Attachment A – IOSCO AA

Administrative arrangement for the transfer of personal data between

Each of the European Economic Area ("EEA") Authorities set out in Appendix A

and

Each of the non-EEA Authorities set out in Appendix B

each an "Authority", together the "Authorities",

acting in good faith, will apply the safeguards specified in this administrative arrangement ("Arrangement") to the transfer of personal data between them,

recognizing the importance of the protection of personal data and of having robust data protection regimes in place,

having regard to Article 46(3) (b) of the 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" or "GDPR")[1],

having regard to Article 48(3) (b) of the Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ("Regulation 2018/1725")[2],

having regard to the relevant legal framework for the protection of personal data in the jurisdiction of the Authorities and acknowledging the importance of regular dialogue between the EEA Authorities and their national Data Protection Authorities, or the European Data Protection Supervisor ("EDPS") in the case of the European Securities and Markets Authority ("ESMA"),

having regard to the need to process personal data to carry out the public mandate and exercise of official authority vested in the Authorities, and

having regard to the need to ensure efficient international cooperation between the Authorities acting in accordance with their mandates as defined by applicable laws to safeguard investors or customers and foster integrity and confidence in the securities and derivatives markets,

have reached the following understanding:

---

[1] OJ L119/1, 04/05/2016
[2] OJ L295/39, 21/11/2018

I. Purpose and Scope

This Arrangement is limited to transfers of personal data between an EEA Authority set out in Appendix A and a non-EEA Authority set out in Appendix B, in their capacity as public Authorities, regulators and/or supervisors of securities and/or derivatives markets.

The Authorities are committed to having in place appropriate safeguards for the processing of such personal data in the exercise of their respective regulatory mandates and responsibilities.

Each Authority confirms that it can and will act consistent with this Arrangement and that it has no reason to believe that existing applicable legal requirements prevent it from doing so.

This Arrangement is intended to supplement existing information sharing arrangements or memoranda that may exist between one or more EEA Authorities and one or more non-EEA Authorities, and to be applicable in different contexts, including information that may be shared for supervisory or enforcement related purposes.

While this Arrangement is specifically intended to provide safeguards for personal data transfers, it is not the only means by which personal data may be transferred, nor does it prohibit an Authority from transferring personal data pursuant to a relevant agreement, another relevant arrangement, or a process separate to this Arrangement, for example pursuant to an applicable adequacy decision.

Effective and enforceable data subject rights are available to Data Subjects under applicable legal requirements in the jurisdiction of each Authority, however this Arrangement does not create any legally binding obligations, confer any legally binding rights, nor supersede domestic law. The Authorities have implemented, within their respective jurisdictions, the safeguards set out in Section III of this Arrangement in a manner consistent with applicable legal requirements. Authorities provide safeguards to protect personal data through a combination of laws, regulations and their internal policies and procedures.

II. Definitions

For the purposes of this Arrangement:

(a) **"applicable legal requirements"** means the relevant legal framework for the protection of personal data applicable to each Authority;

(b) **"criminal data"** means personal data relating to criminal convictions and offences or related security measures;

(c) **"onward transfer"** means the transfer of personal data by a receiving Authority to a third party in another country who is not an Authority participating in this Arrangement and when that transfer is not covered by an adequacy decision from the European Commission;

(d) **"personal data"** means any information relating to an identified or identifiable natural person ("Data Subject") within the scope of this Arrangement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to

an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(e) "**personal data breach**" means a breach of data security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(f) "**processing**" means any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(g) "**professional secrecy**" means the general legal obligation of an Authority not to disclose non-public information received in an official capacity;

(h) "**profiling**" means automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person;

(i) **GDPR Data Subject Rights**: The GDPR generally provides the following Data Subject Rights:

i. "**right not to be subject to automated decisions, including profiling**" means a Data Subject's right not to be subject to legal decisions being made concerning him or her based solely on automated processing;

ii. "**right of access**" means a Data Subject's right to obtain from an Authority confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, to access the personal data;

iii. "**right of erasure**" means a Data Subject's right to have his or her personal data erased by an Authority where the personal data are no longer necessary for the purposes for which they were collected or processed, or where the data have been unlawfully collected or processed;

iv. "**right of information**" means a Data Subject's right to receive information on the processing of personal data relating to him or her in a concise, transparent, intelligible and easily accessible form;

v. "**right of objection**" means a Data Subject's right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her by an Authority, except in cases where there are compelling legitimate grounds for the processing that override the grounds put forward by the Data Subject or for the establishment, exercise or defence of legal claims;

vi. "**right of rectification**" means a Data Subject's right to have the Data Subject's inaccurate personal data corrected or completed by an Authority without undue delay;

vii. "**right of restriction of processing**" means a Data Subject's right to restrict the processing of the Data Subject's personal data where the personal data are inaccurate, where the processing is unlawful, where the Authority no

longer needs the personal data for the purposes for which they were collected or where the personal data cannot be deleted;

(j) **"sharing of personal data"** means the sharing of personal data by a receiving Authority with a third party in its country, or in the case of ESMA the sharing of personal data with a third party within the jurisdictions of the EEA Authorities.

