AIA Group

Data Privacy Policy

Incorporating

All legal entities

Document Details

Document Name	Data Privacy Policy
Document Version	3.0
Originating Business Function	Group Risk & Compliance
Policy Owner	Group Chief Risk Officer
Primary Policy Contact Person	Head of Group Compliance
Secondary Policy Contact Person	Head of Data Privacy Programme and Compliance Operations, Group Compliance
Date of First Issuance	12-NOV-2009
Date of Last Approval	14-MAR-2019
Version Effective Date	31-MAR-2019
Endorsed by	AIA Group Operational Risk Committee and Board Risk Committee
Approved by	AIA Group Board
Review Frequency	Minimum once a year or when needed
Next Review Date	31-MAR-2020
Document Type *Per Corporate Policy Governance Standard*	Group Policy
Information Classification *Per Group Data Protection Standard*	Restricted
Related Policies and Standards	AIA Group Information Security Policy AIA Group Physical Security Standard AIA Group Records Management Policy and Guidelines AIA Group Incident Management Standard AIA Group Sourcing Policy AIA Group Outsourcing Standard

VERSION CONTROL

Version	Amendments	Approval Date	Approved by
1.0	First Release	OCT-2011	Group Risk & Compliance
2.0	Major amendments include: 1. Major provisions of the Hong Kong Personal Data (Privacy) (Amendment) Ordinance 2012; 2. Definition of Personal Data, and the role of the Data Protection Officer; 3. Examples of Privacy Policy Statements, Summary of Direct Marketing Consent Requirements, Guidelines for Handling Third Party Data, and Guidelines for Storage and Retention of Personal Data in Personal Computers and Mobile Storage Devices; 4. Operational Controls updates based on historical incidents; and 5. Various housekeeping amendments.	MAR-2015	Group Risk & Compliance
3.0	Major amendments include: 1. Revising the key data privacy principles from the six Hong Kong principles into 11 principles which closely reflect the major risk areas; 2. Clarifying roles and responsibilities of the Data Protection Officer; 3. Ensuring consistency in assessing and reporting significant breaches to regulators and appropriately notifying customers. (These will be aligned with local regulations, where applicable); 4. Enhancing minimum standards in privacy notice and consent languages to future proof emerging business practices; 5. Requiring cookie policy and pop-up notice in all AIA websites to inform Data Subject on activity tracking; 6. Implementing Privacy Impact Assessment (“PIA”) as a mandatory tool to systemically assess impact of business initiatives on data privacy risk; and 7. Expanding Data Subject Request handling requirements to align with emerging regulatory expectations and subject to local legal requirements.	MAR-2019	Group Risk & Compliance

DISTRIBUTION LIST

All Employees

Contents

1. Introduction

1.1. Purpose and Background

The AIA Group ("AIA" or "the Group") Data Privacy Policy (the "Policy") outlines the Group's statement of values and provides guidance on how Personal Data should be collected, used, stored, transferred and disposed of by the Group. It clarifies the roles and responsibilities of employees, and the relevant standards and procedural controls expected to secure Personal Data in accordance with the Policy objectives.

Please refer to Appendix B for a summary of the Policy.

'DPP #' denotes mandatory Data Privacy Policy requirements, against which the AIA Group ("Group") and Business Unit ("BU") functions should be able to demonstrate adherence to, unless otherwise exempted by the Group Chief Risk Officer ("Group CRO").

2. Scope and Definitions

2.1. Scope

This Policy applies to Company and its Affiliates, collectively referred to as “AIA Group” or “Group”. This includes all employees, temporary staff, contractors and third-party service providers.

This Policy only applies to the collection, usage, storage, transfer and disposal of Personal Data, and compliance with relevant Data Protection laws and regulations.

For the avoidance of doubt, the use or disclosure of corporate information is out-of-scope for this Policy. For further details on managing corporate information, please refer to the relevant Policies from Group Corporate Communications and Group Legal.

2.2. Definitions

A glossary of terms used in this Policy is provided in Appendix G. Terms are capitalised throughout the document.

