Data Protection and Administrative Arrangement FAQs

Q1: What was the purpose of IOSCO's work on data protection and why was drafting an Administrative Arrangement for the transfer of personal data necessary?

A: In May 2018, a new law came into force in Europe: the General Data Protection Regulation (GDPR). The GDPR aims to enhance the rights of individuals as regards the protection of their personal data. It may have an impact on transfers of personal data from European Union (EU)[1] IOSCO authorities to non-EU IOSCO authorities, thereby potentially interfering with exchanges of information under the IOSCO Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (MMoU) and the Enhanced MMoU (EMMoU). One potential mechanism under the GDPR for transferring personal data outside the EU is an administrative arrangement with appropriate safeguards.

In October 2016, the IOSCO Board Sub-group on Data Protection (Sub-group) was formed to explore ways to address this issue and ensure that personal data can continue to be shared under the MMoU and EMMoU between EU and non-EU authorities. The IOSCO Board, at the recommendation of the Sub-group, determined that the best path forward was to draft a non-legally binding Administrative Arrangement (AA) for the transfer of personal data between EU and non-EU Authorities – one of the forms of safeguards permitted under Article 46 of the GDPR for the transfer of personal data.

Since its formation, the Sub-group has negotiated with the European data protection supervisor, the European Data Protection Board (EDPB, which has superseded a previous group known as the Article 29 Working Party or WP29), to agree on an AA that is acceptable to both the EDPB and IOSCO members. In February 2019, both the EDPB and the IOSCO Board approved the AA.

Q2: What is meant by "personal data"?

A: For the purposes of the AA, personal data are information by which a natural living person can be identified, directly or indirectly. Examples of personal data include names, addresses, social security numbers, telephone numbers, bank details, securities holdings, etc. In practice, personal data are included in a number of information exchanges that are made under the MMoU and EMMoU.

[1] For the purposes of these FAQs, EU includes all European Economic Area (EEA) jurisdictions

Q3: What is the Administrative Arrangement for the transfer of personal data?

A: The AA is a non-legally binding arrangement for the protection of personal data that an authority may sign, thereby becoming a signatory (an "Authority" under the AA). An EU authority would join the AA as an Appendix A Authority, and a non-EU authority would join the AA as an Appendix B Authority. Please refer to Q6 for information on the purpose of the AA and Q8 for information on when it may be useful to become an AA Authority.

Q4: What will my Authority need to do if I sign the AA?

A: An Authority that signs the AA will act consistent with the AA with respect to personal data received under the AA. Authorities will treat such data in a manner consistent with the safeguards in the AA. Each authority that considers signing the AA should review those safeguards in advance of signing and determine whether it can act consistently with those safeguards (see Q12 for more information).

Through a combination of laws, regulations and internal policies and procedures consistent with applicable legal requirements in its jurisdiction, an Authority will have in place safeguards related to, e.g.:

- transferring and processing personal data;
- protecting security and confidentiality;
- onward transfers to and sharing with third parties only in certain circumstances;
- retention of personal data; and
- redress to the extent permitted by applicable legal requirements.

Each Authority will publish the AA on its website, along with information about, e.g., data subject rights under applicable legal requirements in its jurisdiction, as well as restrictions that apply to those rights.

Nothing in this document supersedes or modifies the terms and provisions in the AA.

Q5: Who may consider signing the AA as an Authority?

A: A public authority, regulator, or supervisor of securities and/or derivatives markets that is either an ordinary or associate member of IOSCO may sign the AA and become an Authority. Other entities with regulatory or

supervisory responsibilities (Other Authorities) may seek guidance from the IOSCO Board as to whether they may sign the AA. In order to become an AA Authority, the Other Authority must be able to act consistently with the AA and must subject itself to IOSCO's Oversight Mechanism (OM) for the AA.

Q6: Why do we need an Administrative Arrangement / what is its purpose?

A: The GDPR became applicable in Europe on May 25, 2018. It allows sharing/transfers of personal data outside the EU under certain conditions, including pursuant to a non-legally binding administrative arrangement with appropriate safeguards for transferring personal data. The AA offers a mechanism consistent with the GDPR under which EU Authorities can continue to share personal data with non-EU Authorities in connection with enforcement and supervisory matters, when the non-EU authority's domestic legal framework related to data protection has not been recognized as equivalent to the GDPR by the European Commission and when the Public Interest Derogation for transferring personal data is not available (see Q9 for more information).

Q7: What is the scope of the AA and how does it impact the MMoU and EMMoU?

