Feedback for the European Data Protection Board (EDPB)
in response to the public consultation on
'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data'

Prof. Dr. Gloria González Fuster, Vrije Universiteit Brussel (VUB)[1]
Laura Drechsler, Research Foundation Flanders (FWO)/ VUB[2]

Submitted on 21st December 2020

1) The Court of Justice of the European Union (CJEU) emphasised in the '*Schrems II'* judgment the importance of ensuring *'effective and enforceable rights and effective administrative and judicial redress'* for data subjects whenever personal data about them are transferred to third countries.[3] The availability of '*(e)nforceable* ***data subject rights*** *and effective* ***legal remedies*** *for data subjects'* is actually a necessary condition for data exporters to rely on any transfer mechanisms under Article 46 of the General Data Protection Regulation (GDPR).[4] Data subject rights and remedies, however, can only be effectively available to individuals if the data subjects are aware of the existence of such rights and remedies, and if they know how to exercise them. The CJEU has previously stressed that **information** about data processing directly affects the exercise of data subject rights, and that information obligations imposed on data controllers – beyond being directly connected to the principle of **transparency** – are also necessary to comply with the principle of **fairness**.[5]

2) In this contribution, we propose concrete changes to the European Data Protection Board (EDPB)'s Recommendation 01/2020[6] to guarantee that measures that supplement transfer tools under Article 46 GDPR are in line with the **principles of transparency and fairness**. For convenience, the final paragraph 14 lists the issues to be addressed in the revised text.

---

[1] Gloria.Gonzalez.Fuster@vub.be.
[2] Laura.Drechsler@vub.be.
[3] See Case C-311/18, *Data Protection Commissioner v Facebook Ireland and Schrems,* judgment of 16 July 2020 (Grand Chamber) (ECLI:EU:C2020:559), para. 187 (*Schrems II*), esp. paras. 188 and 189; see also Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, judgment of 6 October 2015 (Grand Chamber) (ECLI:EU:C:2015:650) ('*Schrems I'*), para. 95.
[4] Art. 46(1) GDPR: *'In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available'* (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR), OJ 2016 L 119/1).
[5] Case C-201/14, *Smaranda Bara and Others v Preşedintele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF)*, judgment of 1 October 2015 (ECLI:EU:C:2015:638), paras. 33 and 34. The specific connection between information about data transfers and fairness was also highlighted previously in: Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679,* (WP260 rev.01), 11 April 2018, pp. 37-38.
[6] European Data Protection Board (EDPB), *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (Version for public consultation), 10 November 2020.

3) This feedback is grounded on our ongoing research on EU data protection law, including the regular reading of academic literature and data protection notices, and frequent exchanges with a variety of actors. In a nutshell, the current state of the matter is that **there is persistent uncertainty about how to comply with requirements of Articles 13(1)(f) and 14(1)(f) GDPR.**[7] An important unclear element in such provisions is what constitutes a transfer of personal data falling under Chapter V the GDPR, and, thus, what is the meaning of '*to transfer'* under Articles 13(1)(f) and 14(1)(f). We understand that the EDPB is moving towards a clarification of that specific issue, and hope it will be forthcoming soon.

4) The uncertainty around Articles 13(1)(f) and 14(1)(f) has been **further exacerbated** by the '*Schrems II'* judgment. It is thus **indispensable** that the EDPB provides **useful guidance** on these matters in the Recommendations at stake, in order to provide legal certainty to data controllers and data subjects. Such guidance shall also provide useful information on how to comply with information obligations under the right of access as established in **Article 15(2) GDPR**,[8] which concerns specifically transfers under Article 46 GDPR.

5) Footnote 24 of the draft Recommendations is in this context troubling, as it seems to imply that the EDPB's view is that currently, generally speaking, data controllers already regularly provide to data subjects meaningful information about personal data transfers, and that such information is '*correct and current, especially in light of the Court's case law concerning transfers'*.[9] Such a view is **far from accurate**. As a matter of fact, still today, in December 2020, there are many websites that refer to transfers supposedly relying on the invalidated EU-US Privacy Shield. When data controllers assert that they rely on standard contractual clauses, they typically consider it sufficient to direct data subjects to information about such clauses as it is publicly available on the website of the European Commission.[10] Even after exercising a data access request under Article 15 GDPR, the data subject might be provided with some text which refers to a publicly available 'privacy policy' for 'details' on international data transfers. The EDPB **cannot ignore such persistent problems** after two years of applicability of the GDPR.

