I. Introduction: Guidelines 04/2021 as the ‘Last Piece of the Puzzle’

Codes of conduct remain an underlit aspect of the EU’s General Data Protection Regulation (GDPR), which can be found in articles 40 and 41. Member States, supervisory authorities, the Board and the Commission shall encourage the drawing up of such codes ‘intended to contribute to the proper application of this Regulation’ (article 40(1) GDPR). In essence they shall ‘give operational meaning to the principles of data protection’, i.e. help to translate the abstract provisions of the GDPR into concrete obligations and procedures.

The GDPR designs a system consisting of three types of codes, each with a different territorial reach. Article 40(5) and (6) describe ‘national codes of conduct’, which the European Data Protection Board (EDPB) has more clearly defined as ‘a code which covers processing activities contained in one Member State’. Article 40(7) sets out the possibility of a transnational code, which is ‘a code which covers processing activities in more than one Member State’. Finally, article 40(9) speaks of ‘codes having general validity’. Although this type of code is not further defined in the GDPR nor in guidance issued by the EDPB, it is implied that a code of this type can cover processing activities in all EU Member States – going one step further than transnational codes, which may apply in several but not necessarily all Member States. Intra-EU, this means that codes can not only specify the abstract principles of the GDPR for specific sectors, but that they can ‘help to bridge the harmonisation gaps that may exist between Member States in their application of data protection law’.

However, codes have an important extra-EU function. The GDPR’s Chapter V sets out the rules for international data transfers, i.e. the transfer of personal data from the Union to recipients in third countries or to international organisations. These data flows have a dedicated chapter in the GDPR since the European legislator wants to safeguard that the level of protection of natural persons ensured in the EU is not undermined when the data leaves the EU’s territory.

Chapter V of the GDPR is particularly notable because it constructs what Kuner describes as a three-tiered structure. Adequacy decisions are placed at the top of the hierarchy, appropriate safeguards – including the use of codes of conduct – in the middle, and...
derogations at the very bottom. To better understand the use of codes of conduct for data transfers, article 46(1) and (2)(e) GDPR must be considered: According to article 46(1), in the absence of an adequacy decision, controllers or processors may transfer personal data to a third country or an international organisation only if they provide appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. According to article 46(2)(e) such appropriate safeguards may inter alia be provided for, without requiring any specific authorisation from a supervisory authority, by an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights.

Article 46(2)(e) GDPR is meant to be read together with article 40(3) GDPR (they contain cross-references) to fully grasp the requirements to carry out data transfers on the basis of codes. The key understanding here is that not only actors who are already subject to the GDPR can adhere to codes, but also actors who are not subject to the GDPR. The determination whether an actor is subject to the GDPR is based on the territorial scope laid down in article 3 GDPR.

However, actors that are not subject to the GDPR can only adhere to codes if three cumulative criteria are fulfilled: the codes must have general validity pursuant to article 46(9), they must be approved pursuant to article 40(5), and such adherence must be in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in article 46(2)(e). These criteria exclude actors that are not subject to the GDPR from participating in national codes and transnational codes. Actors that are subject to the GDPR can participate in national codes, transnational codes, and codes having general validity.

While the possibility to use codes of conduct for data transfers has been present in the GDPR since its entry into application in 2018, they have not yet been used for this purpose. It appears that the EDPB has deliberately staved off using codes for data transfers until now, as can be gleaned from the EDPB’s approval of the first two transnational codes in May 2021: While it approved both the ‘EU Data Protection Code of Conduct for Cloud Service Providers’ (hereafter: EU Cloud Code) and the ‘European Code of Conduct for Cloud Infrastructure Providers’ (hereafter: CISPE Code) through respective Opinions 16/2021 and 17/2021, finding the codes conform to the GDPR, both opinions contained the identical statement that ‘the present code is not a code of conduct according to Article 46(2)(e) meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in point (e) of Article 46 (2)’.

In all likelihood, the EDPB wanted to first adopt guidelines so a stronger conceptual framework and specific requirements existed before it would allow international data transfers on the basis of codes. Such a prudent approach could not only better safeguard the level of protection that the EU legislator desires, but it could also avoid legal uncertainty caused by disputes before a court (one might think, for example, of the legal uncertainty surrounding transatlantic data flows following the Schrems I and II rulings of the Court of Justice of the European Union (CJEU)).

