Brussels, 14 June 2017

Steven Maijoor
ESMA
CS 60747
103 rue de Grenelle
75345 Paris Cedex 07, France

Dear Mr Maijoor,

We are writing to you, further to our conversation which took place in Paris, in March 2017, as well as to our meeting with IOSCO'S Chair, Mrs. Maureen Jensen, in April 2017, on the issue of exchange of information with third country financial supervisory authorities ("TCAs") and compliance with EU data protection rules. During the meeting, you expressed interest in how to provide appropriate safeguards under Article 46 GDPR in the future. We also understand that ESMA and national competent financial supervisory authorities ("NCAs") want to work with IOSCO to develop such safeguards.

By this letter, the WP29 intends to provide preliminary recommendations and indications to ESMA and NCAs to help them build up appropriate legal instruments for international transfers of personal data occurring, under Article 46 GDPR, to TCAs in countries which have not been recognized by the European Commission as offering an adequate level of data protection.

The rules in the GDPR will apply to transfers made by NCAs. With regards to transfers made by ESMA itself, the respective rules of the text replacing Regulation (EC) 45/2001 will apply. A proposal for that text has been published at the beginning of 2017[1]. The rules on third-country transfers in that proposal (Article 47 and following) are largely similar to those in the GDPR. Recital 5 of the proposal explains that concepts in the proposal should be interpreted homogeneously with the equivalent concepts in the GDPR.

This letter contains (i) a general analysis on the use of appropriate safeguards for the transfer of personal data to TCAs and (ii) recommendations as to the content of the guarantees to be incorporated (as an addendum or in a side letter) in bilateral and/or multilateral agreements concluded with TCAs for that purpose.

The WP29 takes note that only some of the information exchanged between NCAs and TCAs may qualify as personal data and the comments made hereby only apply to information exchanged that qualifies as such.

1 COM(2017) 8 final

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

I. General Analysis

According to the GDPR, when personal data are transferred from the EU to controllers or processors in third countries or to international organizations, the level of protection of natural persons ensured in the EU by the GDPR, should not be undermined and where no adequacy decision is in place, the controller or processor should "make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that they will continue to benefit from fundamental rights and safeguards". The provisions on international transfers (Articles 45-49 of the GDPR) are about "how" the transfer is carried out; if it should be carried out at all depends also on whether, under Article 6 of the GDPR, there is a ground for lawful processing of the personal data to be transferred (in your case it is likely to be Article 6(1)(e) which allows for processing if it is necessary for a task in the public interest/exercise of official authority of the controller).

Therefore, while data sharing can bring benefits in terms of efficient cooperation between EU and third country regulators, it must be done in a way that the full respect for data protection rules is ensured.

Article 46 of the GDPR offers various methods of providing appropriate safeguards for transfers of personal data to third countries or international organisations, including through legally binding and enforceable instruments[2] between public authorities or bodies or (subject to authorisation from the competent supervisory authority) administrative arrangements between public authorities or bodies providing for enforceable and effective data subject rights[3]. In this context, Recital 108 of the GDPR expressly refers to the possible adoption of a memorandum of understanding.

The WP29 considers that such transfers of personal data that are part of a broader exchange of information in the financial sector, which is necessary for the development of an efficient international cooperation, should ensure that the level of protection of natural persons guaranteed the GDPR is not undermined (see 44 GDPR) and a stable and well-structured framework should be provided. This will also help to ensure legal certainty for the transfer.

Such framework could consist of an administrative arrangement such as a memorandum of understanding, which would allow for data transfers subject to prior authorization from the supervisory authority.

NCAs should introduce, through an addendum or in a side letter to the bilateral and/or multilateral agreements concluded, clauses containing a set of necessary guarantees constituting enforceable and effective data subject rights. [4]

Pursuant to Article 46(3) (b), the memorandum of understanding must require authorisation from the competent supervisory authority.

