AMAFI's CONTRIBUTION TO THE EDPB RECOMMENDATIONS 01/2020 OF 10 NOVEMBER 2020

MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA

About AMAFI. The Association française des marchés financiers (AMAFI, herein also referred to as "we") is the trade organisation working at national, European and international levels to represent financial market participants in France. It mainly acts on behalf of credit institutions, investment firms and trading and post-trade infrastructures, regardless of where they operate or where their clients or counterparties are located. AMAFI has more than 150 members operating for their own account or for clients in equities, fixed-income products and derivatives. Nearly one-third of its members are subsidiaries or branches of non-French institutions.

AMAFI welcomes the European Data Protection Board's recommendations 01/2020 (the "Recommendations"). We do much appreciate the opportunity to give feedbacks on the recommendations as the ongoing interaction between public authorities and market participants is of paramount importance.

First of all, and before responding to the various points raised in the document submitted for consultation, AMAFI would like to highlight three aspects on which some comments or clarifications appear necessary.

Although the Recommendations are issued under art. 70.1(e) of the GDPR[1], as recalled in whereas 8 of the recommendations, it is not entirely clear to us what the legal status of the recommendations is: are they enforceable in a court of justice or a guideline for future regulation?

Furthermore, it is currently not entirely clear how else the feedback will be used. In addition to possible amendments to the Recommendations, will the input be used to provide the EU Commission, for example, with advice on future legislation?

Moreover, important legal uncertainty results from judgement C-311/18 of the Court (Grand Chamber) of 16 July 2020[2] ("Judgement Schrems II" or the "Judgement"). They are well reflected in the recommendations and we much appreciate the EDPB's contribution in addressing them. The comments that we will make are largely related to the current legal uncertainty. Whilst neither the GDPR rules should be called into question, nor market participants' obligations to safeguard data, participants are currently between a rock and a hard place. Therefore, AMAFI stresses the urgent need to develop, within the European Union, European technological solutions for the storage and exchange of data. While European market players have strong needs and constraints in terms of data retention[3], we regret that there is currently no

[1] Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
[2] Judgement C-311/18 of the Court (Grand Chamber) of 16 July 2020
[3] Many regulatory texts require that certain data be kept for a certain period of time. This is notably the case of Article 7 of Delegated Regulation (EU) 2017/584, according to which trading venues must keep for at least five years a record

economically and technically viable European alternative to the to the solutions proposed by a few very large non-European suppliers, most of which are now established in the US, especially since in the situation resulting from Judgement Schrems II, exporters and importers might be required to "*suspend the transfer and/or terminate the contract*" (*par. 5 and 52 of the Recommendations*).

It is why AMAFI would like to make the following introductory comments in relation to the consequences of the Judgement and on the recommendations.

We cannot but welcome the Board's statement that the protection granted to personal data in the European Economic Area must travel with the data, wherever it goes and a transfer of personal data to third countries cannot be a mean to water down the protection offered in the EEA. However, the invalidation of the EU Commission implementing decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-U.S. Privacy Shield[4] does raise two types of questions.

- The necessity to develop European technological solutions

The first comments are related to current arrangements under which data is transferred outside the UE. It seems needless to insist on the large share foreign companies, notably American ones, hold in the global business of maintaining, protecting, and treating data of all sorts. This must be read against the numerous obligations put upon financial institutions to maintain data for periods of time up to 10 years. In the immediate aftermath of the Judgement, very few, if any, alternatives exist. At the scale of entire businesses, current arrangements are at risk.

Pending clarification of any kind, including the introduction of proportionality[5] into the foreign laws governing data protection, financial institutions, acting as data exporters, tend to take a "risk based approach" under which on a case by case basis, in consideration of the type of data, the legal environment of the third country or the likelihood to renegotiate terms and conditions with service providers, a decision is taken on the transfer of data. This leads to disparities among institutions and a fractioning of data treatment regimes.

Therefore, AMAFI warmly welcomes the intervention of European authorities to bring harmonisation and clarification of data transfer regimes. In the meanwhile, a temporary solution must be found to the mismatch between the strict obligations under GDPR and financial legislation and the fact that no European solutions exist.

