Brussels, 24 September 2015

Mr David Wright
Secretary General
International Organization of Securities Commissions (IOSCO)
Spain
By e-mail: Hanna@IOSCO.org

Subject: IOSCO's Multilateral Memorandum of Understanding concerning consultation and cooperation and the exchange of information.

Dear Mr Secretary General,

Thank you for your letter dated 12 January 2015 regarding the IOSCO's Multilateral memorandum of understanding concerning consultation and cooperation and the exchange of information (hereafter MMoU).

We took great interest in reading your letter helping to clarify various elements, such as the value of "*minimum standard*" at global level of the MMoU; the fact that its provisions do not supersede domestic laws; as well as the content of the MMoU clauses related to confidentiality, possible usage limitation and onward transfers.

We would like to make clear that the Article 29 Working Party (WP29) wished to comment on your MMoU in a constructive spirit, as the most effective cooperation between securities regulators is indeed critical to combat securities market violations. However, the WP29 feels it is its role to make recommendations with a view of attaining the most appropriate framework for personal data transfers occurring in the context of the cooperation between securities regulators under the MMoU.

We deeply regret that there seems to be some disagreement regarding a lack of safeguards in the framework of the exchange of personal data amongst MMoU signatories.

We still believe it is our common interest to collaborate more closely in the view of taking better into account the substantive data protection principles deriving not only from EU directive 95/46/EC and Member States national laws, but also from other international

instruments such as the Convention 108[1] of the Council of Europe or the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[2].

Please find below further substantiation of our concerns, as well as additional remarks in an attached Annex.

The WP29 would like to recall that, in order to take into account specific needs of activities carried out by authorities legally in charge of exercising inspection, investigation and regulatory powers, the data protection principles and rules must be adapted accordingly in their practical application[3].

It should however be strongly underlined that a MMoU cannot, with a single provision, supersede the exercise by natural persons of the fundamental rights to which they are entitled to on the basis of EU and Members States data protection legislation.

Data protection principles have a broader scope than, strictly speaking, a "Confidentiality" clause (par.11) and a "Permissible uses of information" (par.10) clause.

In this regard, we see the following elements as of particular interest:

- The Working Party considers that some core data protection principles (such as for example, data proportionality and quality principle, the limited data retention period and the rights of the data subjects) are not provided or not sufficiently enough provided for in the MMoU [(see Annex)].

- Paragraph 12 (iii) of the MMoU opens the possibility for authorities to consult periodically each other regarding the MMoU about matters of common concerns and, in particular, where circumstances makes it necessary or appropriate to consult, amend or extend the MMoU in order to achieve its purpose.

- The wording of your position considering not necessary to amend the MMoU "at this time" leaves open the possibility, somewhere in the future, to have the MMoU's text modified.

As regards this last remark, to our knowledge the MMoU was revised in 2012. We would like to ask you whether it is planned to revise or amend the Memorandum in the near future and, if yes, under which timeframe.

Going further into the subject, you specify in your 12 January 2015 letter that all EEA securities authorities have signed the MMoU and that it is incumbent upon each of them to ensure compliance with national provisions implementing the Data Protection Directive when responding to cooperation requests received under the MMoU.

[1] http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

[2] http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[3] For example, the transparency principle which encompasses into a right of the data subject to be informed of the processing can be of course limited in the context of an ongoing investigation in order to avoid to unnecessarily harming the investigation. Similarly, the right of access to police files can be limited, for example by providing an indirect access right instead of a direct access right.

As a matter of fact, EEA securities regulators are bound by obligations set forth by Art.25 and 26 of directive 95/46/EC, under which personal data transfers to third-countries without adequate level of data protection can only be authorized by Member State when sufficient safeguards are ensured. Data protection authorities could be obliged to investigate the circumstances of such transfers should a complaint be received.

Furthermore, the Working Party has long established and stated that interpretation of exemptions under Art.26 (1) must necessarily be strict when data transfers taking place are regular, structured and organized; and that data controllers established in the European Union should favour solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards to which they are entitled as regards processing of their data in the EU once this data has been transferred[4].

There is a risk here that data protection authorities consider that EEA securities regulators are not complying with their obligations because the safeguards provided in the agreement (the MMoU) cannot be considered as sufficient. This could furthermore lead some data protection authorities to refuse delivering, to suspend or retrieve transfers authorization (when such authorizations are needed under their national data protection law).

As a consequence, we see that in order to help EEA participating securities authorities to comply with their obligations under European and national data protection legislation, the best solution is to amend the MMoU in order to reinforce the current wording bring all sufficient safeguards within its text.

We would like to contact you to discuss this matter further.

Yours sincerely,

On behalf of the Article 29 Working Party,

Isabelle FALQUE-PIERROTIN
Chairwoman

[4] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf

Annex:

Data protection principles that should be referred to in the MMoU and examples of clauses

The list below refers to data protection principles that seem to be missing in the MMoU and that should be added in the text in order to consider that the MMoU provides for sufficient safeguards. This list is not intended to be exhaustive. The Working Party would gladly provide you with further guidance on each of these principles.