---

[7] They require that '*where applicable, the fact the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second sub-paragraph of Article 49(1), reference to the appropriate safeguards and the means by which to obtain a copy of them or where they have been made available'.*

[8] Art. 15(2) GDPR: *'Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer'.*

[9] *Recommendations 01/2020,* op. cit., p. 9.

[10] See in this sense, for instance, NOYB's Comments on the proposed Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to Regulation (EU) 2016/679 (https://noyb.eu/sites/default/files/2020-12/Feedback_SCCs_nonEU.pdf). Our research and experience confirm the problematic situation. An example of reply to requests on information about data transfers is: '*Hello Gloria, We previously relied on Privacy Shield which has now been invalidated by the Court of Justice of the European Union. Accordingly, we have moved to Standard Contractual Clauses. Best, (...)'* (a follow-up request for a copy of such clauses has still not been replied three months later). Another example: '*With regard to the US based vendors, I can inform you that – insofar these vendors relied on the Privacy Shield as transfer mechanism – (...).com is currently entering into the EU Standard Contractual Clauses to ensure the proper level of data protection. You can find the text of these Standard Contractual Clauses through the following link*: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087. *I hope this provides sufficient answer to your questions. Kind regards'.*

6) The Recommendations shall thus, on the grounds of this situation and due to the further uncertainty brought in by '*Schrems II',* describe and detail **an additional step, Step Seven,** about '**communicating your transfers'.** This will make manifest it is not sufficient that data controllers 'know their transfers', but that they should also inform data subjects about such transfers in a fair and transparent manner, in accordance with the principles of transparency and fairness. **Data controllers must know their transfers, but data subjects must know their transfers too.** If data subjects are not adequately informed about the transfers taking place or are about to take place, they will not be in a position to effectively exercise any of their rights in relation to the data transferred, or eventually take the necessary steps to have access to administrative and judicial redress. For individuals to be able to pursue legal remedies in order to have access to personal data relating to them, or to obtain the rectification or erasure of such data, when data are transferred to a third country,[11] data subjects must imperatively be informed about the fact that such data are transferred or are about the be transferred, and to which specific, identified, named third country.

7) The only existing guidance on these issues currently endorsed by the EDPB is to be found inside a cell of a table in the Annex of the *Guidelines on transparency under Regulation 2016/679* adopted in 2017 by the Article 29 Working Party (WP29).[12] The guidance states that controllers shall, in line with their GDPR information obligations:

> - specify '*the relevant GDPR article permitting the transfer and the corresponding mechanism*'[13] *(e.g. adequacy decision under Article 45/ binding corporate rules under Article 47/ standard data protection clauses under Article 46.2/ derogations and safeguards under Article 49 etc.)';*
>
> - provide *'(i)nformation on where and how the relevant document*[14] *may be accessed or obtained should also be provided e.g. by providing a link to the mechanism used'*;
>
> - and recommend that *'(i)n accordance with the principle of fairness, the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean that the third countries be named.* [15] *'*

Existing guidance is thus **limited**, **predates the applicability of the GDPR**, and fails to take into account that, in practice, data controllers very often do not name the third countries at stake,[16] or do not make clear which data processing operations are concerned, as well as the many other obstacles which are regularly surfacing in this area.

---

[11] Which is an essential safeguard, as if this was not possible, the essence of Art. 47 of the EU Charter of Fundamental Rights would be affected, as the CJEU has found in *Schrems I* and *Schrems II.* See Case C-362/14, *Schrems I*, op. cit., para. 95; Case C-311/18, *Schrems II*), op. cit., para. 187.

[12] WP260 rev.01, op. cit., pp. 37-38.

[13] Underlined by the authors.

[14] Idem.

[15] Idem.

[16] Or, alternatively, mention many countries in a confusing manner. The data protection notice of Take Away – France (for food deliveries in France) states as follows: '***Transfers internationaux des données*** - *Nous pouvons transférer vos données personnelles dans des pays autres que le pays dans lequel vous résidez. Les serveurs du site web de Just Eat Takeaway.com sont principalement situés au Royaume-Uni et aux Pays-Bas. Toutefois, les sociétés de notre groupe et nos prestataires de services tiers et partenaires exercent leurs activités dans de nombreux pays, incluant, mais ne se limitant pas à l'Australie, le Brésil, la Bulgarie, le Canada, la Colombie, le*