A: The AA is intended to facilitate the transfer of personal data between EU and non-EU Authorities for both supervisory and enforcement purposes. It is intended to supplement, but not conflict with, the MMoU, EMMoU and other arrangements. In practice, an Authority requesting or transferring personal data pursuant to the AA will reference both the AA and any relevant underlying formal or informal arrangement. The AA is not the only means by which personal data may be transferred, and it does not prohibit an Authority from transferring personal data pursuant to a relevant agreement, another relevant arrangement, or a process separate to the AA, for example pursuant to an applicable adequacy decision or binding agreement.

Q8: Does my authority have to sign the Administrative Arrangement to continue sharing personal data under the MMoU and EMMoU to and from the EU?

A: Signing the AA is not compulsory. If a non-EU authority regularly requests personal data from specific EU authorities, it is likely that the EU authority will be unable to repeatedly share personal data with the non-EU authority in the absence of adequate safeguards being in place as a result of the GDPR. An authority may not need to sign the AA if its transfers to or from the EU are occasional and therefore fall within the scope of the Public Interest

Derogation (or another derogation) set out in the GDPR, or if it is covered by a relevant European Commission adequacy decision[2].

Authorities should refer to the Guidelines on Article 49 of Regulation 2016/679 adopted by the EDPB on May 25, 2018 (Guidelines) to help them decide if it is possible that they may be able to rely on the Public Interest Derogation when requesting information from EU authorities (see next FAQ). The Guidelines are available at the following link: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

Q9: What is the scope of the Public Interest Derogation and does my authority fall within it?

A: Authorities should carefully review the EDPB Guidelines to help them to determine whether a transfer can be made by relying on the Public Interest Derogation.

These Guidelines provide information on when the EDPB considers transfers to be "*occasional and not repetitive*" and describes a "*necessity test*" as being one of the overarching requirements for the transfer of personal data relying on a derogation (i.e. is the transfer necessary for the specific purpose of the derogation to be used). The EDPB strongly encourages appropriate safeguards (such as the AA) when transfers are made "*in the usual course of business or practice*". In the Sub-group's discussions with the EDPB, the Sub-group conveyed its belief that IOSCO member authorities can continue to rely on the Public Interest Derogation for transfers made in exceptional circumstances, and the EDPB appeared to accept this.

The Sub-group believes the "*necessity test*" will be met for requests for assistance under the MMoU and EMMoU. Assessment on whether a transfer is "*occasional and not repetitive*" will be made on a case-by-case basis, however if a non-EU authority frequently requests personal data from an EU authority, it may wish to proactively take steps to sign the AA as soon as possible, as this will provide a safe basis to transfer personal data from jurisdictions that are subject to the GDPR and thereby ensure continued smooth cooperation under the MMoU and EMMoU.

Q10: Will it be necessary to enact new domestic laws to comply with the safeguards set out in the Administrative Arrangement?

A: The AA is not legally binding and does not require the enactment of new domestic laws for its implementation. Rather, it is a commitment by the

[2] An EU authority can transfer personal data to an authority in a non-EU jurisdiction if the jurisdiction has been deemed by the European Commission to have domestic laws equivalent to the GDPR to protect personal data: this is known as an "adequacy decision"

Authorities who sign the AA to apply certain safeguards when dealing with personal data. Each Authority who chooses to sign the AA will need to consider the measures it already applies to personal data (e.g., keeping the data confidential, which can be viewed as good practice and already is required for transfers made under the MMoU, EMMoU and most other arrangements) and determine whether any action is needed to allow it to treat personal data in a manner consistent with the safeguards in the AA.

Q11: I have determined that my authority should sign the Administrative Arrangement. What should I do?

A: An authority that decides to sign the AA needs to be comfortable that it can apply the safeguards in the AA to personal data transferred under the AA. This assessment is made by the authority that wishes to sign. If the authority determines that it is able to treat personal data in a manner consistent with the safeguards in the AA, it should sign the signature page and provide this to the IOSCO Secretariat, which will add the authority's name to the master list of Appendix A and B Authorities on the IOSCO website. Please refer to Q12.

Q12: How can I ensure that my authority meets the safeguards in the Administrative Arrangement? What systems should be put in place?

A: The AA has been drafted in a manner that is high-level and not overly granular, to allow scope for interpretation. It is the responsibility of each Authority who signs the AA to act consistent with the safeguards in the AA. Each Authority has discretion over how best to achieve this within its organization. When maintaining a system to handle personal data, an Authority may wish to consult internally with staff in appropriate departments in the organization that might request or receive personal data under the AA, such as (if applicable) the Enforcement Office, General Counsel's Office, Information Technology Office, etc.

Q13: What is the expectation around the *Transparency* safeguard (#3) in the Administrative Arrangement? My authority is not in a position to reach out to individuals to inform them that we are processing or transferring their personal data (nor would we do so even if were in such a position, as doing so would negatively affect our investigative and supervisory processes).

