noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna, Austria
ZVR: 1354838270

noyb's Comments on EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[1]

noyb welcomes the initiative of the EDPB to adopt recommendations on additional measures to supplement the transfer tools and support general direction that is taken in these guidelines. We also welcome the opportunity provided by the public consultation on the Recommendation.

1. Context of the "supplementary measures" in C-311/18 paragraphs 128 to 134

While we are unable to disclose the submissions made before the CJEU, as they are deemed confidential by the CJEU and there is no transcript of the hearing, we would like to highlight that the Judges were especially interested in the problem of surveillance in transit and we understand that the "supplementary measures" to mainly concern these issues. This is indeed a problem for any transit within the Union and even to a fully adequate third country, as many other jurisdictions may be involved on the way (e.g. a transfer from the EEA to New Zealand will necessarily transit countless other countries). Such situations may be overcome by factual and technical solutions that factually "block" the access of third actors.

We have therefore always highlight that in certain cases technical measures may be able to overcome surveillance. These are indeed required under Article 32 GDPR as a bare minimum, in particular when data is transmitted on the internet – an inherently open and unsecure system. Without such approaches, international data transfers would in many situations become illegal, as third countries that do not adhere to minimum standards of rule of law, democracy, or human rights, would be able to undermine transfers between even the most well-intentioned third countries and the EEA. We have therefore always supported the idea of properly designed "supplementary measures", as have many other parties to the procedure before the CJEU.

This logic can clearly be expanded to other situations where data is processed beyond a mere transfer and which are maybe best described as "zero access" approaches:

If a data importer or an authority simply does not have factual access to personal data, then the problem of third party access after transit equally disappears. The only legal basis for this approach in the context of data transfers is however only found in the non-binding recital 108 and in the CJEU's obiter dicta in paragraphs 128 and 134 of C-311/18. In many situations, it may also be derived from the general security requirements of Article 32 GDPR.

Especially in relation to the United States, this factual "blockade" may overlap with the understanding that US law cannot compel a US entity to provide data that is not in "*possession, custody or control*" of that entity, which we understand is the test currently relevant for surveillance laws like 50 USC § 1881a (FISA 702). At the same time, we would like to stress that such "blockades" themselves may regularly violate foreign laws, which may see this as willful acts to undermine the local laws.

[1] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_fr.

2. Equivalent level of protection for data transferred outside of the EU

It may be useful to recall at the outset that for 25 years, the default position under EU law (first Directive 95/46 and now the GDPR) has been that personal data cannot be transferred to third countries. The European Legislator has *de facto* established an export ban for personal data – with various exceptions to that default rule. Obviously this position may be criticized and is largely ignored in relation to certain third countries, but is nevertheless the current state of the law. Its rationale is not one of protectionism, but one of necessary protection of the Unions' Fundamental Right to Data Protection, which would be instantly undermined when data leaves the EU/EEA to jurisdictions without proper protections.

Consequently, Article 44 of the GDPR clarifies that all provisions of Chapter V of the GDPR shall be interpreted in order to ensure that the level of protection guaranteed by the GDPR is not undermined once the data is transferred in a third country. As confirmed by the CJEU in *Schrems II* and the EDPB,[2] an essentially equivalent level of protection must be guaranteed in the destination country, irrespective of the provision of that chapter on the basis of which a transfer of personal data to a third country is carried out.[3]

On this basis, all transfer instruments (*e.g.* BCRs, SCCs, adequacy decisions) should lead to an essentially equivalent level of protection when compared to the GDPR. We want to highlight that there is no hierarchy between these forms of transfer instruments and all require some form of flexibility – be it in the negotiations with a third country, or in what contractual measures (like SCCs and BCRs) can reasonably achieve. In reality, adequacy decisions are even more political and often conflated with trade negotiations than one-sided instruments like SCCs or BCRs. Consequently, there is no logical reason to assume that one transfer instrument may adhere to lower standard than another. None of them may "undermine" the standards of the GDPR, and all of them must provide "essentially equivalent" protection.

Consequently, as confirmed by the EDPB, the same principles also apply for BCRs.[4] All principles of the GDPR should therefore be included in the BCRs, and should not be limited to the list of principles mentioned in Article 47(2) GDPR.[5] We therefore encourage the EDPB to review the relevant BCR working documents in this regard.[6] The same should apply regarding other transfer tools, such as certification mechanisms or code of conduct[7], or ad hoc clauses.

We urge the EDPB to ensure that the rights and principles applicable under all transfer instruments are aligned on the rights and principles contained in the GDPR and to review all relevant transfer instruments equally.

[2] See § 4 of the Recommendations.
[3] *Schrems II,* § 92.
[4] See § 58 and ff. of the Recommendations.
[5] Article 47(2) states that the BCRs shall specify ***at least*** the rights and principles listed in this provision. The list is therefore not exhaustive.
[6] In particular the Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01 and the Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01.
[7] Article 46(2)(e) and (f) GDPR.

3. The suspension or termination of the transfer in the absence of essentially equivalent level of protection is not an option but the default obligation

As mentioned by the EDPB,[8] and in line with the CJEU judgement in *Schrems II*:

> "*Where the controller or a processor established in the European Union is not able to take adequate additional measures to guarantee such protection, the controller or processor or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned*".[9]

Consequently, in instances where an adequate level of protection cannot be guaranteed, the prohibition on starting a transfer, and the duty to suspend and terminate it, are not just options, but rather the clear obligation under the GDPR.

