European Law Blog

"Schrems III?" First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 3)

Theodore Christakis

European Law Blog

Published on: Nov 17, 2020

URL: https://europeanlawblog.pubpub.org/pub/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3

Three Scenarios for the Way Forward (and a Recommendation)

Despite the very short available time, I have tried in Part 1 and Part 2 of this article to carefully review the EEGs and Supplementary Measures guidelines. Based on my review, there are two central conclusions that emerge from the EDPB publications on November 11:

1. Third countries might rarely if ever meet the EEG requirements. This means that, beyond the 8 sovereign States/12 entities that have the opportunity of benefiting today from an EU adequacy decision, few other countries might be considered as offering a protection "essentially equivalent" to that offered by EU law.
2. If third countries are not considered as "adequate/essentially equivalent", then data transfers to them are lawful only if supplemental measures are adopted by the data exporter. The EDPB Guidance seems nonetheless to prohibit almost all such transfers when the personal data is readable in the third country.

Perhaps other commentators will find ways to reach a different conclusion. If not, however, then the implications of the EDPB position in its current writing might be: regular transfers to third countries are almost always unlawful if the personal data can be read in the third country.

As the world cannot suddenly stop moving nor international trade end as a result of *Schrems II* and the EDPB Recommendations, there are in reality at least three possible scenarios/solutions for the future. There might also exist other scenarios. I will present here only the ones which seem more probable to me. These scenarios are not independent from one another, but could be easily combined. I will end by detailing an important first recommendation in view of the expected update of the guidelines by the EDPB after November 30, 2020.

Scenario 1: The Grey Zone

A first scenario would be for companies to ignore the EDPB guidance or to pretend that they are taking it into consideration for their everyday transactions while in reality hardly doing so.

If one excludes Maximilian Schrems and other activists, data protection lawyers were the happiest people on the planet on July 16, 2020. The EDPB Recommendations may well contribute to their joy. While companies around Europe are mystified as to how to comply with *Schrems II* and the EDPB guidance, they may reasonably react by paying out hefty legal bills to obtain advice from specialists. Hardly able to contain their joy, some lawyers went on Twitter immediately after the EDPB guidance was announced to claim that "data protection professionals are known for turning impossibles into possibles!". Maximilian Schrems saw this post, incidentally, and commented ironically, that "these professionals then charge their customers another time when the CJEU says (again and again) that it *was* *really* impossible…".

With or without the help of professionals, companies will try to do what they can to keep operating and engaging in international business transactions.

Those in a position to use the technical measures recommended by the EDPB (strong encryption or other techniques that make the data impossible to read for the recipient) will be in full compliance.

The vast majority of companies will find it very difficult to implement such measures. These companies will have three choices:

1. Stop some activities that involve international data transfers or localise data in Europe – a solution that will ensure full compliance with the EDPB requirements, but which could incur substantial costs and disruption.
2. Do nothing and continue operating as usual – a solution that is good for business but that might be fully in breach of the CJEU/EDPB requirements.
3. Try to supplement technical measures with contractual and organizational measures – despite the fact that the EDPB has expressed doubts about whether this might be sufficient.

Companies that are unable to follow solution (a) and are fearful of adopting solution (b) could instead opt emphatically for solution (c). The new SCCs, freshly published by the European Commission, could be used in conjunction with the measures that appear in pages 28-38 of the EDPB Recommendations on Supplementary Measures as well as other potential measures in order to give the impression that they are "compliant" with the post-Schrems II requirements, despite the non-use of encryption/pseudonymization techniques. **Furthermore, companies will definitely be tempted to use Article 49 GDPR "derogations" extensively**, especially consent (Article 49(1a)) and performance of a contract (Article 49(1c)), despite the fact that the EDPB has mentioned several times (see here, here and para. 24-26 here) that such derogations should only be used in exceptional circumstances and not for regular transfers.

These companies will enter into a grey zone. There are good reasons to believe that, in the overwhelming majority of cases, such a choice could work. DPAs around Europe will be unable (or even unwilling) to check all these practices. Very few violations might be detected. Even if they are detected, even fewer fines might be issued. And even if a fine is issued, companies may feel that the cost of a fine is less than the cost of stopping data transfers.

The "grey zone" policy could thus pay off. However, it could involve significant risks. Over the last few months there has been a substantial increase in lawsuits and other actions filed by activists aimed at challenging international data transfers (see for instance this and this). It is also notable that activists are now directly challenging these transfers in European courts and tribunals – not through DPAs. The risks involved could therefore be significant for companies targeted by activists – particularly since all that needs to be proven is a technical violation of the GDPR, not injury to a user of a service.

Scenario 2: Data Localisation

If European data has almost no way of leaving Europe (that is, in a readable format) that means that it needs to remain in Europe. This is called data localization.

