

Ecommerce Europe's comments and feedback to the (Draft) EDPB Guidelines 07/20212 on certification as a tool for transfers

Ecommerce Europe is the voice of the European Digital Commerce sector. We represent, via our national associations, more than 150,000 companies selling goods and services online to consumers in Europe.

Omni-channel businesses are constantly looking to innovate their operations and better adapt to changing consumer needs. The digital commerce sector is highly cross-border by nature, with businesses increasingly growing internationally. To successfully run their business, retailers often rely on technology and services provided by third parties in the course of which personal data are transferred to third countries. The use of this technologies and services that may entail transfer of personal data, like for instance but not limited to analytic services, payment services, logistics solutions or marketing strategies, is common and widespread and is essential for retailers to remain competitive as customers are increasingly merging online and in-store shopping experiences.

In this context, certification is an important transfer mechanism that may be used by online retailers for framing their data transfers to third countries in a GDPR compliant way. Ecommerce Europe therefore welcomes these guidelines to the application of Article 46 (2) (f) GDPR on the transfers of personal data to third countries or international organisations on the basis of certification, as they will contribute to legal certainty and uniform interpretation of this transfer mechanism.

From the perspective of the digital commerce sector, we like to provide the following comments and feedback to the Draft EDPB guidelines 07/2022.

The key area of concern

Ecommerce Europe recognises clear benefits of certification and of organisations obtaining certification in general. However, we fear that the certification scheme under Chapter V, if the interpretation proposed in the Draft Guidelines is adhered to, will be unlikely to lead to its uptake among the relevant industry players. This can mainly be explained by the way the EDPB currently constructs the data exporter's role & responsibilities when using certification as a tool for transfers. In particular, the Draft Guideline (paragraphs 20-23) requires the data exporter to:

1. check whether the certification is valid and not expired, if it covers the specific transfer to be carried out and whether the specific 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;
2. check whether there is a contract or another legally binding instrument (i.e., the "certification agreement") between the certified data importer and the certification body;
3. 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;
4. 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;
5. require the data importer to put in place adapted supplementary measures or establish them by himself.

While requirements 1 and 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 exporters under the obligation to carry out a so-called transfer impact assessment, even though such assessment has already been carried out by the data importer and been verified (including the necessity of supplementary measures) by the certification body or 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 data importers to the same lengthy due diligence questionnaires as a part of the transfer impact assessment. Thus jeopardising some of the most widely cited benefits of and incentives for certification schemes such as 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 body or 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 constitute the added value (and, arguably, becomes even more cumbersome than the Standard Contractual Clauses mechanism) which would, in any way, incentivize its uptake.

Ecommerce Europe strongly recommends the EDPB to revise paragraphs 21-23 of the Draft Guidelines, limiting the data exporter's obligation to those outlined in paragraph 20 and, if the intended data processing and transfer is in the scope of the certification, allow data exporters to rely on the assurances and guarantees 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 paragraph 16 of the Draft Guidelines, the EDPB proposes three distinct certification scenarios, depending on the nature and stage of the data processing operation:

1. processing (without transfer);
2. processing in transit to a non-EEA country;
3. processing in the non-EEA country.

From the provided visualization, it is unclear for Ecommerce Europe how exactly the certification mechanism under Article 42 should be applied in combination with the requirements stipulated in Chapter V (Article 46(2)(f) GDPR). In this regard, the EBPB is invited to clarify:

- how "certification in principle under Article 42" (scenario 2) has to be interpreted in praxis and what the material difference is with "certification under Article 42" (scenario 1);
- what constitutes "(...) as an exception under Chapter V" (scenario 2), seen the fact that when reference is made to Article 49 GDPR or any other provisions the wording "as an exception" is not mentioned elsewhere in the Draft Guidelines;
- what it means in scenario 3 when reference is made to Article 42(2) GDPR in conjunction with Article 46(2)(f) GDPR.

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.

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>

paragraphs 29, 80 and 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. That is why Ecommerce Europe recommends the EDPB to include practical examples where it considers 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.

Paragraphs 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 paragraph 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 act as data (sub-)processors and data importers. In this scenario, the EU entity, procuring such services from the data importer would act as a data controller. As EU entities need to have clarity on their responsibility for compliance with Chapter V of the GDPR, e.g., *inter alia* Article 46(2)(f) GDPR, in situations where they *de facto* are not a party to the exporter-importer relationship, Ecommerce Europe recommends including practical examples taking into consideration the relationship outlined above, and explain:

- the roles and 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 data exporter;
- the extent and 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) GDPR, when its data processor, acting as a data importer, is relying on certification under Article 46(2)(f) GDPR.