Opinion 4/2019

on the draft Administrative Arrangement for the transfer of personal data between European Economic Area ("EEA") Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities

Adopted on 12 February 2019

Table of contents

The European Data Protection Board

Having regard to Article 63, Article 64 (2), (3) - (8) and Article 46 (3), (b) of the Regulation 2016/679/EU 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 (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018, as amended on 23 November 2018.

Whereas:

(1) With reference to Article 46 (1), (3) (b) and 46 (4) GDPR, in the absence of a decision pursuant to Article 45 (3), a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Subject to authorisation from the competent supervisory authority ("competent SA"), the appropriate safeguards may also be provided for, in particular, by provisions inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

(2) Taking into account the specific characteristics of the administrative arrangements provided for by Article 46 (3) (b)[1], which may vary considerably, each case should be addressed individually and is without prejudice to the assessment of any other administrative arrangement.

(3) The EDPB ensures pursuant to Article 70 (1) of the GDPR the consistent application of Regulation 2016/679 throughout the European Economic Area. Under Article 64 (2), the consistency mechanism may be triggered by a supervisory authority, the EDPB Chair or the Commission for any matter of general application or producing effects in more than one Member State. The EDPB shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter.

(4) The opinion of the EDPB shall be adopted pursuant to Article 64 (3) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

(5) Pursuant to Article 65 (1) (c) GDPR where a competent SA does not follow the opinion of the EDPB issued under Article 64, any supervisory authority concerned or the Commission may communicate the matter to the EDPB and it shall adopt a binding decision.

[1] See also recital 108 GDPR

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. Following several rounds of discussions , the European Securities and Markets Authority (ESMA), acting as facilitator for EEA financial supervisory authorities (NCAs) and in its own capacity, and the International Organisation of Securities Commission (IOSCO) have submitted by official letter the attached draft Administrative Arrangement (hereinafter draft AA) according to Article 46 (3) (b) GDPR to frame the transfers of personal data from EEA NCAs (and ESMA itself) to their non-EEA counterparts. This draft AA was communicated to the Chair of the EDPB on 2 January 2019.

2. Following the submission, the Chair of the EDPB has requested the Board for an opinion pursuant to Article 64(2) GDPR. The decision on the completeness of the file was taken on 15 January 2019.

2 ASSESSMENT

3. The draft AA may be used by all market regulators in the EEA and submitted to the competent SAs for authorisation. As a result, the matter is producing effects in more than one Member States within the meaning of Article 64(2) GDPR.

4. The draft AA is necessary to ensure efficient international cooperation between these authorities, acting in their capacity as public authorities, regulators and/or supervisors of securities and/or derivatives markets, in order to "safeguard investors or customers, and to foster integrity and confidence in the securities and derivatives markets" in accordance with their mandates as defined by applicable laws.

5. In assessing the provisions contained in this specific draft AA, the EDPB has taken into account a number of specific elements for the assessment of possible risks posed by the transfers of personal data including the type of personal data subject to the AA and the objectives pursued.

6. The draft AA which can be found in its entirety in the attachment includes the following guarantees:

   - **Definitions of GDPR concepts and data subject rights:** Section II of the AA contains the relevant definitions necessary to determine the scope of the AA and its consistent application. Among them there are some definitions of key concepts and rights of the European data protection legal framework such as "personal data", "processing", "personal data breach", "right of access", "right of erasure" which are in line with the definitions contained in the GDPR.

   - **Principle of purpose limitation and prohibition of any further use:** Section III (1) of the AA works on the premise that Authorities have specific responsibilities and regulatory mandates, which include protecting investors or customers and fostering integrity and confidence in securities and/or derivatives markets. According to the principle of purpose limitation, the transfers can therefore only take place in the framework of such mandates and

responsibilities, namely if necessary to support their institutional tasks and the receiving Authority will not be allowed to further process the personal data in a manner that is incompatible with these purposes.

- **Principle of data quality and proportionality:** According to Section III.2 of the AA the transferring Authority will only transfer accurate and up to date personal data that are adequate, relevant and limited to what is necessary for the purposes for which they are transferred and further processed. Each Authority will inform the other if it becomes aware that transferred personal data is incorrect. Having regard to the purposes for which the personal data have been transferred and further processed, each Authority will supplement, erase, block, correct or otherwise rectify the personal data, as appropriate.

