17 December 2020

EuroCommerce and NRF joint comments on the EDPB Draft Recommendations on Supplementary Measures following the Schrems II ruling

The following comments on the European Data Protection Board (EDPB) draft *Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* as adopted 10 November 2020 (Draft Recommendations) are being submitted jointly by EuroCommerce, headquartered in Brussels, and the National Retail Federation (NRF), headquartered in the United States, which will be submitting the identical set of comments in parallel to this submission.

As representatives of the retail and wholesale industry engaged in cross-border data flows and on behalf of our members, we welcome the efforts of the EDPB to draft recommendations with respect to supplementary measures required for transfers of personal data to third countries outside the EU, especially in light of this year's *Schrems II* ruling by the European Court of Justice (CJEU). We believe that a framework ensuring both protection of personal data and the maintenance of transatlantic data flows is an essential factor in the proper functioning of the global retail economy. Economic recovery after the present COVID crisis will in large part be driven by data, which is a vital element of retail and wholesale businesses on both sides of the Atlantic, whether as players in both markets needing to transfer sales, supply or personnel data freely between their operations in various territories, or as clients of data processors or cloud providers located in the other market. We therefore welcome the EDPB's efforts in provide clarity on parties' obligations post-*Schrems II* and allow international data transfers to continue while maintaining the high level of protection under EU law.

This important work on Draft Recommendations is closely related to the European Commission's work modernising Standard Contractual Clauses (SCCs), including in light of *Schrems II*, and it will be important – in order to avoid legal uncertainty and confusion – that the EDPB's adopted recommendations are fully in line with the modernised SCCs.

In the light of the above, and as a positive contribution to the work of the EDPB, we are pleased to submit these comments for consideration, divided below into our (i) key points, (ii) specific comments and considerations, and (iii) requested clarifications to the Draft Recommendations and key asks.

Our key points and asks:

1. **Ensure level playing field:** It is essential to ensure a level playing field among entities subject to the recommendations (e.g., exporters vs. importers; controllers vs. processors/sub-processors) to avoid significant competitive disruption to the market.
2. **Provide legal certainty and prevent fragmentation:** The Draft Recommendations are non-binding and therefore subject to differing interpretations by data protection authorities in EU member states.
3. **Apply risk-based approach as in GDPR**: The EDPB should align the Draft Recommendations with the European Commission's modernised SCCs by applying a risk-based approach to data processed by service providers based in third countries.
4. **Fairly allocate liability:** Liability for failure to apply appropriate supplementary measures should fall on those parties best placed to know and analyse the laws of third countries, and to avoid or correct potential violations through consulting with supervisory authorities before any enforcement action.
5. **Include a notice-and-cure period**: In light of our comments, we propose the EDPB include in the final recommendations a notice-and-cure period to allow parties time to correct unintentional violations occurring despite their well-documented *bona fide* efforts to follow the EDPB's recommendations.

Key points

1. **Ensure level playing field:** It is essential to ensure a level playing field among entities subject to the recommendations to avoid significant competitive disruption to the market. The Draft Recommendations risk distorting international data protection arrangements, with data exporters required to apply different rules to jurisdictions offering similar levels of data protection. Such differential treatment of jurisdictions is likely to be viewed as discriminatory and incompatible with existing trade rules where companies in a particular country are placed at a competitive disadvantage in European markets by the EDPB's actions.

2. **Provide Legal certainty and prevent fragmentation:** The Draft Recommendations are non-binding and therefore subject to differing interpretations by data protection authorities in EU member states. Secondly, if adopted in this form, it would mean that any organisation using an online service to process and transfer personal data—including email and hosted applications —could face fines up to 4% of its annual turnover, irrespective of whether public authorities in a third country ever accessed the data in question. Thirdly, the Draft Recommendations would require EU companies to undertake costly analyses of the laws and practices of dozens of non-EU countries, where these are not subject to an EU adequacy decision. This is extraordinarily burdensome and costly for many small and medium-sized enterprises (SMEs), as well as for larger global retail businesses with many data transfer agreements covering data flows to a wide range of third countries. Moreover, while GDPR Recitals 101-108 empower the European Commission to assess the level of data protection in a third country, the Draft Recommendations impose this obligation on exporters and importers. This will likely lead to further fragmentation among businesses and their service providers regarding applicable supplementary measures to implement based on their separate interpretations of the same laws in third countries.

3. **Apply risk-based approach as in GDPR**: The Draft Recommendations are not consistent with the risk-based approach set forth in the General Data Protection Regulation (GDPR). The EDPB should align the Draft Recommendations with the European Commission's modernised SCCs by applying a risk-based approach to data processed by service providers headquartered in the U.S. or other third countries. In the retail sector where risks to data subjects are likely lower than the level of risk found in the *Schrems II* case, the recommendations should not require organisations to adopt supplemental measures, as set out in Article 35 of the GDPR. Additionally, the compliance checks should be based on real risks incurred while taking account of the relevant actual experience of parties in their own sector (e.g., retail) with data transfers to third countries. A risk-oriented approach should include the risk assessment of the likelihood that access will occur, based on the nature of the personal data (e.g., publicly available or private; pseudonymized or in the clear; sensitive or not sensitive) and the data processing, as well as the number of previous requests made to the data importer and other importers in the same area of business.

4. **Fairly allocate liability**: The Draft Recommendations' requirement that exporters be responsible for ensuring sub-processors implement the necessary supplemental measures appears to break with well-established elements of the GDPR. In particular, the GDPR holds processors liable for sub-processors, and the Draft Recommendations appear to impose obligations on the exporter that would make it liable for any omissions or non-action by an importer's sub-processor with which the exporter does not have privity of contract. In these instances, the importer (not the exporter) should ensure that their sub-processors implement the necessary supplemental measures. Additionally, an importer should be separately liable, and not jointly liable with the exporter, for its own assessment of the laws of the third countries in which it operates, and exporters should be permitted to rely on that analysis.

5. **Include a notice-and-cure period:** In light of our key points, we propose the EDPB include in its final recommendations a notice-and-cure period to allow parties time to correct unintentional violations, following notice by supervisory authorities, when those occur despite the parties' well-documented *bona fide* efforts to follow the EDPB's recommendations. We suggest this mechanism because, unless the Draft Recommendations are clarified and modified (including in ways suggested below), many retail and wholesale businesses operating in the EU as data exporters may be unable to complete the recommended processes with any legal certainty and, in turn, may be subject to enforcement actions despite their actions taken in good faith to implement the EDPB's recommendations.

Specific comments and considerations

In light of the key points above, EuroCommerce and NRF offer the following specific comments for the EDPB's consideration when preparing its final recommendations:

The recommendations could make it impossible to use cloud and other service providers established outside the EU. For example, controllers in the EU may not be able to use service providers subject to FISA 702 (a U.S. law), which would significantly alter existing relationships and create major disruption to the operations of global businesses, including retail businesses. Additionally, it is not clear that only cloud service providers within the scope of FISA are targeted by the Draft Recommendations, and likewise other service providers operating outside the EU may no longer be viable options for EU-based businesses.

- Retailers, large and small rely on third-party service providers for a wide range of services which are not linked to their key economic activities but are critical for business operations (e.g., email providers, cloud services, etc.). Many of these service providers are based in the United States and other third countries. Only the largest and most sophisticated businesses with the requisite infrastructure in Europe may have the financial and technical capability to comply with the recommendations by re-architecting these complex services in-house or with third parties in EU member states, or jurisdictions deemed to be adequate. Even then, it would be a heavy burden.
- Unless clarified before final adoption, the Draft Recommendations could therefore be seen as a non-tariff trade barrier on data flows that could have the effect of prohibiting controllers operating in the EU from using processors based outside of the EU.
- The CJEU's opinion in *Schrems II* did not prohibit data transfers to any third country on the basis that this was required to protect fundamental rights of data subjects. This, in turn, provides latitude to the EDPB to create final recommendations that can accommodate both data protection as well as continued viability of businesses to operate on a global basis. In preparing final recommendations, we encourage the EDPB to foster discussions with other interested parties - including World Trade Organization representatives - to ensure that the final recommendations balance data protection rights with other valid business considerations.

The complexity of the proposed assessment process will have a significant impact on EU-based retailers exporting to, or operating in, the U.S. and other third countries. Thus, it will negatively impact international trade and day-to-day communications with their business partners outside the EU. Therefore, it is essential that the EDPB propose measures that are flexible, holistic and, above all, feasible.

- Step 3 of the assessment process involves analysing and documenting, including on an ongoing basis (step 6), "if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer". This will be challenging for SMEs and even for the largest retail businesses that may have greater resources and expertise than SMEs to develop and execute this process. The requirements are extremely burdensome for data controllers in general, and SMEs will likely neither have the resources nor expertise to carry out the required assessments.
- While data importers "should provide […] the latest sources and information relating to […] the laws applicable to the transfer", exporters are required to undertake an assessment taking into account "all the actors participating in the transfer (e.g., controllers, processors and sub-processors processing data in the third country) […] The more controllers, processors or importers involved, the more complex [the] assessment will be. [They] will also need to factor into this assessment any onward transfer that may occur".
- In practice, to implement this effectively, a data exporter will have to maintain real-time awareness of all of the activities of their processors, sub-processors and sub-sub processors, as well as the changing laws of third countries, which would be an unworkable regime for most retail businesses requiring a level of financial capital and diversion of limited resources from activities that already support data privacy and security (e.g., training, investments in technology to protect data, etc.) for no appreciable assurance of greater protection.
- Due to the novelty and complex nature of issues reflected in *Schrems II* and resulting guidance from the EDBP, the final recommendations should create a clearly defined enforcement framework to be followed by all supervisory authorities when assessing supplementary measures. This will provide certainty as businesses consider how to implement appropriate supplementary measures and how to cooperate with supervisory authorities in their enforcement activities. We suggest the following framework derived from GDPR Article 58(2): (1) a supervisory authority should first inform the data exporter about any concern with respect to that data exporter's supplementary measures; (2) before taking any enforcement action, a supervisory authority should issue a warning, allowing the data exporter to cooperate and share information about its compliance efforts and the basis for such

compliance efforts; (3) if a supervisory authority concludes that a data exporter's actions are not compliant and not capable of being remediated after a reasonable period, only then should a formal notice of non-compliance be possible; (4) if the data exporter continues its non-compliance, only then should a supervisory authority draft a decision announcing its intention to fine the data exporter, (5) finally, the decision to fine should only then be submitted to the consistency mechanism set in GDPR (including in article 60), to the extent that the data exporter registers cross-border challenges. Finally, and most importantly, the level of fines should be framed in advance by the EDPB's final guidelines.

- Lastly, the Draft Recommendations state that all transfers to third countries must be mapped, but it is unclear what is meant by "specific transfer" as used in the text of the recommendations. Some retailers are concerned it could potentially cover each individual use case for a data transfer, thereby exponentially increasing the number of assessments required to be mapped for each transfer to a third country. The more transfers that are required to undergo this level of assessment, the greater concern there is about the feasibility and practical application of this recommendation.

The disparity of bargaining power exercised by market-dominant service providers who operate as importers (with few competitors), when contracting with data exporters who have no practical option but to use these dominant service providers, could result in these service providers dictating non-negotiable supplementary measures they are willing to implement for a third country regardless of the exporter's needs.

- In this scenario, the contractual relationship between the data exporter and the importer is not arms-length and this reality must be a relevant factor in a data protection authority's determination of an exporter's liability as it relates to the adoption of supplementary measures for transfers to the U.S. or a third country (e.g., use of cloud services).
- The scope for each individual business, no matter how large, to negotiate changes to contractual provisions is very limited, as they rely on third-party providers to carry out their business. In financial services, specific contractual clauses are being drafted to reduce risk of vendor lock-in, but retailers have no such provision.

Liability for failure to apply appropriate supplementary measures should fall on those parties best placed to know and analyse the laws of third countries, such as processors and sub-processors operating as importers in a third country. These parties are best suited to understand the laws of the third country and identify the supplementary measures required to adequately protect the data. These parties are also able to avoid and correct potential violations through consultation with supervisory authorities before they take any enforcement action.

- In the Draft Recommendations, all the legal responsibilities and the considerable risk of potential sanctions under the GDPR for failure to apply adequate supplementary measures rest with the data controller acting as an exporter.
- Because they are best placed to know and analyse the laws of third countries, the importer should separately, and not jointly, guarantee a certain level of data protection and be liable for making such a guarantee. In this case the exporter should be able to rely on the guarantees made by the importer.
- Given the superior resources of the EDPB, it would be helpful for the EDPB to identify for businesses the legislation in a third country which the EDPB believes is relevant to include in an assessment (without making any assessments on such legislation). This would alleviate the disproportionate burden that each separate company will bear if it has to perform this identification on its own, and this would ensure consistency by defining the same scope of legislation for all companies. This would also be beneficial for data subject rights as the EDPB could ensure that all relevant privacy legislation and other similar documentation is considered by the data controller.

The above comments and considerations support our conclusion that, unless the Draft Recommendations are clarified and modified, many retail and wholesale businesses operating in the EU as data exporters may be unable to complete the recommended processes with any legal certainty and, in turn, may be subject to enforcement actions despite their *bona fide* efforts to implement the EDPB's recommendations.

Suggested clarifications to Draft Recommendations and key asks

Inclusion of use cases and examples of applicable supplementary measures

The technical measures in the Draft Recommendations are quite general, which can lead to legal uncertainty. We would very much appreciate further clarification by the EDPB in the final recommendations, including further explanation of the particular supplementary measures needed for certain use cases that will work in practice.

- For example, the final recommendations could provide a description of the different supplementary measures in relation to actual services (e.g., email services, analytic tools, marketing services, etc).

- Including examples of different use cases would provide more clarity and help businesses implement stronger protections for data subjects when their data is transferred to a third country.

The Draft Recommendations should explicitly recognize that contractual and organizational measures (rather than technical measures) may be adopted by a business as sufficient to mitigate the kinds of risks that were the object of the *Schrems II* decision. Such contractual and organizational measures may be adopted instead of technical measures either because (a) contractual and organizational measures are the most appropriate supplementary measures under particular circumstances; or (b) technical measures may be practically impossible to implement due to limited resources or legitimate business constraints (e.g., maintaining all decryption keys in the EU).

Clarifying parties' responsibilities

We would also suggest that the Draft Recommendations are adjusted to resolve the following issues with respect to parties' responsibilities and liability:

- Data exporters' liability for sub-processors' supplemental measures appears to conflict with the GDPR provision that processors are liable for sub-processors;
- Service providers acting as importers may refuse to negotiate supplementary measures, and present retailers (i.e., exporters) with a "take-it-or-leave-it" proposal excluding any liability for failures and/or disruption of business continuity;
- If supervisory authorities require immediate suspension of transfers until service providers' corrections are executed, this could lead to immediate business harm for exporters; and
- Retailers' operations need liability to fall on the entity (e.g., service providers acting as importers) with the ability to correct the violation by taking additional supplementary measures.

Conclusion

We would ask for:

- **Businesses acting in good faith to be granted a limited grace period**, in line with the transition period provided for in the European Commission's adopted modernised SCCs, to implement the EDPB's final recommendations on supplementary measures following their adoption.
- **Clarification that the "relevant practical experience" element be a risk-based consideration applied to obligations throughout the Draft Recommendations**, in line with the *Schrems II* decision, permitting parties to take into account the specific circumstances of data transfers and their own practical experience of transferring data to third countries when assessing the actual risks and what supplemental measures (if any) are required to mitigate them. This is consistent with the GDPR, which requires companies to assess practical risks to data subjects, not theoretical or remote risks.
- **Application of a risk-based approach, in which the contractual, technical, and organisational measures to be implemented should consider the nature and amount of personal data processed**. For example, processing solely information like IP-addresses should be subject to different measures than processing the most sensitive personal information like health or financial data.
- **EU institutions and member states' supervisory authorities to provide information on enforceable data subjects rights in respective countries, including surveillance laws, etc.** The risk of assessing the legal requirements in the country of destination should not be borne by businesses alone.
- **Liability to be placed on those entities (including processors and sub-processors) best-placed to make changes to avoid violations if they do not take appropriate corrective action**. In particular, we seek your clarification that:
  (i) the controller/exporter is obliged only to ensure that an appropriate contract requiring additional safeguards is in place with the processor/importer where necessary.
  (ii) the obligation rests with the processor/importer to ensure that an appropriate contract is in place between itself and the sub-processor; and
  (iii) the processor/importer is responsible for the sub-processor and its downstream transfers.
- **Inclusion in the final recommendations of a notice-and-cure period** (or similar measure) to allow parties time to correct unintentional violations occurring despite their well-documented *bona fide* efforts to follow the EDPB's recommendations.
- **Public consultation in line with the EU Better Regulation guidelines to accompany any action taken by the EDPB.**

On behalf of our collective members, we appreciate your consideration of these comments, and respectfully request that the EDPB address these concerns before adopting its final recommendations. We stand ready to assist the EDPB in its efforts to provide clarity on parties' obligations post-*Schrems II* in a way that will protect data subjects and be most workable for exporters and importers to implement. We would be happy to provide additional constructive feedback or practical examples with respect to any of the issues above on which you would like further input. Please do not hesitate to contact Ilya Bruggeman (bruggeman@eurocommerce.eu) on behalf of EuroCommerce or Paul Martino (MartinoP@NRF.com) on behalf of NRF.

About EuroCommerce

EuroCommerce is the principal European organisation representing the retail and wholesale sector. It embraces national associations in 31 countries and 5.4 million companies, both leading global players such as Carrefour, Ikea, Metro and Tesco, and many small businesses. Retail and wholesale provide a link between producers and 500 million European consumers over a billion times a day. It generates 1 in 7 jobs, providing a varied career for 29 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.

EuroCommerce Transparency Register ID: 84973761187-60

About NRF

The National Retail Federation, the world's largest retail trade association, passionately advocates for the people, brands, policies and ideas that help retail thrive. From its headquarters in Washington, D.C., NRF empowers the industry that powers the economy. Retail is the nation's largest private-sector employer, contributing $3.9 trillion to annual GDP and supporting one in four U.S. jobs — 52 million working Americans. For over a century, NRF has been a voice for every retailer and every retail job, educating, inspiring and communicating the powerful impact retail has on local communities and global economies.

NRF Transparency Register ID: 441333332953-73