Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CIPL Response to the EDPB Draft Guidelines 07/2022 on certification as a tool for transfers

Centre for Information Policy Leadership (CIPL)

28 September 2022

28 September 2022

CIPL RESPONSE TO THE EDPB DRAFT GUIDELINES 07/2022 ON CERTIFICATION AS A TOOL FOR TRANSFERS

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to comment on the European Data Protection Board (EDPB) draft Guidelines 07/2022 on certification as a tool for transfers.

CIPL recognised the potential of certifications under GDPR as a safe and efficient mechanism for GDPR compliance, including cross-border transfer, early on. In our 2017 discussion paper *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms,*[2] we noted that developing a common EU-wide GDPR certification for purposes of data transfers should be a priority for the Commission and the EDPB. Therefore, CIPL appreciates and welcomes the EDPB's efforts on Guidelines regarding the application of Article 46(2)(f) of the GDPR, especially for the transfer of personal data to third countries or international organisations on the basis of certification. Transfers to third countries have become increasingly challenging to navigate since the *Schrems II* judgment, while the flow of data is vital to large parts of the EU economy.[3]

CIPL continues to believe that certifications, if designed and implemented appropriately, can provide substantial benefits for individuals, industry, and DPAs alike and can significantly contribute to effective and efficient privacy protection for individuals in a globalised world:

Individuals	Certifications create **trust and confidence** in a certified organisation's handling of the transfer of their personal data and improve the transparency of the process.
	Adherence to certifications by organisations will **improve compliance and privacy outcomes** for individuals.
Organisations	**Demonstrate accountability and compliance.** Certification is an element of demonstrating GDPR compliance and accountability. This is an internal benefit vis-à-vis management, the board and shareholders but will also have a positive effect on an organisation's relationships with DPAs, customers and business partners.
	Operationalising compliance. Certifications translate high-level GDPR requirements into operational compliance steps that are closely tailored by subject-matter experts to the organisation and their privacy management

[1] CIPL is a global privacy and data policy think and do tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Centre for Information Policy Leadership, *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms*, April 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.

[3] European Commission, *Factsheet: Trans-Atlantic Data Privacy Framework*, 2022, available at https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100, as noted by the European Commission, the continued data flows between the EU and US alone, underpin more than 900 billion euros in cross-border commerce every year.

	programs. This may result in more relevant, fit-for-purpose and effective privacy and data management programs.
	Scalable for SMEs and start-ups. The increasingly complex reality of international data transfers is a particularly difficult challenge for SMEs and start-ups who have fewer in-house expertise and resources at their disposal. Such organisations will be significantly helped by a well-conceived and properly implemented certification provided by third-party certification bodies with appropriate expertise to ensure that the certifying organisation's policies and processes are compliant. A certification can have important **due diligence functions for controllers** by providing processors or service providers means to evidence their compliance and accountability to potential business partners/controllers. For international transfers, this can be especially advantageous in multiple and repetitive multiple-party transfer scenarios.
Data Protection Authorities	Certification mechanisms help DPAs deploy and maximise their resources more effectively because certification bodies take on and share certain oversight tasks that might otherwise fall on the regulator, including the certification process itself, compliance monitoring and basic complaint handling. Overall, a well-structured certification against which compliance is assessed allows for more efficient and **less resource-intensive DPA oversight**.

It is crucial to ensure that these benefits of certifications are fully enabled by the Guidelines. Any GDPR certification scheme must present tangible benefits for certified organisations to invest time and money in obtaining and maintaining them on top of the many other requirements to which they are already subject.

At present, the Guidelines still lack certain elements that would create those necessary incentives for wider adoption by the industry. Below, we provide more detailed comments on those aspects of the Guidelines that would benefit from further consideration and improvement.

In the context of Guidelines 07/2022, the EDPB should:

- Create a baseline EU-wide certification standard to avoid divergence and proliferation of certifications in the EU.
- Limit national certification schemes to organisations whose privacy programs, services and products are equally limited to a single member state. These national certifications should still be consistent with each other and the general EU baseline standard, and mutually recognised.
- Ensure consistency with other EU-based and global transfer mechanisms and accountability-based instruments and frameworks that substantially align with relevant GDPR standards.
- Avoid certification requirements that would unnecessarily conflict with other international accountability-based systems.
- Give credit to BCR-approved companies towards GDPR certification if their BCR meets the relevant certification criteria.
- Ensure consistency between different certifications and similar transfer mechanisms and interoperability across global jurisdictions.
- Promote and enable interoperability between data transfer mechanisms.

