Consultation response:

EDPB recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

TransUnion Information Group Limited

21 December 2020

1. Introduction

1.1. This is a response to the EDPB's consultation on its draft recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. It is provided by TransUnion Information Group and its subsidiaries ("**TransUnion**").

1.2. We broadly agree with the recommended six-step roadmap that organisations should be following in the wake of the Schrems II decision. However, we have some concerns about the detailed advice contained within some of those steps. These are set out under separate headings below, and paragraphs are numbered for ease of reference.

2. Requirement for individual assessments

2.1. As explained in paragraphs 28 to 44 of the draft recommendations, each organisation is expected to perform its own individual assessment of the law and practice in countries to which it sends personal data, and then to keep that assessment under regular review. There are several difficulties with this approach – for example:

(a) This approach imposes a heavy administrative burden on all organisations transferring data on the basis of GDPR Article 46, but the burden will fall particularly heavily on smaller organisations. For many companies with fewer resources it will simply be unrealistic to expect them to perform these assessments at the level suggested by the recommendations. This will leave them with a choice of either disregarding the law or being unable to take advantage of technologies that larger, better-resourced organisations will have available. This can be expected to have a stifling impact on competition, as newer entrants to the marketplace are put at a competitive disadvantage.

(b) This approach will result in different, inconsistent conclusions being reached by different organisations. Those which are willing and able to follow the guidance to the letter will be at a disadvantage compared to those which are prepared to disregard all or part of the recommendations.

2.2. An alternative approach would be to publish clearer guidance about specific jurisdictions – particularly those, such as the United States, where many organisations are likely to be transferring data. That guidance could provide an overview of relevant law and practice in the

relevant jurisdiction, a view from the EDPB on whether and in what respects it fails to provide a sufficient level of protection, and what supplementary measures might typically need to be put in place as a result.

3. Insufficient weight given to the actual risks of the transfer

3.1. Paragraph 42 of the draft recommendations suggests that the assessment of the law and practice in the destination country should focus on the publicly available legislation, and that where this is unclear organisations should "*… not rely on subjective [factors] such as the likelihood of public authorities' access to [the transferred] data …*".

3.2. It is difficult to see why factors such as the likelihood that public authorities will wish to access the data should be disregarded, or why those factors should be dismissed as "subjective".

3.3. This approach would mean that all transfers of data to a particular country must be treated in essentially the same way when in fact they carry very different levels of risk. This runs contrary to the GDPR's principle-based, risk-based approach. It is also hard to reconcile with paragraph 43 of the recommendations, which seems to envisage a broader range of considerations.

4. Impracticality of the recommended measures

4.1. Paragraphs 48, 72, 93 and 95 of the recommendations indicate that contractual and organisational measures will generally not prevent access to data by public authorities in the destination country, and that technical measures such as strong encryption will therefore be required in order to prevent the public authorities from being able to access the data. Furthermore, encryption is said to be ineffective against the public authorities if the decryption keys are held in the destination country or if organisations within the destination country are otherwise able to access the data (see the example relating to the US at paragraph 76). This appears to mean that transfers to a destination such as the US will only be possible where the data is encrypted before it is transferred, and the decryption keys are retained within the EU (or other adequate jurisdictions) and not made available to anyone in the destination country (see paragraph 79 vs paragraphs 88-91). This may be workable in situations where a data importer is merely providing data hosting services, but it would make many kinds of transfer unworkable, for example:

(a) Many processing activities by data businesses involve sending personal data to US-based vendors which then match that information to their own databases and return information about that individual to the originating organisation in the UK / EU. This matching will not be possible (or at least it will not be as reliable) if the data sent to the US cannot be decrypted by the vendor. The data sent to the US would generally be limited to what is necessary for matching purposes (e.g. name, address and date of birth) and so the risk of US security agencies being interested is very low, and the requirement that the data cannot be read within the US is disproportionately disruptive.

(b) For multinational organisations headquartered in the US, information about employees around the world is commonly hosted in the US, and human resources teams in the US need access to that information for staff management purposes. It is difficult to see how those functions can do their job if they cannot access information about EU or UK staff members.

4.2. Issues such as those described above mean that transfers on the basis of adequate safeguards under Article 46 may often be unworkable on the basis of the draft recommendations. If so, then the derogations in Article 49 would potentially be an alternative, but the recommendations (and previous EDPB guidance) say that Article 49 can generally only be relied

on for occasional, non-repetitive transfers. As a result, these derogations are often also likely to be unavailable for many international transfers.

5. Final remarks

5.1. Overall, the recommendations as they stand appear to rule out many simple and commonplace transfers which carry a minimal degree of risk for data subjects. Laws which prohibit harmless activity in this way will tend to bring the law itself into disrepute, and organisations which view this part of the GDPR as unrealistic may be more likely to take a similar view of other parts of the GDPR. Although the EDPB is clearly seeking to achieve a high level of protection of personal data, these recommendations may prove counterproductive to that aim more broadly.

5.2. Additionally, we are concerned that the recommendations will have a substantial impact on cross-Atlantic data flows which facilitate international trade and support the European economy more broadly. In particular, it appears to be effectively impossible to carry out some types of data transfer on which many businesses routinely rely. This will tend to deter international businesses from expanding into or developing their operations in the EU, and may also lead to a reduction in the scope of existing business operations in the EU.