- Legal uncertainties resulting from the Schrems II judgement

The second comments are related to the way forward for the other jurisdictions for which adequacy decisions exist. The Judgement reveals the legal uncertainty resulting from the current system of adequacy decisions under art. 45 of the GDPR. Twelve countries have been recognised by the EU Commission as offering an adequate level of data protection[6] pursuant to that article. Whilst we wish for the motivations of the CJEU in the Judgement to be verified in the existing adequacy decisions, for the time being, each of the adequacy decisions could potentially be invalidated, thus shifting the subject entities to the regime provided for under art. 46 of the GDPR.

---

of certain elements including the retention of personal data. EMIR (n°648/2012) and MAR (n°596/2014) Regulations also include such obligations (EMIR, art. 9 and 29 governing retention of personal data for a period of 5 to 10 years) (MAR, art. 28 governing personal data to be retained for a minimum of 5 years) as well as numerous European and national regulations. We therefore stress the need, with a view to protecting personal data, to have solutions adapted to these obligations, which are as numerous as they are complex to implement.

[4] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, decision no longer valid,

[5] The lack of proportionality is the reason why the CJEU invalidated the EU Commission's privacy shield implementing decision. Point 178 of the Judgement C-311-/18 of the Court of 16 July 2020

[6] Adequacy decisions on the basis of article 45 of Regulation (EU) 2016/679

The immediate invalidation of the legal regime under which data is transferred to cloud service providers, for example, and the swift to the art. 46 legal regime creates such a risk that exporters might want to act conform article 46, even in the case where data is transferred to one of the twelve counties that benefit from an adequacy implementing decision. Here again, financial institutions might individually take complementary measures, such as pseudonymisation or cryptography.

Our main observations are as follows:

- We seek for a grace period for businesses to implement all relevant procedures and measures in a sufficient period of time.
- AMAFI recommends the EDPB to introduce in its recommendations a risk-based approach, with more nuanced analysis of the kind of data involved in a transfer and the risks associated with such transfers.
- More flexibility in the proposed scenarios/use cases. Businesses need to be able to adapt in their settings the measures that are being proposed. In order to do that, AMAFI would welcome a sectorial approach which would better fit each business.
-

We fear that the burden placed on the data exporter to assess on a case-by-case basis, the level of adequacy of a third country's law to the GDPR, might result in a multitude of divergent interpretations from institutions and would create legal uncertainty and a high risk of fragmentation (different assessment of one jurisdiction).

1. STEP 1: KNOW YOUR TRANSFERS

AMAFI has no comment on this section.

2. STEP 2: IDENTIFY THE TRANSFER TOOLS YOU ARE RELYING ON

As pointed out in the introduction, the current legal uncertainty might lead institutions to ascertain in any case compliance with articles 45, 46 and, to the extent possible, 49 of the GDPR, whilst in the same time also taking fragmented approach.

3. STEP 3: ASSESS WHETHER THE ARTICLE 46 GDPR TRANSFER TOOL YOU ARE RELYING ON IS EFFECTIVE IN LIGHT OF ALL CIRCUMSTANCES OF THE TRANSFER

Par. 28 and following of the recommendations, in conformity with the GDPR, require transferors and exporters to ascertain the effectiveness of any safeguard or procedure that is put in place, pursuant art. 46 of the GDPR. This means that any safeguard, including the mapping exercise that the EDPB mentions in par. 8 and following, and no matter how watertight it is, it is always liable to ex post sanctions when it turns out that it was not effective.

Here we regret that the standard against which the effectiveness is measured is the EU Charter of Fundamental Rights (*whereas 1 and par. 37*). This text proclaims common values, expressed by the EU institutions, and we would expect this to be a valuable guideline for legislation, not a text that is directly enforceable against European citizens and companies. In any case, the EU Charter of Fundamental Rights is so broad a text that it puts the transferor is the position of a guarantor of the effectiveness, including where he as done all that is reasonably possible to safeguard the effectiveness of transfers.