- Accreditation of certification bodies, pursuant to Article 43(1)(a), should also follow common EU-wide accreditation standards approved by the EDPB, taking into account, where relevant, the requirements adopted by the Commission in accordance with Article 43(8) GDPR. While ISO 17065 should be viewed as instructive and useful for guidance, it should not be mandatory.

I. NO COMMON EU GDPR BASELINE FOR CERTIFICATION

The GDPR does allow national and EU-wide certifications to work in parallel. Certifications that currently exist or are under development in the EU at the national level (or may be developed in the future at the national level) should be aligned with a common EU-wide GDPR baseline certification. Currently, the Guidelines do not provide for a common EU GDPR baseline for certification in the context of data transfers.

Instead, the Guidelines note: "Certifications issued according to nationally approved certification schemes in the EEA States are also possible to be used as a tool for transfers, but they are only valid for transfers to third countries from exporters in the EEA Member States where the certification scheme has been approved as there is no mutual recognition of different EEA state certifications".[4] By contrast Guidelines 1/2018 stipulates that "The EDPB acknowledges that it is desirable to avoid fragmentation of the data protection certification market. It notes that Article 42(1) provides that the Member States, the supervisory authorities, the Board, and the Commission shall encourage the establishment of certification mechanisms, in particular at Union level".[5]
Lack of mutual recognition of member state-level certifications will create fragmentation and result in inefficient overlapping certification schemes. Instead, the EDPB should follow its own proposed approach in Guidelines 1/2018 and create a baseline EU-wide certification standard recognised across member states. An overlap and proliferation of certifications in the EU (or elsewhere) should be avoided at all costs as it would lead to confusion for all stakeholders, including individuals, and discourage organisations from seeking certification altogether. A general comprehensive EU certification standard would ensure EU-wide consistency while also enabling specialised application and adaption of that baseline to specific sectors, such as pharma, advertising, credit referencing, et cetera.[6]

National certifications should be only for organisations whose privacy programs, services and products are limited to a single member state. At the same time, these national certifications should still be consistent with each other and the general EU baseline standard and mutually recognised. Otherwise, there will be confusion and inconsistent protections and requirements for individuals and businesses moving and operating across the EU.

II. CLARIFICATION OF CERTIFICATION CRITERIA SPECIFIC TO THIRD COUNTRY LEGISLATION

The Guidelines helpfully clarify that certification as a transfer tool can be applied to a single processing operation or several operations as part of a governance process.[7] As mentioned earlier, there are clear benefits to obtaining certification. However, especially for data transfers, the certification has to

[4] Guidelines 07/2022, paragraph 30.
[5] Guidelines 1/2018, paragraph 35.
[6] See also Centre for Information Policy Leadership, *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms*, April 2017.
[7] Guidelines 07/2022, paragraph 17.

provide added incentives compared to Standard Contractual Clauses or other mechanisms to be more widely adopted by organisations. This would be the case where the certification can provide reliable assurances for the data exporter towards the assessment of third-country legislation required after *Schrems II*.

Currently, paragraph 25 of the Guidelines stipulates that: "The criteria for certification shall include requirements for an assessment of the third country's relevant legal framework to counter the specific risks of transferring personal data in the third country involved and the further processing performed by the data importer". Additionally, paragraph 33 points to the task of the accredited certification body to verify that: "As required by the certification criteria, the importer has in a duly and in a correct way carried out the necessary assessment of the legal situation and practices of the third country/ies where it is located."

However, taking the above into account, it remains unclear to what extent the data exporter, who will often lack the expertise and resources to assess third-country legislation, can concretely rely on the assessment conducted by the importer and verified by the certification body as part of the certification process. Presently, the Guidelines acknowledge that the exporter can use the data importer's assessment "as an element by which to demonstrate compliance" with Chapter V GDPR. This is unlikely to provide sufficient clarity to data exporters with respect to their burden in further assessing third-country legislation and the potential transferer risks after *the Schrems II* decision, considering the consequences of getting it wrong. The EDPB should consider clarifying this aspect further.