A: The *Transparency* safeguard does not require that an Authority provide specific notice to an individual whose personal data are being processed and/or transferred by that Authority. If applicable legal requirements in the jurisdiction of an authority require that individual notice be provided to a

data subject whose personal data are being processed and/or transferred, this should be subject to applicable restrictions by the Authority to ensure that the supervisory and enforcement processes of a transferring or receiving Authority are not harmed.

A general privacy notice on the website of each Authority should be posted, along with the AA. The contents of this notice are at the discretion of the Authority posting it, however the Authority is expected to provide information about how and why personal data may be transferred, the rights available to data subjects under applicable legal requirements and how these can be exercised, and information about circumstances in which data subject rights and/or the safeguards in the AA can be delayed and restricted. A template privacy notice has been developed as a sample/reference tool to assist Authorities when drafting this notice, and this will be shared with IOSCO members.

Q14: Will the *Onward transfers and sharing of personal data* safeguard (#6) prevent me from sharing personal data received under the AA with third-party authorities in my own country, such as the police or other law enforcement authorities? I am not certain that such third parties in my country will be able or willing to provide assurances that are consistent with the AA.

A: This safeguard includes an exception in paragraph 6.2 (3) which allows personal data to be shared by a receiving Authority with a third party in its country without obtaining the prior consent of the transferring Authority, nor assurances from the third-party recipient to act consistent with the safeguards in the AA, if the sharing is for purposes that are consistent with the purpose for which the data were initially transferred or with the general framework of the use stated in the request. This language is intended to ensure that the safeguard does not conflict with Article 10 of the MMoU: *Permissible Uses of Information*.

Q15: My authority is not able to accept liability for data subject redress in cases where domestic data protection laws have not been breached. How will the *Redress* safeguard (#8) affect me in this regard?

A: The *Redress* safeguard is not intended to suggest that Authorities should accept liability for an alleged personal data breach in a dispute with a data subject (indeed, as a non-legally binding arrangement, the AA could never impose liability on a participating Authority). By the terms of this safeguard, an Authority will inform the other Authority of the existence of a dispute or claim, and the Authorities will use best efforts to settle the dispute or claim amicably in a timely fashion.

If the dispute cannot be resolved amicably, the Authority will use other methods to resolve the dispute with the data subject, which will include participation in non-binding mediation or other non-binding alternative dispute resolution proceedings initiated by the data subject or the Authority concerned, provided that the data subject's requests are not manifestly unfounded or excessive.

As the outcome of any such proceedings will be non-binding, it will be at the Authority's discretion whether to follow any recommendation that arises from such proceedings. The ultimate enforcement mechanism will be that an Authority that is not acting consistent with the safeguards in the AA may be removed from participation in the AA and will no longer be able to rely upon the AA for transfers of personal data from EU Authorities.

Q16: <u>What is the Oversight Mechanism and how will it work?</u>

A: The OM ensures oversight of the AA by the Assessment Group (AG).

The AG will consist of 7 members: 3 EU (Appendix A) Authorities, 3 non-EU (Appendix B) Authorities and 1 Chair, who can be an EU or non-EU Authority. All members must be AA Authorities. The AG Chair will be the Chair of the IOSCO MMoU Monitoring Group Steering Committee, provided this Authority is an AA Authority (if it is not, the IOSCO Board will select the AG Chair). The 6 EU and non-EU AG members will be selected by the AG Chair after an open call for nominations, and the IOSCO Board must approve these selections.

The AG will monitor the AA by sending a biennial survey to Authorities to identify any issues with implementation of the safeguards consistent with the AA. An Authority that is unable to effectively implement the safeguards consistent with the AA for any reason is expected to self-report issues to the AG. A transferring Authority also may inform the AG if that Authority is of the view that a receiving Authority has not acted consistent with the safeguards in the AA. The AG may recommend a course of action to address issues that arise in the implementation of the AA, including in relation to issues identified through the AG's review of the biennial survey.

The OM also creates an AA Decision Making Group (AA DMG) that can decide to remove an Authority that is not acting consistent with the AA on the basis of a recommendation from the AG. At all times in this process, an Authority that is the subject of a decision will have notice and an opportunity to be heard. In line with IOSCO procedures, any decision to remove an Authority from the AA is subject to an appeal to the IOSCO Board member AA Authorities, who will make decisions in a manner consistent with Board decision making in policy matters, pursuant to the By-Laws of IOSCO and the Board Working Modalities. Further information on the procedures of the OM, AG and AA DMG are set out in the OM procedures document.