- **Principle of transparency:** A general notice to data subjects will be provided by each Authority in relation to the processing carried out, including the transfer, the type of entities to which data may be transferred, the rights available to them under the applicable legal requirements, including how to exercise those rights and information about any applicable delay or restrictions on the exercise of such rights and the contact details for submitting a dispute or claim. This notice will be provided by each Authority on its website where it will be published along with this Arrangement. Furthermore, individual notice will be provided to data subjects by EEA Authorities in accordance with the GDPR and, in the case of ESMA, in accordance with Regulation 2018/1725.

- **Principle of data retention:** As provided by Section III.7 of the AA the Authorities will retain personal data for no longer than is necessary for the purpose for which the data are processed in compliance with the applicable laws.

- **Security and confidentiality measures:** Section III.4 envisages that each receiving Authority will have in place appropriate technical and organizational measures to protect personal data that are transferred to it against accidental or unlawful access, destruction, loss, alteration, or unauthorized disclosure, including, for example, marking information as personal data and restricting who has access to personal data.

  The AA also envisages that in the case where a receiving Authority becomes aware of a personal data breach, it will inform the transferring Authority as soon as possible and use reasonable and appropriate means to remedy the personal data breach and minimize the potential adverse effects.

- **Safeguards relating to data subject rights:** Section III (5) of the AA provides for safeguards relating to data subject rights. Data subjects can obtain confirmation of whether their data have been transferred to another financial supervisory Authority outside the EEA (TCA). Data subjects will also be provided with access to their personal data upon request. In addition, data subjects may request directly to the concerned NCA or TCA that their data are rectified, erased, restricted or blocked. Information regarding these safeguards are to be provided on the NCA/TCA website. Any restriction to these rights has to be provided by law and is allowed only to the extent and for as long as this is necessary to protect confidentiality or for important objectives of general public interest which when the transferring Authority is an EEA NCA, has to be recognized by the Member State of this NCA (including, for instance, to prevent prejudice or harm to supervisory/enforcement functions).

- **Restrictions on onward transfers:** Onward transfers to a third party in another country who is not an Authority participating in the AA and is not covered by an adequacy decision from the

European Commission will only take place with the prior written consent of the transferring Authority, and if the third party provides appropriate assurances that are consistent with the safeguards in the AA.

The same safeguards are envisaged for cases of sharing of personal data with a third party in the same country of the receiving Authority unless, in exceptional cases, such third party cannot provide the aforementioned assurances. In this case, the transfer may take place only if the sharing is "for important reasons of public interest". When the transferring Authority is an EEA NCA, this public interest has to be recognized by the Member State of this NCA.

Personal data may be shared with a third party in the same country of the receiving Authority (such as public bodies, courts, self-regulatory organizations and participants in enforcement proceedings) without consent from the transferring Authority, or assurances only in two cases:

(i) If the purpose for which the personal data are shared and then used is consistent with the purpose for which the data were initially transferred or with the general framework of the use stated in the original specific request from the receiving Authority, and the sharing is necessary to fulfil the mandate and responsibilities of the receiving Authority and/or the third party.

(ii) When the sharing of personal data follows a legally enforceable demand or is required by law. The receiving Authority will notify the transferring Authority prior to the sharing and include information about the data requested, the requesting body and the legal basis for sharing. The receiving Authority will use its best efforts to limit the sharing of personal data received under this Arrangement, in particular through the assertion of all applicable legal exemptions and privileges.

