Comments on EDPB public consultation R01/2020: 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data'

Joint comments by SRIW, SCOPE Europe, and the EU Cloud Code of Conduct

December 2020

About the authors

Self-Regulation Information Economy (German: Selbstregulierung Informationswirtschaft e.V. – short: **SRIW**) is a Berlin-based non-profit-organization that fosters and promotes data and consumer protection through self-regulation and co-regulation and acts as a monitoring body for data protection codes of conduct. Its Brussels-based subsidiary SCOPE Europe sprl / bvba (**SCOPE Europe**) complements the portfolio of **SRIW** on a European level and is in the process of acquiring accreditation as a monitoring body under the European General Data Protection Regulation (GDPR), pursuant to Article 41 GDPR. **SCOPE Europe** acts as the monitoring body for the EU Data Protection Code of Conduct for Cloud Service Providers (short: **EU Cloud Code of Conduct**).

The **EU Cloud Code of Conduct** is a widely adopted Code of Conduct pursuant to Article 40 GDPR, defining clear requirements for Cloud Service Providers. While the official approval of the current Code by the European Data Protection Board (EDPB) is pending, the **EU Cloud Code of Conduct** General Assembly already started the creation of a new module to the Code for transferring personal data outside of the EU in line with Article 46 GDPR. The EDPB's "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the Recommendations)" are a key piece of guidance to develop this effective but accessible safeguard for third country transfers.

Therefore, **SRIW**, **SCOPE Europe**, and the **EU Cloud Code of Conduct** (we) appreciate the opportunity to share our perspectives in the context of the public consultation and, based on our experience, make the following comments.

1 Introductory remarks

We would like to thank the European Data Protection Board for consistently granting stakeholders the opportunity to offer comments on new guidance. Consultations are an important element of the European Union's 'Better Regulation' strategy. They are imperative to achieve a broad base of support among stakeholders and we greatly appreciate that our comments have been taken into consideration during past projects.

The comments that will follow have been drafted from our viewpoint as an organisation that specialises in the development and monitoring of codes of conduct based on Articles 40-41 GDPR, and our role in the EU Cloud Code of Conduct as mentioned above. As a result, the following comments are highly focused on our expertise within the ecosphere of third country transfers and the relevant facets of these Recommendations. Our comments should be read in this light, and notwithstanding broader comments by other stakeholders.

Our comments follow a twofold structure. First, we will begin with high-level overall observations. Second, we will provide more detailed remarks that centre around specific provisions of the draft Recommendations. A brief conclusion will wrap up our submission.

2 General observations

2.1 Risk-based approach should be further emphasised and integrated more consistently

As a first general remark, we noticed that, overall, the Recommendations seem to **lack a focus on the risk-based approach as introduced in GDPR**. Several provisions of the document do not introduce a risk-based perspective where it seems relevant and appropriate (e.g. see paragraph 42 of the Recommendations). Other provisions already refer to a risk-based approach, such as paragraph 49 which states that the nature of the data should be taken into account as a factor to identify supplementary measures. Footnote 44 puts an emphasis on the importance of enforceable remedies, and paragraph 136 explicitly states that the "risk of the categories of data processed and the likelihood of attempts from public authorities to access it" must be taken into account. We recommend that such **language wielding risk-based principles should be further emphasised throughout the Recommendations** as we consider a risk-based approach could succeed in creating a successful protective regime.

We acknowledge that legitimate mechanisms for third country data transfers should consider at least two factors: (i) the risks to the fundamental rights and freedoms of data subjects ("*appropriate safeguards*"); and (ii) the enforceable data subject rights alongside effective legal remedies for data subjects ("*enforceability and judicial review*"). When considering these two factors, there seems to be no reason not to apply a risk-based approach with respect to the appropriate safeguards.