2.3. Interpretation and Application

In this Policy, the following rules of interpretation apply unless otherwise specified:

a) If applicable local laws, regulations or regulatory guidelines require higher standards than the requirements of this Policy, then the higher local standards must be met. If the definitions of Personal Data or Sensitive Personal Data in local Data Protection laws and regulations differ from the definitions articulated in this Policy, the requirements of this Policy must be adapted according to the local definitions. Where any conflict arises between local requirements and this Policy, BUs should explain to the Group how the implementation of this Policy would be affected and seek necessary exemptions or exceptions;

b) Headings are for convenience only and do not affect the interpretation of this Policy;

c) The singular includes the plural and vice versa;

d) Words and phrases such as: “such as”, “including”, “particularly” and similar expressions are not used as, nor are intended to be interpreted as, words of limitation;

e) If there is any conflict between the body of this Policy and its appendices, schedules, attachments, and other documents, the terms of the main body of this Policy will prevail; and

f) Stakeholders should bear in mind that definitions of Personal Data and Sensitive Data articulated in Appendix G are not exhaustive and will depend on the circumstances. For example, data used in combination with other data may result in it being classified as Personal Data.

The interpretation and application of this Policy is at the discretion of Group Risk & Compliance. Any dispute as to such interpretation and application shall be resolved by the Group CRO.

2.4. Consultation

This Policy has been consulted with the following parties as per the Group Corporate Policy Governance Standard ("CPG Standard"):

- Group Corporate Security
- Group Legal
- Group Sourcing
- Group Technology
- BU Compliance

3. Roles and Responsibilities

High level key roles and responsibilities in relation to the Group's Data Privacy Programme are identified below.

BUs must implement a Compliance programme to enforce and monitor compliance with the Policy. The Policy and any local laws or regulations in relation to Data Privacy should support the programme.

Responsible Party	Key Obligations
All employees	▪ Understand how data protection impacts on the nature of their work, make themselves familiar and follow the terms contained in the Policy when handling or managing Personal Data. ▪ Immediately report any suspected Personal Data Privacy Breaches in accordance with the Policy.
CEOs	▪ Ultimately responsible for the implementation of procedures and controls contained in this Policy and compliance of their respective BUs with the requirements of the Policy, through the relevant Risk and Compliance certification process. ▪ Retain ultimate accountability to relevant authorities for their respective BU's Compliance with its legal and regulatory obligations in relation to Personal Data Privacy.
Business Function Heads	▪ Implement the procedures and controls contained in this Policy.
Compliance / Data Protection Officer or equivalent ("DPO")	▪ Develop, issue and oversee implementation of Group / BU Data Privacy Policy. ▪ Provide advice and consultation on Data Privacy related matters (such as AIA's obligations to comply with relevant regulations) and how to manage the associated risks. ▪ Provide Second Line oversight and monitoring of effective implementation by relevant business functions, including assurance and validation, by testing the adequacy and effectiveness of the Operational Controls. ▪ Monitor regulatory developments and practice to ensure compliance. ▪ Develop, maintain and provide Data Privacy compliance training programmes. ▪ Escalate and consult with Group / BU Data Governance Committee or Steering Group any material Data Privacy issues, which may have wider Group / BU impact. ▪ Oversee incident management and escalate material Policy / Personal Data Privacy Breaches to Group senior management, as appropriate. ▪ Coordinate notification and reporting requirements to individuals and regulators, if necessary.
Legal	▪ Provide legal advice and support for the management of Personal Data Privacy across the Group.
Technology and Operations	▪ Set relevant Information Security Policies and Standards in relation to Data Privacy controls, oversee and provide guidance on their implementation.
Corporate Security	▪ Set relevant physical security standards in relation to Data Privacy controls, oversee and provide guidance on their implementation.

4. Main Provisions

4.1. Mandatory and Minimum Requirements

4.1.1. Key Data Privacy Principles

This table sets out the key data privacy principles that must be followed when Personal Data is collected, accessed, used, stored, transferred, and disposed of.

DPP 1 – Notice/Purpose

Specific information must be communicated in a clear, easy to understand format to Data Subjects by way of a notice when collecting personal data from them. Process personal data only for the purposes notified.

DPP 6 – Direct Marketing

Provide sufficient notices and obtain requisite consents from Data Subjects for direct marketing. Direct marketing must not be conducted outside the scope of notice/consent. Ensure Data Subjects are provided with a specific channel to opt out.

DPP 2 – Consent

Determine whether (explicit) consent from Data Subjects is required. Where required, ensure consent is informed, specific and freely given. Express consent is usually required for direct marketing and when sensitive personal data is involved.

DPP 7 – Security

Ensure appropriate measures are implemented to maintain security and protect against unauthorised access, loss or use of personal data. Follow guidelines set out in relevant information security policies and physical security standards.

DPP 3 – Accuracy/Storage/ Retention

Keep personal data accurate and only for as long as is necessary to fulfil the purpose for which it was collected. Personal data should be deleted or disposed of when it is no longer necessary for any business or legal purposes.

DPP 8 – Data Subject Requests

The Data Subject may have certain individual rights such as access to and correction of personal data. Data Subject requests should be directed to the relevant managers to ensure proper handling.

DPP 4 – Transfers/Processing

Personal data may only be transferred and processed when Data Subjects are informed, and consent may be required. Appropriate safeguards should be put in place when transferring or disclosing personal data to third parties.

DPP 9 – Breach Notification

Any suspected or actual personal data breach must be reported to the relevant managers immediately. Notification to local regulators and (in some cases) Data Subjects may be required.

DPP 5 – Overseas Transfers/ Processing

Ensure special conditions enabling cross-border transfers/processing are met. Assess any potential regulatory implications for cross-border data transfer /processing activities.

DPP 10 – Privacy Impact Assessment

Conduct privacy impact assessment where necessary prior to processing personal data that is likely to present higher privacy risks due to its nature or the scope of the processing operation. Minimise identified privacy risks

DPP 11 – Compliance Controls

Privacy Policy Statement should be established. Adequate education and awareness, and monitoring and testing activities should be put in place.

To comply with these principles in practice, all Personal Data collected by a BU should be managed in accordance with the Operational Controls set out in section 0. BUs may put in place stricter controls to meet local legal or regulatory requirements or best practice guidance.

4.1.2. Operational Controls

4.1.2.1. Notice and Consent for Data Subjects (DPP 1 and 2)

Data Subjects must be provided with specific information about how a BU collects, uses or discloses Personal Data and for what purposes it will be used. Personal Data must only be used for the purposes which have been communicated to the Data Subject. BUs should follow the procedures outlined in the table below in the notice and consent requirements.

Content of Notification and Consent	Timeline for Notification and Consent
As a minimum, the notice must contain: ▪ the AIA entity/ies who is/are the data controller ▪ types of personal data that will be collected, used or disclosed, e.g. name, contact details ▪ the reasons why the personal data is collected, used or disclosed ▪ details of with whom the personal data will be shared, e.g. group entities, services providers, third parties ▪ details of any transfer to other locations outside of the jurisdiction in which the BU operates/Data Subject is located ▪ any rights of the individual to which the personal data relates, e.g. right to request access, right to correction ▪ contact details of the person/role to whom an individual can make a request or compliant or, where relevant, the contact details of the applicable DPO (or equivalent). For direct marketing: ▪ the AIA entity/ies who will be sending the direct marketing communications ▪ types of personal data that will be used for direct marketing purposes, e.g. name, contact details ▪ the types of products or services which will be marketed ▪ whether the personal data will be shared with third parties to carry out direct marketing ▪ how an individual can opt-out of receiving direct marketing materials. ▪ separate non pre-ticked boxes to obtain consent.	Consent from Data Subjects must be obtained **as soon as possible,** before Personal Data can be used or processed. Notice of data collection must be given on or before the Personal Data is collected from the Data Subject (i.e. at the first point of contact). Examples include: ▪ Policy application forms - privacy notice/consent at the end of the application form. ▪ Point-of-sale machines where Personal Data is collected. ▪ Websites and mobile apps - Privacy Statement brought to the attention of the Data Subject before they submit their Personal Data (and which is made available to the Data Subject generally/periodically). ▪ Candidate and employee application/HR forms - privacy notice/consent at the end of the applicable forms and/or employment contracts. ▪ A process should be developed to keep track of what version of the notice has been provided to a particular Data Subject so as to determine under what circumstance consent was given and the relevant notified/agreed to purposes - for example logged on the Customer Relationship Management System.