III. Personal data protection safeguards

1. **Purpose limitation:** The Authorities have regulatory mandates and responsibilities which include protecting investors or customers and fostering integrity and confidence in securities and/or derivatives markets. Personal data are transferred between the Authorities to support these responsibilities and are not transferred for other purposes such as for marketing or commercial reasons.

   The transferring Authority will transfer personal data only for the legitimate and specific purpose of assisting the receiving Authority to fulfil its regulatory mandate and responsibilities, which include regulating, administering, supervising, enforcing and securing compliance with the securities or derivatives laws in its jurisdiction. The receiving Authority will not further process the personal data in a manner that is incompatible with these purposes, nor with the purpose that may be set out in any request for the information.

2. **Data quality and proportionality:** The transferring Authority will only transfer personal data that are adequate, relevant and limited to what is necessary for the purposes for which they are transferred and further processed.

   The transferring Authority will ensure that to the best of its knowledge the personal data that it transfers are accurate and, where necessary, up to date. Where an Authority becomes aware that personal data it has transferred to, or received from, another Authority is incorrect, it will advise the other Authority about the incorrect data. The respective Authorities will, having regard to the purposes for which the personal data have been transferred and further processed, supplement, erase, block, correct or otherwise rectify the personal data, as appropriate.

3. **Transparency:** Each Authority will provide general notice to Data Subjects about: (a) how and why it may process and transfer personal data; (b) the type of entities to which such data may be transferred; (c) the rights available to Data Subjects under the applicable legal requirements, including how to exercise those rights; (d) information about any applicable delay or restrictions on the exercise of such rights, including restrictions that apply in the case of cross-border transfers of personal data; and (e) contact details for submitting a dispute or claim.

   This notice will be effected by the publishing of this information by each Authority on its website along with this Arrangement.

   Individual notice will be provided to Data Subjects by EEA Authorities in accordance with notification requirements and applicable restrictions in the GDPR and the national legal framework applicable in the jurisdiction of the EEA Authorities, or in the case of ESMA in

accordance with Regulation 2018/1725 as may be further amended, repealed or replaced.

4. **Security and confidentiality:** Each receiving Authority will have in place appropriate technical and organisational measures to protect personal data that are transferred to it against accidental or unlawful access, destruction, loss, alteration, or unauthorised disclosure. Such measures will include appropriate administrative, technical and physical security measures. These measures may include, for example, marking information as personal data, restricting who has access to personal data, providing secure storage of personal data, or implementing policies designed to ensure personal data are kept secure and confidential.

   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.

5. **Safeguards Relating to GDPR Data Subject Rights:**

   The Authorities will apply the following safeguards to personal data transferred under this Arrangement:

   The Authorities will have in place appropriate measures which they will follow, such that, upon request from a Data Subject, an Authority will (1) identify any personal data it has transferred to another Authority pursuant to this Arrangement, (2) provide general information, including on an Authority's website, about safeguards applicable to transfers to other Authorities, and (3) provide access to the personal data and confirm that the personal data are complete, accurate and, if applicable, up to date.

   Each Authority will allow a Data Subject who believes that his or her personal data are incomplete, inaccurate, outdated or processed in a manner that is not in accordance with applicable legal requirements or consistent with the safeguards set out in this Arrangement to make a request directly to such Authority for any rectification, erasure, restriction of processing, or blocking of the data.

   Each Authority, in accordance with the applicable legal requirements, will address in a reasonable and timely manner a request from a Data Subject concerning the rectification, erasure, restriction of processing or objection to processing of his or her personal data. An Authority may take appropriate steps, such as charging reasonable fees to cover administrative costs or declining to act on a request, where a Data Subject's requests are manifestly unfounded or excessive.

   Each Authority may use automated means to more effectively fulfil its mandate. However, no Authority will take a legal decision concerning a Data Subject based solely on automated processing of personal data, including profiling, without human involvement.

