

EU DATA PROTECTION: IN A POST-PRIVACY SHIELD, SECTORIAL CODE OF CONDUCT COULD LEAD THE WAY TO SAFEGUARD DATA TRANSFERS OUTSIDE THE EU/EEA

Date: 17 July 2020

Data Protection, Privacy, and Security Alert

By: Claude-Étienne Armingaud

With the recent decision from the Court of Justice of the European Union¹ invalidating the Privacy Shield framework (see our alert here) and subjecting the Standard Contractual Clauses (SCCs) to higher standard of enforcement, global companies with the need to transfer data across the world, and especially across the Atlantic, are now required to re-assess their data transfer mechanisms.

While both Privacy Shield and the SCCs predates the GDPR,² the new regulation aimed at providing stakeholders with additional tools to self-regulate and safeguard the privacy of individuals in the European Union

Among them, and while still confidential, the implementation of codes of conduct is encouraged under Art. 40 GDPR and by the dedicated Guidelines³ of the European Data Protection Board (EDPB). As a matter of fact, the advantages of such codes of conduct go beyond the mere facilitation of data transfers, and provide data controllers and data processors alike with a complete sectorial framework for GDPR compliance.

INITIATING CODES OF CONDUCT

The initiative to implement a Code of Conduct must be carried by associations or organizations (so-called “Code Owners”) acting as representatives of a group of stakeholders (data controllers and data processors alike) in a given ecosystem, to agree on an accountability toolbox taking into consideration the practice of such ecosystem.

Codes of conduct may cover various GDPR's topics such as:

- rules about fair and transparent processing;
- means and best practice for the collection of personal data;
- information provided to the public and to data subjects;
- the use of the legitimate interest as a legal basis, or other available legal bases; and
- the transfer of personal data from the EU/EEA to third countries or international organizations (Art. 40.2 j), Art.46.2 e) GDPR).

However, these codes should not just be a mere copy of the relevant GDPR provisions, and must specifically address issues relating to the specific fields or specific processing operations of the ecosystem represented by

the Code Owners. In that regard, the Code Owners are encouraged by GDPR and the EDPB to consult relevant stakeholders when drawing up, amending or extending their codes of conduct (Recital 99 GDPR).

APPROVAL OF CODES OF CONDUCT

Once the ecosystem has agreed on a draft, the Code Owners may then submit it for approval, either before the competent national supervisory authority (for strictly national processing activities), or to the EDPB and the European Commission (for transnational processing activities). By definition, any Code of Conduct which would also cover the transfers of data outside of the EU/EEA would be deemed transnational.

For transnational codes of conduct, the relevant supervisory authority in view of the Code Owner will centralize the process under the one-stop-shop principle of GDPR, and will then liaise with its counterparts in other Member States to cooperate in the review, and, if necessary, amend the draft Code of Conduct.

Further to this consultation process, the other supervisory authorities will have a 30 day window to submit observations on a finalized version of the document, prior to submission to the EDPB for opinion, which will be communicated to the European Commission. The European Commission may then by way of implementing acts decide that the approved Code of Conduct have general validity throughout the EU (Art. 40.9 GDPR).

BENEFITS OF A CODE OF CONDUCT

Codes of conduct offer many benefits to all stakeholders within an ecosystem and beyond:

- As best practices for a given sector, they act as a guide to achieve and maintain compliance with GDPR requirements;
- Code Owners, as the central nervous system of a Code of Conduct, can centralize new challenges to their ecosystem and harmonize the way an ecosystem may face evolution in GDPR enforcement;
- Codes of Conduct can help demonstrate accountability, be it in case of an audit by the Supervisory Authority or third party to the ecosystem as well as for processors to benefit from a presumption of sufficient guarantees; and
- Adhering to a Code of Conduct projects onto data subjects a corporate culture of data protection and that the companies are processing data in a fair and transparent manner, which will foster trust and confidence from individuals and branding. In that regard, as used to be the case for the Privacy Shield, once approved, Codes of Conduct are publicly listed by the EDPB.

CODES OF CONDUCT AND DATA TRANSFER

In addition to their other benefits, Codes of Conduct may offer a flexible way forward for data transfer in the wake of the Schrems II case invalidating Privacy Shield and adding more scrutiny over SCCs. Adherence to a Code of Conduct can serve as an “appropriate safeguard” allowing for the transfer of data outside the EU/EEA. Article 46.2 e) of the GDPR states that the transfer of data to third countries or international organizations is possible without requiring any specific authorization from a supervisory authority when “an approved code of conduct [...] with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' right.”

The recipient of the data outside of the EU/EEE will need to commit, through contract or any other legally binding documents to apply the appropriate safeguards contained in the code.

MONITORING AND UPDATES TO AN EXISTING CODE OF CONDUCT

Article 41 GDPR requires the appointment of a monitoring body by the Code Owners, which will need to be accredited by the competent supervisory authority. This monitoring body will have to:

- assess for eligibility of controllers and processors to apply the code;
- monitor compliance with its provision; and
- carry out review of the code's operation.

The monitoring body will have the ability to initiate sanctions against those of the stakeholders which adhered to the Code of Conduct, ranging from mandated training, issuance of warning, temporary suspension from the code until remedial action is taken, or even the definitive exclusion.

For each of these measures, both the Code Owner and the competent Supervisory Authority will be notified, which may eventually lead to additional investigation by the latter.

The code owner will also have to implement an appropriate review mechanism to ensure that the code remains relevant and continues to contribute to the proper application of the GDPR. Each amendment or extension of the code will also need to be submitted to the competent supervisory authority for approval.

ADHESION TO AN EXISTING CODE OF CONDUCT

Adhering to a Code of Conduct means that the data controller or the data processor agrees to abide to the requirements set forth in the Code of Conduct.

Any data controller and/or data processor can adhere to Codes of Conduct, regardless of their establishment within the EU/EEA, through an adhesion procedure which will need to be provided within the Code of Conduct itself.

As of today, no Code of Conduct relating to the transfers of data outside the EU and the EEA have been approved. However, in light of the *Schrems II* decision, there is no doubt that such code could emerge as a flexible tool to industry sectors to ensure foreseeability for the processing operations and their transfers.

K&L Gates global data protection team (including in each of our European offices) remains available to assist you in achieving the compliance of your data transfers at global levels.

FOOTNOTES

¹ Court of Justice of the European Union - Grand Chamber - 16 July 2020 - C-311/18 - *Schrems II*

² General Data Protection Regulation 2016/79 dated 27 April 2016, which enter into force on 25 May 2018 (GDPR)

³ Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/79 dated 04 June 2019

KEY CONTACTS



CLAUDE E. ARMINGAUD
PARTNER
PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.