- **Redress:** Section III (8) of the AA provides for a redress mechanism. This mechanism is there to ensure the right to obtain redress and, where appropriate, to receive compensation. In cases where non-compliance of the AA occurs, including where data subject rights are violated, redress can be exercised before a competent body (e.g. court). Redress before such a competent body will be in accordance with the applicable legal requirements, ensuring that the rights of the data subject related to the principles and safeguards provided for under the AA can be effectively enforced. The transferring Authority will be informed about any dispute or claim and the authorities on both sides will use best efforts to settle the dispute or claim amicably. In the event the matter cannot be resolved in this way, other methods will be used to resolve the dispute, including non-binding mediation or dispute resolution mechanisms. If the transferring Authority is of the view that a receiving Authority has not acted consistent with the safeguards set out in the AA, e.g. as it has not followed the decision of the non-binding mediation or alternative dispute resolution mechanism, it will suspend any transfers under the AA to the receiving Authority until the issue is satisfactorily resolved. Moreover, the "assessment group" (as well as all other Authorities) will be notified and can, in case it determines that there has been a "demonstrated change in the willingness or ability of [the receiving Authority] to act consistent with the [AA]", recommend that the receiving Authority's participation in the AA be discontinued. In order to enable data subjects to exercise their right of redress, the AA will be made publicly available.

- **Oversight mechanism:** Section IV of the AA provides for an external oversight mechanism ensuring the implementation of the safeguards of the AA. This oversight mechanism consists of a combination of periodic reviews conducted by the "assessment group" and by each NCA/TCA internally. The combination of the external and internal oversight as well as the

possible consequences following a negative review – which may include a recommendation to suspend an Authority's participation in the AA – provides for a satisfactory level of protection.

7. The EDPB welcomes the efforts made for this multilateral AA which includes a number of important data protection safeguards. In order to make sure that these safeguards continue to ensure an appropriate level of data protection when data are transferred to a third country under this AA, taking into account the unique nature of such non - binding agreements, the EDPB underlines the following:

8. Each competent SA will monitor the AA and its practical application especially in relation to sections III (5), (6), (8) and IV relating to data subject rights, onward transfers, redress and oversight mechanisms to ensure that data subjects are provided with effective and enforceable data subject rights, appropriate redress and that compliance with the AA is effectively supervised.

9. Each competent SA shall only authorise this AA as a suitable data protection safeguard with a view to the cross-border data transfer, conditional to full compliance by the signatories with all the clauses of the AA.

10. Each competent SA, will suspend the relevant data flows carried out by the NCA in its Member State pursuant to the authorization, if the AA no longer provides for appropriate safeguards in the meaning of the GDPR.

3 CONCLUSIONS/RECOMMENDATIONS

11. Taking into account the above and the commitments the NCAs, ESMA and their non-EEA counterparts will undertake by signing this AA in order to have "*in place appropriate safeguards for the processing of such personal data in the exercise of their respective regulatory mandates and responsibilities*" and to "*act consistent with this Arrangement*", the EDPB considers that the AA ensures appropriate safeguards when personal data will be transferred on the basis of this AA to public bodies in third countries not covered by a European Commission adequacy decision.

12. Consistent with the preamble of the AA, acknowledging the importance of regular dialogue between the EEA NCAs and their competent SAs, or the European Data Protection Supervisor ("EDPS") in the case of ESMA, and in order to allow the competent SAs to carry out their task of monitoring and enforcing the application of the GDPR in accordance with Article 57 (1) (a) of the GDPR, the authorisation adopted by the competent SA should envisage that each signatory EEA NCA or ESMA shall inform the respective competent SA of any suspension of transfers of personal data based on Sections III (8) and IV of the AA, as well as of any revision or discontinuation of participation to the AA based on Section V.

13. In addition, the EDPB recalls that, in line with the accountability principle, each NCA and ESMA will need to keep records of information to facilitate the monitoring task of the SAs. This information should in any case be made available upon request from the competent SA. Each SA may also, in its authorisation, request to receive this information from NCAs or ESMA on an annual basis without any prior request. This information should include elements on the number of data subject requests and claims received by data subjects at EU level, details on the cases not resolved through the envisaged dispute resolution mechanisms as well as on respective findings and actions of the "Assessment Group" following the periodic reviews including actions with regards to the sharing of personal data

under Section 6.2.3 of the AA. Information should also be recorded on the notifications received by NCAs on the sharing of information to a third party by the TCA following a legally enforceable demand or required by law.

4 FINAL REMARKS

14. This opinion will be made public pursuant to Article 64 (5) (b) of the GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)