We were surprised to read that the EDPB refers to a case where the controller or processor would nevertheless *"decide to continue with the transfer notwithstanding the fact that the importer is unable to comply with the commitments taken in the Article 46 GDPR transfer tool".*[10] The EDPB suggests that, in such a case, the controller or processor *"should notify the competent supervisory authority in accordance with the specific provisions inserted in the relevant Article 46 GDPR transfer tool".* We are not sure what the legal basis of such self-reporting would be under the GDPR and if it is in any way practical, realistic or useful.

We understand that the EDPB refers, for example, to situations where the SCCs and the BCRs are still in place, and the laws of a third country conflict with them and no further action was taken.[11] We are deeply worried that exporters and importers could interpret the draft guidelines in such a way that the exporter could choose to either suspend/terminate the transfer or to notify the competent SA. This approach seems absolutely unsustainable for the following reasons:

- The law and the transfer instruments mentioned by the EDPB require suspending and/or terminating the transfers. They do not explicitly present the notification of the supervisory authority ("SA") as an alternative to the suspension or the termination of the processing.[12] As such, it is unclear what the purpose and consequences of such a notification would be:
  - Can the exporter continue the unlawful transfer as long as the exporter makes the violation of the GDPR transparent to the relevant SAs?
  - Should it be understood as implying that the exporter would not be liable if it decided to notify the SA of such a situation, which is against any reasonable interpretation of the GDPR but also of the judgment of the CJEU in *Schrems II*?
  - Or does the EDPB expect that exporters report their violation of Chapter V themselves and thereby self-incriminate to then be fined with € 20 Mio or 4%?
- We have doubts about the level of actual compliance with such a requirement to notify the SA, especially given the duty of the SAs to act and the potential fines that they can impose. Current compliance could be easily assessed in light of the number of data exporters that already communicated such notifications to the SAs. We are not aware of such notifications being common.[13] We therefore wonder if the SAs can replace their duty to investigate entities with a mere duty to self-report non-compliance.

[8] See Recital (6) of the Recommendations.
[9] See *Schrems II*, § 135.
[10] See § 53 of the Recommendations.
[11] See Footnote 48 of the Recommendations.
[12] Except Clause 4 (g) of the Clauses annexed to Decision 2010/87/EU.
[13] Did the importers notify the exporters that they were on the Snowden slides? Did the exporters notified the SAs that they would continue the transfer despite of the massive interception of data by the US surveillance agencies?

- In this context, we take note that the new SCCs proposed by the European Commission for transfers have a different wording than the current SCCs. Under the proposed SCCs, it is now clear that the exporter can continue the transfer if, based on its assessment, the additional measures will allow the data importer to fulfill its obligations under the Clauses. As a consequence, the data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured.[14] In both cases (suspension of continuation of the transfer), the exporter has to inform the SA of its decision, which then allows further actions by the SA.

In any event, none of the transfer instruments mentioned by the EDPB[15] or the text of the GDPR support the view that notifications or self-reporting is a viable option. In our view, such an option violates the provisions of the GDPR and the judgement of the CJEU. Consequently, suspension or termination of the transfer is a clear obligation and not an alternative to notifying the SA and continuing an unlawful transfer.

In this context, we note that, like other instruments for transfers,[16] BCRs are approved by SAs after an opinion of the EDPB.[17] In such cases, organisations applying for BCRs have to describe the transfers but also mention the countries where the data will be imported.[18] Therefore, the EDPB and the SAs are already informed about all the circumstances of the transfers and are in a position to conduct an assessment of the transfers when they receive a BCR application. We note in this regard the Opinion 25/2020 on the Tetra pack BCR, where the EDPB refers to the responsibility of the data exporter to assess the level of protection in the third country concerned.[19]

For these reasons, we suggest that the EDPB makes clear that when the controller considers that additional measures cannot guarantee that the data transferred will be granted a protection essentially equivalent to the one provided by the GDPR, they must suspend the transfer, without prejudice to their right to consult the SA regarding any additional safeguards that they could put in place to resume the transfer. Similarly, the EDPB should explicitly state that when the SA considers that the level of protection cannot be guaranteed once the data are transferred, it must suspend or end the transfer where the controller or a processor has not itself suspended or put an end to the transfer.[20]

4. Duty of the SAs to act on data exporter and data importers

In connection to a notification or self-reporting approach that the EDPB guidelines suggest, we would like to again recall that the CJEU highlighted that the SAs have not only the power to suspend or end the transfer, as mentioned by the EDPB,[21] but that each European SA also has the explicit duty to exercise these powers.

[14] Clause 2 of the SCCs available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Data-protection-standard-contractual-clauses-for-transferring-personal-data-to-non-EU-countries-implementing-act-
[15] See footnote 48 of the Recommendations.
[16] Ah contractual clauses, certification, codes of conducts, …
[17] See Article 64 (1) (f) GDPR.
[18] See § 47 GDPR.
[19] See §10 of the Opinion 25/2020.
[20] See Recital 112 of *Schrems II*: *"Although the supervisory authority must determine which action is appropriate and necessary and take into consideration all the circumstances of the transfer of personal data in question in that determination, the supervisory authority is nevertheless required to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence".* See also recital 146.
[21] See §68 of the Recommendations.