Immediately after *Schrems II* some DPAs in Europe were already calling for data localization. "Now is the time for Europe's digital independence," said the Berlin data commissioner Maja Smoltczyk, for instance. Without actually labelling it "data localization", the EDPB's guidance is inevitably leading in that direction.

Given the above, it is interesting to note how DPAs in Europe are lending such strong support to calls by some policymakers to introduce data localization. The most important proponent of data localization in the EU is the European Commissioner for the Internal Market, Thierry Breton who stated, for instance, on August 25, 2020:

> "I have always said that I want Europeans' data to be processed, stored and processed in Europe. I have a feeling that Donald Trump is saying the same thing. The Chinese and the Russians are doing it, we will do it too".

The issue of data localisation is an extremely important one. I analyse it in detail in my forthcoming study: "'European Digital Sovereignty': Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy" (which will be posted online shortly here and here). In this study I show that there are great divergences of views in the European Commission on data localisation. While some policymakers are always supporting the traditional European approach, which is hostile to data localisation and favorable to free data flows, others, like T. Breton, have a different view. As discussed in my study, the new "Digital Governance Act" (due to be announced by the European Commission on November 18, 2020) goes as far as creating a new blocking statute, for non-personal data, which goes far beyond that which is already provided for personal data by Article 48 of the GDPR.[1]

However, data localisation policies do not come about without creating risks and costs. In my aforementioned study, I analyse in detail what the potential negative effects of data localisation mandates could be. These include potential economic costs, cybersecurity risks, risks of policy inconsistencies and potential human rights implications. Before blindly embracing data localisation, Europe should better understand what data localisation technically means and study thoroughly what the adverse consequences of such policies could be.

Scenario 3: Change the World

If the aforementioned solutions are not satisfactory and if Europe does not want to lower its standards of protection, then the only way out of this mess is for Europe to… change the world! Europe has already done so, in many respects, in relation to data protection in general. Is it also going to achieve the amazing feat of changing surveillance laws worldwide?

In the 2016 *Szabó and Vissy v. Hungary* judgment, where the ECtHR concluded that Hungarian legislation on secret anti-terrorist surveillance violated Article 8 of the ECHR, the Court wrote:

> "The techniques applied in monitoring operations have demonstrated remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen […], especially

> when automated and systemic data collection is technically possible and becomes widespread. In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights". (para. 68).

Recent technological developments have indeed provided States with cutting-edge surveillance techniques (including facial recognition) to enable them to invade people's privacy and undertake mass surveillance and bulk collection of data on a scale simply unimaginable a few years ago. *Schrems II* and the EDPB are stressing once again the necessity of appropriate safeguards, enforceable rights and effective legal remedies when personal data is being processed for the purpose of national security and defence.

In the first part of this paper I mentioned that European Courts found several times that surveillance or data retention laws in Europe do not meet the EEG requirements. But the case law of European Courts also includes several "success stories". In 1978 the ECtHR found, for instance, in *Klass and others*, that German lawmakers were very careful to introduce safeguards in German surveillance law (which were adopted after the 1972 Munich massacre) and thus Germany did not violate the ECHR. In 1990 it took only a few months for France to change its surveillance laws in order to comply with ECtHR requirements after the Court found that France violated the convention in the cases of Kruslin v. France and Huvig v. France. Much more recently, countries around Europe have incorporated several (though not necessarily always *all*) of the EEG requirements in their new surveillance laws. One should also note that when the CJEU or the ECtHR adjudicate that surveillance laws in Europe are problematic, they do not bring the whole building crashing down. Instead, in most cases, they find that, while European States have made efforts to incorporate certain EEG requirements, they have not sufficiently committed themselves to others. From this point of view EEGs are not a utopian oddity. They are a useful tool of convergence against abuse and arbitrariness. They are transforming Europe, and they are permitting, step by step, human rights safeguards to reign in increasingly sophisticated new methods of surveillance. While this is a precious state of affairs from a human rights perspective, it must be emphasized that this process of continuously "adapting" European surveillance laws to highly protective standards and safeguards does not lead to blocking trade and business transactions in Europe. There is therefore a fundamental difference between changing European surveillance laws, without affecting the economy, and trying to "change the world" though restrictive measures that may lead to serious disruption for global trade and the European and global economy.

EEGs are therefore certainly changing Europe, and, if effectively used as an instrument of progressive convergence and interpreted with a degree of flexibility, they could also help change the world. Finding adequate universal standards of protection in relation to government access to data is the big question of our times. As shown by Anu Bradford in her "Brussels Effect", Europe already has an important legacy of exporting protective values where data protection and privacy is concerned. Could Europe now succeed in

changing the surveillance laws of foreign countries, an issue that affects the very core of sovereign States, their national security?