Purpose limitation principle

Paragraph 10 (a) of the MMoU already offers provisions limiting permissible uses of information by the requesting authority. However, Paragraph 10 (b) of the MMoU allows the possibility for the requesting authority to use the transmitted information "*for any purpose other than those stated in Paragraph 10(a)*" as long as the requested authority has given its consent.

In order to better implement the data protection purpose limitation principle, the Working Party is of the opinion that:

- specific wording should be inserted to reinforce the limitation of the permissible uses of personal data (for example, the following clause could be inserted: "*Personal data may only be processed by the receiving Party for the legitimate and specified purposes mentioned in Paragraph (xxx) of this Memorandum of Understanding, and in accordance with the conditions imposed by the Party which transmitted the data")*;

- IOSCO should reflect on the necessity to maintain Paragraph 10(b), as the purpose limitation principle would be better taken into account if requesting authorities were not allowed to make any other use of personal data than those stated in Paragraph 10(a). Therefore, Paragraph 10(b) should be deleted of the MMoU;

- If IOSCO can demonstrate valid and necessary reasons to maintain Paragraph 10(b), then the consent of the Requested authority should be explicit and given in writing prior to any different use. It should also be specified in the MMoU as a condition that the further use must be compatible with the initial data processing purpose.

- Any further use by the requesting authority consisting in transmitting the received personal data to another third party should be clearly distinguished as a case of "onward transfer" (see below). Here again, any onward transfer must be compatible with the initial data processing purpose.

Data proportionality and quality principles

These principles should be taken on board in the MoU by inserting more detailed clauses related to personal data. The obligation for both parties to maintain accurate and updated personal data is not only a data protection requirement, but it also a requirement for efficiency of the cooperation by mutual assistance request. The following wording could, for example, be used:

- *"The categories of personal data processed pursuant to this Memorandum of Understanding are: (insert here the list of adequate, non excessive and relevant data which will be processed and transmitted under the Memorandum of Understanding)".*

- *« The Parties shall ensure that the data are accurate and updated. If incorrect data have been transmitted, each Party must notify the other Party without delay. Where it is confirmed that data transmitted is inaccurate, each Party processing the data shall take the necessary measures to rectify the information. »*

- *"If data have been unlawfully transmitted, each Party must notify the other Party without delay and the receiving Party shall delete the information immediately upon becoming aware of such an event."*

Transparency principle and Data subjects' rights

6.(d) specifies that the MMoU does not confer upon any Person not an Authority, the right or ability, directly or indirectly to obtain, suppress or exclude any information or to challenge the execution of a request for assistance under this MMoU.

It is true that, in order to take into account specific needs of activities carried out by authorities legally in charge of exercising inspection, investigation and regulatory powers, the data protection principles and rules can however be adapted accordingly in practice.

Nevertheless, the fundamental data protection principles cannot be purely and simply addressed by a single statement by a MMoU. In that sense, the exercise by natural persons of the fundamental rights to which they are entitled to by virtue of EU and Members States data protection legislation cannot be denied to data subjects.

Therefore, the wording at 6(d) appears to be incompatible with the basic fundamental data protection principles requirements as it seems to deny to data subjects the exercise of any right of access to his/her personal data, right to modify incorrect data, and right to obtain data deletion.Data subjects should exercise the fundamental rights they hold from EU and national data protection legislation (right to be informed, right to access their data, right to obtain modification and right to obtain data deletion).

As however explained before, in the context of cooperation on mutual assistance requests and investigations conducted under IOSCO's MMoU, these principles can be adapted considering the specific needs of the Authorities involved but should still be granted to data subjects.

For example, in order not to harm investigations, the moment when data subject will be informed should be delayed until the moment where the data subject can be informed without harming the purpose of the processing, which is conducting an investigation.

This could translate in the MoU by inserting a specific paragraph, for example:

- *"As soon as it can be given without harming the purposes of this Memorandum of Understanding as deriving from the primary legal basis, the Parties agree to inform the data subjects, at the very least, about the identity of the data controller, the purposes of the data processing, the data recipients."*

The Parties recognize that, in line with the European Union and the European standards on data protection each individual whose personal data are being processed pursuant to this Memorandum of Understanding is entitled to the following rights and commit to ensuring they can benefit effectively from their rights."

- *"Right to information*

The Parties provide data subjects with information relating to: the identity of the data controllers, the nature of the personal data that may be processed, the purpose of the processing of their personal data , the recipients of the data, the rights of individuals with regard to the process of their personal data, the procedures available for the exercise of the rights to redress, the contact information of the person to ask questions or the exercise of one's rights to object, access, rectify or delete data."

