DIGITALEUROPE

Response to public consultation on draft EDPB Guidelines on codes of conduct and monitoring bodies

Brussels, 2 April 2019

EXECUTIVE SUMMARY

DIGITALEUROPE believes that codes of conduct, like certification, can play an important role in facilitating as well as demonstrating compliance with the General Data Protection Regulation (GDPR). The GDPR text provides sufficient flexibility as to how codes can be brought into actual existence, and GDPR implementation must make it practical for organisations to develop and participate in codes.

To date, no EU-wide code has been approved, and the limited number of codes that do exist are all restricted to national application. This inherently fragments the European market for codes of conduct and greatly reduces their potential to facilitate GDPR compliance.

With this in mind, in our response we urge the European Data Protection Board (EDPB) to include the following suggestions in its final Guidelines:

a. Recognising that codes, provided they sufficiently specify the GDPR, can apply to more than one single industry sector;

b. Third-country transfers should be considered as a matter of priority for successful codes;

c. EU-wide codes should feature more prominently and the conditions for their approval should be streamlined to achieve more scale and more consistent protection across Europe; and

d. Ensuring that flexible and harmonised rules for monitoring bodies are put in place.

APPLICABILITY TO DIFFERENT SECTORS

The GDPR's Art. 40(1) provides that codes should contribute to the GDPR's proper application 'taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.'

We understand this language as a general requirement for codes to consider how their application could benefit different industry sectors, types of processing operations and/or SMEs, but not as a hard requirement that codes be applicable *only* to a single industry sector or an SME subset of a single sector. Throughout the draft Guidelines, however, the EDPB describes a code's applicability to a single sector as an absolute requirement.[1]

[1] See in particular paras 35-36.

We believe that the final Guidelines should explicitly recognise that, provided a code 'aim[s]s to codify how the GDPR shall apply in a specific, practical and precise manner,'[2] it can in principle be applicable to more than one industry sector. This also applies to the definition of 'code owners,'[3] which should be clarified as potentially referring to more than a single association hailing from a single industry sector.

Drafting codes for a single sector using legal and technology concepts only applicable to it 'is an acceptable method,'[4] but the GDPR does not prescribe that it be the only one. This should be a factual determination based on the contents and merits of each code.

Organisations from different sectors, or organisations comprising multiple sectors, might find it appropriate to adopt largely similar solutions to implement GDPR compliance, with respect to specific types of data processing or even to their data processing operations as a whole.[5] The fact that a code detailing such solutions might be open to companies – be they multinationals or SMEs – from sectors as varied as retail and manufacturing shouldn't in and of itself preclude its approval.

THIRD-COUNTRY TRANSFERS

We regret the EDPB's choice not to include more detailed consideration of transfers to third countries beyond paragraph 17. Although we appreciate that separate guidelines are being announced, we believe that transfers to non-EEA jurisdictions will represent a key factor in generating uptake of GDPR codes and should therefore be dealt with in the final Guidelines.

Because GDPR codes can in principle allow for a comprehensive assessment of an organisation's processing activities,[6] which may include transfers to third countries or international organisations, we believe the final Guidelines should explicitly state that, to the extent that the commitments required by Art. 46(2)(e) are included in a code, adherence to such code can represent an appropriate safeguard to enable third-country transfers.

IMPORTANCE OF EU-WIDE CODES

The draft Guidelines apply a strict distinction between 'national' and 'transnational' codes and go on to focus purely on procedural aspects based on such distinction.[7]

This approach appears narrow and of limited value. On the one hand, the relatively straightforward procedure described for national codes does not address the complexity generated by different Member State laws. On the other, the procedure described for 'transnational' codes adds layers of redundancy compared to the GDPR text. This will not help in the assessment of codes and, most importantly, will inhibit the approval of EU-wide codes, which contradicts the GDPR's fundamental goal of ensuring the free movement of personal data within the Union.