Format of Notices and Consent	Cookies & Tracking Technologies
▪ **In writing**, unless it is otherwise approved to be given verbally using an approved script. ▪ It must be **clear and easy to understand** (e.g. font size, spacing and layout). The details of the notice cannot be buried among other terms and conditions such that Data Subjects would not read it. ▪ **Prominent** – the notice/consent should be included in all documents that capture Personal Data and prominently posted where Personal Data is gathered through other channels. ▪ Each type of notice/consent must be **tailored** to cover the specific Personal Data collection, use and disclosure proposed, and **must** be endorsed and agreed by the BU Legal. If Personal Data is collected by a Processor, see section 4.1.2.5 or by another third party, section 4.1.2.2.	▪ Before conducting any customer tracking and profiling activities, BUs must understand the scope of such activities so as to check whether such activities are already covered by the scope of an existing notice/consent from the relevant Data Subjects. ▪ BUs should establish a cookies policy if they are using tracking cookies in any of the AIA websites. Please see AIA Group Cookie Policy in Appendix C - BUs should review this and amend as necessary. ▪ Data Subjects should be given to opportunity to accept or reject the cookies policy when they access any AIA website for the first time. If the cookies policy is rejected, no tracking activities should be undertaken/continued.

- Local laws and regulations in some jurisdictions require additional information to be provided, e.g. data retention period; data security measures put in place; and specific additional safeguards for Sensitive Personal Data.
- The notice (especially details about the purposes and transfers) should be as detailed as possible, otherwise new consent may be required to process Personal Data for new purposes or transfer Personal Data to new recipients/locations.
- If consent is obtained it should be freely given, specific and informed – Data Subjects must give consent by a statement or clear affirmative action. Consents should be separated from general terms and conditions. The use of pre-ticked boxes is not permitted.
- Do not conduct any business solicitation activities or marketing activities or target any customers in any EU/EEA countries. This includes any campaigns through websites and social media platforms. Refer to the relevant requirements in the AIA Group Offshore Customer Guidelines.
- Do not include any European language options (except English), and do not allow payment in any European currency on websites or apps, in any e-business initiative.

An example of consent statements is in Appendix D – BUs should review and amend as necessary before deployment.

4.1.2.2. Data Collection from External Sources (DPP 1 and 2)

If Personal Data is bought or obtained from an external source (including any social media platforms), BUs must follow the requirements articulated below:

Due Diligence

The responsible department should undertake a due diligence review on the data provider, supported by the BU Legal.

Written Confirmation

The data provider must provide the BU with written confirmation of the following:

- It has given written notice to the Data Subject and obtained his/her written consent to the Personal Data being supplied to the BU (or a category of business within which the BU falls); and
- The use of the Personal Data (as contemplated by the BU) is consistent with the notice given to, and consent obtained from, the Data Subject.

Validation

The data provider's notice to, and consent obtained from, the Data Subject must be validated by the responsible department.

In validating the notice/consents, the responsible department must look at:

- The manner of collection;
- Whether the data provider has given written notice to the Data Subject and obtained their written consent to the Personal Data will be supplied to the BU **for gain** (if relevant); and
- Whether the consent obtained was consistent with the intended use.

Data Segregation

The third-party data should be retained or backed up in such a way that it can be identified and returned to the data provider if required under the contract with the data provider.