As a result, the EDPB’s publication of ‘Guidelines 04/2021 on Codes of Conduct as tools for transfers’ can be considered the last big ‘piece of the puzzle’ that still needed to be completed to make codes of conduct viable tools under the GDPR’s regime when it comes to international transfers of personal data to third countries and international organisations. Version 1.0 for public consultation was released in July 2021. The EDPB has now adopted version 2.0 on 22 February 2022. This report discusses if the Guidelines succeed in clarifying the rules regarding the use of codes for the purpose of data transfers.

---

10 The cumulative nature is indicated by the ‘and’ in article 40(3) GDPR.
14 EDPB, ‘Guidelines 04/2021’ (n3).
II. Flexibility for the Data Exporter and Amendments to Existing Codes

Guidelines 04/2021 follow the same structure as other EDPB guidelines. After a general description of the aim of the guidelines and what they address, the EDPB in section 2 re-emphasises several important points. Codes of conduct are a potential tool to enable data transfers to third countries and international organisations under article 46 GDPR. To use codes for such a purpose, the code must be approved, must have general validity, and binding and enforceable commitments must be made to apply the appropriate safeguards provided by the code. It is after this short refresher that the EDPB introduces several noteworthy new elements.

First, the EDPB labels codes as having unique strengths compared to other transfer mechanisms. It emphasises the possibility for ‘multiple transfers to a third country that are specific to a sector or data processing activity’. It also singles out the crucial difference between codes of conduct and binding corporate rules (BCRs): whereas codes allow transfers across corporations, BCRs limit transfers to a group of undertakings or group of enterprises engaged in a joint economic activity (article 4(2o) GDPR). Additionally, a presence in the European Economic Area (EEA) is required for a group of companies to use BCRs. Although it may seem evident to distinguish between codes of conduct and BCRs, there has been conceptual conflation in the past that merits an explicit comparative distinction by the EDPB.

Second, and crucially, the EDPB determines ‘that a code intended for transfers adhered to by a data importer in a third country can be relied on by controllers/processors subject to the GDPR (i.e. data exporter) for complying with their obligations in case of transfers to third countries in accordance with the GDPR without the need for such controller/processors to adhere to such code themselves’. In essence then, for a data transfer to take place between a data exporter (i.e. the company that is subject to the GDPR) and a data importer (i.e. the company not subject to the GDPR) only the importer has to adhere to a code having general validity for the transfer to take place and not the exporter (although the GDPR must of course be respected due to the exporter being subject to its rules).

With regard to the underlying reasoning in this interesting construction, in all probability, the EDPB’s most important intention is to nudge actors who are not subject to the GDPR to follow the Regulation’s standards through adherence to a code (which specifies the GDPR’s rules) and a binding instrument such as a contract (which sets out the obligations set forth by the code of conduct and includes data subject rights – see below for a further explanation). This widens the GDPR’s already significant sphere of influence and seemingly acknowledges the ‘Brussels effect’ of EU rulemaking. Additionally, this type of construction allows actors who are already subject to the GDPR to flexibly engage in data transfers, offering the possibility of setting up new or more efficient business constructions by using ‘cheaper’ or more specialised extra-EU companies who are willing to adhere to a specific code. This grants the European data economy more flexibility.

Section 3 provides important practical guidance for stakeholders involved in the development of codes. Here, the EDPB states that codes intended for transfers should be specifically designed for third country controllers and processors – either in part, or as a whole. This means that a code of conduct that has already been designed for intra-EU use may need to be amended to also be used for the purpose of data transfers to third countries or international organisations. This will be nearly inevitable in practice since the EDPB clarifies that for a code to provide appropriate safeguards in the meaning of article 46 GDPR, it will need to include a) essential principles, rights and obligations arising under the GDPR for controllers/processors; and b) guarantees that are specific to the context of transfers. With the latter, the EDPB gives as an example the issue of conflict of laws in the third country, or onward transfers. Importantly, the EDPB clarifies that such an amendment must be submitted to the competent supervisory au-
authority for approval, following the procedures that already exist for transnational codes – including an Opinion from the EDPB.\textsuperscript{22}

The remark that existing codes may need to be amended before they can be used for data transfers refers to the ‘elephant in the room’: the EDPB explicitly excluded the EU Cloud Code and CISPE Code from being used for data transfers to third countries and international organisations. As stated above, the EDPB never outright explained why, but it is likely that it first wanted to develop a proper conceptual framework and specific requirements to achieve a high level of protection and avoid later legal uncertainty (for example through disputes before the CJEU).