[2] Ibid., p. 14.
[3] Ibid., p. 5.
[4] Ibid., p. 14.
[5] We welcome the explicit recognition in the draft Guidelines that adherence to a code can be used as an element to demonstrate an organisation's GDPR compliance as a whole (p. 9). This creates a clear incentive for organisations to participate, provided relevant targets for evaluating compliance are included, while still allowing for more targeted codes.
[6] See p. 9 of the draft guidelines and footnote 5 of our response.
[7] Pp. 15-19. We note that the terms national and transnational cannot be found in the GDPR text with respect to codes.

The GDPR describes a relatively lean procedure for codes that relate to processing in more than one Member State. A code either is solely national in nature, in which case it is assessed by the single national data protection authority (DPA), or otherwise 'relate[s] to processing activities in several Member States' and is therefore referred to the EDPB for an Opinion and subsequently to the Commission, who is empowered to give such code 'general validity within the Union.'

By contrast, the draft Guidelines require the national DPA to whom a code was submitted to individually identify and notify DPAs concerned, letting them participate in a joint review although the final approval of the Code would still rest with the original DPA. In addition, the DPAs concerned subsequently are also provided with an opportunity to raise issues before the code is submitted to the EDPB.

We would find it more beneficial if the final Guidelines focused on the elements necessary for DPAs to determine whether codes submitted to them could be considered as relating to processing activities in several Member States, which would trigger reference to the EDPB as described in Art. 40(7) and the Commission's assessment under Art. 40(9). While it is the Commission alone who can grant a code EU-wide validity,[8] the Commission's assessment is the final step in a longer process that essentially rests with the DPAs and the EDPB, and as such we urge the EDPB to focus on this aspect.

NATIONAL LEGISLATION

The draft Guidelines state that codes must include specific provisions with respect to compliance with national legislation. This seems to cover not only data protection-specific obligations but also other 'relevant legal obligations under national law.'[9]

While codes should quite clearly not contradict Member State – or, for that matter, EU – law, and while in some cases – particularly for solely national codes – specific reference to national legislation might be in order, a general requirement for all codes to explicitly cover national legislation is not included in the GDPR text. The final Guidelines should therefore make it clear that reference to specific Member State law should only be provided if relevant.

LANGUAGE

The draft Guidelines stipulate that transnational codes should always be submitted in the language of the relevant national DPA.[10] We believe that a more pragmatic approach should be described whereby, unless clear exceptions can be found, EU-wide codes can be submitted in English so as to facilitate the procedure for an EDPB Opinion and subsequent Commission implementing act.

FLEXIBLE RULES FOR MONITORING BODIES

We welcome the draft Guidelines' recognition that codes may be monitored by either external or internal monitoring bodies, provided that relevant procedures and structures to ensure their independence and expertise are in place.[11] This flexible approach will make codes more easily implementable and scalable.

[8] We note in passing that, regrettably, the draft Guidelines only devote two lines to the Commission process, p. 19.
[9] Ibid., p. 12.
[10] Ibid.
[11] Ibid., p. 20.

Along the same lines, we'd like to draw the EDPB's attention to the fact that the draft Guidelines state that accreditation 'applies only for a specific code.'[12] However, footnote 11 states that 'a monitoring body may be accredited for more than one code provided it satisfies the requirements for accreditation.' We believe this should be the default position and that this text should be moved to the body of the document.

The draft Guidelines refer in passing to the similarities between internal monitoring bodies and data protection officers (DPOs). We would welcome it if the final Guidelines could elaborate more on this relationship and on whether, or under what additional safeguards, DPOs could be accredited as monitoring bodies in their own right in light of their statutory independence with respect to their tasks and duties.

Finally, it is important to stress that a code cannot be approved if it doesn't identify a monitoring body. As a consequence, it appears that no codes can be submitted unless criteria for the accreditation of monitoring bodies have been approved by the competent DPAs. Given the delays and the potentially divergent results that this process may create, we encourage the EDPB to consider approving an Opinion, or more detailed Guidelines, setting out consistent and harmonised criteria for accreditation.

--

For more information please contact:
Alberto Di Felice, Senior Policy Manager for Infrastructure, Privacy and Security
alberto.difelice@digitaleurope.org or +32 471 99 34 25

[12] Ibid., p. 5.

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's members include in total over 35,000 ICT companies in Europe represented by 66 Corporate Members and 40 National Trade Associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Brother, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: Nederland ICT, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK