Ecommerce Europe's contribution to the EDPB consultation on its Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Introduction

Ecommerce Europe is the sole voice of the European Digital Commerce sector. It represents, via its national associations, more than 100,000 companies selling goods and services online to consumers in Europe. Ecommerce Europe acts at European level to help legislators create a better framework for online merchants, so that their sales can grow further.

On 10 November, the European Data Protection Board (EDPB) issued, for public consultation until 21 December, its Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. The Court in Schrems II held that organisations that rely on standard contractual clauses (SCCs) to transfer data outside the EU may need to adopt additional safeguards to protect personal data from access by public authorities in third countries. Ecommerce Europe welcomes the opportunity given by the EDPB to provide comments on the Recommendations.

Ecommerce Europe's feedback focuses on several substantial concerns and suggestions for improvement of the recommendations. In particular, the recommendations propose a rather prescriptive approach, that goes beyond the requirements set by the Schrems II ruling, and also moves away from the risk-based approach of the GDPR. Ecommerce Europe believes that the EDPB guidance could instead be more helpful by providing data exporters with a "toolbox" of pragmatic, practical measures that would help them comply with the Court's decision.

Comments

Ecommerce Europe finds that, instead of providing data exporters with such a "toolbox", the Recommendations propose a prescriptive, non-risk-based approach that goes beyond the requirements of Schrems II. Ecommerce Europe is of the opinion that the Recommendations, in their current form, will require EU organisations that transfer data outside the EU to countries which are not subject to an EU adequacy decision, to undertake on their own costly analyses of the laws and practices of these countries, which will be unrealistic for most enterprises, especially SMEs, research institutions, and others. Consequently, any organisation that uses an online service to process and transfer personal data - including email, hosted applications, or any other online service - could face fines up to 4% of its annual turnover, irrespective of whether public authorities in any third country ever access the data in question.

From a practical perspective, the complexity of the assessment process (step 3), which 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", does not scale and will not be workable. As a result, the Recommendations will make it highly risky if not practically impossible for EU companies to engage in commerce with non-EU customers or partners, for researchers to share information with foreign colleagues, for companies with non-EU offices or personnel to communicate with them online, or to engage in countless other routine and necessary operational tasks. If adopted, they will force many data operations of EU commerce and society into a pre-Internet era, and/or isolate Europe from the global economy. The potential negative effects on EU competitiveness, innovation, and society will be enormous.

Moreover, it is far from clear that all third countries that have an adequacy decision from the European Commission - or indeed that all EU Member States which are automatically seen as adequate - provide a level of data protection that is "essentially equivalent" to that set out in the GDPR and the EU Charter of Fundamental Rights. By focusing only on non-adequate jurisdictions, the Recommendations threaten to create an unequal international playing field for data protection, where data exporters are required to apply different rules to different jurisdictions even where similar levels of data protection exist between them. Such discriminatory treatment of different jurisdictions is also likely to invite retaliation by jurisdictions whose companies are placed at a competitive disadvantage in European markets by the EDPB's actions.

Ecommerce Europe wishes to raise with the EDPB the following:

1. The Recommendations should allow data exporters to take account of the full context of a transfer

In Schrems II, the Court indicated that data exporters should consider the full context of a transfer when evaluating its legality and, specifically, that transfers should be evaluated "in the light of all the circumstances of that transfer" (nr. 121, 146) and "on a case-by-case basis" (nr. 134). Several passages in the Recommendations, however, appear to foreclose this contextual approach. For instance, they state that, if the data importer falls within the scope of certain national security laws, the data exporter must use additional technical measures (text box before nr. 45) even, presumably, if the data importer has never faced an order under those laws and the data is of no conceivable relevance to national security (e.g. an employee's menu preferences for a holiday party). Other passages similarly suggest that the likelihood that a public authority will ever access the data is irrelevant (nr. 42).

Restricting transfers of personal data even where the context shows there is virtually no risk to data subjects, will harm the EU economy and society. EU researchers sharing health data with foreign partners to fight COVID-19, EU companies engaging in routine communications with employees outside the EU, and even simple commercial transactions with non-EU entities would all be fraught with substantial risk if not be made impossible. Nothing in the Schrems II judgement requires this outcome.

Rather than discouraging EU organisations from considering contextual factors, the Recommendations should encourage organisations to take into account the real-world risks of a transfer, including the relevance of the data to law enforcement agencies and the likelihood that such agencies would request access to the data. If these real-world risks are low or absent, which they are for most categories of data, the Recommendations should not require organisations to adopt any supplemental measures.

2. The Recommendations should propose technical measures that are workable in practice

The Recommendations propose a non-exhaustive list of technical measures that data exporters can use to supplement the safeguards in the SCCs. Unfortunately, the Recommendations' case studies on the use of these measures reflect an unworkable and unrealistic view of how these measures operate in practice. For instance, the Recommendations suggest that organisations can rely on encryption as a safeguard in most cases only if the data never appears in an unencrypted form in the third country and if the decryption keys are held only within the EU or an adequate jurisdiction (e.g. nr. 79(6), 89(2-3), 84(11)). They also suggest that encryption almost never provides sufficient protection where data is accessible "in the clear" in the third country, including where an EU organisation uses an online service that may process the data in the third country (nr. 88-89), or where employees or others in the third country can access the data on a shared IT system, e.g. human resources data (nr. 90-91).

Moreover, because the Recommendations state that even remote access by an entity in a third country to data stored in the EU constitutes a "transfer" (e.g., footnote 22, nr. 13), organisations in many cases would need to apply these technical safeguards to EU-stored data as well. This fact underscores the impracticality of the Recommendations and their incompatibility with other important EU interests, such as promoting open global trade and research necessary to protect vital interests (for instance, in the context of the COVID-19 pandemic). At a time when policymakers across the world, including in Europe, are pressing companies to provide greater access to encrypted communications in order to help governments more effectively fight terrorism and other threats, the proposed Recommendations would appear to penalise companies for making such access possible.

More pragmatically, the Recommendations' positions on technical measures would render the SCCs virtually worthless as a transfer mechanism. In the vast majority of cases, the reason companies transfer data to third countries is to communicate and share information with people in those countries. If those people cannot access the information - as the Recommendations would require - the transfer would be redundant. Similarly, many online services that EU businesses rely on today require processing of the information in unencrypted form in order to work properly. Moreover, given the nature of the Internet and the global economy, such operations might entail some processing that occurs outside the EU, irrespective of where the data controller or data processor is based. The Recommendations would prohibit EU organisations from engaging in these commonplace and essential business activities.

In reality, most EU organisations would not be able to cease these activities entirely and at the same time remain economically competitive. Instead, many would most likely turn to other legal mechanisms, such as the derogations set out in Article 49 of the GDPR. Organisations adopting this approach might transfer data to non-adequate jurisdictions without even adopting SCCs or additional safeguards, leaving EU data subjects worse off, because their personal data would be subject to a lower protection level than they are today. To avoid these consequences, the EDPB should revise the Recommendations to ensure that the proposed technical measures are workable in practice, and should leave it to data exporters to determine case-by-case whether any particular measure adequately protects the transferred data. The Recommendations should not generally prohibit all access to data in the third country; doing so will discourage organisations from adopting technical measures, such as encryption, that in fact provide meaningful safeguards against unauthorised access.

3. The Recommendations should clarify that contractual measures may provide sufficient safeguards

Although the Recommendations propose a non-exhaustive list of contractual measures that can offer additional safeguards, they also include wording suggesting that contractual or organisational measures on their own (i.e. without additional technical measures) in general cannot provide the level of data protection that EU law requires (nr. 48). This position appears to be based on the unjustified assumption that the mere theoretical possibility of access by third-country authorities - even if the practical risk of such access is very small - renders a transfer unlawful.

This position of the EDPB adopts an overly restrictive reading of the Schrems II judgement. The Court in Schrems II held that transfers of data to third countries should be prohibited only "in the event of the breach of [the SCCs] or it being impossible to honour them" (nr. 137). This wording, and similar passages elsewhere in the judgement, suggest that, as long as the data importer does not in fact disclose data to third-country authorities (or, if it does make such a disclosure, it notifies the data exporter accordingly), the involved parties may rely on the SCCs (nr. 139). Under this reading of the Court, it is clear that contractual measures alone can provide the additional safeguards needed to safely transfer data to a non-adequate jurisdiction.

