EGTA – EUROPEAN ASSOCIATION OF TELEVISION AND RADIO SALES HOUSES

Response to the public consultation on the draft Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

---

Egta, the Association of Television and Radio Sales Houses is the media trade body for television and radio advertising, representing 155 companies in Europe and beyond.

Egta members come from both public and private sectors and cover respectively 75% and 50% of the total TV and radio ad spend in Europe.

Contact: *Conor Murray, conor.murray@egta.com*

International data transfers are today integral to the day-to-day operations of many European broadcasters and the sales house which sell their advertising inventory.

First, many of our members' operations extend well beyond Europe. These companies, therefore, need to export personal data to foreign markets for internal purposes such as HR administration or day-to-day business operations (calls, virtual meetings, calendar sharing). Companies may also have outsourced some specific activities (IT maintenance, purchasing) to companies outside Europe which could involve similar data transfers.

Second, digital advertising, be it personalised or contextual, requires the intervention of tech intermediaries (ad servers, supply-side platform, ad exchanges) which are often based outside Europe.

In this light, broadcasters and their sales houses would like to flag some aspects of the draft Recommendations 01/2020 (the "Recommendations") published by the European Data Protection Board (EDPB) which they fear will at best create uncertainty and an additional burden for European businesses at a time of economic difficulties. At worst, the Recommendations would push businesses into making an unpalatable choice between fundamental business reorganisation to stop transfers to partners in third countries or potential exposure to non-compliance with the Recommendations for huge swathes of their business activities, much of which will only involve anodyne or otherwise benign personal data.

THE LACK OF A RISK-BASED APPROACH

The Recommendations pull away from the risk-based approach enshrined in European data protection law (see, for instance, Article 35 GDPR or Recital 20 of the draft implementing decision for the new Standard Contractual Clauses) by refusing to distinguish between high and low risk data transfers involving different types of data. This approach will overburden businesses and indiscriminately restrict the international flow of data by demanding that benign categories of personal data (such as business contact information like email addresses and phone numbers) must be treated equivalently to highly sensitive personal data.

For many businesses, this approach is illogical as many types of personal data processed internally for HR, day-to-day business operations and communications carry little risk for the data subject and could and should instead be dealt with under a more flexible framework. Overall, it makes little sense to equate transfers of these types of data with, for example, transfers of higher risk data (e.g. large volumes of special category data) where the potential impacts on data subjects are much greater.

The absence of this differentiation between high risk and low risk data will inevitably make the transfer of personal data extremely difficult for companies. In many common use cases, such as those set out above involving anodyne data, businesses will find themselves in a 'Catch-22' scenario - taking steps to localize processing of that 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. This points to the need for data controllers to be empowered to adopt a risk-based approach to their international transfers.

We recommend that the EDPB removes its statement at para 42 of the Recommendations that "*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*" and that the Recommendations instead empower data controllers to conduct data transfer impact assessments that take into consideration the risk of public authority access 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, and the actual number of public authority requests the recipient has received in the past for this type of data.

ASSESSMENTS OF HOSTING COUNTRIES

The expectation set out in the Recommendations that data controllers must conduct their own detailed assessments of the legal system and practices of third countries (essentially a "mini-adequacy assessment") is onerous, unrealistic and disproportionate. These assessments should not be necessary for low-risk data transfers, and if these assessments must be carried out in every case by the individual data controller, the only result will be legal uncertainty, as one organisation might reach a wildly different conclusion for the same transfer to the same third country based on its choice of a different local law firm. The extra legal and administrative burden imposed by these assessments would also disproportionately impact SMEs in comparison to larger companies who have the resources to carry them out effectively. Instead the Commission or the EDPB should maintain a database of adequacy local law assessments at EU level, which could evolve as laws and practices change, and freely available to organisations. This would enable organisations across the EU to follow a consistent approach to international transfers.

STRICT TECHNICAL STANDARDS

The EDPB also adopts a particularly strict approach with regard to the technical measures which companies would need to put in place in order to abide by recommendation 01/2020 (cf use cases 6 and 7). In particular, the use of encryption that can resist state sponsored cryptanalysis attempts is highly questionable for benign personal data which in itself carries little risk to individuals. This approach disregards the daily operations of international organisations which require constant interconnections and data flows across frontiers. Encryption should be used according to the type and sensitivity of the data, the likelihood and the severity of potential threats and the role of the organisation as a controller or processor. Oher technical, organisational or contractual measures should be implemented for situations with a low level of risk.

POTENTIAL IMPACTS:

- A large range of ordinary business activity could be considered non-compliant if they did not imminently cease many of their transfers outside of the EEA (including transfers of anodyne and low-risk data); this in turn will create extensive administrative work, external costs and operational adjustments for EU and non-EU businesses.

- It also imposes significant barriers to international trade, with the potential consequence that companies would have to localise their data in the EU and operate in silos. This could undermine the economic attractiveness of the EU and endanger its competitiveness while businesses are struggling in the midst of a global pandemic. At worst, the impact of the Recommendations would 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.

- Broadcasters with an international footprint could see their operations severely hindered, their costs increased and their revenues negatively affected.