Under Articles 3(2), 44 to 48, 58 and 83(5)(c) GDPR, this does not only concern EU data exporters, instead, it also means that in many cases, SAs can equally take action against third country data importers. This is especially relevant, as many large third country processors currently shift the responsibility to small or medium controllers within the EU that cannot possibly oversee or even police these large processors or understand the complex issues of third country surveillance laws. It is a matter of efficiency and fairness to take action against the entities that have the actual economic power over international data flows and factual power over third country access to personal data – which are primarily the third country data importers.

We would further highlight that many players in the industry have voiced the view that the SAs will likely not comply with this duty to enforce the law themselves and therefore will take a "wait and see" approach. This idea is also very dominant in the current talks between the EU and the United States. The relevant exporters and importers seem to view the lack of any clear reaction by the EDPB and the national SAs as equal reluctance by the SAs to comply with the CJEU judgement themselves, insofar as it concerns the SA's duties. This fundamentally undermines the EU position, as it is currently not taken seriously.

In our respectful submission, the industry and the SAs have maneuvered themselves into a "first mover" problem over the past months, where either party points at the other party to take the first step. The EDPB and many SAs point (legitimately) at the responsibility of the data exporters and importers to clarify the legal situation of thousands of different types of transfers that SAs can impossibly give guidance on. The industry in turn ask for "guidance" by the EDPB and the SAs. At least the second argument should be overcome by the adoption of these draft guidelines.

While the primary responsibility clearly lies with the exporters and importers, we believe that the EDPB and the SAs cannot shift the responsibility of compliance entirely on them. In line with the judgement of the CJEU, the SAs have a special responsibility to suspend or end transfers when needed, and should not hide behind general guidelines and the hope that there will be self-reporting by the industry.

Furthermore, since the CJEU judgement in 2020, we are not aware of any suspension or termination of transfers that have taken place. Enforcement of the judgement in *Schrems II* currently seems as low as after *Schrems I.* We therefore count on the SAs to join their efforts within the EDPB to identify the problematic transfers, investigate the cases, and take the appropriate measures, without waiting for data subjects and NGOs to bring them to their attention.

We would therefore very much urge the SAs to quickly issue national and/or European action plans for enforcement: Such action plans may contain first steps like questionnaires which are sent based on Article 58(1) GDPR to relevant controllers and processors or formal letters to confirm compliance. Such information gathering could be done in very effective ways by using online forms that require filling out the relevant information to ensure that the resources of SAs are not overstretched. Such a simple multilingual reporting platform could easily be established on a European level. The publication of the final guidelines seems to be a logical point in time to start such coordinated enforcement actions.

We suggest that the EDPB further highlight this clear duty in its recommendations by amending the following wording accordingly:

> *"The competent supervisory authority has the ~~power~~ duty to suspend or end transfers of personal data to the third country if the protection of the data transferred that EU law requires, in particular Articles 45 and 46 GDPR and the Charter of Fundamental Rights, is not ensured".*[22]

[22] See § 68 of the Recommendations.

This may also give some national SAs the European backing to take the legally required action, which may otherwise be criticized by political actors and or even some courts that oversee the SA's actions under national law.[23]

Finally, we would like to highlight that Article 58(1) GDPR seems to give SAs some flexibility to square the requirements of the GDPR and the CJEU judgment and possible factual limits in implementing them. The GDPR would in our view allow reasonable implementation periods for bans on data transfers or issue temporary measures in cases where major changes to running systems are required.

For these reasons, we urge the EDPB and the SA to fulfill their responsibilities when it comes to suspending data flows, instead of relying on self-reporting. It is important that the EDPB does not only highlight the duties of the controller and processors, but also the clear duties of the SAs that it represents. We further urge the EDPB and the SAs to launch a coordinated action plan within the EDPB to identify transfers that are not compliant with the *Schrems II* judgement, to investigate these cases, and adopt the appropriate measures.
The SAs should make sure that additional measures are actually adopted and put in place by the data exporters, and conduct investigations and audits (by virtue of their powers under the GDPR and the various transfer instruments) to assess the efficacy of these measures.
The exporters have now, with the draft SCCs on transfers and the present Recommendations, all the information required to implement additional safeguards where needed. Therefore, the SAs should without delay proactively investigate whether additional measures and safeguards were put in place and should start investigations on the various practices of the sector, which may lead to enforcement actions.

5. The emphasis on the "accountability" principle

The EDPB Recommendation mentions the principle of accountability in several instances throughout the document.[24] Accountability is a general principle[25] which is composed of two key elements: First, the accountability principle makes it clear that the organizations are responsible for complying with the GDPR. Second, they must be able to demonstrate compliance.[26]

However, the assessment of the compliance of a transfer with the GDPR (and its Chapter V) is not primarily a matter of accountability, but of compliance with the law. In other words: in addition to comply with the requirements of Chapter V, controllers need to demonstrate this compliance in order to meet their accountability obligations.[27] At the same time, producing paperwork while not complying with the obligations of the GDPR leads nowhere.

[23] See Facebook's litigation against the DPC in Facebook v. DPC, Irish High Court Record No. 2020/617JR.
[24] See in particular title 1 of the Roadmap: "Accountability in data transfers" and title 2: "Applying the principle of accountability to data transfers in practice".
[25] Article 5(2) GDPR. As examples of the accountability principle, controllers should implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing us performed in accordance with the GDPR (Article 24 GDPR), maintain documentation of all processing operations (Article 30 GDPR), implement appropriate security measures (Article 32 GDPR), or designate a DPO (Article 35 GDPR). All these measures will help the controllers to achieve compliance and are part of an active process to meet the requirements of the GDPR.
[26] See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/#whataccountability.
[27] According to the EDPS: *"The General Data Protection Regulation (GDPR) integrates accountability as a principle which requires that organisations put in place appropriate technical and organisational measures and be able to demonstrate what they did and its effectiveness when requested. Organisations, and not Data Protection Authorities, must demonstrate*

Considering the above, we are concerned that the multiple references to accountability in the Recommendations may be used by some controllers to solely follow the various steps of the "Roadmap" suggested by the EDPB, leading them to believe that proper documentation would be sufficient to meet one's obligations under the GDPR.

This is supported by our past experience: *noyb* has for example asked 33 various controllers about their data transfers, who regularly neither explained the legal basis for their data transfers after the CJEU judgment, nor factually complied.[28] In countless webinars, discussions and bilateral talks, we regularly witness that exporters draft papers, documents and assessments, while ignoring the notion that their own data processing is in itself non-compliant. We are therefore concerned that this wrong understanding of "accountability" may be further promoted by the EDPB guidelines.

We support the EDPB when it already acknowledges the documentation component of accountability when it refers to the *"need to document appropriately this assessment and the supplementary measures"* selected and implemented and to *"make such documentation available to the competent supervisory authority upon request"*.[29] Even though we recognize and understand the need to document the way transfers are organized, to implement organisational and technical measures, and to make sure to regularly review and update the measures implemented[30], this only forms the second element of accountability, *i.e.* demonstrating (previously achieved) compliance. To avoid any uncertainty, the EDPB should make clear that documentation is not a way to escape to liability, but a way to demonstrate it.

Another source of concern is that accountability is sometimes mixed up, or associated with the so-called "risk-based approach".[31] As developed in section 7 below, we strongly reject such an approach for transfers. In this context, the Article 29 Working Party already made clear that *"controllers should always be accountable for compliance with data protection obligations including demonstrating compliance regarding any data processing whatever the nature, scope, context, purposes of the processing and the risks for data subjects are."*[32]

On the basis of the above, and in order to avoid that exporters may see the Recommendation as a mere documentation exercise: We strongly suggest that the EDPB clarifies that the "Roadmap" is only one way to demonstrate previously achieved compliance,[33] and that exporters always remain responsible towards the data subjects and the SAs regarding their respect of the remaining provisions of the GDPR applicable to transfers. Accordingly, we also suggest to amend title 1 with the following wording: "Compliance in data transfers" and to replace title 2 as follows: "Roadmap: how to make your transfers compliant with the GDPR in practice".

that they are compliant with the law. Such measures include: adequate documentation on what personal data are processed, how, to what purpose, how long; documented processes and procedures aiming at tackling data protection issues at an early state when building information systems or responding to a data breach; the presence of a Data Protection Officer that be integrated in the organisation planning and operations etc."

[28] See https://noyb.eu/en/opening-pandoras-box-companies-cant-say-how-they-comply-cjeu-ruling.

[29] See §7 of the Recommendations.

[30] Step 2.6 of the Recommendation, "Re-evaluate at appropriate intervals" is definitively an example of the principle of accountability.

[31] See for example Article 29 Working Party, Statement of the WP29 on the role of a risk-based approach in data protection legal frameworks, adopted on 30 May 2014, 14/EN WP 218.

[32] Article 29 Working Party, Statement of the WP29 on the role of a risk-based approach in data protection legal frameworks, adopted on 30 May 2014, 14/EN WP 218.

[33] And to some extent, being able to show that an organization actively considered the risks and put in place measures and safeguards can help it to provide mitigation against any corrective measure in the course of potential enforcement action.

6. Law *and* practices must comply with EU law

We note that in its recommendations, the EDPB suggests to assess the law *or* practice of the third country in order to determine whether they may impinge on the effectiveness of the appropriate safeguards.[34] We consider that the wording used in this context ("*or*" or "*and*") is particularly important and urgently needs revision to be in line with the clear decision of the CJEU.

As we already submitted in our comments regarding the SCCs on transfers, we want to highlight that the relationship between law and practice is often confused with a "law *or* practice" approach, where either the law or the practice could be considered compliant with EU law.

This approach was pleaded in *Schrems II*[35] for example by the US Government or Facebook and excessively spread by law firms and scholars with close industry ties. However, this approach was explicitly not adopted by the CJEU and there is clearly the need for a "law *and* practice" approach.

Practice must follow the laws of a country.[36] This follows a painfully obvious logic, as it is neither helpful to only have a practice (as this does not constitute legally binding protections for the data subject) nor helpful to have "dead law" (that is not complied with in practice).

Such a holistic approach taking into account both law and practice should be followed to conclude how adequate a non-EU country is, and has also a long-standing history in ECtHR case law.[37] The EDPB should ensure that controllers and processors may not use the guidelines to depart from the clear case-law by the CJEU and ECtHR.

In our view, firstly, the laws and practices of a third country should be taken into account as a whole for the assessment of the level of protection granted to the data once transferred, which should be essentially equivalent.

We urge the EDPB to make it even clearer that EU law requires third country laws that are also followed in practice ("law and practice"). Mere practice cannot overcome laws that violate EU Fundamental Rights, just as factual violations of EU Fundamental Rights cannot be camouflaged with a law that only exists on paper.

We also suggest that the EDPB adapts the drafting of its Recommendations accordingly and ensures consistency in the wording used.[38]

7. There is no "risk-based approach" in Chapter V GDPR

We are also concerned to see an increasing number of papers and statements suggesting that transfers should be assessed on a case-by-case basis, following the so-called "risk-based approach". This is even used by large companies that e.g. clearly fall under mass surveillance laws to argue that the "risk" of being subject to government surveillance or to suffer secondary consequences from it would be low. This idea is fundamentally flawed on multiple levels:

[34] See §§30 and 41 of the Recommendations.
[35] See Opinion of the Advocate General Saugmandsgaard ØE in *Schrems II,* §271: Practices or instruments that do not have an accessible and foreseeable legal basis may be taken into account in the global assessment of the level of protection guaranteed in the third country in question in such a way as to support guarantees which themselves have a legal basis which is accessible and foreseeable.
[36] See Opinion of the Advocate General Saugmandsgaard ØE in *Schrems II, ibid.*
[37] See, for example, *Malone v.United Kingdom*, 8691/79, 2 August 1984; see also *Centrüm för Rättvisa* , 19 June 2018.
[38] See §§ 29, 30, 41 and 42 of the Recommendations.

First, the risk-based approach is not a general principle applicable to all provisions of the GDPR and is especially not included in Chapter V GDPR. Despite massive lobbying, the "risk based approach" was implemented only in certain elements of the GDPR. The EU legislators adapted and scaled certain obligations and requirement of the GDPR on the basis of the risk for the individuals. This is the case in the following examples:

- assessment of the security measures of a specific processing (Article 32(1) GDPR)
- assessment of the risks resulting from a data breach (Articles 33(1) and 34(1) GDPR)
- data protection impact assessment and assessment of potential high risks to the rights and freedoms of individuals (Articles 35 and 36 GDPR).

Nothing in Article 46(1) or 46(1)(c) indicates that a transfer my take place when it presents a low risk (risk of interception by a public authority for example), or that it would require a so-called "transfer impact assessment", even if some proponents of this approach are surely happy to sell such assessment to controllers and processors right now.

Second, the approach equally fails in practice, as can be seen from the following examples:

- Government surveillance is at the core aimed to take action against individual persons or groups. The mere fact that there is a "low risk" of a secondary violation of fundamental or other rights (such as imprisonment, financial loss or denial of entry) does not make the violation of the fundamental right under Article 7, 8 and 47 CFR less relevant.
- In practice, the fact that such surveillance is secret makes it virtually impossible to know which data subject was actually harmed.
- There is also no explanation as to how a controller or processor can reasonably take into account that certain vulnerable groups (e.g. religious minorities, holders of certain political views, journalists, public servants in relevant positions, political figures or activist) are usually under a much higher "risk" to fall under government surveillance than an average data subject. Would these groups have to be exempt from a transfer in a "risk based approach"?
- A data exporter might decide to transfer some data which are, in his view, at low-risk for the individual (*e.g.* a few cookies per user, but overall tracking data of billions of users):
  - Who is going to determine the threshold for the acceptable risk and what will be this threshold? Leaving this in the hands of data exporter does not provide the appropriate guarantees for the individuals.
  - Millions of data exporter transferring thousands of cookies will still amount to a high risk in general, as even such meta data is commonly used for bulk surveillance. Each isolated transfer can therefore not be assessed separately.

The Article 29 Working Party (WP29) has already expressed concerns that the risk approach is being *"increasingly and wrongly presented as an alternative to well established data protection rights and principles, rather than as a scalable and proportionate approach to compliance*"[39]. We agree with the WP29's statement: *"even with the adoption of a risk-based approach there is no question of the rights of individuals being weakened in respect of their personal data. Those rights must be just as strong even if the processing in question is relatively 'low risk' "*.[40]

Contrary to some reporting, we would like to add that we were recently informed by the European Commission, that debated elements[41] in the newly proposed SCCs should not be misunderstood to suggest the endorsement of a "risk based approach".

[39] Article 29 Working Party, Statement of the WP29 on the role of a risk-based approach in data protection legal frameworks, adopted on 30 May 2014, 14/EN WP 218.

[40] Article 29 Working Party, Statement of the WP29 on the role of a risk-based approach in data protection legal frameworks, adopted on 30 May 2014, 14/EN WP 218.Ibid.

[41] Recital 17, 19 and 20 of the SCCs and in the Annex, Section II, Clause 2.

In this context, we welcome the common approach that the European Institutions seem to follow, in rejecting assessment based on the likelihood of interception, which would not be in line with EU law and urge the EDPB to make this even more explicit for controllers and processors.