To align with the Schrems II judgement, the Recommendations should remove all wording suggesting that contractual measures alone are insufficient safeguards to satisfy EU law. The Recommendations should instead articulate several possible contractual measures that EU organisations may consider when transferring data to a non-adequate jurisdiction, and leave it to the discretion of data exporters and importers to evaluate which measures are appropriate in the context and "in the light of all the circumstances of that transfer" (Schrems II, nr. 121, 146).

4. The Recommendations should make clear that enforcement by supervisory authorities should be measured, proportional and appropriate

The Court's holding in Schrems II was a major and unexpected development, one that requires organisations across the EU to prepare new data transfer impact assessments and, in certain cases, to overhaul aspects of their data transfers. In many cases, these efforts require changes not only to contracts, but also to the underlying infrastructure, software, and systems. Undertaking these changes is a complex task that often will involve many different parties, both inside and outside an organisation.

Notwithstanding these facts, the Recommendations imply that supervisory authorities should move directly to "corrective measure[s] (e.g. a fine)" if they determine that a data transfer does not comply with the Recommendations (nr. 54). This focus on sanctions will lead EU organisations to rush through changes to their data transfer practices—making it far less likely that organisations address these issues carefully and precisely. To avoid this outcome, the Recommendations should expressly advise supervisory authorities, when they determine that a specific data transfer does not comply with EU law, to work and cooperate with data exporters to find acceptable safeguards and practical solutions, and give them sufficient time to implement such solutions. This approach will provide incentives for EU organisations to address these issues thoughtfully, while also encouraging good-faith and collaborative solutions to these quite difficult legal and technical issues. Moreover, it will encourage data exporters to seek adequate solutions in full cooperation with supervisory authorities instead of not contacting them to avoid serious repercussions.

With this new guidance, Ecommerce Europe believes that the EDPB is shifting responsibility from the European Commission (usually responsible to take 'adequacy decisions' and with the knowledge and experience to do so) to companies, which we see as a concerning development. Eventually, Ecommerce Europe finds that this shift will result in companies requiring significant legal assistance or having to implement AI-based tools to do the important (individual) 'adequacy' assessment work that the European Commission is/was originally meant to do. We seriously doubt that personal data of EU residents would be better protected with this approach.

Ecommerce Europe stresses that the scale of the effort required to comply with the requirement to review all data sharing contracts on a case-by-case basis. Even for multinational companies, we believe the work might take months if not years and at considerable costs. As a result, we believe that data exporters should be granted a transition period of at least 1 year.

Ecommerce Europe considers that the EDPB Guidance on Schrems II adds several far-reaching requirements to the existing GDPR requirements, and thereby goes beyond the actual GDPR text. Although we realise that the EDPB guidance is factually only a non-binding guidance issued by the assembly of EU data protection authorities, it will have a far-reaching effect, especially for the interpretation and enforcement by EU data protection authorities. Considering that the Recommendation's additional privacy requirements will in effect result in a change in the politically agreed system of the GDPR, the EDPB is not the right institution within the EU's political and legislative landscape with the power to enact legislative changes. Ecommerce Europe therefore urges for a proper legal basis, issued by the right legislative

institution, which in our view would be a GDPR amendment or revision of the GDPR and not a guidance by the EDPB. In our view, the EDPB's mandate is on enforcing the GDPR and not on changing it unilaterally. In the same logic, it is important to note that companies that rely on Binding Corporate Rules (BCRs) have invested a significant amount of time, effort and money in their approval. The EDPB guidance now adds additional assessment requirements to BCRs even though these additional requirements are not covered by the GDPR.

5. The Recommendations should maintain a risk-based and proportionate approach to transfer assessment

The absence of a risk-based approach in the Recommendations will, in our view, lead to significant administrative burdens and legal uncertainty without positively impacting the protection of fundamental rights and individual freedoms. In line with a risk-based approach, the Recommendation should provide room for the assessment of the likelihood of public authorities accessing data handled by a specific supplier.

As we see the guidelines the European Data Protection Board (EDPB) does not consider 'likelihood' to be an objective factor in transfer impact assessments. This decision, in our perspective, is not in line with the GDPR, which evidently refers to the concept of 'likelihood' in the context of other obligations (e.g. under Articles 32 and 35 GDPR) while supervisory authorities historically have recognised this concept that requires data exporters to assess and identify the most high-risk data transfers subject to eventual public authority's requests .