2.2 Technical measures should not be preferred to organizational and contractual ones

Our second general remark concerns the current **distinction made between technical measures on the one hand, and organizational and contractual measures on the other.** Technical measures particularly seem to enjoy explicit preference (paragraph 48). Such an approach ignores the reality that technical measures can never be treated in a standalone manner. For example, the proper implementation of encryption (likely understood as a technical measure under the Recommendation) requires proper oversight and management (an organizational measure). Thus, the distinction currently made by the Recommendations is overly simplified. The Recommendations themselves also back this up: paragraphs 86-87 and 94 emphasize the importance of organizational measures specifically. By **providing a less black-and-white view of the different types of measures**, we are convinced the Recommendations would not only better reflect reality, but also **encourage companies to take robust, complete and synergetic measures to secure the safety of their transfers**.

3 Specific remarks

3.1 Step 1: Know your transfers

We welcome the first step of the Recommendations issued as a **very relevant addition** to the EDPB's ongoing guidance. Not only are the Recommendations helpful in providing concrete steps to make a prima facie assessment of transferring operations, but they also successfully consider the on-the-ground conditions under which market players operate. Please note, that this requirement is already incorporated in the current version of the EU Cloud Code of Conduct.[1]

However, an important issue is **the lack of clarity surrounding the term 'transfer' itself**. As stated in paragraph 13, "remote access from a third country (for example in support situations) and/or storage in a cloud situated outside the EEA, is also considered to be a transfer". However, in paragraph 33.5, the Recommendations seemingly indicate that remote access should be regarded differently by use of the word "only". For the sake of legal certainty, it is thus essential that the EDPB not only clarifies what 'transfer' encompasses, but also how seemingly related operations might differ. In that regard, it would be helpful to align terminology between the EDPB, the European Commission and other relevant stakeholders. This includes, but is not limited to, the existing discussions if and whether it shall be considered a data transfer at all if and to the extent the receiving party is already subject to the GDPR pursuant to Article 3.2 GDPR. Related to this terminological discussion, we point out that paragraph 4 mixes up transmission and transfer. We recommend rectifying the terminological conflation by clearly separating 'transfer' and 'transmission'.

Additionally, paragraph 11 determines that it should be verified whether "the data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred to and processed in the third country". To our understanding, the Recommendations conclude that to the extent a third country transfer is not (technically) necessary – e.g. by technical availability of EEA storage / processors – a transfer is not legitimate. Such a notion does not appear required under European data protection law or its application, i.e. court decisions such as Schrems I or II. Data minimisation is of course a key principle of GDPR, but this applies to the processing as such. Any – certainly unintended –notion that third country transfers – to the extent properly safeguarded – must not take place, appears far too restrictive, in particular in a controller-processor scenario. We recommend rephrasing this paragraph so that this ambiguous provision is removed.

[1] Please see version 2.6 of the Code, section 4 International Transfers of the Customers Personal Data: https://eucoc.cloud/en/contact/request-the-eu-cloud-code-of-conduct.html

3.2 Step 2: Identify the transfer tools you are relying on

This section provides a **streamlined overview of the available transfer tools** and we appreciate the explicit inclusion of codes of conduct as one of the main tools. We look forward to the publication of the "Guidelines on Certification and Codes of Conduct as a tool for transfers" as stated in the EDPB Work Program 2019 / 2020 for **further guidance on how to develop, implement and monitor provisions relating to third country transfers**. It is worth pointing out that the EU Cloud Code of Conduct already in its current form includes requirements that Cloud Service Providers document the specific safeguards under Chapter V GDPR a data transfer to a third country is based upon, including the obligations to establish documented procedures safeguarding that no transfer of data takes place without appropriate safeguards in place.[2] We appreciate the coherent approach between existing market standards and the Recommendations.

Related to the intersection of the first and second step, we also want to highlight that we appreciate and acknowledge the value of transparency along the processing chain, including the obligation of the data exporter to have detailed documentation about every transfer within its processing chain, including the exact transfer mechanisms and receiving entities. Following the notion of Article 13.1 f) GDPR the controller certainly needs transparency about all third countries (or international organisations) where personal data might be processed. It is worth highlighting that for scenarios where more than one transfer mechanism pursuant to Article 46 GDPR are implemented, it should be sufficient to document the one (overarching) mechanism. Requirements going beyond this would create unreasonable burdens to those data exporters and data importers that allow for more than one safeguard.

