes of conduct as tools for transfers have also appropriately been reflected in the requirements** relating to the standards and quality of **the monitoring of such Codes**.

3.2 Specific remarks

3.2.1 Codes of conduct as tools for transfers do not have to be adhered by both the data importer and the data exporter

We welcome the approach adopted by the Guidelines in **paragraph 7** by which **codes of conduct intended for transfers adhered by a data importer can be relied on by controllers/processors subject to GDPR (i.e., data exporter) for complying with their obligations in case of transfers to third countries without the obligation for them to adhere themselves to such Code.** Therefore, we understand that codes of conduct as transfer tools **do not have to be complied with by both the importer and exporter of data and that, in turn, it is not the intention that they constitute a copy of existing Binding Corporate Rules (BCRs), or standard data protection clauses (SCC / SDPC) supplemented by a monitoring body**. It is very welcome that the guidelines emphasize the specific advantage of codes of conduct: whereas BCRs are tailored to justify transfers within a group of companies, codes of conduct allow for data flows across group boundaries. This also reinforces the GDPR's intent to make codes of conduct an **independent safeguard mechanism for data transfers to third countries**. This approach also **permits to not interfere with other agreements**, and on the contrary, **enables but also does reinforces complementarity** with tools such as **BCRs** and **standard data protection clauses**.

Similarly, in the context of the **Third Country Transfer Initiative**, the intent is to frame data flows from exporters that have not adhered to the Code to adhering cloud service providers acting as importers.

This approach is an advantage for **Customers subject to the GDPR acting as data exporters, as they may rely on adhering cloud service providers (CSPs) acting as data importers**. By choosing an adhering Cloud Service Provider, we believe that data exporters **especially SME's** will be supported in their compliance exercise and, consequently, the level of data protection within the European Union will be raised.

Finally, referring also to **paragraph 18**, it is greatly appreciated that this is also **clearly reflected in the monitoring process** as only controllers/processors that have adhered to a code of conduct will fall under the scrutiny of the Monitoring Body.

3.2.2 An approved Code of Conduct may be amended to cover third country data flows

We appreciate the approach taken in **paragraph 13 of the Guidelines**, which provides **that an approved code of conduct established on the basis of Article 40-2 GDPR may be amended and expanded in its scope to cover third country data transfers** pursuant to Article 40-3 GDPR. We welcome the flexibility of this approach, as it allows for **market-friendly configurations** to be made for stakeholders already engaged in the ecosystem of an existing code of conduct, thereby encouraging adoption of these instruments. For example, we understand that this flexibility **allows building on an existing code of conduct and adding modules that specifically cover the appropriate safeguards needed for GDPR-compliant international transfers**.

Under the Third Country Transfers Initiative, effective protection for third country transfers is to be created in the form of an **add-on module to the EU Cloud Code of Conduct**. This module will be linked to the existing provisions of the EU Cloud Code of Conduct and cover the legal requirements for third country transfers under Chapter V of the General Data Protection Regulation. As the Third Country Transfer initiative is not a stand-alone initiative, we foresee that compliance with the EU Cloud Code of Conduct will be a prerequisite. In this respect, we consider this approach to be consistent with the wording of paragraph 13 of the Guidelines providing that a Code of Conduct may be amended to cover all requirements for data flows to third countries.

3.2.3 Cross-sectoral perspective

Referring to **paragraph 6** it is greatly appreciated that the Guidelines provide further flexibility with regard to the fact that codes of conduct can be **sector specific or cross-sectoral provided that they**

are drawn-up by separate sectors that have common processing activities that share the same processing characteristics[3].

This gives the market the **flexibility to adopt an appropriate working structure** and provides an incentive to develop codes of conduct focusing, for example, on processing fields such as **pseudonymisation** or **anonymisation**. By specifying and concretising the GDPR's legal requirements in those processing fields, codes of conduct will not only contribute to **raising the data protection standards at the European level** especially but also concomitantly **boost innovation** as prescribing appropriate technical and organisational measures will result in a faster technological evolution.