Furthermore, identification of supplementary measures should account for the nature of the data being transferred and not only for the data protection legislation in the third-country recipients. Not all information is relevant or would be subject to law enforcement requests (e.g., processing of employee credentials or limited profiles to provide access to a technical solution that does not process personal data as its primary function). Proportionality always needs to be taken into account when performing an assessment on eventual risks and additional measures. A potential infringement and need for additional safeguards always need to be put in relation to the importance of the personal data concerned and the parties involved.

In that perspective, there is a need for clarity in the guidelines on the division of responsibilities between data exporter and importer that should consider which of the involved parties is in a better position to conduct assessments both from competence and scalability standpoints. Introducing requirements upon data exporter only would most likely create extensive administrative burdens for companies that might not operate in the specific jurisdiction they are required to assess and consequently are not able to assess its judicial privacy remedies. As data importers mostly are in a better position to know which laws apply to them in both import and export markets, and as they often typically serve multiple exporters, standardised assessments performed by the data importer could benefit all of their exporter customers and consequently should be supported in the EDPB guidelines. The same clarity is needed to allocate responsibilities among joint controllers and processors, especially in cases where only one of them is basically determining the purpose and the functioning of the data transfer service which is offered to the joint controller on a ready tailored and non-negotiable basis. Examples of such scenarios would be more than welcome and should preferably focus on most common cases.

Furthermore, any suggestion that controllers are liable for sub-processors' supplemental measures appears to be inconsistent with the requirements in the GDPR. In relation to this, the contractual relationship between the exporter and the importer must consequently be considered as a relevant factor. When it comes to the many vendors on which retailers rely, the bargaining power of each individual business, no matter how large, vis-à-vis the vendor is limited. This contractual imbalance is being addressed in certain sectors, such as financial services (where specific contractual clauses are being drafted to reduce risk of

vendor lock-in) but is not currently available in the retail content. It is therefore likely, on the basis of the recommendations as drafted, that such vendors will also insist on an agreement from retailers that these measures are sufficient on a take-it-or-leave-it basis. In line with the practical realities and contractual imbalances noted above, we would like the recommendations to direct greater responsibility towards these vendors.

6. Further clarification with regards to various elements of the Recommendations.

The division of responsibilities between two or more data exporters in a joint controllership setting should be clarified and examples of such a scenario should be provided. The example in the box following paragraph 44 should be clarified, notably with regards to whether data exporters are exempt from the obligation to undertake and document transfer impact assessment pursuant to paragraphs 34-43, in case they ascertain that a data importer falls under Section 702 FISA. The recommendations seem to faithfully transpose the requirements of Schrems II into guidance but in a way that could lead to a de-facto prohibition of use of U.S.-based telecom, cloud and other service providers subject to FISA 702, significantly altering existing relationships. For this reason, only the largest and most sophisticated businesses could comply with the recommendations and this may therefore amount to a non-tariff trade barrier on data flows, which only a political solution (out of the hands of industry) would solve. On this issue, the EDPB has included some examples of supplementary measures but it would be helpful if the EDPB would provide practical examples on how to shape this process/ analysis in practice and in writing, especially in the situation where an EU-based controller is transferring personal data to a U.S. processor subject to FISA 702.

- Use case 6 should clarify whether EDPB Recommendations apply when cloud service providers do not need continuous access to the data. Data is often primarily hosted in an encrypted form within the EU and will most likely only be subject to access from a third country in specific and limited cases.
- Use case 7 should specify whether the use of personal data by the exporter *'for its own purposes'* is a relevant criterion for the scenario assessment, especially given outsourced business services are typically provided under instruction of the data controller.
- The EDPB should clarify in use cases 6 and 7 the meaning of *"the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society"* as a criterion. Further clarification is notably needed on whether EDPB conclusions apply in situations where third-country laws prevent data importers from fulfilling their obligations under a data transfer tool (e.g., a third country does not permit encryption at rest) and how to assess whether public authorities' powers are deemed as not going beyond what is necessary and proportionate. We would also welcome further clarification on whether this criterion would also apply in use cases 1 to 5.
- The EDPB should introduce specific non-US examples to understand how different criteria should be interpreted in the context of jurisdictions which have not come under CJEU scrutiny.