3.3 Step 3: Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer

3.3.1 Obligations for private actors – particularly SMEs – and need of practical guidance

Step 3 contains our main reservations regarding the Recommendations. First, while acknowledging the Schrems II ruling, it is important to note that **the obligations set out in this section are burdensome to corporate actors,** especially taking into account that global data flows are a key requirement for the majority of Cloud Service Providers, regardless of their size or business models. **We believe that such a requirement will create a competitive disadvantage for small-to-medium enterprises in particular**. Whereas

[2] Please see version 2.6 of the Code, section 4 International Transfers of the Customers Personal Data, in particular control 5.4.E: https://eucoc.cloud/en/contact/request-the-eu-cloud-code-of-conduct.html

paragraphs 34 to 37 seem to create a manageable and even desirable obligation of assessment, paragraphs 38 to 44 impose a complex and stringent test.

The current wording of these paragraphs implies that corporations should take on a role they are not meant to fulfil: assessing whether nation state "requirements or powers are limited to what is necessary and proportionate in a democratic society" is a test carried out by courts. It is welcomed of course that due diligence and a human rights-based approach in the sphere of transfers is put forward, but we believe much more guidance from the EDPB is necessary to assist private actors in carrying out analyses of Article 45 (2) (a) (see also our comments under Annex 2, first paragraph). Although we understand that there is a certain history of this approach, for example with regard to the old Standard Contractual Clauses, we believe it is too burdensome to ask enterprises – in particular SMEs – to conduct such an assessment. In contrast to the burdensome assessment of Article 45 (2) (a), **we argue that Article 45 (2) (b) and (c) are much more manageable elements for private actors to assess.**

We understand and appreciate that EDPB guidance in general is limited, as data transfers need to be assessed on a case-by-case basis and the EDPB cannot generally allow or generally prohibit supplementary measures. However, we would like to emphasize that the industry would appreciate if the EDPB could invest more heavily in Annex 3 to these Recommendations. It can be helpful to expand the work related to the Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, e.g., by benchmarking third country surveillance laws against EU privacy criteria and proposing processes which companies may use to mitigate against such risk. The latter is a valuable framework that would also benefit from real-life examples and cases to assist enterprises in making assessments. In this context we want to refer to our remarks in 3.5 regarding Codes of Conduct as suitable transfer mechanism. Acknowledging the complexity of needed benchmarks, it would be highly appreciated if the Recommendations will – at a minimum – allow for related possibilities to develop such benchmarks cooperatively with relevant stakeholders, such as Code owners.

3.3.2 Elements are in place for a clear risk-based approach

It is worth highlighting once more the above-mentioned **lack of the risk-based approach**. In particular, paragraph 42 discusses the relevant sources to assess third country legislation and explicitly recommends to "not rely on subjective [factors] such as the likelihood of public authorities' access to your data in a manner not in line with EU standards". We believe that a risk analysis, including the probability of public authorities' access, is a relevant piece in assessing whether an Article 46 GDPR transfer is effective in light of **all circumstances of the transfer**. It can also be argued that the incorporation of the risk-based approach here in the context of paragraph 42 goes hand in hand with several of the transparency and accountability measures introduced in Annex 2 and is in line with the recently

updated draft implementing decision on new standard contractual clauses for the transfer of personal data to third countries of the European Commission.[3]

3.3.3 Additional elements need clarification

In addition, paragraph 35 also raises important questions. This provision seems to imply that a 'right to redress' exists in any case of public authorities accessing transferred data. Such an interpretation would, however, be overly broad. Even national EU Member State provisions have determined that it is not required to notify data subjects and grant redress avenues for every single instance of access by public authorities. Consequently, exemptions already exist under national Member State law if and to the extent individuals cannot be duly identified without overburdening efforts, and if the access likely resulted only in minor or no consequences to individuals. We recommend introducing similar exemptions into these Recommendations.

Finally, we would like to point to paragraphs 42 (discussing the public availability of legislation in third countries) and 43 (obtaining other sources for the assessment), and the points made in this document regarding interception. It is important to note that – unlike what paragraph 43.2 seems to imply – interception takes places in transit, and not after a transfer has been completed. Additionally, we believe that these provisions as well as paragraph 77 point a) imply that interceptions can only occur in the event of third country transfers, while, as practice shows, severe inner-EU risks exist as well. It is well documented that e.g. (international) surveillance agencies accessed data collected by interception at DE-CIX and other European locations. As a result, we recommend that paragraphs 42-43 and 77 point a) are re-worded to remove this apparent bias against third country transfers as being especially vulnerable to interceptions.