Direct Marketing Consent

The BU should take specific actions, and obtain the necessary consent from the Data Subject, before using the Personal Data for the BU's own direct marketing purposes, even if the relevant consents obtained by the data provider have been validated.

Check Do Not Call Register

If a BU holds a Do Not Call ("DNC") list or there is a national DNC register or similar registers, the BU must run through the DNC lists/registers against the third-party data for outbound telesales activity and any business activities restricted by such lists/registers.

The contract with the data provider (see above) should also explicitly state which party is responsible for checking data against a national DNC register or similar registers, if such registers exist.

Note: If the external source is a bancassurance partner, the relevant Partner Distribution function can determine the extent of due diligence, written confirmation and validation process.

4.1.2.3. Data Collection via Monitoring and Surveillance (DPP 1 and 2)

Personal Data collected via monitoring or surveillance (e.g. through monitoring of employees' emails or online activities, or through targeted CCTV surveillance) must be handled in accordance with applicable Personal Data Protection laws and regulations.

BUs should conduct an assessment of the risks of monitoring against the benefits derived, having regard to the business needs and purpose for monitoring, and consider whether less privacy intrusive alternatives are available which may be equally cost effective and practical. The purpose is to assist in determining whether monitoring and surveillance is the best in a range of options given the risk and activities to be managed.

In particular, BUs should consider:

- Formulating policy that clearly specify the monitoring purposes, the circumstances under which monitoring may take place and the purposes for which Personal Data obtained from monitoring records may be used;
- Communicating with Data Subjects to inform them of the nature of, and reasons for, the monitoring of their activities prior to undertaking monitoring; and
- Implementing controls over the holding, processing and use of monitoring records to safeguard the protection of Data Subject's Personal Data contained in them.

It is also advisable to have transparent CCTV notices, policies and practices. Additional issues to be considered for CCTV use include:

- Ensuring it is necessary to use CCTV;
- Positioning of cameras and notices;
- Handling of recorded images, and
- Transfer of CCTV records to third parties.

Please also refer to Group Physical Security Standards for CCTV requirements.

4.1.2.4. Data Accuracy, Storage and Retention (DPP 3)

- Practical steps must be taken to ensure that Personal Data is accurate and up to date.
  - Establish processes to verify accuracy of Personal Data, and rectify any incorrect, inaccurate, ambiguous, misleading or outdated Personal Data which is known to AIA.
  - Do not use Personal Data that may be inaccurate.
  - BU should consider refreshing any Personal Data provided to Data Processor periodically to ensure the most up-to-date information is always processed.

- Only Personal Data that is necessary for the notified/relevant/ related purposes must be retained.
- Personal Data should be kept for only as long as is necessary for business or legal purposes, or for the period notified to Data Subjects. Where Personal Data is no longer needed, it must be irretrievably anonymised (if can be achieved at a reasonable cost) or permanently deleted/destroyed.
  - BUs must follow the data retention periods, and the deletion/destruction/anonymisation procedures set out in the AIA Group Records Management Policy and Guidelines.
  - Ensure contractual arrangements with Processors prevent any Personal Data transferred to them be kept for longer than necessary.
  - Personal Data should not be permanently stored on the company's desktop or notebook computer hard drive or any mobile storage devices.

4.1.2.5. Data Processor Engagement (DPP 4)

Appointing Data Processors

Where a BU engages a third party to process Personal Data on its behalf, certain safeguards must be put in place, including:

- Verifying (through due diligence, contractual assurances and monitoring) that the Processor adopts appropriate security measures to prevent the unauthorised or accidental access, loss or use of Personal Data
- Ensuring clear instructions are given to the Processors in respect of the use, transfer, disclosure, transmission, storage and destruction of the Personal Data given to them. In particular, the Processor should not transfer or disclose the Personal Data without the BU's consent
- Ensuring the Processor implements appropriate data retention and data accuracy measures, and more generally complies with Group Policies, applicable laws and regulations, and industry practices
- Ensuring the Processor flows down data protection/ security obligations to its subcontractors to ensure they too protect the Personal Data
- Having a right for the BU (and its regulators) to monitor and audit the Processor's (and its sub-processors') compliance with data protection/ security obligations
- Regular reporting by the Processor to the BU on its processing activities
- Immediate notification by the Processor to the BU in the event of an actual or suspected Personal Data Breach
- Ensuring at the end of the engagement, Personal Data is returned or deleted/destroyed unless it is required by law for the Data Processors to retain the Personal Data

If the Processor is a business partner or another AIA Group entity, the BU Department Head should determine if a similar assessment/engagement process will be conducted.