There are at least three paths that will enable this to happen.

First, the EEG Recommendations could be used by foreign countries as a useful "user manual" for introducing safeguards in surveillance laws. Foreign countries could use them to increase their chances of obtaining an adequacy decision; or, more simply, because they might consider that doing so is justified from an ethical and a human rights perspective.

The second path is though bilateral cooperation. From this point of view the transatlantic dialogue is of paramount importance. After *Schrems II* several commentators adopted a positive attitude, emphasizing that "Schrems II Offers an Opportunity—If the U.S. Wants to Take It" and that "When There Is a Will, there Is a Way". The new US administration should not interpret the EDPB recommendations as a "provocation". Rather, they are further proof of the need to work faster and more strenuously together to achieve a solid and long-lasting transatlantic arrangement as soon as possible. From a formal point of view, the idea of putting in place non-statutory (but binding) modifications as a means of fixing the perceived defects in US surveillance law (first advanced by Swire and Propp at the Cross Border Data Forum) is perfectly compatible with EEGs as I explained in Part 1 of my analysis. From a substantive point of view the gap might be less significant than some people fear. The EU and the US should also take advantage of the dynamic created by the transatlantic negotiations launched in September 2019 to conclude a transatlantic agreement on Law Enforcement Agents' (LEAs) access to data. As shown in our forthcoming IDPL study on this issue, this represents a great opportunity to create a workable regime for LEAs' access to data, to prevent conflicts of laws and to provide legal certainty for companies, whilst ensuring all necessary human rights safeguards.

The third path is one of multilateral cooperation. Indeed, in the aftermath of *Schrems II*, several voices have been calling for a legally binding international agreement for the protection of privacy and personal data with respect to intelligence agencies activity. As the Council of Europe emphasized in a recent statement, a robust basis for a future solution could be Convention 108+ - this is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) as amended by the 2018 Protocol. Other initiatives, such as the "Data Free Flow with Trust" ("DFFT" or "Osaka Track"), launched by Japan in 2019, are also based on the idea that countries that support an open, rules-based trading system need to agree on core principles and common rules, including for government access to data.

Recommendation: Introduce a Proportionate and Risk-Based Approach

While waiting for the world to change, the EDPB should try to provide some breathing space for those who need to conduct international data transfers. The 5300+ companies who were using Privacy Shield, as well as thousands of other data controllers and data processors in Europe, are not NSA, CIA or other intelligence

services' agents or accomplices. They are organisations that are unwillingly "trapped" in inextricable conflict of laws situations. It is for sovereign countries to clean up the mess. The private sector could help by lobbying heavily in favour of international solutions – instead of "pretending" that everything is fine. But whilst waiting, (and without taking the pressure off), the EDPB and national DPAs should help international trade maintain its current course. They could do so by showing more flexibility, beginning with integrating a proportionate and risk-based approach in the updated final guidance (to be released after November 30).

Given that one of the key criticisms made against *Schrems II* is that it is difficult for controllers to assess the adequacy of third country laws, one could argue that this might add an additional layer of complexity for them. One could also ask whether controllers might be able to assess likelihood of access in sectors such as intelligence which operate opaquely. While such arguments are founded, increased complexity will certainly be better for companies than complete disruption. Moreover, some categories of data transfers (for instance the "consulting the agenda of the company's members in order to fix a call" use case mentioned above) could be logically considered *prima facie* as "low risk" – especially when the recipient country is a democratic one offering assurances that it does not collect such kind of data. Last, but not least, instead of prohibiting almost all transfers when the personal data is readable in the third country, the EDPB should work hard in order to dress a scale of risks depending on a series of risks factors, including the nature of the data being transferred. This would help to ensure consistency of risk assessments by companies and data controllers around Europe.

The result of such a **proportionate** and risk-based approach could be that technical measures that have appeared in the Recommendations (that data should be strongly encrypted or otherwise made impossible for the recipient to read) should be mandatory only for high-risk situations, while organizational and contractual measures should suffice in low-risk situations (which probably represent the vast majority of daily business transactions). Such flexibility would enable the baby not to be thrown out with the bathwater.

Aknowledgments: The author would like to thank all the colleagues who contributed useful comments for this article: Vanessa Franssen and Orla Lynskey (as ELB Editors), DeBrae Kennedy-Mayo, Kenneth Propp and Peter Swire. All errors mine.

Footnotes

1. According to Article 10(i) of a leaked version of the "Digital Governance Act": "The provider of data sharing services shall have adequate safeguards in place, including of a technical, organizational and legal nature, that prevent it from responding to requests from authorities of third countries with a view of obtaining access to non-personal data relating to companies established in the Union and Union public administration, unless the request is based on a judicial decision from the Member State in which the company to which the data relate is established". ↩