On the basis of the above, we suggest that the EDPB keeps its clear position and explicitly reaffirms in its Recommendations that it reasserts the statement of the WP29 that a "risk-based approach" cannot be followed in order to assess the compliance of a transfer.

8. Assessment of the protection in the third country on the basis of the European Essential Guarantees

The *Schrems II* judgment[42] confirms that compliance with the GDPR and in particular Articles 45 and 46 GDPR should be done in the light of all the circumstances of the transfer. Even when a transfer instrument mentioned under Article 46 GDPR is used, the protection of data should be essentially equivalent to the one granted in the EU.

We fully support the view of the EDPB that "essential equivalence" cannot be achieved when the data importer is prevented from complying with their obligation under the transfer instrument due to the *"third country's legislation and practices applicable to the transfer".*[43]

We welcome the EDPB European Essential Guarantees (EEG) Recommendations, which provide elements which have to be assessed to determine whether the legal framework governing access to personal data by public authorities in a third country, being national security agencies or law enforcement authorities, can be regarded as a justifiable interference (and therefore as not impinging on the commitments taken in the art 46 GDPR transfer tool) or not. [44]

We also welcome the approach of the EDPB regarding the assessment of the third-country, according to which, in case where the legislation of the third country is lacking, the exporter should not rely on subjective factors such as the likelihood of public authorities' access to data which would not be in line with EU standards.[45]

We would however like to clarify the role of practice and laws in the third countries when assessing the transfer on the basis of the Essential Guarantees as identified in the Recommendation of the EDPB, building on the following three cases:

i) The law is clear and accessible
As stated by the EDPB, *"the assessment should be based first and foremost on legislation publicly available".*[46] In such a case, it may still be that these laws applicable to the transfer do not pass the necessity and proportionality test as described in the Second Essential Guarantee (*e.g.* if they allow a massive and indiscriminate collection and access of data). The transfer is not in line with EU law and cannot take place.

ii) The law is not clear or ambiguous
When the legislation governing access to date by public bodies is ambiguous or not clear[47], it is likely that it will not meet the foreseeability and precision requirements as mentioned in the first

[42] See *e.g.* §§ 121 and 146.
[43] See §§29 and 44 of the Recommendations.
[44] See §39 of the Recommendations.
[45] See §42 of the Recommendations.
[46] See § 42 of the Recommendations.
[47] See § 39 of the Recommendations.

Essential Guarantee.[48] The transfer should therefore not be conducted. The same applies when the surveillance law is not publicly accessible.

iii) There is no law or no publicly available law on surveillance

Finally, in situations where there is no legislation on surveillance in the third country[49], the EDPB suggests to rely on relevant and "objective factors" to determine whether public access to data takes place despite the existence of a law organizing it. In such a case, we agree with the EDPB that the practice observed in the third-country should be taken into account to assess the protection of the data transferred. In our view, in such a case, the existence of surveillance without a law would automatically amount to a violation of the first Essential Guarantee, that is the existence of a clear and accessible legal basis.

As a conclusion, we suggest that the EDPB:

Explicitly states that the law of the third country should be easy to understand and interpret for the data importer and the data exporter, in order to determine whether the data transferred are subject to surveillance laws. Should this not be the case, one should draw the conclusion that the law in the third country does not meet the standard of precision and foreseeability required under EU law.

Explicitly states that when a practice of interception is not based on a law within the meaning of the case-law of the CJEU and the ECtHR, such practice does not meet the standard of a clear legal basis as required under EU law and as mentioned in the EDPB Essential Guarantees.

9. Step 4 in the Guidelines: Fact-Based Problem & Measure Assessment

It seems to us that recent developments lead to a rush by controllers and processors to just add anything to the existing SCCs and then sell any additional provision as an "additional measure" to customers, data subjects and even some SAs – with partly surprising success (see below on the approach that Microsoft took as a good example).

While randomly adding as many shiny elements as possible is a somewhat reasonable approach to decorating a Christmas tree, supplementary measures to overcome violations of Fundamental Rights in a foreign legal order, require a more careful assessment and detailed planning.

Despite the rather clear wording in paragraphs 46 of the guidelines, we would therefore recommend that the EDPB makes it even clearer that controllers and processors must clearly (A) identify the problem or issue under the suggested Step 3 and then (B) implement a fitting and relevant supplementary measure under the suggested Step 4. This must include a clear and affirmative finding that the supplementary measure under Step 4 actually remedies the inefficiency identified under Step 3.

For example: Encryption of traffic between a browser and a server is irrelevant when a foreign government has access to data that is stored on that server after the encrypted transfer. Equally,

[48] In situation where, as it is the case regarding the US legislation after *Schrems I* and *II*, a never-ending debate on the scope of the applicable surveillance law is observed, it seems that the legislation at stake does not meet the requirement of foreseeability, as developed by the ECtHR in Zakharov, §229 or Malone, §§ 65, 66.

[49] See § 42 of the Recommendations.

encryption of the mere content of an email (e.g. via PGP) is irrelevant when government entities may use the meta information of an email to conduct surveillance or filter such encrypted emails to then run a massive decryption effort on that individual email. In such a case, the relevant information (here: email meta data) may be outside of the encrypted message.

As always, increased transparency (publication or a request by SAs to provide such an assessment) would likely increase the sincerity of such an assessment and ensure that "supplementary measures" can become more than mere window-dressing.

