**European Law Blog**

# Schrems III? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1)

**Theodore Christakis**

**European Law Blog**

**Published on:** Nov 13, 2020

**URL:** https://europeanlawblog.pubpub.org/pub/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1

No, there has been no new "Schrems" judgment from the CJEU. But the publication of the post-Schrems II "Recommendations" by the European Data Protection Board (EDPB) on November 11, 2020, is such a huge aftershock than one could mistake it for an entirely *new* earthquake shaking the international data transfer system.

After the Court of Justice of the EU (CJEU) in *Schrems II* on July 16, 2020 (analysed here, here and here in the blog) almost closed the door on personal data being allowed to leave Europe, some might have hoped that the EDPB would open several windows to enable the data to find its way out of the bloc. It did not. When one reads its "Recommendations on Supplementary Measures", it appears that any transfer of the personal data of Europeans to countries that do not benefit from an EU adequacy decision will be extremely difficult – the principal permitted mode of export is to encrypt the data so thoroughly that it cannot be read by anyone in the recipient country, even the intended recipient. Furthermore, one wonders how many surveillance laws around the world meet the requirements of the "European Essential Guarantees for Surveillance Measures" (EEG Recommendations), also published on November 11 by the EDPB. For the thousands of companies and other data controllers or data processors around Europe faced with the herculean task of assessing whether countries to which they wish to transfer personal data meet the EEG requirements, here is some quick advice: start with the assumption that, in principle, they don't!

I will not summarize here the two lengthy documents issued by the EDPB (54 dense pages!). This has already been carried out very well by Caitlin Fennessy here or in the EDPB's own press release. Suffice it to explain that the EDPB adopted two complementary documents:

First, it issued the "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" ("Recommendations on Supplementary Measures"). This guidance had been eagerly expected since *Schrems II*. In fact, the CJEU referred to the possibility that, even if the importer's national laws do not offer an "adequate" and "equivalent" level of protection in relation to government access to data, international transfers could still take place if the data controller puts in place "additional safeguards" or "supplementary measures" to ensure the protection of the data transferred by other means. This is an absolutely key concept, as it is the only way to continue regular[1] data transfers from the EU to the US and also to a great number of other countries which, like the US, very probably do not offer what the Court would recognize as an "equivalent" level of protection. The EDPB "Recommendations on Supplementary Measures" propose a step-by-step roadmap for implementation, and include six steps[2] that all data controllers and data processors should follow before transferring data. Even more important than the description of these six steps, is the 17 page-long Annex 2 to the Recommendations which provides a "non-exhaustive" list of "examples of supplementary measures" considered by the EDPB to be acceptable sometimes for data transfers and not acceptable at other times.

The second document published by the EDPB is the "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures" ("EEG Recommendations"). The objective of these (updated[3]) EEG Recommendations is to provide data exporters with a guide, based on the two European Courts'[4] jurisprudence, in order to determine whether foreign countries surveillance laws meet the European human rights requirements.

The two EDPB "Recommendations" require much more careful study. I will offer here just a few quick thoughts, as a follow-up to my previous analysis of Schrems II in this blog. **Part I** of this article will feature some preliminary commentary on the "EEG Recommendations" which look like a kind of "Surveillance Laws Survival Guide". **Part II**, which will be published shortly, will focus on the "Recommendations on Supplementary Measures" and will argue that the EDPB's approach appears excessively restrictive and sets the bar so high that it will be extremely difficult to reach. Lastly, a conclusion will present three possible scenarios for the way forward.

**Part I**

**Who Can Survive the "Surveillance Laws Survival Guide"? (Thoughts on the EDPB's "EEG Recommendations")**

(Part 2 will be published here on November 16th)

In the EEG Recommendations the EDPB tried to gather all the requirements of European law and jurisprudence in order to show how surveillance laws ought to be assessed in respect with their compatibility with EU Law.

Despite some cautionary notes from the EDPB, the "EEG Recommendations" pretty much appear to be a kind of "Surveillance Laws Survival Guide" – in the sense that if foreign surveillance laws do not meet the EEG requirements they "would not offer a level of protection essentially equivalent to that guaranteed within the EU".

I will first discuss the importance of the "EEG Recommendations" (1), then make a few preliminary remarks on their content (2), and end this section by asking how many countries in the world could pass the "EEG Test" (3).

**1) More Important Than It Seems**

The EEG Recommendations are of great importance not only when data controllers and processors wish to use Standard Contractual Clauses (SCCs) (Article 46 GDPR) and Binding Corporate Rules (BCRs) (Article 47 GDPR), but also when the European Commission wishes to issue an adequacy decision under Article 45 GDPR.

