Legal Affairs and Administration
Sanna-Maria Bertell

EUROPEAN DATA PROTECTION BOARD

ON RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA

Confederation of Finnish Industries ("EK") is the leading business organization in Finland.[1] EK represents majority of private sector enterprises and companies of all sizes. We serve 24 member associations, with over 15,300 companies across all business sectors. Vast majority of our members are SME companies.

The European Data Protection Board ("EDPB" or "the Board") has invited public consultation on its *Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* ("Recommendation"), published on November 11, 2020. On the same date, the EDPB published *Recommendation to European Essential Guaranteed for Surveillance Measures* ("EEG", and together with the former, "Recommendations").

KEY CONCLUSIONS

We endorse strong protections for personal data, including when data is transferred to third countries. But **we have substantial concerns about some potential interpretations of the Recommendations, as they**:

- **Treat all data flows similarly**, whereas in reality context and nature of data matters;
- **Diverge from GDPR's risk-based approach** and are based on very narrow and strict reading of case law;
- **Create uncertainty to EU law interpretation**, partly based on a regime that EU institutions are not bound to;
- **Are impracticable as they force certain technical measures** in all situations, and seem to offer very little role to organizational and contractual measures;
- **Mandate encryption** with additional measures so that the intended recipient outside Europe cannot even access data.

We strongly urge the EDPB to revise the recommendation, and especially work towards a more reasonable, proportionate approach as suggested below (see section Suggested Tools – Going Forward below).

GENERAL COMMENTS

In the Shrems II ruling, the CJEU explicitly referred to the possibility to carry on data transfers if the controller implements "additional safeguards" or "supplementary measures", in the case that the destination country does not offer equivalent or adequate level of protection. Further, **the Court stated that the transfers should be assessed "in the light of all the circumstances of that transfer", "on a case-by-case basis"**.[2]

[1] EU Transparency register 1274604847-34
[2] See 121, 145 and 134.

Data transfer out of the EU should not automatically and *per se* be considered as high-risk processing, even in the absence of an adequacy decision. In the light of the Schrems II ruling, transfers should be assessed in context. Further, there is no apparent reason to derogate from the general GDPR risk-based approach and instead, prefer the strictest standard of interpretation, implicitly requiring the assessment in abstract (or, threat-based).[3]

What concerns us is that the EDPB recommendation seems to set the standard as "one-size-fits-all", and the recommendation lacks both brevity and depth in assessment. This does not correspond to modern business models and practices.

In general, the spirit in the Recommendation is that data transfers outside EU (and naturally EEA) are undesirable. **It is important to highlight the fact that companies cannot work only in EU without connection outside EU since most companies are fully dependent on service providers outside EU.** In addition, many service providers are obliged to transmit communications or services throughout the world, and it is vital that data is also transferred outside EU to make that happen. Service provider has an obligation to provide secure and functioning services and service providers are needed to provide incident and maintenance support 24/7 in accordance with "follow the sun principle". Also, companies shall have the freedom to choose their service providers and structure their business in a way that supports their business and operations in the best possible way. Any further clarification from the EDPB on that matter would be highly appreciated, how the Recommendation takes such necessities and practicalities of modern life into account.

Should the Board not change this, any EU-based organization using everyday online applications and tools such as email, calendars, HR systems or cloud services, could risk fines up to 4% of their annual turnover. This is regardless if these tools or data are of any perceivable interest to foreign authorities, or whether there is any foreseeable harm to data subjects.

EU companies are put in an impossible and unfair situation. Without an adequacy decision, only allowed mode of transport is encryption (or pseudonymization) that leaves the recipient practically unable to read the data. Any other method puts the company at a risk of fines. Thus, whenever doing commerce or using service partners, doing research, having personnel or operations, or simply just communicating with anyone outside the EU, EU-companies are forced to put themselves at a significant risk. This practically puts up walls around the EU.

