Guidelines 07/2022 on certification as a tool for transfers

About EuroCommerce

EuroCommerce is the principal European organisation representing the retail and wholesale sector. It embraces national associations in 27 countries and 5 million companies, including leading global players and many small businesses. Over a billion times a day, retailers and wholesalers distribute goods and provide an essential service to millions of business and individual customers. The sector generates 1 in 7 jobs, offering a varied career to 26 million Europeans, many of them young people. It also supports millions of further jobs throughout the supply chain, from small local suppliers to international businesses. EuroCommerce is the recognised European social partner for the retail and wholesale sector. We welcome the opportunity to contribute the EDBP consultation. Please find below our main concerns.

Main concerns

- Even though there are clear benefits of organizations obtaining certification in general, it is very unlikely that the certification scheme under Chapter V, if the interpretation proposed in the Draft Guidelines is adhered to, will lead to its uptake among the industry players. The main reason for that is the way the EDPB currently constructs the data exporter's role & responsibilities when using certification as a tool for transfers. Specifically, the Draft Guideline requires the data exporter to (paras. 20-23):
    - check if the certification is valid and not expired, if it covers the specific transfer to be carried out and whether the transit of personal data is in the scope of certification, as well as if onward transfers are involved and adequate documentation is provided on them
    - there is a contract or another legally binding instrument between the certified data importer and the certification body, i.e. the 'certification agreement'
    - assess – depending on the concrete roles as controller or processor – whether the certification it intends to rely on is effective in the light of the law and practices in force in the third country
    - verify the supplementary measures provided by the data importer holding certification and if it is able to answer the technical and (if any) supplementary measures asked for by the data importer
    - require from the importer to put in place adapted supplementary measures or establish them by himself.

- While requirements 1-2 essentially instructing the data exporter to verify the scope of certification against the intended data processing and the validity of the 'certification agreement' are widely accepted parts of the due diligence process under other certification schemes (e.g., ISO27001), requirements 3-5 effectively put data exporter under the obligation to carry a so-called transfer impact assessment, even though such assessment might have already been carried out by the data importer and verified (including the supplementary measures) by the certification authority. The major drawback of such an approach is that it disregards the review already carried out by the certification authority, and reiterates the *status quo* (i.e., the current approach to Standard Contractual Clauses as a data transfers mechanism) whereby multiple data exporters subject the data importers to the same lengthy due diligence questionnaires as a part of the transfer impact assessment. Some of the most widely cited benefits of and incentives for certification schemes are standardisation, legal certainty and medium to long-term reduction of compliance costs (beyond the initial short-term investment in obtaining certification).[1] If the data exporters are unable to rely on the certificate issued by the certification authority and effectively have to perform the same exercise themselves, and if the data importers are unable to present the certificate to the data exporters without being repeatedly subjected to multiple assessments, the certification under Chapter V does not carry the added value (and, arguably, becomes even more cumbersome that Standard Contractual Clauses mechanism) which would, in any way, incentivize its uptake.
    - It is recommended to revise paras 21-23 of the Draft Guidelines, limiting the data exporter's obligation to the one outlined in para. 20 and, if the intended data processing is in the scope of the certification, allow data exporters to rely on the assurances provided in the certification document without the requirement to repeat the transfer impact assessment and related exercises.

Other questions and recommendations

- According to the visualization enclosed in para 16. Of the Draft Guidelines, the EDPB proposes three distinct certification scenarios, depending on the nature and stage of the data processing operation:
    - processing (without transfer)
    - processing in transit to a non-EEA country
    - processing in the non-EEA country

  From the provided visualization, it is unclear how exactly the certification mechanism under Article 42 should be applied, in combination with the requirements stipulated in Chapter V (Article 46(2)(f)). In this regard, the EBPB is invited to clarify:
    - What does "certification in principle under Article 42" (scenario (ii)) mean in practice and what is the material difference with "certification under Article 42" (scenario (i)).
    - What does "(...) as an exception under Chapter V" (scenario (ii)) of the GDPR constitute and if the reference is made to Article 49 of the GDPR or any other

[1] See e.g., European Commission, Directorate-General for Justice and Consumers, Bodea, G., Stuurman, K., Brewczyńska, M., et al., Data protection certification mechanisms : study on Articles 42 and 43 of the Regulation (EU) 2016/679 : final report, Publications Office, 2019, pp. 138-173, https://data.europa.eu/doi/10.2838/115106

provisions, given that ”as an exception” wording is not mentioned elsewhere in the Draft Guidelines.
    - If in scenario (iii) the reference is being made to Article 42(2) in conjunction with Article 46(2)(f).
- On numerous occasions, the Draft Guidelines refer to the discretion of the data importer to include or exclude ”the transit” in the scope of the certification. From the data exporter’s perspective, and taking into consideration *EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* which make numerous references (e.g., paras. 29, 80, 90) to the requirement to assess and secure data in transit, it is questionable if excluding ”the transit” from the scope of the certification would not, in the majority of cases, undermine the efficacy of certification as a data transfer mechanism.
    - It is recommended to include practical examples where EDPB considers that excluding ”the transit” from the scope of the certification would be feasible and would not undermine the intent behind certification as a data transfer mechanism.
- Paras. 19-23 of the Draft Guidelines outline the data exporter’s role in the use of certification as a tool for transfers. As the EDPB correctly points out in para. 6 of the Draft Guidelines, data exporter and data importer can fulfil different roles depending on the nature of the processing. From a practical standpoint, and in the case of large SaaS and PaaS providers headquartered outside of the EEA, the ”typical” set-up often involves an EU subsidiary of such provider acting as a data processor and a data exporter, while non-EEA headquarters or affiliates acting as a data (sub-)processor and a data importers. In this scenario, the EU entity, procuring such services from the data importer would act as a data controller. The EU entities need to have clarity on their responsibility for compliance with Chapter V of the GDPR, *inter alia*, Article 46(2)(f) in situations where they *de facto* are not a party to the exporter-importer relationship. It is recommended to include practical examples taking into consideration the relationship outlined above, and explain:
    - the roles & responsibilities of the EU entity acting as a data controller for subsequent transfers of personal data entrusted by such entity to another EU entity acting as a data processor, and, ultimately, as a data exporter.
    - the extent & nature of verification the EDPB expects a data controller who is not a party to the exporter-importer relationship to perform in order to comply with the accountability obligation under Article 5(2) when its data processor, acting as a data importer, is relying on certification under Article 46(2)(f).
- We want to also note that while we have specific commetns on the guidelines in some countries like Austria the certification system has not yet implemented in practise, and the data protection authority has not yet carried out any accreditation of certification bodies in accordance with Article 42 GDPR.

Contact:
Savvina Papadaki - +32 2 738 06 41 - papadaki@eurocommerce.eu Transparency Register ID: 84973761187-60