The EDPB should also further consider whether elements of the legal assessments of third country law, to the extent these are made public in line with Article 48(8) GDPR, can find application as elements in other transfer risk assessments more generally, where relevant considerations such as a group of data subjects, transfer purpose, industry, are comparable. Further, in order to make certifications viable and advantageous transfer options for organisations, the EDPB should also consider ways to support the required transfer risk assessments. For example, the EDPB (or the EU Commission) could provide detailed guidance for organisations involved in certification-based transfers (exporter/importer/certification body) on the specific transfer risks associated with particular third countries and consider types of supplementary measures that could meet certification requirements

III. SYNERGIES WITH OTHER GDPR SAFEGUARDS AND INTERNATIONAL TRANSFER MECHANISMS

GDPR certification mechanisms must be consistent with other GDPR-based transfer mechanisms and consider similar instruments and frameworks within and outside the EU that substantially align with relevant GDPR standards.

For instance, BCR-approved companies might be given credit for their BCR towards GDPR certification if their BCR meets the relevant certification criteria. The coexistence of certifications for data transfers and other transfer mechanisms such as BCR or the future data transfer framework to replace the EU-US Privacy Shield Framework should not lead to additional costs, investment of resources, or duplication of efforts. Companies that are validly registered in one system should be able to leverage that registration to obtain the other without unnecessary additional burdens. Otherwise, organisations will be reluctant to invest time and money in obtaining and maintaining GDPR certifications on top of the many other certifications and requirements to which they are already subject.

Further, any new transfer-related certifications should, where possible, avoid creating conflicting procedural and substantive requirements with other international systems. Particularly in the context of data transfers, organisations will favour global schemes that are more broadly recognised, resulting in more consistent protection of individual rights and efficient data flows.

Certifications based on the APEC Cross-Border Privacy Rules (CBPR), which are currently being expanded to become the first global transfer mechanism, the Global CBPR, are an example of a framework having particular importance in this regard. It is crucial to avoid the unnecessary proliferation of different certification schemes that are based on similar substantive standards and the process of developing GDPR certifications should be used to harmonise, consolidate and make existing mechanisms interoperable, where possible. This requires an assessment of other data protection certifications already existing in the marketplace, in the EU and globally, particularly such prominent systems as the CBPR, which currently already includes 50 CBPR certifications covering 1887 organisations.[8]

This also requires consultation and collaboration with the foreign jurisdictions that operate such other certification schemes. The European Commission noted in its 2017 communication *Exchanging and Protecting Personal Data in a Globalised World* that EU data protection rules do not have a one-size-fits-all approach to international data transfers and considered BCR-CBPR convergence as well as the development of alternative data transfer mechanisms.[9] Many global companies have a single baseline privacy management program, with all of its essential elements and substantive privacy requirements, that they apply consistently and comprehensively to their processing activities in all countries where they operate. Thus, organisations will leverage the same privacy management programs to obtain different certifications, such as under the anticipated Trans-Atlantic Data Privacy Framework, the Global CBPR, and the BCR in Europe. Therefore, it would be appropriate to ensure that applicable approval and certification rules are as consistent and interoperable as possible across global jurisdictions and between different certifications and similar transfer mechanisms. CIPL recommends that the EDPB formally recognise and include cross-jurisdictional interoperability as a core objective of any EU GDPR certification scheme from the start.

CIPL is encouraged to see the Guidelines allow for the possibility of subcontracting to local "experts or establishments" located outside the EEA.[10] This can provide an opportunity for EU-based certification bodies to cooperate with and leverage the expertise of non-EU monitoring bodies that are otherwise involved in providing certifications under the Cross-Border Privacy Rules (CBPR) and the Privacy Recognition for Processors (PRP).