3.4 Step 4: Adopt supplementary measures

In this section, the distinction between technical measures vs. organizational and contractual measures is made most clearly. We would like to refer to "2 General Observations" for our comments on why we believe this element should be adjusted. And, in line with the arguments made above, this section also lacks a risk-based analysis when adopting supplementary measures.

Finally, we would like to note that **some language used in this section conflates possible measures that could be taken to mitigate third country transfer risks with the provisions of Article 28 GDPR.** We are convinced both should be more strictly separated since they operate in such different contexts. Articles 44-50 GDPR

[3] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

focus on the context of third country transfers, whereas Article 28 GDPR is only aimed at the intra-EU context. This is a logical distinction that should also be reflected in these Recommendations through distinct language.

3.5 Step 5: Procedural steps if you have identified effective supplementary measures

We believe this chapter falls short by **not addressing all existing transfer mechanisms, but instead limiting itself to the current three**. For the sake of clarity and comprehensiveness, we would therefore highly appreciate it if all transfer mechanisms – including codes of conduct – would be highlighted in Step 5. In line with our comments issued under 3.2 regarding Step 2, we would look forward to assessing **the EDPB's dedicated guidelines on the use of codes of conduct for the purpose of transfers to third countries**.

3.6 Step 6: Re-evaluate at appropriate intervals

We appreciate the notion of re-evaluating the developments in the third country that could affect initial data protection assessments and the decisions taken accordingly on transfers. Along those lines, we would like to emphasize that the EU Cloud Code of Conduct already contains a robust ongoing monitoring scheme including provisions setting out a mandatory annual verification of compliance, while there is also an obligation in place to inform the monitoring body of significant changes.4 We therefore appreciate the concepts introduced in step 6 as this also reflects the methodology of the current Code monitoring.

3.7 Annex 1: Definitions

The terms 'data exporter' and 'data importer' are insufficiently precise and too limited in scope to encompass all possible situations that might arise related to the Recommendations. The frequent situation where a processor in a third country would enlist the help of another processor or several other processors (who may or may not be situated in the same jurisdiction), cannot be adequately captured by relying on those two terms. For that reason, we believe a more accurate terminology / wording that allows further (sub-)processing mandated by the 'data importer' should be used[5],

[4] Please see version 2.6 of the Code, section 7 Monitoring and Compliance: https://eucoc.cloud/en/contact/request-the-eu-cloud-code-of-conduct.html

[5] As way of illustration, we would like to refer to the draft Standard Data Protection Clauses that SCOPE Europe developed together with a consortium of different European and international companies. In this context, the more generic and flexible terms 'transferring party' and 'receiving party' (reflecting the idea that the data exporter is the one transferring the personal data and the data importer is the one receiving the personal data from the data exporter). The terms 'data importer' and 'data exporter' do not reflect common processing procedures in the market, e.g. if the 'data importer' contracts another sub-processor in the same third country. Please see here for more information on the notion of 'transferring party' and 'receiving party': https://scope-europe.eu/en/projects/standard-data-protection-clauses/

provided that any such terminology / wording will be used consistently throughout all official, applicable documents.

3.8 Annex 2: Examples of Supplementary Measures

Annex 2 introduces highly relevant principles, examples and use cases related to the appropriate supplementary measures. Therefore, we would like to share several observations regarding the content of Annex 2.

3.8.1 Ambiguities related Encryption as Supplementary Measure

We would like to refer to paragraph 79.3, where one of the factors mentioned is whether "the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved". While we certainly appreciate the underlying notion of a risk-based approach, this seems like an unclear criterion. From a practical perspective, it will be highly appreciated if the Recommendations clarify that the estimate of the flexible, but indefinite "period of time" also allows for a case-by-case risk analysis taking into account the expected realistic resources available to and spent by potential attackers.

