Ecommerce Europe's contribution to the EDPB consultation on its Draft Guidelines 05/2021

Ecommerce Europe's comments provide feedback to the (draft) EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

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. Ecommerce Europe is also an affiliated member of EuroCommerce, who has also contributed to the EDPB consultation on its Draft Guidelines 05/2021. Please note that Ecommerce Europe fully supports the points that have been raised by EuroCommerce in its contribution to the EDPB, thus these points are reiterated in this contribution and highlighted.

Omnichannel retail 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, especially to the U.S. 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.

From the perspective of online retailers, we would like to provide the following comments to the Draft EDPB guidelines 05/2021.

- Paragraphs 3, 7, 10 and 18 of the Draft Guidelines seems to be in contradiction to recital 7 of the Commission Implementing Decision 2021/914 on standard contract clauses (SCCs) for the transfer of personal data to third countries. While the Implementing Decision on SCCs specifies that the SCCs should NOT apply if the processing by the data importer falls within the scope of the GDPR, the EDPB argues (in our opinion rightly) that appropriate safeguards (such as SCCs) must also be included in these cases. This contradiction on the use of appropriate is highly confusing for retailers transferring data to third countries and in our opinion does not contribute to legal certainty. We therefore would like the EDPB guidance to provide a clear explanation on why it is opposing the Implementing decision and what opinion should prevail.

- We would like to reiterate and support the comments made by EuroCommerce in its contribution to the EDPB consultation regarding paragraph 7 of the Draft Guidelines, according to which three cumulative criteria must be met to qualify data processing a transfer:

    - The **first criterion** reads as follows: ”A controller or a processor is subject to the GDPR for the given processing”. Paragraph 25 of the Draft Guidelines further specifies that controllers and processors are under obligation to comply with Chapter V of the GDPR when they disclose personal data to controller or processor in a third country and that this requirement also applies to data exporters not established in the EU but subject to GDPR by virtue of Article 3, even where data importers are based in the same third country. In this perspective, as rightly pointed out by EuroCommerce in its contribution, we believe the criterion under paragraph 7.3 creates

a paradoxical situation whereby for instance a California-based data controller, subject to GDPR by virtue of Article 3(2) would be placed under the obligation to comply with Chapter V of the GDPR when transferring personal data to its California-based data processor. It is not clear how such reasoning aligns with the understanding of ”transfer” embedded in the relevant recitals of the GDPR, where transfers are only considered to be data processing operations when personal data is originally shared, from the geographical perspective, “from the Union” to ”third countries”. See:

- Recital 101: ”(w)hen personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined”
- Recital: 110: ”A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings”.

In that perspective, we would like to stress EuroCommerce’s point about the lack of clarity on how such reasoning aligns with the fundamental rationale of data transfer rules to remedy the risks of data processing to data subjects arising from third country legislation and/or practices which do not guarantee a level of protection provided by EU law. If personal data is already processed in the third country which does not offer essentially equivalent level of protection (e.g., the US as in the example above), the question is how, from legal standpoint, transferring data within the same jurisdiction could change the level of data protection, and what compensatory effect Chapter V data transfer rules are expected to have in this situation.

Ecommerce Europe supports EuroCommerce’s view, outlined in its contribution, with regards to the lack of clarity on ‘how transfer impact assessments would need to be conducted in this situation, and, from a policy perspective, it is not in line with the intention of GDPR drafters to expect EU supervisory authorities to enforce GDPR Chapter V rules on data transfers between two US (or any other third country) based companies’.

- The **second criterion** in paragraph 7 reads as follows: “this controller or processor (“exporter”) discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor (“importer”)”. Article 4(9) of the GDPR defines “recipient” as the natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. Similarly to EuroCommerce, we would like to suggest to clarify, in the guidance, that “recipient” as defined in Article 4(9) of the GDPR and as explained in EDPB Guidelines 07/2020 is equal to the term “importer”, and if not, specify the difference between the two notions.

  As EuroCommerce, we also recommend to elaborate further on the concept of disclosure “by transmission, or otherwise”, to explain which technical data sharing scenarios would qualify or not qualify as such disclosure. We would also like to suggest the EDPB to provide more practical examples. With regards to examples 2-4, we support EuroCommerce’s view to ensure that they reflect diverse real-world practices of businesses sharing the data and include more details of data sharing arrangements, not limited to generic “sending” and “providing” data concepts. In that perspective, it would also be useful to understand which specific data sharing

scenarios would not constitute disclosure “by transmission or otherwise”, as pointed out by EuroCommerce in its contribution.

- In paragraph 14 example 5 and Paragraph 17 situations and operations are mentioned that do not qualify as data transfer between two different parties being controller or processor, for instance in case of access of an employee to his employer’s data during a business trip in a third country and processing carried out by the employee in that third country. Ecommerce Europe agrees with the conclusion that, in such cases, no data transfer to another party takes place. As in paragraph 17 the Draft Guidelines conclude that such “internal” processing of personal data can however still be associated with risks and that the controller is accountable for its processing activities and must comply with the GDPR including Articles 24, 32, 33, 35, 48, Ecommerce Europe would like to suggest the EDPB to further elaborate on practical examples of such risks and on what technical and organisational measures the controller could take to mitigate these risks.

- Finally, Ecommerce Europe would like to draw attention to the fact that recently (December 2021) the Austrian Data Protection Authority ("Datenschutzbehörde") has ruled that web analytics tools developed by Google involve transfers of personal user data to the United States which are non-compliant with the General Data Protection Regulation (GDPR). The ruling stems from the decision made in 2020 by the EU Court of Justice that declared the Commission’s Privacy Shield Decision invalid due to invasive US surveillance programmes, thereby making transfers of personal data on the basis of the Privacy Shield Decision illegal because the U.S. is no longer subject to an adequacy decision as meant in Article 45 GDPR. The Austrian DPA ruling is the first decision on the 101 model complaints filed by *noyb,* which is led by privacy activist Max Schrems, following the so-called "Schrems II" decision. However, it is possible that similar decisions could follow in other EU member states and on the use of other services that entail data transfers to the U.S.. For instance, the Dutch Data Protection Authority is currently also investigating two complaints about the use of Google Analytics in the Netherlands. Additionally, France’s DPA is also expected to reach a decision in the coming month on the complaints filed by Schrems’ organisation.

  The developments of the last weeks clearly illustrate that retailers relying for their daily business operations on this commonly and widespread used services cannot rely on the mere application of Standard Contract Clauses or Binding Corporate Rules (BCRs) to tackle the specific risks in a third country and have to take additional technical and organisational measures to mitigate effectively these risks. In that perspective, Ecommerce Europe would recommend the EDPB to provide practical examples and best practices of these technical and organisational measures (besides SCCs and BCRs) that retailers could take to avoid the mentioned risks.