Answer to the EDPB consultation

Critical Points of the draft EDPB Recommendations on international transfers

Whether engaged into BtoC or BtoB business model, most of European companies undertake commercial activities around the world and rely on a worldwide footprint of affiliates and suppliers to this purpose. Common tools are deployed for various purposes: HR, marketing, communication, production etc. Significant data flows are generated in this context within this footprint.

The draft EDPB Recommendations would require on top of transfers mapping, the businesses to assess the surveillance laws of the country in which they export the data against certain European Essential Standards as published by the EDPB in order to determine whether additional technical means are required. Very strict technical protection would be required for countries not meeting these standards.

This raises a number of very critical issues:

- The first issue is that **the country assessment can't be reasonably expected from the businesses** due to the nature of the work (high profile legal assessment of the importing country laws); on this ground, even the EU Commission has been sanctioned by the Court of Justice through the Privacy Shield invalidation. How to expect that this work is now done by the various businesses?
- The second issue is the **volume of work** that the Recommendations would generate in term of mapping details, country assessment and technical protection implementation. All these combined would generate a very heavy legal and technical workloads generating huge costs for big companies. This is even more obvious when considering mid or small companies, which form the bulk of the supply chain.
- The third issue which **is very critical** is that the systematic implementation of technical measures in countries not meeting the European Essential Guarantees will make the **transfer not legally feasible where the data needs to be available in the clear for the data importer**. Under use cases 6 and 7 the data shall remain encrypted and not be available in the clear. Most of intra-group transfers in the above countries would then be impacted while access in clear is needed for global company business continuity. Thus a blocker as to the operating model of **most** European companies with international footprints.
- Finally, it seems that these requirements would apply **whatever the data/ processing sensitivity**. Use cases 6 and 7 are indeed totally irrespective of the data sensitivity. The above requirements would then apply to names, e-mail addresses, which by nature are required just to be able to communicate. This is exchanging personal data at all which would be made almost impossible, even basic profile business personal data while a must in this digital age for business companies

Finally due the above reasons, the Recommendations as drafted would be **a very disruptive and dramatic obstacle for the management and the development of the European businesses around the world**.

More detailed criticisms and proposals:

1. Technical measures shall be required for the most sensitive data/ processing

Articles 24 and 25 of the GDPR refer to technical and organisational measures taking into account the **nature**, **volume** and **risks** of the data for the data subjects. State of the art and costs are also to be taken in the context of Privacy by Design. The data controller is responsible to apply a protection proportionate to the data at stake (nature, volume, purposes etc.).

1.1 Imposing technical measures such as encryption for all transfers to countries not meeting the EEGs goes therefore **beyond the terms of the GDPR requirements**. This would raise a legal issue. Arguably only a GDPR amendment could come to this result. Despite the fact that the Recommendations would not be directly enforceable, it is clear that all GDPR data protection authorities will rely and apply the Recommendations in their legal assessment and decisions and that this Recommendations would therefore have in practice legal effects although indirect.

1.2 Imposing technical measures such as encryption in particular for the transfers to countries not meeting the EEGs would also disregard a **fundamental principle of data protection and the GDPR: the protection should be proportionate to the risks**. This proportionality is expressed in all articles related to the protection of the data: articles 24 and 25 of the GDPR. The Recommendations can't just ignore this fundamental principle. Nature, purpose, volume and risk triggered by the data is only considered in the Recommendations for the country assessment while taken into account in the EU Commission SCC draft (see §1.4).

1.3 Applying technical protection under such strict conditions as defined in the Recommendations (Use Case 6 and 7: data not to be available in the clear at all in the importing country) **would make a multitude of transfers with no purpose any longer**. Why exchanging the data, if the data cannot be read on the other side? Intra-group transfers are immediately impacted as well as any exchange which would be necessary for business operations. Even intra-group intranet platforms for transnational communication with the employees would be hardly operable. Article 49 cannot obviously offer a reliable alternative channel for communication.

1.4 The Recommendations and the SCCs draft as issued by the EU Commission do not match, creating a dilemma for the data controllers/ processors. The new SCC draft, provides that **technical protection shall be "*considered … where it does not prevent fulfilling the purpose of the processing*"** suggesting that other means are possible and that the availability of the data in the clear may be needed and satisfied. Shall the various businesses apply the Recommendations or the SCC approach when considering their transfers ? We would suggest that the EDPB aligns with the EU Commission approach.

2. Country assessment by the data controller must not be responsibility of the data controllers

2.1 Assessing whether local surveillance requirements or powers are limited to what is necessary and proportionate in a democratic society, is an **extremely difficult** appreciation/ assessment, despite the European Essential Guarantees for Surveillance Measures, dated 10 November 2020, published by the EDPB. Requiring each business/ company to undertake this task in respect of its own processing will come to 1) the assessment not being done since requiring resources not available in many companies (competences, proper information availability, budget); 2) if work done, very inconsistent results across the players for similar countries and processing; 3) in all cases a huge workload and heavy costs

considering the numerous countries to cover for most businesses and the need to undertake/ update the assessment for each transfer ; 4) creating obstacle to the competitiveness of the European players.

2.2 The absence of clear reference regarding the countries critical in respect of personal data protection will also create a **major legal security issue** which combined with the possible several interpretation by the data authorities across Europe will not be manageable for businesses.

3. A guidance specific to cloud services is needed

Exhaustive mapping of the international transfers in the context of the cloud providers very evolutive and complex supply chain is not feasible without such providers being addressed and made specifically responsible.

Similarly in this context, maintenance services may require in certain instances access to the data: the full protection of the data not being readable would require the services to be relocated in Europe, triggering a major renegotiation with the providers and requiring their consent. This would require that the cloud providers are legally and directly bound by the same obligations. The SCCs are helpful in this respect but will take time to be effective, and **EDPB specific Guidelines** would certainly help both the final result and the SCCs to signed/ implemented quickly.

Proposal:

The Recommendations need to better and more realistically reflect **a risk-based approach orientation** regarding determination of the protection additional to the BCRs and SCCs. In the current form, the Recommendations may appear as not proportionate as it would jeopardize the possibility to exchange personal data at all in certain countries and thus the business continuity. The risk-based approach orientation would better align the Recommendations with the spirit and letter of the GDPR and of the EU Court of Justice Schrems II judgment while keeping a strong control of the cross-boarder transfer with appropriate level of protection adapted to the risk. This would also reconcile the Recommendations and the new SCCs.

Clearer top down determination of critical countries is also needed since the EEGs alone would create an absence of legal security and the situation would not be manageable for the European companies.

A specific guidance should be set out with respect of cloud services, where transfer mapping are by definition very difficult to implement.

Finally the Recommendations in the current form would generate a heavy and costly workload resulting from the combination of exhaustive and detailed transfer mapping, countries assessment and the technical protection implementation. This would as a minimum require a grace period of one year.

***