8) Crucially, it now needs to be **urgently clarified** exactly how must the GDPR and the existing EDPB guidance **be interpreted in light of *'Schrems II' and the related EDPB Recommendations***, specifically clarifying:

> - when data exporters rely on standard contractual clauses accompanied by supplementary measures in order to provide for *'appropriate safeguards'* in line with Article 46 GDPR, what is exactly covered by the '*appropriate or suitable safeguards'* as referred to in Articles 13(1)(f) and 14(1)(f)? Does the notion of '*corresponding mechanism'* as put forward by EDPB guidance (in WP260 rev.01) correspond to both the relevant standard contractual clauses and supplementary measures?
>
> - if supplementary measures must be made available under Articles 13(1)(f) and 14(1)(f), **how?** Should they be included in the information made generally available to individuals (for instance in the form of a data protection notice), or provided only upon request? What does the notion of *'the relevant document'* as put forward by EDPB guidance (as in WP260 rev.01) encompass precisely, specifically when supplementary measures are in place?
>
> - if the relevant information is to be provided upon request:
>
> - do the general modalities of Article 12 GDPR apply to such a request? and
> - can any individual, and thus not necessarily a data subject in the case at stake, request such information?, and
>
> - as it would not make sense for data subjects to be told that their transfers rely on standard contractual clauses and additional necessary supplementary measures without explicitly mentioning to them the third country of destination, is it correct to interpret that **in light of *'Schrems II'* whenever data controllers rely on standard contractual clauses, and most notably standard contractual clauses accompanied by supplementary measures, they must imperatively <u>always</u> inform data subjects of the exact third country of destination?**

9) In addition, it is extremely common for data controllers relying on Article 46 GDPR to refer to such a fact with a generic statement, **without specifying exactly which data or data processing operations are concerned**. For instance, data controllers might just list all the different mechanisms they use for transfers.[17] This is in tension with the notion that information

---

Danemark, la France, l'Allemagne, l'Irlande, l'Italie, l'île Maurice, le Mexique, les Pays-Bas, la Norvège, la Nouvelle-Zélande, les Philippines, l'Espagne, la Suisse, l'Ukraine et le Royaume-Uni. Ce qui signifie que lorsque nous collectons vos données personnelles nous pouvons les traiter dans un quelconque de ces pays.' (Take Away – France, Politique de confidentialité et de protection de la vie privée', https://www.just-eat.fr/privacy-statement#international-data-transfers, accessed 20 December 2020). Such a sentence is disconcerting and might lead the data subject to believe that the flow of data from France to Spain, for instance, constitutes an 'international data transfer', as it is described under such a heading; more broadly, it fails to provide meaningful information as to what will occur to the data. In contrast, the equivalent Take Away - Belgium notice, for food deliveries in Belgium, makes no reference at all to any international data transfers: https://www.takeaway.com/be-en/privacy-statement.

[17] For example: '*Uber operates, and processes data, globally. We may also transfer data to countries other than the one where our users live or use Uber's services. We do so in order to fulfill our agreements with users, such*

should be granular and specific,[18] and crucially leaves data subjects without any concrete knowledge about exactly which data or to be transferred or have been transferred on the mentioned grounds. Thus, the Recommendations should explicitly state that **data controllers must inform exactly about which data transfers are concerned by the supplementary measures.**

10) The EDPB established in its *Guidelines 2/2020 on Articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies* that relevant international agreements must contain '*clear wording describing the transparency obligations of the parties'*, which '*should include* (...) *the rights available to data subjects and applicable restrictions,*[19] *available redress mechanisms and contact details for submitting a dispute or claim'.*[20] In principle, it is reasonable to expect that any standard data protection clauses to be adopted in the future by the European Commission will include similar requirements, at least obliging data exporters to inform data subjects about applicable rights and redress mechanisms insofar as the standard data protection clauses apply.