- *"Right to access*

Any person shall have, in principle, the right to obtain access to his/her personal data."

However, limitations to this principle can be introduced in the context of administrative cooperation between securities regulators. In this view, the following wording could be, for example, be used:

"*Following requests made at reasonable intervals, any person shall have the right to obtain without constraint and without excessive delay at least a confirmation transmitted through their Data Protection Authority to whether that person's data protection rights have been respected in compliance with this Memorandum of Understanding."*

- *"Right to rectification and deletion*

Any person has the right to seek the rectification, erasure, or blocking of their personal data processed by the Parties pursuant to this Memorandum of Understanding when the data are inaccurate or the processing contravenes this Memorandum of Understanding."

Finally, the MMoU lacks reference to the competent authorities (in each Member State) to turn to for enforcement as regards privacy matters (i.e. the EU national data protection authorities). Therefore, a general provision referring to the competent Privacy enforcement authorities should be added in the MMoU.

Limited data retention period principle

This principle is also very important, as it prohibits data controllers and processors to be able to keep personal data forever. In the context of cooperation between securities regulators, limited data retention of 10 years could be relevant, as a similar limited period is set in the context of the market abuse context. In any case, a time limit to the retention of personal data must be determined. This could translate through the following example wording:

- *"The Parties shall ensure that personal data are retained for a period no longer than which is necessary for the purposes for which data are transmitted."*

- *"The transmitting Party shall notify the receiving Party of the intended data retention period and of any particular time cycle periods before erasure under the national law of the exporter concerning the transferred personal data."*

- *"The receiving Party shall irremediably delete the information transferred as soon as the purposes for which data are transmitted are completed or as soon as the maximum data retention period imposed by the transmitting Party is met."*

Data protection rules for transferring personal data outside the European Union territory

Under the Article 25 of the Directive 95/46/CE, Member States shall only allow a transfer to take place if the receiving party in the third country ensures an adequate level of protection.

Where there is an absence of adequate protection in the sense of Article 25 (2), the directive envisages in Article 26(2) the possibility for data controllers to adduce adequate safeguards by the adoption of commitments in legal instruments. Those kinds of instruments, such as international cooperation agreements, aim to ensure that the level of protection remains even after the transfer of personal data in third countries.

Limitation of onward transfers

As a rule, onward transfers to other receiving third-parties not bound by the agreement should be specifically excluded by the agreement, for example with the following clause: "*Any onward transfer to any other recipient is prohibited."*

However, onward transfers might be allowed under specific conditions when it is possible to legally bind such third parties to respect the same data protection principles and to provide to the data subjects the same data protection guarantees expected from the first recipient.

Countries where the powers of state authorities to access information go beyond those permitted by internationally accepted standards of human rights protection will not be safe destinations for transfers based on contractual clauses.

Additional safeguards for the data subject are all the more necessary when the recipient in the third country is not already subject to an enforceable set of data protection rules providing an adequate level of protection.

The wording of the MMoU could be reinforced by make use of the following examples:

- *"The communication of personal data to a third party shall only be authorized after prior express and written approval of the Party that transmitted the data and shall be referred to as "onward transfers".*

- *Onward transfers shall only be permitted for the purposes mentioned in this Memorandum of Understanding. With respect to the data protection principles, any onward transfer shall therefore be lawful, legitimate, specific, adequate, relevant and not excessive, accurate and not kept longer than necessary.*

- *Each onward transfer shall be duly documented, logged and comply with the protection standards set out in this Memorandum of Understanding.*

- *Any further recipients of personal data transferred by onward transfer shall also be bound by all data protection clauses and safeguards set out in this Memorandum of Understanding or by a legally binding instrument imposing at least the same level of data protection provided for in this Memorandum of Understanding."*

Security principle

Under the Directive 95/46/EC and applicable national laws, data controllers are bound to an obligation to ensure the security and the confidentiality of the personal data processing and transfers they carry out. These obligations also extend to the receiving Party, which must be reflected into the agreement.

Therefore, signatories to the Memorandum of Understanding should be encouraged to provide more details on security and confidentiality in specific provisions, for example by using the wording below.

- *"Each Party shall be responsible for the security and the confidentiality of the processing of personal data."*

- *"The Parties shall ensure that appropriate technical and organizational measures are implemented to protect personal data processed and transferred pursuant to this Memorandum of Understanding against accidental, unlawful or unauthorized access, destruction, disclosure, alteration, in particular since the processing involves the transmission over a network. Moreover, these measures shall protect against all unlawful forms of processing, taking into account the particular risks represented by the processing and the nature of the data to be protected. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."*

- *"All transmissions, consultations and receptions of personal data are to be logged or documented. The Parties shall communicate to each other the list of authorities or services authorized to consult the logs or documentation. The data must be kept at disposal of the Data protection supervisory authority and the competent body in charge of ensuring lawful data processing as well as data integrity and security."*