Also related to encryption, but from another perspective, we would like to raise attention that case 3 paragraph 84 is creating some concerns. It is not yet clear, whether the aspect "*experience with vulnerabilities of the infrastructure or the software used*" needs to be considered as a mere factor or, to the extent vulnerabilities exist, an end-to-end encryption shall become mandatory. We recommend clarifying that also in this regard a risk-based approach will be feasible and appropriate. This recommendation considers the complexity around IT-security as well as that some already existent vulnerabilities are not related to software anymore but affects broadly used hardware as well. Consequently, such flaws cannot be easily resolved by virtual updates but will require resource intensive hardware replacements. Some flaws might not even be resolvable by replacements, as such flaws could relate to the very core design of such hardware. Clarifying that a risk-based approach may be taken in this regard, will allow for alternative mitigating measures, expected to be broadly accepted and adopted. Neither data exporters nor data importers should be enforced to implement end-to-end encryption where alternate, equally efficient measures are at hand. Especially, as such implementation may even operate counterintuitive as it will lead into a false sense of security.

3.8.2 Allowing for more flexibility regarding Trustees

Also in paragraph 79.6, we appreciate that the EDPB has thoroughly considered the role and situation of the trustee and considers this a supplementary measure. It is especially appreciated that the implementation of such a trustee is not considered mandatory in any case. Against this background, it

is recommended to implement a staggered approach, allowing for more flexibility and even a low threshold of implementation for a trustee framework. For example, one could consider different qualities in trustees; trustees that are subject to the same jurisdiction and thus access-requesting authorities; trustees subject to a different jurisdiction than the processor and thus less likely to the same access-requesting authorities; and – at the highest level – a trustee within the EEA.

Related to use case 5 paragraph 86.2, it seems overly restrictive that a factor is whether "each of the pieces is transferred to a separate processor located in a different jurisdiction". It should suffice to impose a split within one jurisdiction or even within one data centre on multiple storages, as "re-combining" data that is randomly split over different storages seems highly unlikely, also provided that data centres nowadays easily host (ten-)thousands of storages. We therefore recommend adding a notion to this requirement that allows for a case-by-case analysis on the probabilities if split data might be re-combined by third parties. This will also ease the service provision by SME, as it will certainly be SMEs that may lack an infrastructure spread over multiple jurisdictions.

3.8.3 Enhance neutrality of the Recommendation –focussing on distinct risks and mitigating actions instead of business models

In addition, we also feel compelled to comment on **use case 6, as the focus of this section is on "data in the clear".** Somehow, however, this section places "cloud service providers" as the protagonist in the issue at hand. From our perspective, this seems unnecessary, since it creates the perception that the problem is created by enterprises in the cloud industry. Once again, the core of this section is "data in the clear". We would therefore kindly ask **to change "cloud service provider" into "service provider"**. This also helps this use case to remain technologically neutral and thus be more futureproof. Also, it is not clear if 'data in the clear' is understood as an equivalent to 'plain text' as used in the rest of the Recommendations.

Use case 7 paragraph 90.2 determines that one of the factors is whether "the importer uses the data in the clear for its own purposes". This is not only a matter of transfer but also transmission, meaning that the receiving party needs to assess the data transfer, not the transferring party[6].

3.8.4 Enhanced language to better reflect technical boundaries will be appreciated

One of the conditions for effectiveness mentioned in paragraph 109 is that the clauses "should provide for a quick mechanism whereby the data exporter authorises the data importer to promptly

[6] Again, we would like to reference the draft Standard Data Protection Clauses as outlined here: https://scope-europe.eu/en/projects/standard-data-protection-clauses/

secure or return the data to the data exporter, or if this is not feasible, delete or securely encrypt the data without necessarily waiting for the exporter's instructions, if a specific threshold to be agreed between the data exporter and the data importer is met. The importer should implement this mechanism from the beginning of the data transfer and test it regularly to ensure that it can be applied on short notice". Such a provision may function well for smaller amounts of data, but not for corporations who store terabytes, if not petabytes, of data in the cloud. Besides the data itself, larger organizations apply many automated scripts and processing algorithms that deal with such an amount of data. We therefore caution that "quick mechanisms" might create a misleading notion in practise.