With the additional clarification in section 3 of the Guidelines 04/2021 on the safeguards that codes should contain, it will now be possible to adapt the existing codes in such a way that they can be used for both intra-EU and extra-EU functions.

\section*{III. Specific Requirements for Monitoring Bodies}

Section 4 contains some of the most interesting passages in Guidelines 04/2021 and explains the different actors and their roles in the construction of a code to be used as a tool for data transfers. The explanations on the code owner, the monitoring body, supervisory authorities, and the EDPB are all closely aligned with those in Guidelines 01/2019 – which seems logical, since these actors are involved in the development of any code, whether it is intended for data transfers or not.

The most important actor to discuss in the context of using codes for data transfers is the European Commission. After all, this is the only body that can ‘decide by adopting an implementing act that a code intended for transfers and approved by a SA has general validity within the Union’. However, Guidelines 04/2021 fail to provide more clarity on the exact procedure or timeline for the Commission to adopt such an act. In fact, the Guidelines never go beyond what is found in the provisions of the GDPR itself (see article 40(9) GDPR). As a result, there is still a significant degree of legal uncertainty regarding the development of codes intended for data transfers.

Arguably the most crucial parts of the Guidelines are found in paragraphs 18 and 19. Here, the EDPB specifies what is expected of monitoring bodies in the context of codes for data transfers. To briefly reiterate, articles 40(4) and 41 GDPR lay down the obligation for a code to have a monitoring body. It is ‘a body/committee or a number of bodies/committees (internal or external to the code owners) who carry out a monitoring function to ascertain and assure that the code is complied with’.\textsuperscript{23}

Monitoring bodies that are linked to a code intended for data transfers are subject to several important requirements. First, the EDPB lays down important location requirements: a monitoring body must be either located only in the EEA or have an establishment in the EEA which shall be the one where the body has its headquarters or ‘the place where the final decisions concerning monitoring activities are taken’.\textsuperscript{24} Although these essential criteria are mentioned in paragraph 18 of the Guidelines, the paragraph unfortunately ends with an unclear sentence that states: ‘and also requires [sic] that an EEA entity shall be able to control the monitoring body’s entities outside the EEA and demonstrate full accountability for all decisions and actions (including its liability for any breaches).’\textsuperscript{25} Presumably, this should be read that the EDPB requires this control.\textsuperscript{26}

Second, the EDPB gives important guidance regarding monitoring bodies and subcontracting. It clarifies that monitoring bodies in the EEA may make use of subcontracting to external entities outside the EEA if the following conditions are met cumulatively: a) the extra-EEA entity must maintain the same competence and expertise as required by the code and accreditation requirements, and b) the EEA monitoring body must ensure effective control over the services provided by the contracting entity and retain decision-making power about monitoring activities.

Monitoring bodies that would like to use subcontracting should establish a contract or other legal acts under EU law binding on the subcontractor so that all subcontracted tasks will meet the requirements of the GDPR. Only then will the monitoring body be

\begin{itemize}
\item \textsuperscript{22} ibid 10–11.
\item \textsuperscript{23} EDPB, ‘Guidelines 1/2019’ (n 2) 7.
\item \textsuperscript{24} EDPB, ‘Guidelines 04/2021’ (n 3) 9.
\item \textsuperscript{25} ibid.
\item \textsuperscript{26} The author reached out to the EDPB for clarification but did not receive a response at the time of writing.
\end{itemize}
considered being compliant with the accreditation requirements. The EDPB also emphasises that subcontracting does not alleviate the monitoring body of its responsibilities: it remains responsible for monitoring compliance with the code, and it must ensure that subcontractors meet accreditation requirements such as independence, absence of conflict of interest and expertise. Finally, and importantly, the EDPB states that the monitoring body must include a specific clause in the contract signed with subcontractors to ensure the confidentiality of personal data that may, where applicable, be disclosed to the subcontractor executing monitoring tasks and puts in place appropriate safeguards in case of transfer of personal data to its subcontractors.