At the same time, we appreciate the notion that codes of conduct still require a **clear scoping and focus**, which allows for practical particularisation of GDPR requirements, thus fostering its implementation. Highly demanded flexibility for businesses to scope codes of conduct must go hand in hand with **ensuring the possibility for Monitoring Bodies to determine compliance**. The scoping and the drafting of codes of conduct must take monitoring (monitoring-by-default) into account as early as possible to safeguard their success.

3.2.4 Requirement to ensure that the level of data protection provided for in the GDPR is also committed by members located outside the EEA.

We consider that the Guidelines appropriately flesh out the requirements of codes of conduct as a justification ground for international data flows. More precisely referring to **paragraph 7**, we appreciate that the Guidelines require that **controllers and processors not subject to GDPR must make a commitment in the form of a legally binding document to comply with the obligation set forth by the code of conduct when processing the transferred data, including with regard to the rights of data subjects**.

By specifying that this applies for controllers and processors not subject to GDPR, our understanding is that for codes of conduct covering third country transfers it is not mandatory to cover all other main GDPR requirements provided that they are **committed to legally binding instrument covering the basic safeguards**. We appreciate this clarification as we understand this requirement **as a way to avoid redundancy for EEA-based entities that already implement tools to cover all aspects of processing related to the GDPR core safeguards**.

[3] Paragraph 10 of the Guidelines.

In addition, because the Guidelines are **flexible in terms of the choice of legally binding instrument**, we understand - and certainly in the context of a code's provisions - that **this requirement can be satisfied by signing a code of conduct and consequently by being listed as an adherent in a code's register**.

3.2.5 Code owner

Also referring to the **Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679** it is highly appreciated that the Guidelines further specify that the development of a Code of Conduct can be steered by associations or other bodies representing categories of controllers, processors, or a separate sector as this would enable to address the specific processing needs of their sector or common processing activities.

However, given that the Guidelines refer to the definition of **Code Owners as included in the Guidelines 1/2019**, we would like to re-emphasize our remarks made in the context of the consultation of the latter regarding **the ambiguities around the "*appropriate legal status*" of Code Owners**.

Considering that the first codes of conduct received their positive opinion, and subsequently their approval, we consider that our first understanding is confirmed. That is, that **the "*appropriate legal status*" relates to having an appropriate addressee in the sense of Member State law** for the approval by the competent supervisory authority.

3.2.6 General validity

As an initial remark, we consider the Guidelines to be useful in that they further specify the process for approval of codes of conduct, in particular for codes that are **amended/expanded** in their scope **with a view to also being used as a tool for transfers**. From our standpoint, they have to some extent the potential to streamline the procedures involved in the assessment process with the Commission, however **further clarification is sought on the general validity mechanism.**

Paragraph 21 of the Guidelines provides that *"the Commission may decide by adopting an implementing act that a code intended for transfers and approved by an SA has general validity. Only those codes having been granted general validity within the Union may be relied upon for framing transfers".* However, referring also to Articles 40-3 and 40-9 GDPR we note that **the general validity mechanism as an implementing act as well as its related legal effects remain generally unclear**. Thus, additional guidance at would be appreciated on how the general validity mechanism will be implemented by the European stakeholders aside the EDPB. More specifically, 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 by the European Commission 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**. This means that **the substantive assessment of the code by both institutions should, to some extent, be carried out simultaneously** and thus at an earlier stage than described in Annex 1 of the Guidelines. Notwithstanding and in fully appreciation of the powers of the European Commission, procedures by the European Commission should not – by any means – foresee any timelines that exceed the suitable blueprint provided by **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.

Still regarding **paragraph 21**, we realised that the Guidelines do not reflect the language of Article 40-3 GDPR anymore but **creates the confusing impression that safeguarding codes of conduct need a general validity in any case**. The Guidelines provide that safeguarding codes of conduct may signed either by EEA companies, non-EEA companies or even both. Especially, if the scope of a Code only foresees EEA companies to adhere to, the requirement of a general validity appears exceeding. Thus, the Guidelines should be clarified and aligned with Art. 40-3 GDPR.

Furthermore, **paragraph 5 of the Guidelines** provides that codes of conduct may be relied by **processors not subject to the GDPR** located in third countries for the purpose of providing **appropriate safeguards to data transferred to third countries only once approved by the competent SA** and having been granted **general validity within the Union by the Commission**.

Given the recent green-lights of the EDPB to codes of conduct that were not related to third-country transfers and their scoping, it is our understanding that the general validity is not required for non-EEA entities to adhere to such general codes of conduct.

We recognize that the Guidelines are mirroring GDPR in their language. Thus, it is our understanding, that in contrast to general codes of conduct, for third country transfers codes of conduct, and only in this scenario, general validity will be required for non-EEA entities to adhere to such code. In this respect, as **Article 40-3 GDPR specifically covers the third country transfers codes of conduct, it is a provision governing subject matter** (***lex specialis*). Therefore, we consider that the general validity mechanism provided for in this Article must not be applied to non-third country transfers codes of conduct**. Reading paragraphs 5 and 21 of the Guidelines, we understand that this also the interpretation of the EDPB. Following the first approvals of transnational codes of conduct, the interest in this tool appears significantly raising, hence the tool is likely to become as prosperous as once

intended by the regulator. We recommend that any confusion related to the necessity of a general validity for non-third-country transfers codes of conduct will be avoided.

3.3 Requirements relating to the Monitoring Body

Concerning **paragraph 18**, we interpret the language "headquarters" from a non-corporate law perspective, whilst even this legal interpretation is not considered having adverse effects on ourselves. However, we would like to raise a general remark, **to allow for an open and fair competitive market for monitoring bodies**. We appreciate and acknowledge that they **must be fully liable and subject to the supervision of European Authorities**. However, we do not recognize any legal requirements under GDPR to call for a European headquarter, alongside the accreditation criteria within Article 41 GDPR. We therefore understand the Guidelines to intend a European establishment, thus we recommend clarifying the Guidelines accordingly.

Contents / Summary / Key Notes

We greatly appreciate the opportunity to share our perspectives in the context of the present public consultation. We consider the Guidelines to be an essential piece of guidance for the development of a robust privacy standard in the context of international data transfers in line with Article 46 and, in particular, for the ongoing work on the EU Cloud CoC's Third Country Initiative.

Our main points and high-level observations can be summarised as follows:

- Overall, we believe that the guidance provided can clearly foster the development of codes of conduct as transfer tools and thus the practical implementation of Article 40-3 GDPR within the market. The concepts and processes described by these Guidelines are highly appreciated and provide clarity. We welcome the flexibility that the Guidelines provide with regard to:

    - the cross-sectoral perspective;
    - the fact that the Guidelines provide that it is not mandatory for a Code to be relied by both the data importer and the data exporter; and
    - the fact that the Guidelines provide that approved Code of Conduct may be amended to cover third country data flows.

    We consider that this approach notably allows stakeholders to develop tools raising the bar of data protection in the context of third country data transfers, while enabling at the same time market-friendly work configurations and innovation.

- Although we recognize the potential of these Guidelines to streamline the approval process between the EDPB and the European Commission, further clarifications are welcome on the implementation of the general validity mechanism provided for in Articles 40-3 and 40-9 GDPR. In addition, further clarification is also sought with regard to paragraph 18 of the Guidelines relating to the requirements for the Monitoring Body.

We hope our feedback will contribute to the update of the Guidelines and we look forward to continuing our engagement with the EDPB as well as other key stakeholders in this context.

About EU Cloud CoC

The EU Cloud Code of Conduct is an approved and fully legally operational Code of Conduct pursuant to Article 40 GDPR. Defining clear requirements for Cloud Service Providers to implement Article 28 GDPR, the Code covers all cloud service layers (IaaS, PaaS, SaaS), has its compliance overseen by an accredited monitoring body, and represents the vast majority of the European cloud industry market share.

About SCOPE Europe

SCOPE Europe sprl / bvba (SCOPE Europe) is a subsidiary of SRIW. Located in Brussels, it continues and complement the portfolio of SRIW in Europe and is an accredited monitoring body under the European General Data Protection Regulation since May 2021, pursuant to Article 41 GDPR. SCOPE Europe gathered expertise in levelling industry and data subject needs and interests to credible but also rigorous provisions and controls. SCOPE Europe also acts as monitoring body for the EU Data Protection Code of Conduct for Cloud Service Providers and is engaged in other GDPR code of conduct initiatives.