   Safeguards relating to GDPR Data Subject Rights are subject to an Authority's legal obligation not to disclose confidential information pursuant to professional secrecy or other legal obligations. These safeguards may be restricted to prevent prejudice or harm to supervisory or enforcement functions of the Authorities acting in the exercise of the official authority vested in them, such as for the monitoring or assessment of compliance

with applicable laws or prevention or investigation of suspected offenses; for important objectives of general public interest, as recognised in the jurisdiction of the receiving Authority and, where necessary under the applicable legal requirements, of the transferring Authority, including in the spirit of reciprocity of international cooperation; or for the supervision of regulated individuals and entities. The restriction should be necessary and provided by law, and will continue only for as long as the reason for the restriction continues to exist.

6. **Onward transfers and sharing of personal data:**

6.1 Onward transfer of personal data

An Authority receiving personal data pursuant to this Arrangement will only onward transfer the personal data to a third party with the prior written consent of the transferring Authority, and if the third party provides appropriate assurances that are consistent with the safeguards in this Arrangement.

6.2 Sharing of personal data

(1) An Authority receiving personal data pursuant to this Arrangement will only share the personal data with the prior written consent of the transferring Authority, and if the third party provides appropriate assurances that are consistent with the safeguards in this Arrangement.

(2) Where assurances contemplated under the first paragraph cannot be provided by the third party, the personal data may be shared with the third party in exceptional cases if sharing the personal data is for important reasons of public interest, as recognised in the jurisdiction of the receiving Authority and, where necessary under the applicable legal requirements, of the transferring Authority, including in the spirit of reciprocity of international cooperation, or if the sharing is necessary for the establishment, exercise or defense of legal claims.

(3) Where sharing of personal data is for the purpose of conducting a civil or administrative enforcement proceeding, assisting in a self-regulatory organization's surveillance or enforcement activities, assisting in a criminal prosecution, or conducting any investigation for any general charge applicable to the violation of the provision specified in the request where such general charge pertains to a violation of the laws and regulations administered by the receiving Authority, including enforcement proceedings which are public, a receiving Authority may share personal data with a third party (such as public bodies, courts, self-regulatory organizations and participants in enforcement proceedings) without requesting consent from the transferring Authority, nor obtaining assurances, 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, and is necessary to fulfil the mandate and responsibilities of the receiving Authority and/or the third party. When sharing personal data received under this Arrangement with a self-regulatory organisation, the receiving Authority will ensure that the self-regulatory organization is able and will comply on an ongoing basis with the confidentiality protections set forth in Section III (4) of this Arrangement.

(4) A receiving Authority may share personal data with a third party without requesting consent from the transferring Authority, nor obtaining assurances, in a situation where

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.

7. **Limited data retention period:** The Authorities will retain personal data for no longer than is necessary and appropriate for the purpose for which the data are processed. Such retention period will comply with the applicable laws, rules and/or regulations governing the retention of such data in the jurisdiction of the receiving Authority.

8. **Redress:** Each Authority acknowledges that a Data Subject who believes that an Authority has failed to comply with the safeguards as set forth in this Arrangement, or who believes that his or her personal data have been subject to a personal data breach, may seek redress against that Authority to the extent permitted by applicable legal requirements. This redress may be exercised before any competent body, which may include a court, in accordance with the applicable legal requirements of the jurisdiction where the alleged non-compliance with the safeguards in this Arrangement occurred. Such redress may include monetary compensation for damages.

   In the event of a dispute or claim brought by a Data Subject concerning the processing of the Data Subject's personal data against the transferring Authority, the receiving Authority or both Authorities, the Authorities will inform each other about any such disputes or claims, and will use best efforts to settle the dispute or claim amicably in a timely fashion.

   If an Authority or the Authorities are not able to resolve the matter with the Data Subject, the Authorities will use other methods by which the dispute could be resolved unless the Data Subject's requests are manifestly unfounded or excessive. Such methods will include participation in non-binding mediation or other non-binding dispute resolution proceedings initiated by the Data Subject or by the Authority concerned. Participation in such mediation or proceedings may be done remotely (such as by telephone or other electronic means).

   If the matter is not resolved through cooperation by the Authorities, nor through non-binding mediation or other non-binding dispute resolution proceedings, the receiving Authority will report this to the assessment group and to the transferring Authority, as outlined in Section IV of this Arrangement. In situations where a Data Subject raises a concern and a transferring Authority is of the view that a receiving Authority has not acted consistent with the safeguards set out in this Arrangement, a transferring Authority will suspend the transfer of personal data under this Arrangement to the receiving Authority until the transferring Authority is of the view that the issue is satisfactorily addressed by the receiving Authority, and will inform the Data Subject thereof.