We argue that the EU Charter of Fundamental Rights shouldn't be directly applicable against EU Companies and the conditions of transfers in the absence of an adequacy decision should be made more explicit. A transferor can't be the absolute guarantor.

More specifically, the draft recommendations place the onus on the exporter to assess the third country's law (*EDPB recommendations, par.30, 32, 35*), on a case by case basis, before any transfer of personal data (unless there is an adequacy decision with the third country in question). AMAFI finds that the European Commission and the EDPB would be better equipped to provide clear indications on the possibility of transferring personal data to a third country and on the additional measures to be implemented in case of insufficient protection. Indeed, they have access to more resources to carry out in-depth studies of third country laws and would provide more legal certainty where it would require institutions to have more resources they do not have, particularly in terms of costs.

Moreover, leaving it to the institutions to make their own analysis on a case-by-case basis would result in a multitude of divergent interpretations which would complexify competent authorities' supervision of data transfers from the Union to a third country.

We therefore urge the European authorities to continue establishing adequacy decisions and revise the existing adequacy decisions in the light of the judgement.

4. STEP 4: ADOPT SUPPLEMENTARY MEASURES

As regards the proposals for additional measures to be put in place where Article 46 is not sufficient to guarantee an equivalent level of protection to that of the Union, AMAFI considers that they are impossible or at least extremely complex to implement.

Some technical measures such as encryption can only be a solution for storage transfers but not for operational transfers. Moreover, sometimes only partial data is transferred. It therefore seems disproportionate to set up these demanding processes where little data or data of little importance is transferred. In addition, "bad practices" such as remote access to data for professional purposes are presented. AMAFI is wondering whether this means that some transfers become prohibited in certain cases.

Furthermore, the EDPB in its recommendations *(EDPB recommandations, par. 48, 49)* makes it clear that the contractual and organizational measures that are proposed are often not sufficient to prevent access to data by third countries authorities and only technical measures might hinder access to the data by third county authorities. However, the proposed technical measures are not practical or precise enough for all situations. We welcome a more granular and sector-specific or sectorial approach (eg: for the financial sector, X types of data can be transferred as the transfer does not create an excessive risk for the data subject).

Furthermore, operationally, and technically, institutions may not have the tools nor the technique to implement these "complementary measures" proposed by the EDPB, except at exorbitant costs. The proposed solution is not economically viable and places establishments in the situation where they might be at breach.

The direct consequences to these observations are that European firms might have to entirely stop their transfers to third countries, even for intra-group transfers, since no data storage project at a European level exists today. The European data market lacks the right tools and sufficient service providers. AMAFI would have liked the EDPB to provide risk-based recommendations. In fact, no grace period has been given to institutions to review and stop all their transfers to providers outside the EU. By adopting a risk-based approach, entities may assess the risk of litigation or breach of legislation their transfer might create and cease any transfer that has a high risk profile while maintaining transfers that have low risk profiles.

Furthermore, AMAFI is in favor of a more nuanced analysis of the data involved in a transfer and the risks associated with such transfers. Depending on whether the data concerns a natural person or a legal entity, for example, the data will not have the same sensitivity. Article 35 of the GDPR on Data protection impact assessment mentions these analyses, the granularity of which depends on the situation. An idea might be to categorize data according to a sectorial approach It would be interesting to introduce a concept of data codification according to their risk and sensitivity. In fact, some personal data can be transferred without putting the data owner's privacy at risk. A risk proportional analysis could be interesting to develop, at least for now, while establishments do not have many solutions except trying on a case-by-case basis to stop transfers that represents a high risk.

5. STEP 5: PROCEDURAL STEPS IF YOU HAVE IDENTIFIED EFFECTIVE SUPPLEMENTARY MEASURES

Although we understand that procedural steps may diverge according to the transfer tool and the supplementary measures that have been put in place, AMAFI wished for more support from the EDPB, mostly in terms of practical examples.

6. STEP 6: RE-EVALUATE AT APPROPRIATE INTERVALS

In line with our previous comments, if institutions are to ensure that the measures they have put in place remain valid, AMAFI wonders whether the European Commission and the EDPB are not better equipped to review the law of third countries frequently enough to ensure a sufficient level of protection.