ID Register: 52431421-12

Telefónica Comments on the EDPB
Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Introductory Comments

Telefónica welcomes the opportunity to make comments to the Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data ("the Recommendations") and to EDPB´s intention to "*provide controllers and processors, acting as exporters, with recommendations on the process they may follow to identify and adopt supplementary measures.*". We do believe that this is an important exercise to provide the necessary certainty about the identification of additional measures to the safeguards of the intentional data transfer tools regulated in the Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016, the General Data Protection Regulation ("GDPR").

International data flows are essential in today's digital information society. The covid-19 crisis has proven more than ever that data transfers are critical to keep economy moving, societies functioning and citizens safe. The vast majority of data is part of a communication process and cannot be excluded of the digital flow. This is the interconnected world in which economic operators work. This interconnectedness needs certainty so that economic operators can devote themselves to what they do: educate, heal, protect, communicate, sell. The proper functioning of the economic flows requires a regulatory environment that generates legal certainty and, at the same time, responds with practical solutions to the real needs of the stakeholders involved in the digital ecosystem. This legal certainty is also necessary for Supervisory Authorities and more importantly for citizens.

With these comments, it is Telefónica's interest to foster a practical approach to the matter, allowing to comply with the Court of Justice of the European Union's judgement C-311/18 and, at the same time, having a toolbox that provides practical solutions for data controllers and processors across the EU.

As it could not be otherwise, the basic principles of the aforementioned European Court of Justice (ECJ) judgement on Schrems II stressed GDPR underlying philosophy

regarding the need to ensure that the **protection granted to personal data by GDPR must travel with the data** when it is transferred outside the European Union and the European Economic Area.

The Court follows by stressing the important role of organisations exporting data, but also of Supervisory Authorities, as both are responsible for verifying that the Law and practice of third countries will not undermine the level of protection of the transferred data. However, EDPB departs from ECJ view's and wrongly suggests that this duty falls almost exclusively on the organisation exporting data. This duty can turn to be a disproportionate burden for EU private companies in the digital and global economy in which they operate, limiting their freedom to conduct a business, right to free competition, development and innovation of their products and services, and all other principles, rights and freedoms that guide the EU.

The American *Big Tech* companies are a main and necessary actor in the EU economy, acting as partners, clients and/or suppliers of such EU private companies in a relationship and negotiation model, in many cases, of imbalance. This fact must be taken into account by the *Supervisory Authorities* when they participate in their aforementioned duty of verifying whether the level of protection of the data transferred to these data controllers, processors or other recipients in third countries is adequate. Normally, this assessment of adequacy was ensured by European Commission with Adequacy Decisions confirming the level of adequacy of a given country.

Therefore, we strongly call for European Commission to work on new Adequacy Decisions, confirming the existing ones and, more importantly, addressing new Data Protection frameworks adopted in multiple geographies in the last years. These efforts will ease the burden put on private companies when they need to continue exporting data.

1. A risk based approach

As already stated by the EDPB, the approach to international data transfers in light of the ECJ ruling, must be understood around the principle of accountability under Recital 76 and article 5.2 of the RGPD. In accordance with this principle and the risk based approach as fundamental basis of the practical track for GDPR compliance: "*The likelihood and severity* (impact) *of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk".*

Consequently with the risk based approach, we do not agree with EDPB statement which considers that likelihood of public authorities access must not be considered when carried out an assessment of the transfers. Likelihood of a potential event that may cause a negative impact to the rights and freedoms of data subject, together with the evaluation of the impact, are the main factors to evaluate risks, and take

accountable decisions under the GDPR. This is the corner stone of the principle of accountability. This evaluation consists on identifying risks based on impact and the probability of occurrence of the potential harmful event. Once evaluated the risks, assessment must be done with the objective of identifying proper measures to mitigate such risks, which could apply to each dimension of impact or probability or both. In this sense, it is not the same the impact depending on the characteristics of the data such as sensitivity, publicly available/private data or the position of data subjects.

In this sense, the European Commission's draft Standard Contractual Clauses, to be adopted early 2021, are more aligned with GDPR's risk based approach and accountability principle and recognise the importance of taking into account any relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from Public Authorities received by the data importer for the type of data transferred.

Therefore, we kindly ask EDPB to consider the risk based approach as a proper way to evaluate the impact of a data transfer as already it's used when evaluating different aspects of data processing activities, as happens for example when assessing security privacy risks. Such risk approach must be based on different factors such as type of data, availability, characteristics of data subjects, confidentiality of the information potentially accessed, transparency and data subject control, alternative access mechanisms for authorities, etc. EDPB Recommendations should better acknowledge the role of data exporters in line with GDPR and ECJ case law, which is basically to ensure a high level of data protection for data subjects, by minimizing risk in the most efficient manner according to a risk assessment and accountability principle.

2. Non-technical measures

According to the Recommendations, contractual and organizational measures must be always accompanied by technical measures. Additionally, the Recommendations consider that only few technical measures (basically, encryption) can be applicable in very limited cases, according to the use cases in the Recommendations. We consider that organizational and contractual measures must play a more important role in mitigating risks associated with potential access from public authorities in third countries. The combination of proper technical, organizational and contractual measures must be identified by the data controller and data processor accordingly with the risk analysis, but without limiting a priori the application of each one in the combined solution.

Conclusion

Telefonica understands that in order to provide practical solutions to international data flows, EDPB Recommendations should be aligned with the risk based approach supported by the GDPR and reinforced by the interpretation of the ECJ, which must apply to any type of impact to the rights and freedoms of data subjects without exempting international transfer rights from such approach. In addition, encryption is a concrete measure that could be applicable in a very limited use cases, but we should not generally conclude that no other measures can be suitable to mitigate the identified risks.

18th December 2020