3.8.5 Indefinite legal terms should be prevented

Besides, we would like to ask for **clarification of the phrase "text in the normal course of business"** as noted in paragraph 116 related to empowering data subjects to exercise their rights. What are the repercussions of data controllers who engage a processor for the very distinct purpose of accessing plain text data – e.g. to print, sort and send mailings? Paragraph 116 thus seems overly burdensome for what is a very common real-life practice.

Finally, in paragraph 120, **the provision that "[t]he contract could commit the exporter and importer to assist the data subject in exercising his/her rights in the third country jurisdiction through [...] legal counselling" is unclear in scope.** To the extent a receiving party should provide data subjects with legal advice, we strongly recommend to re-assess such a requirement. It is furthermore recommended to add a notion that it may already suffice if and to the extent both parties publish general advices – e.g. by means of whitepapers or FAQs.

3.8.6 Overall structure of Annex 2

We appreciate that Annex 2 tries to give as detailed recommendations as possible. Partaking in several working groups and drafting a dedicated third country transfer module for the EU Cloud CoC, we are aware of the complexities and obstacles in doing so. These recommendations are expected to have significant influence on data exporters and data importers. By that, they will certainly be shaping the European economy. Especially SMEs, eager to circumvent any legal ambiguities and by that preventing themselves from spending unnecessary resources for legal defense, will most likely refer to those Recommendations in a strong manner. Their processing activities, type of data but also used business models involved in the transfer of personal data are uncounted. These recommendations should neither expose SMEs to ambiguities nor should SMEs be left alone. We therefore recommend in structuring Annex 2 more generically by listing specific third country transfer specific risks on the one hand and listing potential supplementary measures to such risks on the other hand. Such an

approach would be aligned to the neutrality of GDPR regarding technical means and translate such neutrality to business models.

Concluding remarks

We appreciate the opportunity to share our perspectives in the context of the public consultation and consider the Recommendations as a key piece of guidance for future data transfers in general and in particular for the on-going work on the new module to the EU Cloud Code of Conduct for transferring personal data outside of the EU in line with Article 46 GDPR.

Our two main points and high-level overall observations can be summarized as follows:

- Overall, the Recommendations seem to lack a focus on the risk-based approach as introduced in GDPR, even though some provide a risk-based perspective that seems relevant and appropriate. We therefore propose to further emphasize risk-based principles throughout the Recommendations as we consider a risk-based approach could succeed in creating a successful protective regime.
- We further spotted a distinction between technical measures on the one hand, and organizational and contractual measures on the other, whereas it seems like technical measures particularly seem to be given explicit preference. We caution that such an approach ignores the reality that technical measures can never be treated in a standalone manner and therefore recommend providing a less black-and-white view of the different types of measures.

Second, we provide more detailed remarks that centre around specific provisions of the draft Recommendations, namely Step 1 to 6 and the Annexes.

We hope our detailed comments may contribute to the update of the Recommendations and we look forward to further engaging with the EDPB and other key stakeholders in this context.

About the authors:

Self-Regulation Information Economy (German: Selbstregulierung Informationswirtschaft e.V.) is a Berlin-based non-profit-organization that fosters and promotes data and consumer protection through self-regulation and co-regulation and acts as a monitoring body for data protection codes of conduct. Its Brussels-based subsidiary SCOPE Europe sprl / bvba complements the portfolio of SRIW on a European level and is in the process of acquiring accreditation as a monitoring body under the European General Data Protection Regulation (GDPR), pursuant to Article 41 GDPR. SCOPE Europe acts as the monitoring body for the EU Data Protection Code of Conduct for Cloud Service Providers (short: EU Cloud Code of Conduct).

The EU Cloud Code of Conduct is a widely adopted Code of Conduct pursuant to Article 40 GDPR, defining clear requirements for Cloud Service Providers. While the official approval of the current Code by the European Data Protection Board (EDPB) is pending, the EU Cloud Code of Conduct General Assembly already started the creation of a new module to the Code for transferring personal data outside of the EU in line with Article 46 GDPR. The EDPB's "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the Recommendations)" are a key piece of guidance to develop this effective but accessible safeguard for third country transfers.