DIGITALEUROPE

30 SEPTEMBER 2022

Certification as a tool for transfers: diversifying safeguards

Executive summary

DIGITALEUROPE welcomes the European Data Protection Board's (EDPB) work to enable certification as a tool for transfers.[1] Certification relies on internal company processes which can provide for structured, documented and controllable safeguards to enable international transfers of personal data.

Since the onset of the General Data Protection Regulation (GDPR),[2] and increasingly after the *Schrems II* ruling,[3] businesses in Europe have been diversifying the range of technical and organisational measures to protect transfers and continue playing an active role in global trade. In this context, the final Guidelines should do more to fully establish certification as a reliable legal tool for transfers.

For certification to be safely relied upon by exporters and importers, the final Guidelines should:

- Build upon existing certification practices and clarify the conditions upon which a certification can be called into question;
- Further recognise that certification can bolster good practice across the EU, without adding excessive criteria for transfers; and
- Bring practical and positive examples of how certification can be put in place.

[1] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-072022-certification-tool-transfers_en.

[2] Regulation (EU) 2016/679.

[3] Case C-311/18.

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

Table of contents

Actors involved and responsibilities

Existing certification models are used by industry to demonstrate GDPR compliance and attribute roles to the different parties involved, often by contractual means. The final Guidelines should build on existing practices and clarify certain points on rejecting or withdrawing certification.

Existing certification models

Over time, different certification models have been implemented by industry to facilitate and demonstrate GDPR compliance, including aspects that are critical to the GDPR such as cybersecurity. Companies have therefore accumulated experience and knowledge around certification mechanisms, which can serve as a reliable framework to ensure stable data flows. For this reason, existing practices and contractual freedom should be considered in the final Guidelines.

For example, the draft Guidelines stipulate that the importer's assessment of a third country's legislation and practices should itself be assessed by the certification body. More precisely, that certification bodies should have the necessary resources to be able to verify that 'the importer has carried out an assessment of the legal situation and practices of the third country/ies where it is located.'[4] It is important to ensure this wouldn't lead to excessive levels of assessments of a third country's legislation and practices.

The control is then further reinforced by the possibility of onsite audits. However, if the certification body has the obligation to monitor changes in third-country legislation, communication should be established between the body and the importer or exporter. The task of monitoring a third country's legislative developments is costly and time-consuming. Cooperation and exchange between the parties involved should be promoted by the final Guidelines, rather than imposing control upon control. Different actors could rely on contractual warranties that the laws and practices in the third country allow the fulfilment of their commitments, as suggested later in the draft Guidelines.[5]

The role of authorities

As consistently stated in our previous positions, the success of certification frameworks will rely on all parties involved, including data protection authorities (DPAs).[6] Although the roles of the data importer and exporter are detailed in the

[4] Para. 33 of the draft Guidelines.

[5] Para. 51 of the draft Guidelines.

[6] DIGITALEUROPE, *Response to EDPB consultation on draft guidelines on certification and identifying certification criteria*, available at:

draft Guidelines, the basis upon which certification could be rejected by supervisory authorities, or upon which the EDPB could give a negative Opinion, should be clarified. This would afford importers, exporters and accreditation bodies alike more legal certainty as to what is expected by authorities.

Last, we commend the draft Guidelines for not focusing on the applicability of certification only to individual industry sectors. We have consistently argued in favour of the recognition of certification across different industries and activities. This cross-sectoral approach can facilitate scalability of solutions to common issues.

A safeguard to increase resilience

The *Schrems II* ruling has caused European exporters as well as importers to seek further legal safeguards and prevent disruptions to data flows that would be damaging to the European economy. Our survey on the use of standard contractual clauses (SCCs) showed that only about 9 per cent of companies based in Europe do not transfer any data outside the EU.[7]

Strong EDPB Guidelines play a key role in enabling companies to find firmer ground to actively take part in global trade and increase resilience. Certification can bolster best practices by diversifying the options available to companies to ensure appropriate safeguards for data transfers in compliance with the GDPR. Certification should remain adaptable to different cases, without complexity and cost increasing.

We commend the EDPB for recognising that safeguards can be diversified and encourage the final Guidelines to reinforce this approach, as further discussed in the section below.

> '*Safeguards should of course be in place to ensure that European data is not misused, including outside Europe. Yet, the way we go about it can make all the difference between Europe thriving in the global data economy, or missing out.*'[8]

https://www.digitaleurope.org/wp/wpcontent/uploads/2019/01/DIGITALEUROPE%20response%20to%20EDPB%20consultation%20on%20draft%20guidelines%20on%20certification.pdf.

[7] DIGITALEUROPE, *Schrems II impact survey report*, available at: https://www.digitaleurope.org/wp/wpcontent/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf.

[8] DIGITALEUROPE, *Data transfers in the data strategy: Understanding myth and reality*, available at https://www.digitaleurope.org/wp/wpcontent/uploads/2022/06/DIGITALEUROPE_Data-transfers-in-the-data-strategy_Understanding-myth-and-reality.pdf.

Making certification a practical tool

Certification in practice

The draft Guidelines state that certification criteria should 'adequately assess whether and to what extent [transparency and data subject rights] are enforceable.'[9] This criterion is listed just after requiring that an appropriate complaint-handling procedure be established, hence ignoring the fact that complaint-handling procedures are themselves a means to enforce rights.

The expansive list of additional certification criteria given in the draft Guidelines is detailed in the form of an extensive number of questions. We recommend that the final Guidelines specify that the additional criteria supplement existing standards for certification without making the tool more difficult to attain.

Last, the examples given in the annex could represent an opportunity for practical guidance. However, they are critical of technical measures such as pseudonymisation without illustrating cases where such measures can in fact serve as effective protections. These examples do exist and their proactive acknowledgment in the final Guidelines is essential to make certification a practical tool.

Aligning certification with other available tools

Certification is one of several tools listed under Art. 46 GDPR. Considering the similar approval process for other tools, interoperability between certification and binding corporate rules (BCRs), in particular, should be recognised. If substantive and procedural requirements overlap, organisations having adopted one or the other mechanism should be able to rely on both.

The final Guidelines should further recognise European certification standards (e.g. CEN/CENELEC JTC13). The possibility of following one certification model across the EU could help avoid a fragmented single market and allow more cohesive application of transfer tools. Mapping existing certifications and identifying common standards across the EU would enhance compliance efforts and help DPAs in cross-border enforcement.

Although the draft Guidelines note that binding and enforceable commitments may be taken based on contracts, they do not specify which other instruments can be used. Other instruments, such as adherence to state-of-the-art technical standards, could however widen the possibilities for importers and exporters to use certification.

[9] Para. 41 of the draft Guidelines.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy & Security Policy

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

Beatrice Ericson

Policy Officer for Privacy & Security Policy

beatrice.ericson@digitaleurope.org / +32 490 44 35 66

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, Banco Santander, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eli Lilly and Company, Epson, Ericsson, ESET, EY, 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, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, RELX, 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
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
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: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK