

Your path to **trusted** cloud services in Europe



selbstregulierung
informationswirtschaft e.V.



SCOPE
EUROPE



EU
CLOUD
COC

<https://eucoc.cloud>

Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR

Joint comments by SRIW, SCOPE Europe and the EU Cloud CoC

January 2022



selbstregulierung
informationswirtschaft e.V.



SCOPE
EUROPE



EU
CLOUD
COC

1	About the authors.....	2
2	Preliminary Note	3
3	General Remarks.....	3

1 About the authors

Self-Regulation Information Economy (German: Selbstregulierung Informationswirtschaft e.V. – short: “**SRIW**”) is a Berlin-based non-profit-organisation that fosters and promotes data and consumer protection through self-regulation and co-regulation. Its Brussels-based subsidiary SCOPE Europe sprl / bvba (“**SCOPE Europe**”) complements the portfolio of **SRIW** on a European level and 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 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.

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

The EU Cloud Code of Conduct is a widely adopted code of conduct pursuant to Article 40 GDPR. The EU Cloud Code of Conduct solidifies 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 as a vital instrument to solidify and generalise 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 additional module to the EU Cloud Code of Conduct creating a dedicated safeguard for transferring personal data outside of the EU in line with Article 46 GDPR. In this context, the EDPB’s “Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR” (the “**Guidelines**”) constitute essential guidance for the development of robust privacy standard at the European level. Therefore, SRIW, SCOPE

Europe, and the EU Cloud Code of Conduct (“**We**”) appreciate the opportunity to submit this comment in support of the Guidelines.

2 Preliminary Note

We consider the Guidelines to be an essential piece of guidance given to ensure a common understanding and interpretation of Article 3 in relation with the provisions on international transfers under Chapter V of the GDPR. This is particularly important in the aftermath of the so-called “Schrems II” ruling of the European Court of Justice, which has caused uncertainty within the cloud industry on how to interpret and implement the GDPR with regards to transfer of personal data outside the EU, triggered discussions among legal experts and authorities on adequate next moves, and highlight the necessity to streamline an aligned strategy for a harmonised implementation of the GDPR.

The comments that 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 and are consequently highly driven by our expertise within the ecosphere of third country transfers.

3 General Remarks

As a general remark, we highly welcome the Guidelines as the reasoning and examples presented therein shed light on the purpose of Chapter V to ensure a continued level of protection guaranteed by the GDPR in cases of third country personal data transfers and provide a helpful input in a vivid and ongoing debate in this context.

In the absence of a legal definition in the body of the GDPR, the clarification of the notion of a “transfer of personal data to a third country or to an international organisation” is very much appreciated. From a methodological perspective, the structure of the Guidelines outlining the criteria alongside concrete examples for each case facilitates understanding of the matter. With respect to the substance, we fully second the importance of identifying the criteria which qualify a processing as a transfer under Chapter V and underlining that these criteria must be cumulative. This is an essential element of guidance, particularly in the context of the Third Country Transfers Initiative, as the criteria will help to appropriately delineate what shall be considered as transfer under this code of conduct, as well as its scope.

With regards to the first criterion, the Guidelines state that non-EU controllers and processors may be subject to the GDPR pursuant to Article 3(2) for a given processing and, thus, will have to comply with



Chapter V when transferring personal data to a third country. We appreciate the EDPB's clarification under paragraph 10 that the interplay between Article 3(2) and Chapter V is of a complementary nature, in a sense that the implementation of the one does not exclude the other. Rather both are needed to guarantee that the protection provided by the GDPR is not undermined by an unfavourable legislation that the importer may fall under. Whilst awaiting additional Guidance, the Third Country Transfers Initiative also preliminarily accepted the understanding that transfer mechanisms, such as codes of conducts, will be required irrespective of if GDPR already applies directly to processing by virtue of Article 3(2). The Guidelines reflect a common understanding of practitioners, until the publication of the updated Standard Data Protection Clauses¹.

Regarding the second criterion the Guidelines differentiate between the "exporter" and the "importer" of personal data clarifying thus, that the concept of transfer only applies to disclosures of personal data where the involved controllers, joint controllers or processors are different parties. We welcome the guidance provided by example 5 to the extent that remote access of personal data by an employee, since the employee is not another party, is not regarded as a transfer under Chapter V of GDPR. Further, we particularly appreciate the differentiation between the terms "data subject" and "controller/processor" whereby it is ascertained that a data subject disclosing their own personal data cannot be considered an "exporter" and therefore the second criterion cannot be considered fulfilled in such cases.

For the fulfilment of the third criterion the Guidelines consider it irrelevant whether the importer is subject to the GDPR in respect of the given processing or not and clarify once more the complementary implementation of safeguards so that effective detection and supervision mechanisms are strongly dependent on the individual case. We consider this clarification highly relevant to our activity developing an additional module to the EU Cloud Code of Conduct dedicated to third country transfers pursuant Article 46 GDPR and view the clarification under paragraph 23 as an important orientation point in this context.

Finally, especially from a Monitoring Body's perspective, we share EDPB's view of drawing attention to the obligation and overall necessity of implementing appropriate technical and organisational

¹ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en



selbstregulierung
informationswirtschaft e.V.



SCOPE
EUROPE



EU
CLOUD
COC

measures in compliance with Article 32 as the very minimum for any kind of data processing regardless of whether the data flow constitutes a third country transfer under Chapter V or not.

Summary

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, particularly for the ongoing work on the EU Cloud CoC's Third Country Initiative.

We welcome the clarifications outlined in the Guidelines and look forward to continuing our engagement with the EDPB as well as other key stakeholders in this context further in the future.



selbstregulierung
informationswirtschaft e.V.



SCOPE
EUROPE



EU
CLOUD
COC

About SRIW

Selbstregulierung Informationswirtschaft e.V. is a non-profit association supporting the self-regulation of the information economy. It acts as a think tank to discuss and debate key issues in digital policy and provides an umbrella organisation for a range of self-regulatory measures in the digital industry. We are calling for suitable regulatory methods to foster innovation and the digital transformation and, at the same time, promote corporate social responsibility, in particular with regard to the appropriate measures for data and consumer protection.

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.

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.