Moreover, we find it ironic that EEG test seems to pass a very high bar for surveillance laws, such that even the European countries themselves do not respect the requirements, as exemplified by the rulings of the CJEU of 6 October, 2020 finding that surveillance law in France, Belgium and UK did not meet the standards either. Hungary[4], Romania, Bulgaria[5]

[3] 42 of the "Recommendations on Supplementary Measures": "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".
[4] https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-160020%22]}
[5] https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-81323%22]}.
Hungary https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-160020%22]}
Romania https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58586%22]},
https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-80352%22]} ,
https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-104864%22]}
Bulgaria https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-81323%22]}

have also been found wanting in this respect by the European Court of Human Rights (ECtHR).

RECOMMENDATION EEG

The EEG are grounded on European case law on surveillance by the CJEU and the ECtHR. While understanding the drivers for the Recommendations, we note that **the EDPB has erred on the side of strictest possible requirements.** This raises two serious constitutional considerations.

The Recommendations are meant to cover the interpretational white-space in the EU law after the Schrems II ruling, which the EDPB fills partly based on the ECtHR jurisprudence. This leaves question whether the GDPR and EU jurisprudence should rely so heavily on case law from an institution which it is not a party or subject to. As a matter of principle, if the case in Schrems II is to be made about not subjecting EU law under foreign regime, it raises the question whether comparison should be made to ECtHR in similar manner.

The EDPB recommendation and reference to the ECtHR seems to also narrow the Commission mandate to make adequacy decisions. This is clearly not directly based on EU law and again, subjects EU institutions under regime that it is not legally bound to. We find this dilemma concerning and suggest that the constitutional questions raised by this are clarified.

While seeking legal guiding principles, the Recommendations seem to cover the principles established in the ECtHR jurisprudence only partly. If the EDPB seeks its guidance from these rulings, for completeness attention should be paid to the full picture of the principles.[6]

National margin of appreciation: as a tool described by the ECtHR this concept defines relations between the domestic authorities and the Court:

> *"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.*
>
> *Therefore, 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]

The ECtHR has in recent rulings supported this principle further:

- **Centrum för Rättvisa[8]:***"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*"
- **Big Brother Watch[9]:** "*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*". Further, "*the decision to operate a*

[6] See further Prof. Theodore Christakis: https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/
[7] Source / para
[8] June 19, 2018, para. 112
[9] 13 September, 2018, para. 386 and 387.

bulk interception regime [is] one which falls within the wide margin of appreciation afforded to the Contracting State"

While citing and referring to other parts of the same case law, the Board does not refer to this principle at all. **Understanding that the ECtHR sets safeguards *as a counterpart to this margin of appreciation*, the Board has for some reason made an apparent decision to exclude half of the equation.** We strongly urge the Board to review its position and include national margin of appreciation, to complete the concept as per ECtHR jurisprudence.

In accordance with the law: the ECtHR extends the concept of law beyond statutory texts, as it "[h]as 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."[10] Similarly, the GDPR 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 (…)."[11] Recommendations should therefore clarify that non-statutory remedies and modifications can and should be taken into consideration in case the importer´s country is seeking to address possible defects.

SUPPLEMENTARY MEASURES

Encryption is often not a suitable solution because it blocks the usability of the data and prevents necessary data processing activities by the recipient. Following 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.[12] The branch of a European company outside EU might not even be able to consult the online calendar of its European members to set up a meeting. All this could lead to huge disruption for everyday operations with low or no risk. It is not enough that the data is only decryptable in case of legal privilege or professional secrecy.

The EDPB should clarify how a combination of safeguards (technical, contractual, and organisational) can be effective**.** In some cases, technical safeguards can be the most effective additional safeguard, for example to avoid covert surveillance under authorities such as the U.S. Executive Order 12333. In other cases, organisational safeguards can be effective, such as to challenge orders. And contractual safeguards can buttress these measures by imposing liability on data importers to comply.

Further, we request the EDPB to clarify relation to finding effective supplementary measures or whether GDPR Article 49 (1) (a) or (b) could be used, as exemplified in the two use cases below:

- *Case 1*: considering the footnote 22 in the Recommendations which states that remote access by an entity from third country to data located in the EEA is also considered a transfer it would be appreciated to get a further clarification in regard to how third level support ((meaning escalation to rare, impactful incident requiring deep

[10] See for instance the case of Kruslin v. France, Judgment of April 24, 1990, §29 https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57626%22]}
[11] Recital 41
[12] Requiring the strongest encryption at all times for transferred data in 3rd countries seems ironic when at the same time within the EU Member States are entertaining the idea of backdoors to encrypted communications, as suggested by the German presidency.

technical expertise) should be addressed in such cases? The question relates to situations where a supplier's support is needed in the technical environment to solve an incident, where first (simple, routine help desk response)- and second-line support (specialist support) has not been able to solve the matter. These cases can be done in a very controlled manner without any access to personal data and if data needs to be accessed, it is done in a strictly monitored way, etc.