Managing Data Processors

- Ensure periodic monitoring of Processors, in accordance with the AIA Group Sourcing Policy, AIA Group Outsourcing Standards, and the Group IT Third Party Security Standard.
- Keep a list of all third-party business partners that process or handle AIA's personal data in the EU/EEA countries, and keep a record of all Personal Data that has been disclosed to Processors; and Processors in the EU/EEA countries.
- Do not disclose Personal Data to a Processor unless it is absolutely necessary for them to complete the task. Do not disclose Personal Data for testing purposes.

4.1.2.6. Personal Data Transfer Protocol for Corporate Solutions Business (DPP 4)

In general, BUs should only transfer aggregated, anonymised data to employers/intermediaries, be rigorous in adhering to practices that ensure data is truly anonymised; and do not provide individuals' claims data or data that can be traced back to an individual in any form to intermediaries or employers.

Individual claims data can only be provided in exceptional cases. Even where local regulations would allow the transfer of individual data, it should not be done unless Group Corporate Solutions, BU Compliance and BU Legal have been consulted.

For any provision of individual's data, BUs must ensure that:

- There are appropriate agreements in place limiting the transferee's use of the data, requiring them to protect the data and giving AIA contractual remedies, and
- Group IT and Operations are consulted to ensure that the appropriate security checks have been carried out on the transferee's IT systems.

Refer to Group Corporate Solutions for any clarifications.

4.1.2.7. Overseas Data Transfers and Cloud Storage (DPP 5)

Certain jurisdictions require additional measures to be put in place for overseas data transfers (i.e. outside the jurisdictions in which the Personal Data was collected), or if it involves processing or storage of Personal Data in a cloud environment. Such measures will vary between jurisdictions: for example, some jurisdictions prohibit the transfer of Personal Data overseas or consent of the Data Subject will be required.

This includes transfers of data between BUs in different jurisdictions, including by storing the data in a centralised system or cloud storage.

The following should be put in place to strengthen controls over overseas data transfer activities:

- Conduct due diligence on the destination jurisdiction in relation to the adequacy of its privacy regime.
- Verify written consent from the Data Subject to the transfer activities.
- Adopt appropriate contractual measures such as model contract clauses or intra group data transfer agreements.
- Implement adequate technical controls for data transmission, e.g. encryption.

For any intra group data transfer activities, both sending and receiving BU should have appropriate intra group data transfer agreements in place to strengthen governance in data transfer. Consult BU Legal and BU Compliance if necessary.

In addition to the general safeguards to be put in place when transferring or sharing Personal Data, seek advice from BU Legal and Compliance on the following potential recipients. These recipients, owing to their nature, may pose significantly higher business, regulatory and reputational risks in case of any Personal Data Breach incidents:

- Overseas regulators;
- Medical experts and private detectives;
- Bancassurance partners, in particular on direct marketing activities and sharing of customer databases; and
- Brokers and Corporate Solutions customers.

