EBU

OPERATING EUROVISION AND EURORADIO

17 December 2020

EBU STATEMENT ON EDPB DRAFT RECOMMENDATIONS 01/2020 ON SUPPLEMENTARY MEASURES:

INTERNATIONAL DATA TRANSFERS NEED A FLEXIBLE AND RISK-BASED APPROACH

The European Data Protection Board draft recommendations 01/2020 on “measures that supplement international transfer tools to ensure compliance with the EU level of protection of personal data” provide useful further guidance on how to comply with the CJEU ruling in Schrems II.

However, practical implementation of these recommendations will be very difficult for organizations. A major challenge is that it is organizations themselves, and not the European Commission (EC) and/or national regulators, that must do due diligence assessments of third countries’ local (surveillance) laws. This is onerous and it risks not being effective. Much will depend, for example, on how good - or bad - data importers are in providing data exporters with the “relevant sources and information” about the third country legal regime (unless there is an EC adequacy decision). It would be far more efficient and useful if those assessments were carried out by the EC or the EDPB and published in a database, or at least if standard checklists and questionnaires, were made available to organizations.

What’s also important is that when carrying out their due diligence assessment of data exports to third countries, controllers and processors can take into account the type of personal data and processing activity in question. Not all data is equal: some personal data are more sensitive than others and would thus require stronger safeguards. Where the data and processing activity relate to a rudimentary standard business process (for example non direct identifiable personal data such as cookie or user ids for analytical purposes) that is unlikely to be of interest to a State security agency or to present a risk, then that should inform the due diligence assessment, the necessity for supplementary measures and what those supplementary measures may be. Controllers and processors should also have some scope for a more subjective/flexible assessment of third country authorities’ interests in sets of data.

Some technical and contractual measures mentioned by the EDPB do not seem very realistic and effective for data access by public authorities and for organizations that routinely transfer data as part of their activities. End-to-end encryption or pseudonymization of all data in international data traffic seems almost impossible to implement. Furthermore, insufficiently concrete answers are provided in particular regarding measures for data transferred to a cloud service provider (including cloud storage) outside the EEA.

For GDPR compliance, the EDPB and regulators throughout the EU have been calling for organizations to take a “risk-based approach”. It now seems that for international data transfers, the EDPB is departing from this and has a more restrictive approach than the European Commission’s revised Standard Contractual Clauses and "modular design" (which includes for example information duties clauses such as “as far as” and “as much as possible").

EUROPEAN BROADCASTING UNION
L’Ancienne-Route 17A
PO Box 45
1218 Le Grand-Saconnex
Geneva, Switzerland
Tel. +41(0)22 717 21 11
www.ebu.ch

Indeed, it is worth noting that in the EDPB Guideline 4/19 Data Protection by Design and Default, the word "*risk*" appears many times whereas the word "*risk*" appears only four times in the recommendations 01/2020.

The current guidance is complicated and will require focus and considerable effort to result in transfers that are compliant. The EBU therefore urge the EDPB to adopt a more flexible and risk-based approach and outline more realistic and proportionate technical measures for companies to work with.