We would recommend making it even clearer that controllers and processors must clearly identify the problem or issue, and then explain how the suggested "supplementary measure" is in fact capable of overcoming precisely that problem or issue.

The additional measure should be described in detail and communicated to the SAs and the data subject for analysis. Without such communication, we are concerned that the data exporters and data importers will keep their additional measures for themselves, leaving the data subjects and the SAs in the dark regarding the assessment performed and the measures adopted. This should clearly form part of the accountability obligation of the controllers (see Section 3 above).

10. Examples of additional measures

We welcome the efforts made by the EDPB to list several examples of technical, organizational and contractual measures to help the data exporter to implement the appropriate safeguards in order to implement the findings of the CJEU. At the same time, we would like to highlight that the EDPB may be able to add some clearer concepts (such as "zero access") that smaller controllers and processors, as well as data subjects, may easily understand.

We will not comment on each additional measure suggested by the EDP in the context of this consultation, but we would like to make the following observations on some of these measures:

Technical Measures

- **Cases 1 and 3** both address a situation where encryption is involved with a "blocking" solution. We very much welcome that the EDPB highlights these options. In order to make it easier for the reader to understand which specific solution is envisaged, we recommend referring to a term that is easily understood (like "zero access").
- **Case 2** refers to pseudonymisation as another technical measure that could be envisaged. We are concerned that this solution does not still provide the guarantee for the privacy of individuals. The GDPR does not create any exception for pseudonymised data regarding the rules of transfer. We therefore fail to see the legal basis for this recommendation by the EDPB. The mere fact that the data cannot be attributed to a specific person is not enough, as recognised by the EDPB: it should also be avoided that the data can be used to single out an individual. We are equally concerned that the level of pseudonymisation required is not clearly described in the Recommendation. Especially when thinking about the vast powers by foreign surveillance authorities, we fail to see how "keeping data separate" would be effective, given the known countless techniques to overcome pseudonymisation of personal data. For these reasons, we suggest that the EDPB refrains from using case 2 in the final guidelines.
- **Case 5:** While we can see that there could theoretically be options that would make data "pseudonymous" we are not sure if the approach described has larger practical application. We further like to highlight that cooperation by surveillance authorities across jurisdictions (e.g. the "Five Eyes") may equally undermine such an approach.

- **Case 6:** We welcome the conclusion reached by the EDPB regarding the use of a Cloud provider located in a jurisdiction where the Essential Guarantees cannot be provided (*e.g.* the US) is not compliant with EU law. We suggest that the EDPB makes clear that, in such cases, no other additional measure (contractual or organizational) can be effective.
- **Case 7:** We welcome the clarification by the EDPB that mere location of the stores information is not sufficient, when there is *de facto* access from a third country. As this has a broad application when third country entities promote their EU data centers as an alternative, despite managing them from outside of the EU, we would urge the EDPB to maybe use this more practical example for Case 7 or add another case whit this set of facts.

Contractual Measures

We note that the contractual measures are inherently more flexible but may often be less effective in practice. We would highly recommend highlighting this, as many controllers and processors will prefer to add one or two easily implementable contractual measures instead of re-engineering their systems. The EDPB should highlight that adding some "light weight" contractual measures will usually not be sufficient to achieve adequate protection. In more detail:

- On the contractual requirement to provide for additional technical measure, we suggest that this option should not be seen as an additional measure, but a logical requirement when the data exporter or importer rely on any technical measure.
- On the transparency obligations: We are concerned that,
  - the listed information suggests a "risk based approach" that the Guidelines reject,
  - the example refers to the situation where there is no law governing the public authorities' access to data. As developed above, such a situation seems likely to be against the Essential Guarantees due to the lack of legal basis in the third country and
  - there seems to be no information towards the actually concerned data subjects, which after all is the holder of the Fundamental Right to Data Protection and often the only person that has an interest to take relevant actions.
- On the examples mentioned in §§ 103, 105 and 107 of the Recommendation are welcome as far as they strengthen the obligations of the importer, but we are concerned that they do not really bring the "guarantees" expected. They are just additional contractual obligations.
  - Especially the option to terminate the contract between data exporter and data importer does not seem to remedy the rights of data subjects who's data was already transferred. Usually data exporters have good reasons to keep an existing transfer, as switching providers usually involves enormous costs and overhead.
  - As with the other information duties, the clear link to information towards the data subjects seems to be missing, as the current suggestion would allow entities to keep the results of any review confidential towards the actual holder of the Fundamental Rights.
- The examples mentioned in § 110 has some "James Bond" charm to it, but we are equally concerned that it may be misunderstood to be an option for third countries that do not have adequate laws in the first place. The "add-on" nature of such suggestions should be clarified.
- The example mentioned in §§ 112 and 114 refers to the commitment to review the legality of any order to disclose the data. We think that challenging an order that is considered as illegal is the minimum that one could expect from an organization outside the EU and processing one's data. Moreover, in such a case, Article 48 GDPR requires a MLAT or other international agreement for the order to be recognized under EU law. We refer on this point to the EDPB guidelines on derogations where the EDPB already stated that *"decisions from third country authorities, courts or tribunals are not in themselves legitimate grounds for data transfers to third countries".*
- We generally welcome the suggestions in §§ 116 to 121, while they seems to be combined with each other and the other suggestions before at a bare minimum.