*(a) Importance for the Use of SCCs and BCRs*

The "EEG Recommendations" are directly linked to "Step 3" of the "Recommendations on Supplementary Measures" which is, along with "Step 4" (see note 2), by far the most important step to follow before proceeding to international data transfers from the EU. Based on *Schrems II* and the procedure explained in the EDPB's "Step 3", data controllers and processors who cannot use an "adequacy decision" as the legal basis for international data transfers must themselves conduct a very important assessment: they must assess whether the surveillance laws of the country to which they wish to export data offer an "adequate level of protection". The "EEG Recommendations" constitute a guide that is intended to help them conduct this very difficult assessment.

The EDPB does not go so far as to suggest that the law of a foreign country that does not meet all the EEG requirements should be considered *ipso facto* as not offering an "equivalent" level of protection. Indeed, paragraphs 8 and 9 of the "EEG Recommendations" feature (in a rather unclear way) some cautionary notes indicating that the EEG should not be read as "a list of elements to demonstrate that the legal regime of a third country as a whole is providing an essentially equivalent level of protection". Moreover, the EDPB emphasises that "these guarantees require a certain degree of interpretation, especially since the third country legislation does not have to be identical to the EU legal framework" (§49). This leaves room for different approaches to foreign surveillance laws.

However, the EDPB also strongly indicates that a country that does not meet the EEG requirements should be considered as having failed the "equivalent protection" test. Paragraph 51 of the Recommendations highlights that if "the assessment of the third country surveillance measures against the EEG" leads to a situation whereby "the third country legislation at issue does not ensure the EEG requirements", then it should be concluded that:

> "the third country legislation would not offer a level of protection essentially equivalent to that guaranteed within the EU".

In other words, if companies and other data controllers and data processors find that foreign countries' surveillance laws do not meet the EEG requirements, then it should normally[5] be concluded that exports of data **cannot take place towards these countries** without using some of the (mostly technical) "supplementary measures" put forward in "Step 4" and Annex 2 of the "Recommendations on Supplementary Measures" (which will be discussed in Part II).

*(b) Importance for Adequacy Decisions*

But the "EEG requirements" are not only important when data controllers and data processors use SCCs or BCRs. They also seem to be fundamental when determining whether the European Commission can (or cannot) issue an "adequacy decision" under Article 45 of the GDPR. The EDPB is clear in this regard. It states in paragraph 52 of the "EEG Recommendations" that:

> "When assessing the adequacy of the level of protection, pursuant to Article 45 GDPR, the Commission will have to evaluate whether the EEG are satisfied as part of the elements to be considered to guarantee that the third country legislation as a whole offers a level of protection essentially equivalent to that guaranteed within the EU."

In my July article in this blog, I explained the constitutional implications of *Schrems II* and how the EDPB "becomes the grand assessor of global legal adequacy", affecting the European Commission's powers under Article 45 of the GDPR. Paragraph 52 of the "EEG Recommendations" is a "warning shot" that the European Commission cannot afford to ignore: the message is that future adequacy decisions should ensure that the requirements found in the "EEG Recommendations" are met in the foreign country. The Commission now has an updated "user's manual" for adequacy decisions that should be taken into consideration.

Going even further, a devil's advocate might argue that the "EEG Recommendations" could be a valuable tool in the hands of activists, as a means of challenging the validity of *existing* adequacy decisions through action at the CJEU. Do the twelve States or entities that have until now benefited from adequacy decisions *all* meet these EEG requirements? Does Israeli or Japanese surveillance law, for instance, really meet the EEG requirements? And what should the consequences be if they do not?

**2) Has Something Been Forgotten?**

We have seen in the previous section that the "EEG Recommendations" are of paramount importance and their application could have significant consequences. This immediately raises the question of how to assess their content. I will advance here the following preliminary thoughts.

*(a) The Strictest Denominator of Them All?*

In important respects, the "EEG Recommendations" appear to be a faithful compilation of the surveillance requirements set over the years by European jurisprudence (see this for instance). The Recommendations are based on the most important judgments on surveillance by the CJEU and the European Court of Human Rights (ECtHR), from *Schrems I* and *Schrems II* to the recent data retention/collection judgments rendered by the CJEU on October 6, 2020; and from the 1978 *Klass and others* Judgment to more recent ECtHR judgments such as *Zacharov* and *Big Brother Watch*.

