18 December 2020

Access Now's comments to the EDPB consultation on Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Introduction

Thank you for the opportunity to provide comments to the EDPB draft Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world.[1] We work on data protection and privacy around the world and we maintain a presence in 13 locations around the world, including in the policy centers of Washington DC and Brussels.[2]

In our submission, we will provide comments on the following issues:

- The assessment of laws and practices of a third country;
- The supplementary measures; and
- The re-evaluation at appropriate intervals the level of protection afforded to the data transferred to third countries.

The assessment of laws and practices of a third country

Concerning the assessment to be conducted, on a case by case basis, by the data exporter with support from the data importer, to evaluate whether the laws and practices of a third country do not prevent them from complying with obligations under EU law, including the General Data Protection Regulation and specific rules including in data transfers mechanisms, we broadly support the approach taken by the EDPB in the draft recommendations.

Specifically, we support paragraphs 3 to 5, 28 to 30, and 34 to 35 of the draft recommendations. We would also like to particularly highlight our support to paragraphs 42 and 43 regarding the sources that data exporters and importers may use to conduct the assessment.

---

[1] Access Now, https://www.accessnow.org/
[2] Access Now - About Us, https://www.accessnow.org/about-us/

The CJEU requires that the assessment take into account "the relevant aspects of the legal system of that third country" to evaluate the possibility of "any access by the public authorities of that third country to the personal data transferred". It is important to ensure that such assessment is based on the basis of these objective factors. In that sense, we support the language suggested by the EDPB to clarify that the assessment can "not rely on subjective ones such as the **likelihood** of public authorities' access to your data in a manner not in line with EU standards" (emphasis added).

We strongly discourage the use of a so-called "risk-based approach" to conduct this assessment and suggest that the EDPB confirms the need to rely on objective, legal, factors.

The supplementary measures

Regarding the section on supplementary measures, first, we would like to suggest the following modification to paragraph 45:

> *45. If your assessment under step 3 has revealed that your Article 46 GDPR transfer tool is not effective, then you will need to consider, where appropriate in collaboration with the importer, if supplementary measures exist, which, when added to the safeguards contained in transfer tools, could ensure that the data transferred is afforded in the third country a level of protection essentially equivalent to that guaranteed within the EU. "Supplementary measures" are by definition supplementary to the safeguards the Article 46 GDPR transfer tool already provides* ***and to any other security requirements established in the GDPR****.*

Second, we would like to express support for paragraph 70 in Annex 2 and the statement in the executive summary that clarify that if no supplementary measure can ensure an essentially equivalent level of protection for a specific transfer, then such transfer must not happen. It is important to recall that neither these recommendations nor the parallel documents prepared by the European Commission have the objective to allow for each and every transfer but instead to clarify the rules that data exporters and importers must follow to determine *if* and *how* transfer can happen.

Third, we would like to suggest the deletion of the section on "pseudonymised data" under paragraphs 80 to 83. We do not consider pseudonymisation a sufficient safeguard to counter the effect of potential access to data by public authorities in third countries.
Solutions proposed regarding the use of encryption to protect data in transit and stored are more appropriate, although we do recommend adding a note to indicate that it may sometimes not be sufficient to prevent access to data by public authorities that may rely on tools to break encryption.

Fourth, we would like to suggest the following changes to the subsection on "empowering data subjects to exercise their rights" under "additional contractual measures":

*116. The contract could provide that personal data transmitted in plain text in the normal course of business (including in support cases) may only be accessed with the express or **implied consent** of the exporter and/or the data subject.*

117. Conditions for effectiveness:

- *This clause could be effective in those situations in which importers receive **requests from public authorities to cooperate on a voluntary basis**, as opposed to e.g. data access by public authorities that occurs without the data importer's knowledge or against its will.*
- *In some situations the data subject may not be in a position to oppose the access or to give a consent that meets all the conditions set out under EU law (freely given, specific, informed, and unambiguous) (e.g in the case of employees).*
- *National regulations or policies compelling the importer not to disclose the order for access may render this clause ineffective, unless it can be backed with technical methods requiring the exporter's or the data subject's intervention for the data in plant text to be accessible. Such technical measures to restrict access may be envisaged in particular if access is only granted in specific support or service cases, but the data itself is stored in the EEA.*

We strongly caution against the use of "implied consent" and "voluntary cooperation" with authorities as they do not provide adequate protection for users and potentially contradict EU law. In fact, EU law does not recognise the concept of "implied consent" which can be abused and used to force users into giving consent. Finally, access to data by public authorities should be governed by law and have proper safeguards. Suggesting that companies may voluntarily share information with authorities removes the application of safeguards and proper oversight.

The re-evaluation of the level of protection afforded to the data transferred to third countries, at appropriate intervals

Finally, we support the language suggested by the EDPB in the draft guidelines on the need for data exporters, together with data importers, to monitor development in third countries and re-evaluate regularly the level of protection applicable. We therefore support paragraphs 62 and 63.

Final remarks

We appreciate the opportunity given by the EPDB to submit comments to the draft Recommendations 01/2020 and the openness to engage with stakeholders in this process.

We remain available for any questions you may have.

For more information, please contact
Estelle Massé, Global Data Protection Lead (estelle@accessnow.org)