Through these detailed provisions on the location of monitoring bodies and by explicitly addressing the possibility of sub-contracting, the EDPB provides practical guidance to actors in the field. In this way, it raises the level of legal certainty that has been lacking until now for actors who wish to develop business models in the context of data transfers.

IV. Formal and Substantive Requirements for Binding and Enforceable Commitments

Section 5 focuses on the exact process that should lead to the adoption of a code. However, this section does not contain particularly important new information since it outlines almost exactly the steps that had already been explained in Guidelines 1/2019. In fact, the Annex to Guidelines 04/2021 does a remarkable job at presenting the procedure to follow in a concise, schematic way. Annex 1(a) outlines the procedure for the adoption of a transnational code intended for transfers; Annex 1(b) hammers the point home that amendments to a transnational code to be used as a code intended for transfers must also go through an established process.

Section 6 closes the Guidelines by further clarifying the requirement in article 40(3) GDPR that controllers or processors ‘shall make binding and enforceable commitments, via contractual or other legally binding instruments’ to apply appropriate safeguards.

First, it discusses the formal design of the binding and enforceable commitments that should be implemented. While the EDPB mentions a contract as the most straightforward choice to contain such commitments, it states that there should be flexibility to choose the most appropriate option depending on the specific situation. Other instruments may be used if a) their binding and enforceable character under EU law can be demonstrated, and b) if they are binding and enforceable by data subjects as third-party beneficiaries. An existing contract can be used to include the binding and enforceable commitments (e.g. a service agreement based on article 28 GDPR). The parties may use a separate contract by adding to the code intended for transfers a model contract that would need to be signed.

Second, it discusses the substantive content. The instrument must contain the commitment of the controllers and processors to comply with the rules in the code, and it must also contain enforcement mechanisms. As regards code members located outside the EEA, the ultimate goal is to ensure that they commit to adhere to a ‘specified level of data protection’ (in the words of the EDPB) that guarantees the level of data protection established by the GDPR.27

The EDPB then specifies these general tenets. Most interestingly, the instrument should specify how liability is handled when code members outside the EEA breach the code. Particularly salient is the necessity of a ‘jurisdiction clause noting that data subjects shall have the possibility in case of violation of rules under the code by a code member outside the EEA to bring a claim, by invoking their third-party beneficiary right, including for compensation, against that entity before an EEA supervisory authority and EEA court of the data subject’s habitual residence.’ It is further determined that data subjects should be able to bring claims ‘arising out or from the respect by the importer of the code of conduct against the data exporter before the supervisory authority or the court of the data exporter’s establishment or of the data subject’s habitual residence’. In this way, the EDPB grants more legal certainty regarding enforcement to both data subjects and corporate entities involved in codes for data transfers.

Finally, the EDPB provides a check-list with the most important elements that should be included in the code itself. While many of these do not surprise (such as the need to describe the transfers covered by a code or the provision of data subject rights) or

---

27 EDPB, ‘Guidelines 04/2021’ (n 3) 11.
play into existing GDPR elements (such as the need for a data protection impact assessment to check compliance with the obligations resulting from the code). Some do stand out. In particular, the EDPB speaks of a data protection audit. However, problematically, this most potentially innovative element is also somewhat unclear. It calls for a data protection audit (by either internal or external auditors) or other internal mechanisms for monitoring compliance with the code, independently from the oversight to be performed by the monitoring body as for any code of conduct. Whereas the aim of the data protection audit program is to ensure and demonstrate compliance with the code, the aim of the audits performed by the monitoring body is to assess whether the applicant is eligible to participate to the code, continues to be eligible once it is a member, and whether sanctions are necessary in case of infringements.

The constant use of the term ‘audits’ is highly confusing because the Guidelines simultaneously distinguish them from what it calls ‘the oversight to be performed by the monitoring body as for any code of conduct’. The EDPB probably means that audits can/should be carried out internally (with the possibility of delegating these to external consultants) as a sort of ‘supplement’ to data protection officers, in order to assess compliance internally on an ongoing basis. Meanwhile, the monitoring body is posited as a supervisory body that carries out an external assessment in addition. While it is understandable that the EDPB would call for ‘auditors’ as a particular extra way to perform compliance checks, it does muddle the relationship vis-a-vis the monitoring body. After all, assessing an applicant’s initial and continued eligibility, and considering sanctions are part of a monitoring body’s regular tasks. The fact that the phrasing has not been clarified vis-à-vis the first version of the Guidelines is disappointing.

V. Conclusion: A Positive Evolution with Some Drawbacks

The EDPB has by now built up a coherent body of work that provides guidance to private actors on how to engage with the different aspects of the GDPR – including codes of conduct. This is highly important since codes under the 1995 Data Protection Directive were considered unsatisfactory by the European Commission. Industry actors echoed this, with critique mostly aimed at the lengthy procedures before national data protection authorities and the Article 29 Working Party (respectively the predecessors to the EDPB). A lack of procedural clarity and guidance can be considered partly to blame for this outcome.

The EDPB has certainly addressed this by providing crucial clarification on the exact steps to follow for the approval of national and transnational codes via Guidelines 1/2019, acknowledging explicitly the need for increased legal certainty when using codes. Guidelines 04/2021 build upon this solid foundation by repeatedly referring to Guidelines 01/2019, pointing out established terms and procedures in the context of codes. This significantly strengthens the regulatory ecosystem for codes of conduct.

However, Guidelines 04/2021 never once refer to ‘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’. On the one hand, this is logical since Guidelines 05/2021 have not yet been adopted. Its consultation period ended on 31 January 2022. Nonetheless, the subject matter of both guidelines is so inherently intertwined that cross-references should be included in both. Perhaps the EDPB will build in references in the final version of Guidelines 05/2021, and perhaps it will update Guidelines 04/2021 once Guidelines 05/2021 have become final. To achieve true consistency in its body of work, the EDPB may want to avoid unfortunately incompatible timelines for future related guidelines. It does refer to ‘Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection

28 ibid 13.
33 EDPB, ‘Guidelines 1/2019’ (n 2) para 23.
of personal data’ to rightfully point out that codes may need additional measures for their use as transfer tools.

The biggest point of criticism should be focused on the fact that Guidelines 04/2021 are sometimes ‘sloppy’. The document has several grammatical errors. This causes the sentence in paragraph 18 regarding an EEA entity’s abilities in particular to be unclear (as discussed above). Just as unclear is the provision on data protection audits, although this is the result of the concepts and procedures remaining conceptually unclear – especially when considering their relation to the existing guidance.

The comments received during the public consultation period showcase the importance of legal certainty regarding codes for transfers for actors in the field. Besides more traditional industry groups such as Digital Europe and FEDMA (Federation of European Data and Marketing), the Guidelines also drew comments from two medical research groups. The Multi-Regional Clinical Trials Center of Brigham & Women’s Hospital and Harvard (MRCT Center) noted that the GDPR made cross-border research challenging and explicitly mentions that national supervisory authorities have held off on approving codes until the EDPB had issued this guidance. Similar concerns have been raised by the International Cancer Genome Consortium (ICGC) where ‘a number of difficult barriers (...) for international transfers of personal data essential (...) to accelerate research in genomic oncology’ were reported. The importance of tools such as codes of conduct to enable international research simply cannot be overstated.

The European Commission has spoken out on the potential for codes as compliance tools. Guidelines 04/2021 are a very positive step forward in realising that goal for the use of codes as transfer tools, due to many well-considered provisions. Now it is up to private actors to prove the guidelines’ feasibility in the field.

34 See on page 6: ‘Codes of conduct (...) will notably allow a given controller or processor in a third country to providing appropriate safeguards’. See also on page 9: ‘[C]odes of conduct (...) are also or more specifically aimed for third country controllers/processors’.

35 Multi-Regional Clinical Trials Center of Brigham & Women’s Hospital and Harvard, ‘Feedback reference 04/2021-0009’ (29 September 2021).