However, the impression remains that the "EEG Recommendations" always "pick and choose" the strictest requirements found in this jurisprudence and somehow neglect elements that could be used to provide more flexibility for foreign countries' surveillance laws. As I explained in this blog in 2018 (read here) and in 2020 (read the last part here), European law in this field is far from being a monolithic bloc. The EDPB hints at this point in paragraphs 10 and 11 of the "EEG Recommendations". Nevertheless, it clearly indicates its preference for stricter standards by stating that its guidelines "will continue to be partly based on the jurisprudence of the

ECtHR", but only "to the extent that the Charter as interpreted by the CJEU does not provide for a higher level of protection which prescribes other requirements than the ECtHR case law" (§11).

This decision to retain the "strictest" jurisprudential standards results in the EDPB ignoring certain "classical" elements of ECtHR surveillance case law in its "EEG Recommendations". Here are two notable examples.

*(b) No National Margin of Appreciation?*

First, the EDPB does not refer to the concept of "margin of appreciation",[6] renowned for its widespread use in ECtHR case law.

The ECtHR has described this concept as a "tool to define relations between the domestic authorities and the Court". According to the classical position of the ECtHR State authorities "are in principle in a better position than the international judge to give an opinion" on the "necessity" and "proportionality" of a derogation or restriction authorized by human rights law. As a consequence, international courts "should grant national authorities an important degree of deference and respect their discretion" with regard to the implementation of exceptions. Thus, without precluding judicial review of a State's action in this field, the doctrine intends to "limit the scope of this review" and to impose some degree of judicial self-restraint where an assessment of the attitude of national authorities is concerned.[7]

In two important recent judgments, the ECtHR gave the impression that it recognised a considerable margin of appreciation in favour of States adopting surveillance measures.

Indeed, in *Centrum för Rättvisa* rendered on June 19, 2018, the Chamber stated that "the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation" (para. 112).

In the *Big Brother Watch* judgment, issued on September 13, 2018, the Court went even further by saying that: "It is clear that bulk interception is *a valuable means* to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime". The Court added that "the decision to operate a bulk interception regime [is] one which falls within the wide margin of appreciation afforded to the Contracting State" (para. 386 and 387).

The EDPB does not mention these elements at all (despite the fact that it quotes other aspects of these judgments where, for instance, the ECtHR sets strict safeguards as a counterpart to this margin of appreciation). On the contrary, its analysis on the principle of necessity (§ 37) leaves no room for a national margin of appreciation. The EDPB clearly concludes that:

> "[L]aws permitting public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter."

The two ECtHR judgments mentioned above are now being challenged by the applicants, inviting the Grand Chamber of the ECtHR to apply more robust scrutiny to the necessity and proportionality of bulk surveillance and to adopt the "strict necessity" test proposed by the CJEU. The "EEG Recommendations" exert further pressure on the ECtHR to do so. If the ECtHR does not follow this path, it could lead to further fragmentation of EU/ECHR law on surveillance. On the contrary, if it does, the ECtHR would reinforce the CJEU/EDPB restrictive approach on surveillance.

*(c) Better Understanding of the Meaning of "In Accordance With the Law"*

The EDPB logically refers in paragraphs 26-31 of the "EEG Recommendations" to the "in accordance with the law" requirement found in both the Charter and the ECHR. The EDPB rightly explains that, according to European standards, surveillance measures "must be provided by law" in clear, precise and accessible rules. However, it is weird that the EDPB does not include an important piece of information for the thousands of data controllers and data processors that need to apply these guidelines: that the term "in accordance with the law" does not necessarily refer to statutory texts (i.e. acts of parliament). Only a strange footnote (number 24) seems to address this point, presenting it almost as a linguistic curiosity of the French translation of a CJEU judgment.

Nonetheless, the ECtHR has consistently explained that it:

> "has always understood the term 'law' in its 'substantive' sense, not its 'formal' one; it has included both enactments of lower rank than statutes and unwritten law." (See for instance the case of Kruslin v. France, Judgment of April 24, 1990, §29)

In a similar way, recital 41 of the GDPR clearly states that:

> "Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament (…)."

This is an important element in the assessment of foreign surveillance laws.

On the one hand, in order to assess foreign surveillance "laws" data controllers and data processors should not only focus on statutory law but also administrative acts, case law, etc., even though that is a challenging research task.

On the other hand, non-statutory additions to existing foreign surveillance laws could suffice in terms of reaching "essential equivalence status" as long as these acts are "legally binding under domestic law" ("EEG Recommendations", § 27). This is important. We should recall, for instance, that the US are seeking ways to fix the perceived defects in US surveillance law through non-statutory modifications (see for instance this and this).

**3) Who Could Pass the Test? (And Free Advice for Dummies)**

Having carefully studied the "EEG requirements" the big question arises: who could pass the "EEG Test"?

The US certainly *is not passing* the test for the time being; the CJEU has clearly said so in the Schrems II Judgment.