Organisational measures

- We welcome the internal policies for governance suggested in § 124 of the Recommendation. However, we remind the EDPB that organizational measure will never replace compliance and should be in any event implemented on the basis of the principle of accountability.
- We also welcome the transparency obligations suggested by the EDPB in §§127 and 129. We suggest however to delete the "where required" at the end of § 127 and to make such information automatic for the data subjects, like it is for the exporter. Also, we suggest to further specify that the information to be provided in the transparency reports mentions the specific national entity within a group of companies to which the request was addressed (*e.g. "Google Inc," 'Google France"* instead of *"Google"*). This information usually lacks in the transparency reports and would allow the data subject to know exactly to which specific controller the request was addressed.
- We welcome the data minimization measures suggested in § 131. However, we think that such an obligation is already a basic obligation of the GDPR and should not be considered as an "additional measure". When a transfer is not necessary, it amounts to a violation of Article 5 (c) and 6 GDPR, since both articles are built on the principle of necessity: any processing operation (including transfers) should therefore be necessary to achieve its purpose. As a consequence, any transfer of data that is not necessary is *de facto* not compliant with Articles 5 and 6 GDPR. In this respect, we refer to the numerous documents of the EDPB/Article 29WP affirming that the processing of data should first be compliant with the general principles of the GDPR before being assessed under Chapter V GDPR.

We suggest the EDPB to take our comments here above into account when finalizing the list of additional measures suggested in its Recommendations. The EDPB should regularly conduct a review of these recommendations, based on the experience and the information communicated made by the data exporters.

11. Clear rejection of deceptive "supplementary measures" by certain data importers

In recent months, we had to witness that not only the EDPB has thought about "supplementary measures" but a whole wave of alleged additional measures that range from deceptive promises all the way to fraudulent behavior. A very illustrative example is the alleged "additional measures" by Microsoft that were even publicly welcomed by some SAs,[50] and promoted by Microsoft as even "*exceeding the EDPB's recommendations*". For illustrative purposes, we would like to highlight these alleged actions by Microsoft, as one of many examples in the industry:[51]

- "*Challenging every government request where there is a lawful basis to do so*" is nothing but a commitment to not provide data without a valid legal basis. This is not a supplementary measure, but a direct consequence of compliance with Article 6(1) GDPR: Where there is no legal basis, the controller or processor may not provide personal data to any authority (including non-EU authorities). It would be appalling to find out that a company like Microsoft would have provided personal data of customers when there was no legal duty to do so, even if other US providers have voluntarily provided personal data under EO 12.333 without a legal requirement to do so.

[50] See, for example, the Baden-Württemberg supervisory authority: https://www.baden-wuerttemberg.datenschutz.de/dsgvowirkt/.
[51] Microsoft on the Issue - New steps to defend your data: https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/

- "*We will provide monetary compensation … if we disclose their data … in violation of the EU's General Data Protection Regulation*" is not a supplementary measure, but the very core of Article 82 GDPR. Contrary to the existing obligation under the GDPR, Microsoft even tried to attach conditions to this, such as denying data subjects to form a class or partly shifting the burden of proof to the data subject. This "supplementary measure" therefore falls short of the bare minimum rules of the GDPR.
- "*We use strong encryption*" is not a supplementary measure, but a requirement under Article 32 GDPR, even if many entities now try to sell this bare minimum a second time under Chapter V of the GDPR.
- "*We do not provide any government with direct, unfettered access to customer data*" is at best deceptive (by using the word "unfettered"), when Microsoft clearly complies with FISA702 in the United States, which the CJEU held to violate Article 8 CFR and even reports high numbers of government access under this provision.[52]
- "*We have … published information about government demands for customer data*." The mere fact that entities are open about the violation of fundamental rights of data subjects does not constitute a "supplementary measure" but instead makes immanent action by data exporters and SAs necessary.

As such deceptive "supplementary measures" are getting more and more common, we would urge the EDPB to highlight that general compliance with the GDPR are by no means "additional measures" but rather a bare minimum requirement and that deceptive "supplementary measures" will be a priority of SA's enforcement actions. This seems especially relevant, as large processors are clearly misleading controllers in the SME sector that are themselves often unable to understand the complex technical and legal situation.

We urge the EDPB and the national SAs to call out deceptive "supplementary measures" and make EU data exporters or third country data imports that spread deceptive "supplementary measures" a priority in any enforcement plan.

12. Country Specific Guidance

Finally, we would like to highlight that most SMEs and data subjects will not profit from rather abstract and generic guidelines, as they would have to assess the law of e.g. the United States. We would very much welcome if the EDPB, national SAs or the European Commission could either themselves provide neutral information on the laws of the most relevant third countries, or at least encourage neutral third parties to make such assessments publicly available. Obviously, the United States and the UK would currently be on top of such a list.

While large corporations may be able to engage international law firms to conduct the relevant review of national laws, data subjects and SMEs will usually be unable to engage in the complex exercises that the EDPB suggests, which fundamentally disadvantages them.

We would recommend thinking about ways to provide neutral and accurate information about the laws of the most relevant third countries for the use by SMEs and data subjects.

[52] Microsoft Transparency Report: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report