DIGITALEUROPE

DIGITALEUROPE response to EDPB consultation on draft guidelines on certification and identifying certification criteria

Brussels, 12 July 2018

DIGITALEUROPE is pleased to provide its input to the European Data Protection Board's (EDPB) draft guidelines on certification and identifying certification criteria in accordance with Arts. 42 and 43 of the General Data Protection Regulation (GDPR).

DIGITALEUROPE believes that certification, like codes of conduct, can play an important role in both facilitating and demonstrating GDPR compliance. The GDPR provides for detailed rules for the approval of certification mechanisms, but at the same time also allows sufficient flexibility as to how the instrument can be brought into actual existence. Hence, the success of GDPR certification will be a function of how Arts. 42 and 43 are implemented by all parties involved – Member State data protection authorities (DPAs), the EDPB, the European Commission and industry.

Implementation must make it practical for organisations to participate in certification mechanisms, seals and marks developed under the GDPR. In our response, we would like to put forward some suggestions for areas where the draft guidelines could be improved to ensure more coherence and effectiveness in the development of these instruments.

INTEROPERABILITY WITH OTHER SCHEMES

Certification is a lengthy and costly process, with organisations already presented with a broad range of options in terms of scope (multi-sector vs. single-sector, comprehensive vs. single-issue, based on technical standards or legal requirements, applying to products, services or processes, etc.) and geography (international, regional or national).

The more GDPR certification is interoperable with existing or prospective schemes – e.g. ICT cybersecurity certification under the proposed Cybersecurity Act, which in turn should allow for interoperability with existing frameworks and standards[1] – the more organisations will find it useful and practical to certify. To facilitate organisations' participation, GDPR certification should allow companies to leverage compliance with other schemes to the extent that substantive and procedural requirements overlap.

[1] See DIGITALEUROPE's position paper on the European Commission's proposal for a European framework for cybersecurity certification schemes for ICT products and services, available at http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&entryID=2587&language=en-US&PortalId=0&TabId=353

The draft guidelines partially address this point in section 6.1 – which only refers to national initiatives, while EU-level and global initiatives should also be included – but we believe this short section underplays the relevance of interoperability for both the substantive protection afforded by the GDPR and the actual uptake of GDPR certification in the market.

SCOPE OF CERTIFICATION

The draft guidelines (section 1.2) stress the relevance of some *specific* obligations in the GDPR where certification can be used as an element to demonstrate compliance, notably in terms of technical and organisational measures and sufficient guarantees. However, we believe it would be incorrect to interpret the fact that certification is explicitly called out in Arts. 24(3), 25(3), 32(3) and 28(5) to mean that certification is *only* available in these instances.

In addition to the fact that Art. 42(1) considers 'processing operations' more in general, rather than specific obligations, the very fact that all above-mentioned articles refer to organisational and technical measures illustrates that the scope of certification can be very broad; therefore, the availability of certification should not be limited to proving compliance with respect to specific articles but not others.

Section 5.1 of the draft guidelines seems to recognise that 'the GDPR provides a broad scope for what can be certified,' but the examples contained in the following section 5.2 frustrate this by describing very narrow targets of evaluation.

In this context, we believe it is important for the guidelines to explicitly recognise that certification can be used as an element to demonstrate compliance of an organisation's personal data processing activities as a whole. This would create clear incentives for organisations to certify, provided relevant targets for evaluating compliance are included, while still allowing for more targeted forms of certifications, seals and marks.

INTERNATIONAL DATA TRANSFERS

Although we appreciate that the EDPB will publish separate guidelines concerning third-country transfers in accordance with Art. 42(2), we believe that transfers to non-EEA jurisdictions will represent an important factor in generating uptake of GDPR certification and should therefore be dealt with to some extent in the final guidelines.

Because GDPR certifications can in principle allow for a comprehensive assessment of an organisation's processing activities, which may include transfers to third countries or international organisations (as currently reflected in example 5 in the draft guidelines), we believe the final guidelines should explicitly state that, to the extent that the commitments required by Art. 46(2)(f) are included in a given certification mechanism, certification can represent an appropriate safeguard to enable third-country transfers.

INTEROPERABILITY WITH BINDING CORPORATE RULES

Interoperability plays an important role not only in relation to other existing or prospective certification schemes and standards, but also in relation to other GDPR accountability tools such as binding corporate rules (BCRs).

In line with the previous sections of our response, we note that BCRs in particular must not only contain the appropriate safeguards for third-country transfers under the requirements laid down in Art. 47(2), but also provide a comprehensive tool to assess the substantive and procedural requirements needed to

demonstrate compliance with the GDPR at large. The BCR approval process is in fact very similar to certification, where the competent DPA effectively acts as a certification body within the meaning of Art. 43(1)(a).

For these reasons, we suggest that the final guidelines should explicitly recognise BCRs as an accountability tool that is interoperable with certification. Organisations that have already adopted BCRs should be able to rely on them, should they want to certify, to the extent that substantive and procedural requirements overlap. Similarly, the upcoming guidance to ensure a harmonised approach for DPAs when approving certification criteria (Arts. 42(5) and 43(2)(b)) could build on the Article 29 Working Party's (WP29) previous work on BCRs.

HARMONISED ASSESSMENT OF CERTIFICATION CRITERIA

The flexibility available for the creation of GDPR certifications, seals and marks may lead to unnecessary duplication and fragmentation. While it is important to allow for the development of certification mechanisms that cater to specific sectors, products/services or national needs – including competing mechanisms if the market can accommodate them – ensuring EU-wide harmonisation is vital to generate the scale necessary for industry to see value in certifying.

In this context, we believe that rules on the approval of certification criteria should be tackled as a priority by the EDPB. The draft guidelines announce upcoming guidance that will be made available at a later stage as an annex. We recommend that such guidance should be adopted swiftly and on a standalone basis.

Early clarity as to the verifiability, significance and suitability of criteria (p. 10 of the draft guidelines) will facilitate EU-wide harmonisation and global interoperability that could be applied to certifications across sectors, products/services and Member States. The same applies to delegated and implementing acts adopted by the European Commission under Art. 43(8) and (9).

Proper involvement of the private sector in the development of rules and requirements for certification – as well as due consideration of other existing frameworks, standards and mechanisms, including BCRs as per the previous section of our response – will be key to generate scale and market uptake. This is particularly important given the possibility for the EDPB itself to approve criteria on the basis of the consistency mechanism, thus resulting in a European Data Protection Seal available at EU level.

CERTIFICATION AND FINES

Because certification can only be used as an element in demonstrating compliance but does not in itself guarantee compliance, we would like the EDPB to clarify its statement that DPAs should consider adherence to approved certification mechanisms as an *aggravating* factor when considering fines. We believe the letter of Art. 83(2)(f) gives consideration to certification first and foremost as a mitigating factor, except where repeated or serious violations or misrepresentation might indeed require heavier fines. Moreover, if non-compliance is unrelated to the certification, certification should not be used as an aggravating factor.

--

For more information please contact:
Alberto Di Felice, DIGITALEUROPE's Senior Policy Manager for Infrastructure, Privacy and Security
alberto.difelice@digitaleurope.org or +32 2 609 53 10

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 63 Corporate Members and 39 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

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

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
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