DIGITALEUROPE

1 OCTOBER 2021

Response to draft EDPB Guidelines on codes of conduct as tools for transfers

Executive summary

DIGITALEUROPE welcomes the draft Guidelines on the use of codes of conduct (CoCs) for the purpose of transferring personal data to third countries published by the European Data Protection Board (EDPB).[1]

Data transfers are part and parcel of a functioning modern economy,[2] and it is vital for industry to be able to rely on the full set of transfer mechanisms established by the General Data Protection Regulation (GDPR).[3] We believe, in particular, that CoCs can bolster best practice, improve the public's understanding of data transfer requirements, and improve enforcement.

In this context, we commend the draft Guidelines' practical approach, which allows stakeholders to duly consider the necessary aspects needed to develop CoCs for transfers.

In particular, we welcome the explicit recognition that CoCs can address common needs of more than one sector.[4] As we have consistently argued, this approach can facilitate scalability of solutions to common data protection problems encountered across different industries and activities.[5] Similarly, the recognition that existing CoCs can be amended to include transfer provisions,

[1] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-042021-codes-conduct-tools-transfers_en

[2] On the value of data transfers for the European economy, see our report *Data flows and the Digital Decade*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2021/06/DIGITALEUROPE_Data-flows-and-the-Digital-Decade.pdf

[3] Regulation (EU) 2016/679.

[4] Para. 6 of the draft Guidelines.

[5] See our *Response to public consultation on draft EDPB Guidelines on codes of conduct and monitoring bodies*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2019/04/DIGITALEUROPE-response-to-draft-EDPB-guidelines-on-codes-of-conduct-and-monitoring-bodies.pdf

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

consistent with Art. 40(2) GDPR, will promote due consideration of transfers under this tool.[6]

In our comments we focus on minor areas where we find the final Guidelines should still be improved. Notably:

- Recognising that CoCs can adhered to by data exporters alone, and not necessarily also by data importers;
- That, subject to all other relevant criteria, monitoring bodies need not necessarily be headquartered in the EU; and
- That CoCs for transfers can also be purely national in nature, depending on the needs of the relevant processing sector.

Table of contents

[6] Para. 13 of the draft Guidelines

Who can adhere to a CoC

We welcome the draft Guidelines' explicit statement that CoCs do not necessarily have to be adhered to both by data exporters and by data importers, including those not subject to the GDPR.[7] This allows importers to adhere to a CoC without the need for exporters to do so themselves. This stems from Art. 40(3) GDPR, and supports the use of CoCs as not simply a copy of existing binding corporate rules (BCRs) or standard contractual clauses (SCCs) but as an independent transfer mechanism. This will be of particular advantage to SMEs, who may lack the resources necessary for drawing up and implementing BCRs and SCCs.

It should also be noted, however, that CoCs can also be adhered to solely by data exporters, be they controllers or processors, provided they offer binding and enforceable commitments to apply the identified appropriate safeguards.[8] Indeed, this seems to be the primary scenario envisaged under Art. 40(2) GDPR.

By contrast, the draft Guidelines appear to assume that CoCs are 'in part, or as a whole, more specifically designed for third country controllers/processors.'[9] While a CoC will obviously need to provide appropriate safeguards for the specific transfers it covers, in theory nothing prevents these safeguards to be put forward solely by the data exporter, who must in any event back up such safeguards with binding and enforceable commitments. This assessment is contingent on the specific types of processing and transfer situations addressed by a given CoC.

In light of this, the final Guidelines should recognise at Para. 11 that CoCs – depending on the specific types of processing and transfers they cover – do not necessarily have to provide for direct actions and commitments by data importers but can also take the form of appropriate actions and commitments undertaken by adhering data exporters.

Monitoring bodies

The draft Guidelines appear to require monitoring bodies for CoCs valid for transfers not only to be headquartered in the European Economic Area (EEA), but also to 'be able to control the monitoring body's entities outside the EEA.'[10]

---

[7] Paras 7-8 of the draft Guidelines.

[8] This is supported by Art. 40(3), which states that adherence by entities not subject to the GDPR can be '[i]n addition to adherence by controllers or processors subject to this Regulation.'

[9] Para. 11 of the draft Guidelines.

[10] Para. 18, ibid.

However, while we believe in most cases this will indeed be the case, there is no requirement under the GDPR for monitoring bodies to be headquartered in the EEA. Similarly, and correctly, such requirement is not mentioned in previous EDPB guidance.[11]

While it is obviously vital to ensure the monitoring body fulfils all the criteria laid down in Art. 41(2) GDPR, it cannot be excluded that such criteria can be met by an EEA establishment of a non-EEA-headquartered body.

The fact that a specific CoC deals with data transfers does not create a need to restrict the criteria for accreditation of monitoring bodies to EEA entities, as in any event a non-EEA-headquartered monitoring body with an EEA establishment would not be involved in the data transfers covered by the CoC themselves.

Transnational codes

The draft Guidelines assume that CoCs used for transfers will need to achieve general validity in the Union in order to be valid.[12] This, however, has no basis in the GDPR.

While we believe that CoCs inherently benefit from the scale that can be provided by pan-European applicability – and while we urge the EDPB and the Commission to further incentivise the creation and approval of transnational CoCs – a CoC, even if used for transfers, need not necessarily imply transfers involving more than one Member State.

For example, a sectorial association in a Member State may wish to develop a CoC for a particular sector that also includes relevant provisions for transfers. Such CoC would only apply to data processing activities, including transfers, in the context of the activities performed by that particular sector in that Member State. As such, the association should be able to have its CoC approved by the competent supervisory authority without any need to activate the procedure for a transnational CoC.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security

[11] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679.

[12] See, in particular, paras 9 and 21–23 of the draft Guidelines.

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Martin Bell

Privacy and Security Policy Manager

martin.bell@digitaleurope.org / +32 492 58 12 80

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, ESET, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK