December 2020

Consultation on recommendations on supplementary measures of EDPB

MEDEF Comments

MEDEF

By its decision of July 16, 2020 (Schrems II), the Court of Justice of the European Union (CJEU) invalidated the decision of the European Commission of July 12, 2016 which recognized the possibility of transferring personal data to the United States within the framework of the *Privacy Shield*, noting that American laws allow unrestricted interference by public authorities for reasons of national security and public interest.

This decision also called into question the processes of data transfers to non-EU countries more generally insofar as supplementary measures should be put in place for transferring data, where usual mechanisms (such as *Standard Contractual Clauses* or *Binding Corporate Rules*) do not guarantee a level of protection equivalent to the General Data Protection Regulation (GDPR), with regard to the applicable law.

In an increasingly international and digitized context, and with the approach of Brexit in particular, it is essential for companies **to quickly have a stable, secure and efficient legal solution that enables them to maintain and continue personal data transfers to third countries**, especially since the standard contractual clauses remain the tool most used by companies for data transfers[1].

It is also essential for companies to have proportionate mechanisms, based on the key principles of the GDPR and taking into account political, judicial and above all economic realities. However, as it stands, the draft recommendations of the European Data Protection Board (EDPB) do not meet these objectives and raise serious concerns for businesses.

Questions on the adoption of recommendations instead of guidelines

- ✓ The EDPB has chosen to adopt recommendations and not guidelines. Considering this choice, it is important to determine whether these recommendations are destined to guide organizations in the practical arrangements to be put in place or if the measures presented are prescriptive and considered as such by national authorities.

- ✓ The form of the draft recommendations is very appreciable in that it presents in a practical way the actions to be followed in 6 steps, thus allowing companies to clearly visualize the process that they must put in place.

A disproportionate draft recommendation compared to the GDPR

• An analysis of national laws which should be the responsibility of institutions

Steps 3 and 4 of the draft recommendations consist in analyzing the applicable foreign law in order to put in place the appropriate measures according to the risks associated with that country. However, while governments have the capacity to conduct precise analyzes to determine which law is applicable and if the country offers sufficient guarantees, companies are not sized to analyze foreign laws, especially if they are not present in these countries. This analysis of the applicable law even becomes almost impossible for an SME that does not have sufficient resources or even when a big company has to process data in several third countries. For example, postal operators would have to carry out these assessments for all third countries.

An assessment of national laws of third countries that would be realized by companies (or external advisers) would place too much responsibility on them insofar as it must emerge from this assessment the definition of appropriate measures to be put in place.

The study of the national laws of third countries must remain the responsibility of the authorities (European Commission or EDPB) for a homogeneous application of the rules and greater legal certainty for companies or organizations exporting data, as is already the case for European Commission adequacy

[1] Survey realised by BusinessEurope and Digital Europe in October / November 2020.

decisions. Putting such an obligation on companies is seen as a waiver of the authorities to assume this burden.

- **A necessary return to the risk-based approach**

While **the GDPR adopts a risk-based approach by giving accountability to companies and allowing them to carry out analyzes of their needs and risks to adopt the appropriate security measures or guarantees**, the draft recommendations question this risk-based approach. However, this approach is fundamental for a company because it makes it possible to assess the risks to its activity and to choose a solution that corresponds to its needs. **By imposing measures to be put in place, this deprives companies of their freedom of choice of their co-contractors**.

Indeed, the adoption of expensive and not necessarily appropriate technical measures could discourage a company from contracting with a service provider located outside the EU because of a cumbersome and costly process. The company could therefore no longer decide on the policy and governance for the data it holds since it is thereby constrained in the choice of service and provider.

Risks have to be assessed on a case-by-case basis and to include the likelihood of an access request and interference by a foreign government. It is up to the company to take into account the sensitivity of the data concerned and the measures to be put in place to protect the data it holds according to the needs.

The EDPB has adopted a very strict approach by considering that data transfers to third countries should not take place (or under conditions almost impossible to implement) if the intelligence laws of these countries are not compatible with European standards.

