ACT COMMENTS ON EDPB RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA

REFERENCE DOCUMENT

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.

CONTEXT

This paper's aim is to give feedback on the EDPB's draft recommendations and outline the Association of Commercial Television in Europe's views on issues related to international data transfers.

Data is and will increasingly be an integral part of the content production, distribution and monetization process. Data provides broadcasters with important insights on how content is consumed by audiences and helps them make important business decisions around content production, programming and financing, and how to operate and improve our services and enhance the content's value on the advertising market, ultimately benefiting European consumers.

Furthermore, many broadcasters have operations and employees, such as journalists, in many corners of the globe. Modern production (eg. shooting in different locations, third party vendors) and distribution processes imply international activities and cooperation that make unhindered international data transfers essential.

ACT COMMENTS

ACT is worried that the EDPB recommendations in their current state would impose enormous burdens on broadcasters at a time when they are already struggling to deal with the effects of the COVID-19 pandemic. Short of fundamental business reorganization to essentially stop transfers to partners in third countries, which would be impracticable to virtually every organization with both an EU and an ex-EU presence, huge swathes of ordinary business activity would suddenly be potentially non-compliant with the recommendations, and exposed to all the risks that such non-compliance entails.

Lack of risk-based approach. A risk-based approach to GDPR compliance is a core principle recognized by European legislators and regulators. For instance, recital 20 of the European Commission's draft Standard Contractual Clauses encourages organisations to take into account the specific circumstances of the transfer, including, *inter alia*, the nature of the data transferred, the type of recipient, and relevant practical experience about the practices of local public authorities. This is reasonable because higher risk data requires a higher level of protection, and it is disproportionate and unduly burdensome to require the highest standards of security for low risk data, such as a person's name and business email address used for ordinary everyday business communications. However, the recommendations do not reflect this at all. Instead they propose a "one-size-fits all" approach for data transfer impact assessments which effectively rules out transfers of any type of personal data to many countries: para 42 states: "you should […] 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". This is disproportionate and can only lead to a chilling effect on data transfers *overall*. We recommend that the EDPB removes the statement on "*subjective factors*" mentioned above, and that the EDPB's Recommendations empower data controllers to conduct data transfer impact assessments that take into consideration the risk of public authority access (low in the case of the kind of personal data processed by broadcasters) based on the type and sensitivity and volume of the data, the nature and purpose of the processing activity, measures in place to protect the data, the actual number of public authority requests the recipient has received in the past for this type of data and so on. Organisations should be allowed to follow a flexible approach that allows consideration of the risks to the individual and the specific circumstances. This would allow them to effectively allocate their resources and

efforts to ensuring the security of higher-risk or more sensitive transfers, while allowing low-risk transfers (of, for example, business contact information) to continue without interruption.

Data localization. In many instances, the Recommendations would make data transfers of any data (both in the clear and encrypted, with the recipient organization receiving a decryption key) to a number of countries simply impossible (see, in particular, use cases 6 and 7). EU operations and reporting lines would have to be siloed, separate sets of infrastructure and providers would have to be built / bought and company-wide data analytics would likely be out of the question. In addition to being extremely burdensome, in particular for broadcasters with operations spread around the world, this would increase costs almost universally and put broadcasters with operations in the EU at a competitive disadvantage. In many common use cases, such as those involving business contact information, businesses will find themselves in a 'Catch-22' scenario – taking steps to localize processing of anodyne data would be utterly disproportionate to the real risks of processing that data outside of the EEA, but strict compliance with the EDPB Recommendations would permit nothing else. Additionally, and perhaps obviously, the impact of such rules will be to effectively terminate digital trade between countries in the EU and many outside, with all the political, economic, and socio-cultural downsides that would entail. These, very heavy, impacts, point again to the need for data controllers to be empowered to adopt a risk-based approach to their international transfers.

Assessments of hosting countries. According to the guidelines, organizations would have to conduct their own detailed assessments of the legal systems, precedents and practices of third countries. Essentially, they would have to do the work that underpins a Commission's adequacy decision. Mandating such an assessment, regardless of the nature or quantity of the data being transferred, is extremely onerous and disproportionate. First, this requirement should only apply to medium or high risk transfers. Second, even the Commission, with the extensive resources it has at its disposal and the active cooperation of the country being reviewed, takes years to issue adequacy decisions, and does not always get it right – the collapse of Safe Harbor and Privacy Shield are prime examples of how the CJEU can come to a radically different conclusion to that reached by the Commission after years of work. Imposing such an obligation on companies is disproportionate and brings a lot of legal uncertainty – one organisation might reach a wildly different conclusion on a third country's legal framework than another, due to, for example, instructing a different local law firm. This obligation would be anti-competitive at its core, as it would disproportionately impact SMEs who are not equipped to carry out such assessments while favouring larger and better resourced multinationals and tech companies. Instead, there should be exceptions to the transfer assessment process (or at least a streamlined, fast-track process) for low risk data. Additionally, organisations should have free or low cost access to a database of local law assessments at EU level (including a list of countries whose surveillance laws and practices are not adequate), which could evolve as laws and practices change. This would enable organisations across the EU to follow a consistent approach to international transfers.

Overreliance on technical measures. The EDPB Recommendations prioritize technical measures (particularly flawless encryption able to resist state sponsored attacks) over organizational and contractual measures. Technical measures, such as encryption, should be seen as a tool amongst a larger toolbox of measures to reduce the risks of government access to data (which again is low for broadcasters). Organizations should be allowed to rely on a combination of measures, as envisaged by the GDPR. Encryption is not always appropriate, as it is often necessary for data to be accessed in the clear by the service provider or group company in the third country. In the vast majority of cases, this data is of no interest to the intelligence community, and it is disproportionate to require it to be protected by encryption.

Joint liability. Paragraph 134 of the Schrems II judgment states, on the one hand, that the liability for the assessment of the level of protection of personal data lies with the exporter and, in the alternative, with the competent supervisory authority, in cooperation with the importer. Paragraph 142, on the other hand, requires the importer to inform the exporter of his possible inability to comply with the standard contractual clauses. In particular, according to existing and the Commission's draft Standard Contractual Clauses, the importer certifies that it has no reason to believe that the applicable legislation would prevent him from fulfilling its obligations under the contract concluded and commits to informing the data controller as soon as it becomes aware of

changes in its national legislation that may affect the guarantees and obligations provided in the clauses. Therefore, the collaboration of the importer must be deemed instrumental and necessary to verify the level of protection and the liability for failure to verify should be joint between the parties involved. In light of the above, the Recommendations should encompass the specification of the joint liability for failure to verify.

Consultation of the supervisory authority during the pre-contractual phase. In the event of no contractual relation between the parties or in cases where the transfer has not yet been established, non-compliance and/or the impossibility for the importer to comply with the standard contractual clauses would entail the interruption of negotiations, thus preventing the exporter from benefitting of the importer's service, with all the related damages, including economic ones. In particular, when negotiating with large non-European players and in the event of non-equivalent levels of data protection, data exporters could face severe difficulties in identifying valid alternative products/services: while the interruption of the pre-contractual phase in the absence of adequate guarantees for the transfer abroad protects personal data, it also reinforces the regulatory imbalance between the parties. For this reason, exporters should be explicitly granted the right to refer the matter to supervisory authorities already during the pre-contractual phase.

Entry into force. Even though the Recommendations are soft law they would essentially be binding. Complying with them will require significant time and monetary investments for companies to adapt their operation and renegotiate their contracts. We would therefore suggest a transition period to give companies sufficient time to adapt.