---

2 Article 46.2.a GDPR

3 Article 46.3.b GDPR

4 Cf. Recital 108 which clearly assumes that enforceable and effective rights for data subjects might be provided even in an administrative arrangement such as a memorandum of understanding. It will be up to the NCAs to demonstrate to the DPA that the provisions, even if included into an administrative arrangement which as such might not be enforceable by the NCAs and TCAs against each other, nevertheless provide for enforceable (and effective) rights for the data subjects, as presumed by Recital 108 of the GDPR.

II. Recommendations

This addendum or side letter should include all the basic data protection principles as imposed by European data protection legislation and, in particular, *as a minimum*:

- **effective and enforceable rights for the data subjects**, the relevant provisions should expressly confer rights to data subjects to enforce the rules as third-party beneficiaries. The rights should cover the judicial remedies for any breach of the rights guaranteed, the right to obtain redress and where appropriate, to receive compensation. Specifically, **effective remedies and redress mechanisms** must be provided to data subjects in case of violation of their rights due to the transfer of their data to TCAs. The agreement should foresee a system enabling the data subjects to continue to benefit from redress mechanisms even after data has been transferred. In order to enable data subjects to exercise their right of redress, the parties should make sure that at least the data protection part of the agreement has been made publicly available. Another option would be for the data exporter to provide specific guarantees assuming liability in case that the safeguards in the addendum or side letter are not complied with by the data importer.
- **The transparency principle and rights of data subjects** including the right to be informed; the provisions must contain the transparency principle and clear wording describing the data subjects' data protection rights. The party before which an individual invokes his/her right must have in place specific and accessible procedures enabling and facilitating the exercising of the data subjects rights. Taking into account the nature of the investigatory and enforcement activities of NCAs and ESMA, a general wording on the possibility that the data subject's personal data may be transferred to a third country, including information on the purposes of this transfer should be provided by the responsible party at the moment of the collection of the data. This prior information should take place in order to avoid interference with the investigation. Depending on the nature and of NCAs and ESMA's activities, and on the risks that this might provoke to the said activities, a general wording can also be provided on the information to be provided to the data subject once the procedure concerning him/her has ended.
- definitions for the **basic personal data concepts** including among others those of "*personal data",* "*data controller*", "*data processor*", "*processing of personal data"* and "*special categories of personal data/sensitive data*".
- the respect of the **principles of purpose limitation and prohibition of any further incompatible use**; The relevant clause should carefully and clearly specify the purposes for which personal data is to be transferred and processed outside the EU, as well as to ensure that the data will not be further processed for incompatible purposes. In addition, it should also be specified that transferred data cannot be used for any purpose other than those expressly mentioned in the agreement.
- the **data proportionality and necessity (data minimization)** of processed data, starting with its collection. The categories of data that may be processed and transmitted shall be precisely listed. In addition, the data processed and transferred must be adequate, relevant and not excessive in relation to the purposes for which they are transmitted. Moreover, data should be correct and updated.

- the **data retention principle**; Personal data shall not be retained indefinitely but shall be kept only for the time necessary to carry out the purpose for which it was collected and transmitted. Where feasible, a maximum retention period should be set in the text of the agreement.
- **restrictions on onward transfers**; Onward transfers to other recipients not bound by the agreement should be, as a rule, specifically prohibited. However, if needed, the parties may allow onward transfers under the condition that the purpose limitation principle is respected, the transferring party authorizes it, it is possible to legally bind the receiving third parties to respect the same data protection principles and to provide to the data subjects the same data protection guarantees that the first recipient has committed to provide.
- the establishment by the requesting authority of organizational and technical measures with regards to **security and confidentiality** in order to protect the data from any accidental or illegal access, destruction, loss, alteration or publication of the data.
- the designation of the appropriate external **supervision mechanism** in terms of data protection, for example the designation of an independent data protection authority, leads to boosting confidence that data protection principles are respected after data is transferred.
- specific safeguards in respect of **special categories of data**[5] such as sensitive data.

We hope that this letter has provided sufficient information and guidance in order to ensure compliance with the European data protection principles as established by the GDPR for the transfer of personal data to TCAs under Article 46 GDPR.

Yours sincerely,

On behalf of the Article 29 Working Party,

Isabelle FALQUE-PIERROTIN
Chairwoman

[5] Article 9 and 10 GDPR.