However, it is important to stress that **the European Commission understands that data transfers to third countries are not without risks, but considers that it is up to the company to decide to take the risk while putting in place appropriate guarantees**, it being specified that all the measures taken will in no way put an end to the incompatibilities of laws.

T**he draft recommendations do not distinguish between purposes or the different categories of data** (paragraph 42). This differs from the general approach taken by the GDPR which makes a distinction between the processing of "classic" personal data from the processing of "sensitive" personal data (art 9). Likewise, the GDPR also recognizes that security risks, to which personal data is subject, and the measures to be defined and be put in place accordingly vary depending on the nature of the data, the sensitivity of this data and the risks for the data subjects.

- **Too strict measures and unrealistic expectations**

The draft recommendations set out technical measures as a keystone, to the detriment of organizational or contractual ones.

Indeed, the draft, especially paragraph 48, establishes the primacy of technical measures over organizational and contractual ones when the national law of a third country allows public authorities to access data, without appropriate guarantees.

However, **technical measures, such as encryption, are costly, difficult to implement and do not necessarily prevent access by foreign public authorities to data, nor the problems of incompatibility of laws** and therefore of contradictory obligations to which companies are subject to.

- ✓ Technically difficult measures to put in place: all technical measures are not effective in the same way. For encryption, the EDPB recommends encryption where only the customer has the data decryption key ("*Bring your own key*"). This poses the problem of the use of its data by the customer with an external service provider. In this case, a company that exports data is compelled to implement encryption and decryption mechanisms independent of the latter (if the customer wants to have this data at all times). Such a system would entail **very significant additional software development costs** for data exporting companies. It is therefore generally reserved for the most sensitive data from both data protection or economic points of view. Indeed, although

the encryption remains the most relevant option to protect data, this solution is very expensive and unsuitable for certain types of data and certain business models.

- ✓ Costly measures: likewise**, these technical solutions and in particular the encryption mechanisms which are not "off-the-shelf" imply high costs for the companies** exporting data, especially if this must be done constantly. Encryption costs include both the service purchase and the interoperability with the entire IT system of the company. These costs will have consequences for all actors wishing to store data. **These mechanisms are therefore not within everyone's reach and requiring the use of such measures would severely penalize the smallest structures**. SMEs will prefer to take basic off-the-shelf encryption measures, **which are less expensive but technically insufficient**, as they cannot afford such additional costs for their data.
- ✓ Measures that do not correspond to operational realities: imposing the use of technical measures does not take into account technical, operational and economic realities and permanent data encryption would make certain operations impossible.
  - ➢ On the one hand, encryption can run against security concerns as end-to-end encryption prevents a vulnerability from being identified. The temporary decryption of data allows the analysis of this data and thus to carry out **imperative security checks**. For example, certain IT security processes, such as data packages inspection, are necessary in preventing malicious traffic and DDoS attacks.
  - ➢ On the other hand, partial decryption of data is necessary for essential operations. It allows **the implementation of software functions** (*Software as a Service* / SaaS) related to data, for example the suggestion of a file stored in a cloud based on a meeting of a calendar recorded on the same cloud. These services are included in the offers proposed by companies that export and manage data.

Finally, it is **difficult for a company to ensure a total foolproof encryption over the long term**. However, use cases 1 and 3 of the EDPB recommendations use the term "flawless" which could be dangerous in terms of responsibility for companies exporting data.

Thus, **while encryption is necessary for the most sensitive data, it should not be systematically imposed on companies in the transfer of personal data outside the EU. Again, applying the risk-based approach, it is up to the company to determine the data and circumstances that require encryption**. In some cases, the encryption is simply not suitable for processing because the data must be transmitted in the clear.

By imposing measures that cannot be realized in practice, both for SMEs which do not have sufficient resources and for companies which will not prefer to risk sanctions, **the draft recommendations of the EDPB do not encourage to use standard contractual clauses, or even questions the usefulness and the very principle of the SCCs of the European Commission. This will have the effect of slowing down the development of French and European companies internationally.**

It is therefore essential that the EDPB grants greater flexibility to companies in the implementation of data transfer mechanisms outside the EU in order to offer sufficient legal certainty to companies.