- *Case 2*: A service provider is acting as a processor in B2B relationship and an incident has occurred to the platform of that service provider. The supplier providing third level support may process the incident ticket in the third country (usually US). The data processed by the supplier are the data in the incident support ticket sent by the service provider to the supplier who provides a platform.

These cases are everyday examples of transfer situations in a globally connected world, and we would therefore appreciate if EDPB could clarify whether such use cases could be considered as scenarios for which effective supplementary measures could be found? Further question to be clarified is of GDPR Article 49 (1) (b) could be used for such third level support cases? The aim is to understand whether controller could use GDPR Article 49 (1) (b) for the third level support cases as such cases are by nature impossible to predict and control in advance. If Article 49 (1) (b) is not applicable in such context, could that be considered an acceptable approach for the EDPB that for such use cases consent would be acquired based on Article 49 (1) (a) instead (following all applicable conditions to acquisition of valid consent based on GDPR)?

SUGGESTED TOOLS – GOING FORWARD

We were hopeful that the Board would offer practical, tool-box like guidance, relying on risk-based approach and proportionality principle. Unfortunately, there is very little that is practicable or achievable in the requirements the Recommendations set forth. What would be helpful is a risk matrix, based on several factors which may be meaningful but not all equally decisive, especially without context.

We strongly encourage the EDPB and other institutions to work together on a database of risk assessments and adequacy levels of countries. Otherwise this delegation of adequacy assessments would put an insurmountable administrative, resource and cost burden on the companies. Cost of compliance would be prohibitive to SME sector, and privatize assessments that by law a duty for the Commission.[13]

We suggest replacing the Use Cases in Annex 2 with a toolbox of safeguards from which exporters can choose depending on the nature of the transfer. The proposed one-sized-fits-all approach to safeguards is not workable, and it is not necessary. Instead, the Recommendations should identify a list of potential safeguards, but be clear that data exporters should be free to choose whatever safeguards they deem most appropriate based on the context of the transfer.

[13] See study by ETLA's (a Finnish independent economic research institute) empirical analysis suggests that the costs of the GDPR during the first year of its implementation were substantial, at least for some European companies. The profit margins of the data-intensive firms increased, on average, by approximately 1.7 to 3.4 percentage points less than the profit margins of their US counterparts. The European data-intensive SMEs were the most disadvantaged group regarding their post-GDPR profit developments, while the large European data-intensive companies' short-term post-GDPR profit margins dropped relatively less. ETLA-Working-Papers-77.pdf

Further, the suggestion that data must always be encrypted at rest, with all encryption keys held solely in the EU (or other adequate jurisdiction), is practically impossible. Any use of data, such as sending emails or texts, processing customer payments, or engaging in business collaborations, requires data be available in a decrypted format. By applying these extreme safeguards to transfers regardless of risk, the Draft Recommendations will disrupt many transfers that are low or no-risk, and in many cases make transfers impossible altogether, including in cases where the transfer of data would be tremendously beneficial to the data subject or society more broadly.

Lastly, building walls around Europe will eventually put at risk maintaining and developing our cybersecurity. Covid-19 alone has shown how at critical times also cyber attacks increase, which we have witnessed happening in the healthcare sector. The pandemic has underlined the importance of data transfer and getting use of the best resources around the globe.[14] We cannot isolate ourselves and put our security in risk if we are not able to reach out for the best expertise, which may not at that time reside within EU borders.

[14] Etla study: cyber crime is increasing and Finland is vulnerable due to lack of experts. This study shows that we need the best experts to solve issues, and they may not reside in an EU country (in Finnish only: https://www.etla.fi/ajankohtaista/kyberrikollisuus-yleistyy-ja-suomi-kompuroi-tietoturvassa-osaamispula-jarruttaa-kehitysta/)