11) However, as stressed by the CJEU in '*Schrems II'*, there are some situations in which **standard contractual clauses will not, by themselves, provide all necessary 'appropriate safeguards' and might not govern a specific data processing**, especially in relation to access by third country public authorities to the transferred data. In those cases, it is still necessary to make sure that the data exporter provides to the data subject with meaningful information as to which are the applicable rights and remedies, especially their right to redress, and any applicable restrictions to such rights and remedies. In Annex II of the draft Recommendations, the EDPB refers to 'transparency obligations' as potential additional contractual safeguards,

---

as our Terms of Use, or based on users' prior consent, adequacy decisions for the relevant countries, or other transfer mechanisms as may be available under applicable law, such as the Standard Contractual Clauses' ('Privacy Policy' connected to the Uber Eats Belgium website, https://www.uber.com/legal/en/document/?country=united-states&lang=en&name=privacy-notice). See also: '*International transfers of data - In some cases the personal data we collect from you might be processed outside the European Economic Area ("EEA"), such as the United States, the Philippines and the countries in which Deliveroo operates (which are set out on www.deliveroo.co.uk). (...) There are therefore certain safeguards in place when your data is processed outside of the EEA. We ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented: your personal data is transferred to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission; we use the EU approved Standard Contractual Clauses; and where your personal data is transferred to third party providers based in the US, data may be transferred to them if they have self-certified under the Privacy Shield framework in relation to the type of data being transferred, which requires them to provide similar protection to personal data shared between the EU and the US.'* (Deliveroo, https://deliveroo.be/en/privacy, Section 10, accessed 20 December 2020); and '*Alors que ces pays peuvent avoir des lois sur la protection des données différentes des lois de votre pays, vous pouvez être rassuré, Just Eat Takeaway.com veille à mettre en œuvre des garanties appropriées afin de protéger vos données personnelles dans ces pays conformément à cette Politique de Confidentialité. Certaines des garanties seront basées notamment, le cas échéant, sur l'utilisation des clauses contractuelles types approuvées par la Commission européenne avec nos fournisseurs, les accords de transfert au sein du groupe (de sorte que nous puissions transférer en toute sécurité vos données entre les sociétés du groupe Just Eat Takeaway.com dans le monde entier) et la conclusion de contrats avec des sociétés certifiées « Privacy Shield » aux États-Unis, le cas échéant.'* (Take Away – France 'Politique de confidentialité et de protection de la vie privée', already quoted).

[18] The importance of specificity and granularity of information for the data subject have notably been discussed in the context of consent by the EDPB. See EDPB, *Guidelines on consent under Regulation 2016/679*, (Version 1.0), 4 May 2020, pp. 11-15.

[19] Underlined by the authors.

[20] EDPB, *Guidelines 2/2020 on Articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies* (Version 2.0), 15 December 2020, p. 10.

but covering only transparency obligations from the data importer to data exporter.[21] Emphasis is also put on the possible notification of data subjects when there is a request from a third country authority. Such obligations might not as such be sufficient, as **data subjects must be informed about their rights and available remedies** not after the transfer has taken place and when the third country authority is already seeking access or already obtained access to the data concerning them, but before.

12) In light of the significance of **onward transfers**, the EDPB must clarify whether data subjects must be informed about onward transfers, and, if so, how.

13) Finally, the draft Recommendations refer to the European Commission's website information on adequacy decisions mentioning the URL of a page with general information about adequacy,[22] but fail to mention that the European Commission's website also includes a page on EU-US transfers which states, still today, that the Privacy Shield '*protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States for commercial purposes'* and '*allows the free transfer of data to companies that are certified in the US under the Privacy Shield'*.[23] The fact that this information is online months after '*Schrems II'* is extremely problematic, confusing for both data controllers and data subjects, and potentially in breach of Article 45(8) GDPR.

14) To sum up, the revised Recommendations should notably:

a) clarify **exactly which information** must be provided by data controllers to data subjects under **Articles 13(1)(f) and 14(1)(f) GDPR in case of transfers referred to in Article 46**, and how;
b) clarify **exactly which information** must be provided by data controllers under **Article 15(2) GDPR,** and how; and
c) explicitly recommend that data subjects are always informed about the third country to which data are transferred in case of transfers referred to in Article 46 GDPR, as well as of the data or data processing operations at stake;
d) clarify which are the information requirements towards the data subject in relation to onward transfers; and
e) further detail which **additional information obligations** are applicable when there exist in the third country of destination restrictions or special rules for data subject rights and remedies, notably in relation to access by third country public authorities to the transferred data, to the extent that such information might not be provided in the relevant standard data protection clauses.

These clarifications are of the utmost urgent importance also in light of the imminent 'Brexit', which is to multiply the instances in which the discussed provisions might be applicable. The need for clarity becomes thus even more crucial to guarantee the level of data protection required by the EU Charter of Fundamental Rights.

---

[21] *Recommendations 1/2020*, op cit., pp. 29-30.
[22] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
[23] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.