

European Law Blog

"Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 2)

Theodore Christakis

European Law Blog

Published on: Nov 16, 2020

DOI: <https://doi.org/10.21428/9885764c.ebe1e61e>

License: [Creative Commons Attribution-ShareAlike 4.0 International License \(CC-BY-SA 4.0\)](https://creativecommons.org/licenses/by-sa/4.0/)

In the first part of this analysis, published [here](#), I explained why a great number of third countries might not meet the “Essential European Guarantees” (EEG) as set forth by the EDPB. In the second part of this paper I will assess the important difficulties entities will face in using supplementary measures that would enable transfers to countries that lack such guarantees. Tomorrow morning the ELB will publish the final part of this article which includes a discussion of three possible scenarios for the way forward and an important first recommendation in view of the expected update of the guidelines by the EDPB [after November 30, 2020](#).

Part 2

“Only Non-Readable Data Can Be Exported”

Thoughts on the EDPB’s Recommendations on Supplementary Measures

On July 16, 2020 the CJEU mostly closed the door on personal data being allowed to leave Europe without an adequacy decision, but left some windows open to enable data to find their way out of the bloc. Following several letters from industry protesting that Schrems II could have a “massive negative impact” on the European and World Economy and inviting the EDPB to be flexible enough (see for instance [this](#), [this](#), [this](#) and [this](#)), some might have hoped that the EDPB would open more windows. In its [Recommendations on Supplementary Measures](#), adopted on November 10, 2020, the EDPB not only did not do so, but it also closed most of the windows that might have remained open following the CJEU judgment. To sum up, the EDPB’s guidance clearly indicates that no data transfer should take place to non-adequate/non-essentially equivalent countries unless the data is so thoroughly encrypted or pseudonymised that it cannot be read by anyone in the recipient country, not even the intended recipient.

There are at least three striking features in the EDPB Recommendations on Supplementary Measures that deserve closer attention.

1) The EDPB Ignores the Risk-Based Approach

The first observation is that the EDPB seems to have omitted, or even rejected, the possibility of a risk-based approach despite the fact that such an approach is now enshrined in the GDPR.¹

In advance of the adoption of the “Recommendations”, several companies and organisations had invited the EDPB to focus its guidelines on the assessment of the **real risks** and **likelihood** that personal data transferred outside of the EU might be requested by foreign surveillance authorities. They had tried to convince the EDPB that there is an extremely low likelihood of this happening in a great number of cases and that as a consequence, the EDPB should not throw the baby of international trade/data transfers out with the bathwater for the sake of such a limited risk.

One of the best examples is the White Paper [“A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision”](#) published in September 2020 by the Centre for Information Policy Leadership (CIPL), a think-tank which counts among its members 85 EU, US and other global companies. CIPL’s main recommendation was that the EDPB guidelines should “contain a toolkit of possible measures that can be deployed by organisations based on context and risk, rather than prescribe strict technical or procedural requirements” (p.2) – which is exactly the opposite of what the EDPB did. The CIPL paper explained in a more precise way that:

“Consistent with the GDPR’s risk-based approach, **organisations assess the risk** of transferring data outside of the EU in light of their specific situation, as well as the likelihood and severity of risks to individuals”. (p.3)

CIPL called for “the creation of a single database of risks assessments across countries at the EU level, so that transfers are assessed in a consistent way”. It considered that:

“The **data transfer risk assessment** is a key step in identifying potential risks associated with an organisation’s data transfers and identifying mitigating measures commensurate with those risks. It is important that any regulatory guidance recognises the importance of these risk assessments in light of the risk-based approach enshrined in the GDPR. Consistent with the EDPB guidelines on DPIAs and high risk processing (WP 248), transfers to third countries should not automatically and *per se* be seen as constituting high risk processing under GDPR. It should instead be determined whether such transfers could result in a high likelihood and severity of risk of harm, for example due to governmental access to that data”. (p.8)

CIPL then moved on to propose a series of “risk factors” that should be taken into consideration before transferring data, such as the “nature of the data being transferred” or the “likelihood of government access to certain types of data (both from intelligence and other law enforcement authorities such as securities, anti-trust, anti-bribery, safety, pharmacovigilance etc.) and whether the data that is subject to the transfer is within the scope of intelligence and law enforcement activities” (p. 9).

The White Paper ([“Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II”](#)) published by the US Government in September 2020 adopted exactly the same risk-based approach. The US Government argued that:

“As a practical matter, for many companies the issues of national security data access that appear to have concerned the ECJ in Schrems II are unlikely to arise because the data they handle is of no interest to the U.S. intelligence community. [...] Companies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence

agencies would seek to collect that data. Indeed, the overwhelming majority of companies have never received orders to disclose data under FISA 702 and have never otherwise provided personal data to U.S. intelligence agencies. [...] The theoretical possibility that a U.S. intelligence agency could unilaterally access data being transferred from the EU without the company's knowledge is no different than the theoretical possibility that other governments' intelligence agencies, including those of EU Member States, or a private entity acting illicitly, might access the data". (p. 2-3).

None of these arguments have convinced the EDPB. Not only does the Board not endorse a risk-based approach, but it also gives the impression that it wishes to reject it in para. 42 of the "Recommendations on Supplementary Measures" when it writes, for the attention of data controllers/data processors, that:

"if you still wish to envisage the transfer, you should look into other relevant and objective factors, and not rely on subjective ones such as the likelihood of public authorities' access to your data in a manner not in line with EU standards".

