DataRep
Your Data Protection Representative

To: European Data Protection Board

3rd December 2020

Dear EDPB Members,

Feedback in respect of: EDPB Recommendation 01/2020 re: additional safeguards

Summary:

- European Data Protection Board Recommendation 01/2020 (hereafter the "**Recommendation**") would make the protection of EEA data subjects' personal data more effective if it referred specifically to the obligation on a non-EEA data importer to appoint an EEA Representative (pursuant to GDPR Article 27).
- Most companies which are obliged to appoint a Representative under GDPR Article 27 will be impacted by the Recommendation. The appointment of a Representative is required for the same purpose as this document (enabling exercise and enforcement of GDPR rights against non-EEA controllers/processors), so it is appropriate to add reference to the Representative obligation in the Recommendation.
- We have undertaken research which indicates that fewer than 8% of Privacy Shield participants which are obliged by GDPR to appoint an EEA Representative have done so – we anticipate that the wider level of compliance with this obligation is no higher.
- A small amendment to the Recommendation would improve this, adding a paragraph in Section 2.1 ("Know your transfers") along the lines of:
    - *"In addition to the information gathered in the Article 30 records of processing activities, also consider whether the non-EEA data importer meets their other GDPR obligations including, if they have no EEA establishment, the obligation to appoint a Representative in the EEA (pursuant to GDPR Article 27). If, post-transfer, the personal data is not processed by the data importer in line with GDPR standards, the transfer mechanism itself will not remedy any ongoing processing shortcomings."*

Detailed feedback:

Firstly, we wish to thank you for preparing a presenting Recommendation 01/2020 (and also connected Recommendation 02/2020) within a relatively short timescale following the Schrems II judgement which necessitated them – we appreciate that this must have been a major undertaking.

We have no objections to the existing content of the Recommendation 01/2020 (hereafter the **Recommendation**), but we believe that an opportunity has been missed to recommend that data exporters confirm the wider GDPR protections applied by non-EEA data importers to which they send personal data. Whilst a valid mechanism for data transfer is important, the continuing protection of the personal data being processed outside the EEA – after the transfer has been completed – is also essential to protect the data subjects' rights and freedoms on an ongoing basis.

In the proposed 'Step 1' (Recommendation section 2.1, paragraphs 8-13, which is being largely overlooked as simply a 'data-mapping step' while more attention is paid to the additional protections[1]), there is a brief summary of the activities expected to be undertaken by entities which are seeking to transfer EEA personal data to an entity outside of the EEA. This follows much the same pattern as the usual advice in this regard, but fails to take into consideration additional due diligence which should be undertaken on a data importer *outside* of the EEA, because it follows the same structure used in other guidance, which is designed mainly with relevance to EEA-based controllers and processors.

What Step 1 fails to highlight to data exporters is that identifying the data *transfers* alone is not sufficient; basic information should also be gathered about the data *importer* receiving the data, to enable an assessment of whether the personal data being exported will be processed by the non-EEA importer in a manner compliant with GDPR. Our concern is that many, if not most, will simply skip over this first step – having followed previous guidance about assessing data processors (which is designed for EEA-based data processors and accordingly doesn't mention the Representative) without having considered if the due diligence they have undertaken is adequate.

This is particularly relevant in respect of data transfers which make use of the standard contractual clauses, as those SCCs are often perceived to set out all the relevant obligations to achieve GDPR compliance. However, neither the current SCCs, nor the proposed replacements, place an obligation to appoint an EU Representative where necessary (as the current SCCs were drafted before regulation 674/2016 was in place and this obligation became more widespread). Although the draft new SCCs make reference to the Representative "if required", this won't help significantly, because most data exporters and importers are not aware if or when this is required, so will assume that it is not.

The Recommendation's focus on Article 46 in this regard is obviously relevant. However, while a great deal of attention has been devoted in the Recommendation to the first part of Article 46(1) in respect of safeguards:

- " … 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, … ",

an opportunity has been missed to provide recommendations in respect of the second and third condition of that Article, that:

[1] https://iapp.org/news/a/a-break-down-of-edpbs-recommendations-for-data-transfers-post-schrems-ii/

- " … a controller or processor may transfer personal data to a third country or an international organisation only … on condition that enforceable data subject rights and effective legal remedies for data subjects are available."

In particular, the opportunity has been missed to clarify the GDPR obligation to appoint a Representative in the EEA (Article 27), which is relevant to a large proportion of personal data transfers made outside of the EEA, and is a key part of GDPR's access to data subject rights. The Representative is also a major part of the process by which GDPR can be enforced against non-EEA data importers.

Appointing an EEA Data Protection Representative ensures non-EEA data importer clients meet the principle of accountability by:

- Enabling enforcement of data subject rights by providing an easier route for data subjects to raise their subject access requests, in their own country and language, against the non-EEA data controller/processor (GDPR Article 27(4)), and
- Assisting supervisory authorities bring effective legal remedies against non-EEA data controllers/processors by:
    - providing the easier route for communication, as with the data subjects (GDPR Article 27(4)),
    - being quickly able to provide a copy of their client's records of processing activity on the supervisory authority's request (GDPR Article 30(4)), and
    - being a potential secondary point of responsibility for any enforcement action (GDPR Recital 80 and EDPB Guidance 03/2018)

Following the Schrems II judgement, we undertook research into the extent to which Privacy Shield participants were meeting visibly-ascertainable elements of GDPR, which included whether they had appointed a Representative if they had no EEA establishment, as is required by GDPR Article 27. The published results of this research are submitted with these comments, but in summary over 90% of the companies which appeared to need a Representative (because they had no EEA establishment listed) had failed to do so.[2] Because the benefit of participating in Privacy Shield was specifically to provide reassurance as to that organisation's ability to process personal data in line with GDPR's requirements, we do not anticipate that compliance with the Representative obligation is any higher outside Privacy Shield participants.

Our research indicates that many (if not most) EEA-based data exporters do not know that a non-EEA data controller or processor is required to appoint a Representative (because it doesn't apply to EEA companies so the exporter never considered it a relevant part of GDPR), so those exporters are not asking their non-EEA importers to make this appointment, leaving both the exporter and importer potentially in breach of GDPR Article 27.

[2] The report of this research can be viewed here: https://www.datarep.com/wp-content/uploads/2020/10/Privacy-was-it-shielded.-DataRep-October-2020.pdf

In conclusion:

- The obligation to appoint a Representative under GDPR Article 27 is a requirement placed on the data importer in a large proportion of the cross-border transfers to which the Recommendation is intended to apply.
- The existence of that Representative provides significant assistance to any EEA data subject who wishes to exercise their rights against a non-EEA data importer (and also to the EEA Supervisory Authorities when seeking to enforce those rights). Conversely, the lack of a Representative for a non-EEA data importer makes the exercise and enforcement of those rights more difficult.
- Despite this being such a widely-applicable obligation, it remains hidden from most of the companies to which it applies, as a result of:
    - Little advice being provided by the EDPB on this role (outside of guidance 03/2018, which focussed mostly on the applicability of GDPR outside the EEA);
    - EEA data exporters not being aware of this obligation because it simply isn't being discussed in the EEA; it isn't a requirement for companies in the EEA, so they don't know to include it as part of the due diligence on non-EEA data importers; and
    - The smaller non-EEA data importers to which the Representative obligation applies (being companies which aren't large global organisations with a European presence) having fewer resources to appoint a GDPR expert with knowledge of this role
- Appointing a Representative (aside from being an obligation under GDPR) would assist many of the aims of the Recommendation, specifically:
    - The principle of accountability (paragraph 3 etc) – if the data importer cannot be easily contacted, it is more difficult (or impossible) to hold them accountable;
    - The need to ensure processing of personal data is carried out in compliance with the level of protection set by EU data protection law (paragraph 5); and
    - Connected obligation in Recommendation 02/2020 that effective remedies need to be available to the individual.

Recommendation:

- A small amendment to the Recommendation would improve this, adding a paragraph in Section 2.1 ("Know your transfers") along the lines of:
    - *"In addition to the information gathered in the Article 30 records of processing activities, also consider whether the non-EEA data importer meets their other GDPR obligations including, if they have no EEA establishment, the obligation to appoint a Representative in the EEA (pursuant to GDPR Article 27). If, post-transfer, the personal data is not processed by the data controllers or processors in line with GDPR's requirements, the transfer mechanism itself will not remedy any ongoing processing shortcomings."*

If you have any questions about these suggested amendments, or would like to discuss why we believe them to be necessary, please don't hesitate to contact me at the email address linked to the account raising these comments.

Tim Bell

Managing Director
Data Protection Representative Limited (trading as DataRep)