[8] See CBPR compliance directory at http://cbprs.org/compliance-directory/cbpr-system/, listing all organisations covered by CBPR certifications. As with the EU/US Privacy Shield, a CBPR certification can cover corporate subsidiaries and affiliates that adhere to the same privacy policy as the certifying parent company. Currently, there are about 50 CBPR certifications covering 1887 entities.
[9] European Commission, Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World, COM/2017/07 final, 2017, p. 11.
[10] Guidelines 07/2022, paragraph 12.

IV. CERTIFICATION BODIES ACCREDITATION STANDARDS

CIPL already commented extensively on the Art. 29 Working Party's "Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679", [11] specifically raising the issue regarding the reference to ISO 17065 as a guiding principle for accreditation requirements.[12] As we have stated before: "Strict adherence to the ISO standard may lead to the introduction of prohibitive burdens and costs, thereby limiting the pool of potential certification bodies entering the market. A costly accreditation process or unsustainably high liabilities of certification bodies would create a more costly certification process for controllers and processors. This may practically render Article 42 certifications unavailable to micro, small and medium-sized organisations."[13] CIPL agrees with the aim of the Guidelines 4/2018 to: "Establish a consistent, harmonised baseline for the accreditation of certification bodies that issue certification in accordance with the GDPR"[14], but we would also remind the EDPB that there is no requirement under the GDPR for this to be based in ISO 17065, or any other conformity assessment based frameworks, where the supervisory authorities are charged with developing accreditation requirements. An EU-wide approach to the accreditation of certification bodies to be developed by supervisory authorities has to be designed with sufficient scalability and flexibility to enable the GDPR and equally support the European Commission's stated policy of promoting convergence or interoperability with non-EU cross-border transfer standards and systems.[15]

***

[11] Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679" available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_wp29_guidelines_on_accreditation_of_certification_bodies_under_the_gdpr.pdf.

[12] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) Version 3/04 June 2019, p. 8.

[13] Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679", p. 7.

[14] Ibid, p. 6.

[15] See CIPL's discussion paper on certifications under the GDPR, footnote 5 supra, discussing the Communication from the Commission to the European Parliament and the Council; Exchanging and Protecting Personal Data in a Globalised World, Brussels 10.1.2017, COM (2017) 7 final (Emphasis added), available at http://ec.europa.eu/newsroom/document.cfm?doc_id=41157.

As noted, CIPL provided a more detailed discussion of future GDPR certifications, including for transfer purposes, in its 2017 white paper on *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms*.[16] The top ten messages articulated in that paper are as valid today as they were then:

CIPL's top ten messages on GDPR certifications:

1. Certification should be available for a product, system, service, particular process, or an entire privacy program.
2. There is a preference for a common EU GDPR baseline certification for all contexts and sectors, which can be differentiated in its application by different certification bodies during the certification process.
3. The Commission and/or the EDPB, in collaboration with certification bodies and industry, should develop the minimum elements of this common EU GDPR baseline certification, which may be used directly, or to which specific other sectoral or national GDPR certifications should be mapped.
4. The differentiated application of this common EU certification to specific sectors may be informed by sector-specific codes of conduct.
5. Overlap and proliferation of certifications should be avoided to avoid consumer/stakeholder confusion or make it less attractive for organisations seeking certification.
6. Certifications must be adaptable to different contexts, scalable to the size of the company and the nature of the processing, and affordable.
7. GDPR certifications must be consistent with and take into account other certification schemes with which they need to be able to interact and/or be as much interoperable as possible. APEC (and Global) CBPR are an example of such a transfer scheme.
8. Developing a common EU-wide GDPR certification for purposes of data transfers pursuant to Article 46(2)(f) should be a priority for the Commission and/or the EDPB.
9. Organisations should be able to leverage their BCR approvals to receive or streamline certification under an EU GDPR certification.
10. DPAs should incentivise and publicly affirm certifications as a recognised means to demonstrate GDPR compliance and mitigation in case of enforcement, subject to the possibility of review of specific instances of non-compliance.

We look forward to providing additional input as the Guidelines are finalised.

***

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@HuntonAK.com, Markus Heyder, mheyder@HuntonAK.com, Natascha Gerlach, ngerlach@HuntonAK.com or Lukas Adomavicius, ladomavicius@HuntonAK.com.

[16] Centre for Information Policy Leadership, *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms*, April 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.