The EDPB also clearly indicates (see the next section) that "organisational measures" (of which risk assessments form a part) do not provide enough safeguards without the addition of technical measures. Even in a situation where the law of the foreign country clearly exempts some categories of data from the reach of government authorities (such as data covered by legal privilege or medical/professional secrecy) the EDPB considers that the data can only be transferred using strong encryption (cf. §85). The idea is, it seems, that whatever the content of and guarantees offered by foreign surveillance laws, we cannot trust foreign governments unless their entire legal regime has "essentially equivalent protection"! Part 1 of my discussion showed however why few, if any, countries would be "essentially equivalent" according to the "EEG requirements".

The debate between a risk-based approach and a rights-based approach is an old one as far as the EU is concerned and has been well analysed by [Raphaël Gellert in his recent OUP book](#). The EDPB post-Schrems II "Recommendations" clearly show a preference for the rights-based approach, despite the fact that the risk-based approach also forms part of the data protection GDPR iceberg. The rejection of the risk-based approach by the EDPB is odd. Combined with the interpretation of "supplementary measures" by the Board (see below), it might lead to important disruption for business activities that could be incompatible with the respect of the principle of proportionality.

2) The EDPB is Highly Suspicious of the Use of Solely Non-Technical Measures

In the aftermath of *Schrems II* several commentators suggested that contractual and organizational measures could suffice in terms of transferring data to "non-equivalent" countries, perhaps even making technical measures such as encryption unnecessary. The [CIPL paper](#) included several "legal", "organizational" and "governance" measures as well as "technical measures (except encryption)" and "encryption" suggesting that

companies could “consider” and “choose from” these categories. It clearly advised the EDPB not to limit its guidelines to “strict technical or procedural requirements” but to offer a set of tools which could be used at the operator’s discretion depending on the circumstances and the risks involved. Similarly, lawyers have indicated that contractual measures rather than technical measures could suffice (see [here](#), [here](#) and [here](#) for instance).

The EDPB however seems highly suspicious of a scenario in which non-technical measures are used without technical measures being used simultaneously.

Paragraph 48 of the Recommendations reads as follows:

“Contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country (where this unjustifiably interferes with the data importer’s obligations to ensure essential equivalence). Indeed, there will be situations where only technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes”.

Paragraph 95 is even more clear:

“As said, contractual measures will not be able to rule out the application of the legislation of a third country which does not meet the EDPB European Essential Guarantees standard in those cases in which the legislation obliges importers to comply with the orders to disclose data they receive from public authorities”.

And in other parts of the Recommendations the EDPB seems to indicate that contractual or organisational measures may “complement” – but may not be a substitute for – technical measures. Their only function would thus be to “strengthen the overall level of protection of data” (see for instance para. 48 and 122).

This position makes understanding of the suggested technical measures very important.

3) The EDPB’s Technical Measures: Make the Data Unreadable!

The EDPB presents a list of “examples of technical measures” in para. 72-86 that could be used to transfer data to a non-adequate country. While the list is “non-exhaustive” (which might offer room for other solutions) the examples put forward lead to the conclusion that the EDPB will accept the legality of transfers only if the data are rendered non-readable for the importer in the recipient country.

Indeed, these technical measures are considered effective only if data are strongly encrypted and “the importer does not have the key; if data are pseudonymized and the importer has no way of identifying; plus a couple of less common scenarios (e.g., multi-party computation)”. (see [here](#)). The only scenario where the EDPB accepts the possibility of the importer being able to decrypt the data is that mentioned above (section 1) concerning data protected by legal privilege or medical/professional secrecy.

In contrast, the EDPB clearly rejects (in para. 87-91) two scenarios [“accounting for the vast majority of real world transfers”](#). First, the EDPB considers that it is not possible for a data exporter to use a cloud service provider in order to have personal data processed according to its instructions in a third country. And, second, the EDPB considers that it is not possible for a data exporter to make personal data available to entities in a third country (for instance a branch of the same company or subcontractors) to be used for shared business purposes.

There is a certain irony to the fact that the EDPB considers strong encryption (as well as irreversible pseudonymization) as the only effective technical means of transferring data to non-adequate countries. This is occurring at exactly the same time as EU Member States’ wishing to oblige platforms and communication organisations to introduce “backdoors” to encrypted communications so that data can be available to government security, intelligence and law enforcement agencies. Indeed, on November 6, 2020 the German Presidency of the Council introduced a non-binding resolution that seeks to give national authorities access to encrypted communications. (posted by Politico behind a paywall [here](#)).

Another irony (or negative ‘side-effect’) could be that the protective position of the EDPB could only make law enforcement and intelligence authorities look for more intrusive tools (obligation for suspects to hand over incriminating data, increased government hacking, etc.).

But the main issue is what happens with all these companies and other data controllers and data processors that are unable to use these technical measures. First, some companies, especially SMEs, might not have the tools/means to apply such strong encryption. Second, and more importantly, encryption is often not a suitable solution because it blocks the usability of the data and prevents necessary data processing activities by the recipient. If we follow the EDPB guidance, companies in Europe will be unable to share their HR and employee data, customer files, or to operate any other intra-group transfers including personal data with their counterparts outside Europe. The branch of a European company in the US might not even be able to consult the agenda of its European members in order to fix a call. All this could lead to huge disruption for the everyday operations of international corporations.

The final part of this article will be posted here tomorrow at 7:30 AM. It includes three possible scenarios for the way forward and an important first recommendation in view of the expected update of the guidelines by the EDPB.

Footnotes

1. The GDPR contains many references to risk factors and the risk-based approach. Prominent among them is article 35 combined to recitals 89, 90 and 91. The 2017 [Art. 29 Working Party Guidelines on Data Protection Impact Assessment \(DPIA\)](#) develops these articles and emphasizes “the risk-based approach embodied by the GDPR” (p. 5). Indeed, A DPIA is a process designed to describe the processing, assess its

necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data. [↵](#)