IV. Oversight

1. Each Authority will conduct periodic reviews of its own policies and procedures that implement this Arrangement and of their effectiveness, the results of which will be communicated to the assessment group described in paragraph IV (4) below. Upon reasonable request by another Authority, an Authority will review its personal data

processing policies and procedures to ascertain and confirm that the safeguards in this Arrangement are being implemented effectively. The results of the review will be communicated to the Authority that requested the review.

2. In the event that a receiving Authority is unable to effectively implement the safeguards in this Arrangement for any reason, it will promptly inform the transferring Authority and the assessment group described in paragraph IV (4) below, in which case the transferring Authority will temporarily suspend the transfer of personal data under this Arrangement to the receiving Authority until such time as the receiving Authority informs the transferring Authority that it is again able to act consistent with the safeguards.

3. In the event that a receiving Authority is not willing or able to implement the outcome of the non-binding mediation or other non-binding dispute resolution proceeding referred to in Section III (8) of this Arrangement, it will promptly inform the transferring Authority and the assessment group described in paragraph IV (4) below.

4. An assessment group ("Assessment Group") established as a sub-committee of the Authorities by the International Organization of Securities Commissions ("IOSCO") will conduct periodic reviews on implementation of the safeguards in this Arrangement, and will consider best practices with a view to continuing to enhance the protections of personal data where appropriate. Following notice and opportunity to be heard, if the Assessment Group determines that there has been a demonstrated change in the willingness or ability of an Authority to act consistent with the provisions of this Arrangement, the Assessment Group will inform all other Authorities thereof. For purposes of its review, the Assessment Group will have due regard to the information provided by a receiving Authority not being willing or able to implement the outcome of the non-binding mediation or other non-binding dispute resolution proceeding referred to in Section III (8) of this Arrangement. Personal data pertaining to Data Subjects involved in any such proceedings will in principle be anonymized before being provided to the Assessment Group. In addition, the Assessment Group may develop recommendations with respect to the enhancement of the Authority's policies and procedures for the protection of personal data.

5. The Assessment Group will make written recommendations to an Authority where the Assessment Group finds material deficiencies in the policies and procedures that the Authority has in place to implement the safeguards. If the Assessment Group determines that material deficiencies are not being addressed and that there has been a demonstrated change in the willingness or ability of the Authority to act consistent with this Arrangement, following notice and an opportunity to be heard, it may recommend to the AA Decision Making Group ("AA DMG") that the Authority's participation in this Arrangement be discontinued. Any decision of the AA DMG may be appealed by an Authority or by the Assessment Group to the IOSCO Board members that are Authorities.

6. In situations where a transferring Authority is of the view that a receiving Authority has not acted consistent with the safeguards set out in this Arrangement, a transferring Authority will suspend the transfer of personal data to the receiving Authority under this Arrangement until the issue is satisfactorily addressed by the receiving Authority. In the event that a transferring Authority suspends the transfer of personal data to a receiving

Authority under this paragraph IV (6) or under paragraph IV (2) above, or resumes transfers after any such suspension, it will promptly inform the Assessment Group, which will in turn inform all other Authorities.

V. Revision and discontinuation

1. The Authorities may consult and revise by mutual consent the terms of this Arrangement in the event of substantial change in the laws, regulations or practices affecting the operation of this Arrangement.

2. An Authority may discontinue its participation in this Arrangement, vis-à-vis another Authority or Authorities, at any time. It should endeavour to provide 30 days' written notice to the other Authority or Authorities of its intent to do so. Any personal data already transferred pursuant to this Arrangement will continue to be treated consistent with the safeguards provided in this Arrangement.

3. The European Data Protection Board ("EDPB"), or the EDPS in the case of ESMA, will be notified by IOSCO of any proposed material revisions to, or discontinuation of, this Arrangement.

Attachment B – Signature Page

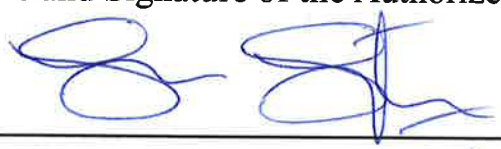
Administrative Arrangement for the Transfer of Personal Data between each of the European Economic Area ("EEA") Authorities set out in Appendix A and Each of the non-EEA Authorities set out in Appendix B

Appendix A Signatory ☐ or Appendix B Signatory ☑ (please select)

Name of the Signatory:

Australian Securities and Investments Commission

Name and Signature of the Authorized Representative:



James Shipton, Chair, Australian Securities and Investments Commission

Date of Signature:

2 SEPTEMBER 2019