China clearly fails the test also – no need to even discuss this.

I am not familiar enough with Indian surveillance laws, but I would be very surprised if they could pass the "EEG Test". See for instance this and this.

Closer to Europe, Russia does not pass the test either. In December 2015 the ECtHR found in the landmark *Roman Zakharov* judgment that Russia violated Article 8 of the ECHR because Russia's legal provisions governing communications surveillance did not provide adequate safeguards against arbitrariness or abuse. As an immediate response, the Russian government enacted a law… allowing it to overrule international court orders to "protect the interests of Russia" (see the BBC Report here).

In more general terms, the ECtHR, even applying its less strict standards than the CJEU, has found that almost all the surveillance laws of Members of the Council of Europe that have been brought under its scrutiny since 2001 have violated the ECHR. This was the case for Hungary, Russia, Romania (here, here and here), Bulgaria, Moldova, Turkey and more recently the UK in the *Big Brother Watch* case. One of the only recent cases where the Court found a surveillance law to be in conformity with the convention was in relation to Sweden, in the *Centrum för Rättvisa* case. But, as has already been mentioned, this case has now been referred to the Grand Chamber by the applicants.

If one now turns to the CJEU, it is worth recalling that in its October 6, 2020 data retention/collection judgments it found that the laws of France, Belgium and the UK did not meet the European standards either.

One can conclude from this first section that surveillance laws rarely survive the scrutiny of European tribunals. If the surveillance laws of European countries themselves most often do not respect the "EEG requirements", how many States around the world could be expected to do so?

In my July post on Schrems II, I wrote the following under the title "Companies to Assess Sovereign States Surveillance Laws? Well, Good Luck With That!":

> "Beyond diplomatic, political and economic considerations, the "privatization" of adequacy assessments will undoubtedly be extremely difficult from a legal point of view. The European Commission itself, with its giant technocratic expertise and its armada of high-skilled lawyers, proved to be wrong twice in relation with such assessments, once with Safe Harbor and once with the Privacy Shield (not to mention the PNR Agreement with Canada or the first PNR Agreement with the US). How could European SMEs

> do any better than the Commission? On the basis of what legal expertise are they going to assess third-countries laws?".

Well, on second thought, and in light of the analysis above, I now have some advice for companies and other data controllers and data processors who need to ascertain whether foreign surveillance laws meet the "EEG requirements": **bear in mind that they probably don't**! If you use such a negative presumption, then in most cases you will be right. It is only if you are able to demonstrate that, despite the odds, the surveillance law of the country to which you wish to export data meets the "EEG requirements",[8] that you could be able to transfer data based on the assumption of "essential equivalence".

As a legal matter, therefore, it appears that the preponderance of transfers to third countries do not meet the essential guarantees as set forth by the EDPB. Tomorrow, I will assess the difficulties entities will face in creating any supplemental measures that would enable transfer to countries that lack such guarantees.

## Footnotes

1. Article 49 derogations could also be used but normally on a rather exceptional basis and for occasional and non-repetitive transfers. ↩
2. The six steps are as follows: "1) Know your transfers ; 2) Identify the transfer tools you are relying on; 3) Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer; 4) Adopt supplementary measures; 5) Procedural steps if you have identified effective supplementary measures; 6) Re-evaluate at appropriate intervals". ↩
3. The Article 29 Working Party had already adopted in April 2016 a Working document on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees). See WP237. ↩
4. Explanation for non-European readers: this expression refers, on the one hand, to the Court of Justice of the European Union (CJEU), the judicial branch of the EU based in Luxembourg; and, on the other hand, to the European Court of Human Rights (ECtHR), which is an international human rights court based in Strasbourg, France, which has jurisdiction over the 47 Member States of the Council of Europe, parties to the European Convention of Human Rights (ECHR). ↩
5. Unless a particular set of circumstances occur, not described in the EDPB document, that could lead to a reversal of the "not equivalent protection" presumption. ↩
6. However, I think that paragraph 49 of the "EEG Recommendations" could be used to work towards recognition of some margin of appreciation. The EDPB emphasises there that the EEG "guarantees require a certain degree of interpretation, especially since the third country legislation does not have to be identical to the EU legal framework". ↩

7. For an analysis and sources of these quotes please see here, here and here. ↩

8. It might well also be that some countries do not have surveillance laws. Does Nauru or Vanuatu have a surveillance law for instance? Several other countries might lack the advanced technological capabilities required to carry out surveillance. However, the fact that dozens of countries in the world have a very poor track record in the field of human rights will immediately exclude them from being "equivalent protection" candidates for other reasons. ↩