Management of Personal Data in the Cloud Environment

If Personal Data is to be processed on or stored using cloud computing (whether the cloud service is operated by a BU or a Processor), applicable Personal Data Protection laws and regulations, and AIA Group IT Standards must be complied with. In particular, a PIA should be undertaken and the following should be considered:

- Whether the relevant PICS permits transfer to the cloud, and/or is consent required (e.g. because of the additional purposes/transferees or overseas data transfers).
- What type of cloud is being proposed – public, private, hybrid etc.
- Consider any local regulatory restrictions in storing the Personal Data in question in the cloud environment. It may not be appropriate for certain types of Personal Data (e.g. government issued id), or may only be appropriate for encrypted or anonymised data.
- Ensure that the cloud storage service/platform in practice enables the BU to fulfil its legal and regulatory obligations (e.g. enables the BU to respond to Data Subject access/correction requests within required timeline).
- Put in place robust contractual safeguards with the cloud service provider, including (without limitation):
  - Appropriate security levels and data protection commitments, and audit rights to verify data protection and security commitments;
  - Erasure or return of Personal Data (including backups if technically feasible) upon request, contract completion or termination; and
  - Personal Data Breach notification and remedy obligations.
- Ascertain the cloud service provider's sub-contractors and ensure contractually that the same level of protection (both technical and administrative) and compliance controls (monitoring and remedial actions) are equally applicable to the cloud service provider's sub-contractors.
- The laws and regulations on cross-border transfers of Personal Data may apply certain relevant conditions to permit the cross-border transfer. In addition, identify whether:
  - The BU knows in which jurisdictions the data will be stored; and
  - The laws and regulations in those jurisdictions provide adequate safeguards of the data (including checking whether there are substantially similar protections to those in the Jurisdiction of the relevant BU and protections regarding local law enforcement agencies' access rights to the records).

4.1.2.8. Direct Marketing (DPP 6)

BUs may collect Personal Data from individuals in different situations for different purposes, e.g. during insurance application or in an insurance claim. BUs should ensure that the privacy notice referred to in section 4.1.2.1 is tailored to fit the particular circumstances in which Personal Data is collected. BUs should observe the following when undertaking direct marketing communications. In addition, BUs are prohibited from selling any Personal Data to any third parties for profit.

Personal Data Requirements for Direct Marketing Communications

- Before using Personal Data in any direct marketing programme, BUs must inform the Data Subject of certain prescribed information (either verbally or in writing) and obtain their consent to the intended use.
- Direct marketing consent is a mandatory requirement some jurisdictions. A summary of direct marketing requirements applicable to the Group's internal and third-party usage is included below.
- Each BU shall determine how and when the direct marketing consent shall be obtained, based on local regulations and practices.
- As a minimum, the prescribed information shall include:

- The AIA entity/ies who will be sending the direct marketing communications
- Types of Personal Data that will be used for direct marketing purposes, e.g. name, contact details
- The types of products or services which will be marketed and whether it is for gain
- Whether the Personal Data will be shared with third parties to carry out direct marketing
- How an individual can opt-out of receiving direct marketing materials
- Separate non pre-ticked boxes to obtain consent
- If the reply is given verbally, BUs must send written confirmation to the Data Subject within 14 days (or a period as stipulated in local regulations) of the reply receipt date before using the Personal Data in direct marketing

- A list of opted-out Data Subjects or a DNC list must be maintained.
- The updated opt-out list or DNC list must be passed to call centres, agents and any other parties who contact customers on the Group's behalf.
- BUs must notify Data Subjects of their opt-out right when using Personal Data in direct marketing for the first time, irrespective of whether the Personal Data is obtained directly from a Data Subject or from other sources.
- If at any point a Data Subject requests their Personal Data not to be used for direct marketing, communications, BUs must comply with the Data Subject's opt-out requirement.
- Identify customers residing in any EU/EEA countries (or flag such customers in the system) – for example, when processing requests for address change, identify if an address is in the EU/EEA countries. Include them to “Do Not Call” or similar list to avoid active selling / marketing to them in future.
- Include remarks in any direct marketing communications and e-business websites that products can only be purchased locally (i.e. onshore in the jurisdiction of AIA’s operations) and limit address fields to capture local address only.

Please also see below additional requirements on the use and provision of Personal Data for direct marketing activity.

	Use of Personal Data in Direct Marketing by BUs that collected the Personal Data	Provision of Personal Data for use in Direct Marketing (to other BUs or third parties)
Prescribed Information (to be provided to Data Subject)	▪ Intention to use Personal Data for direct marketing ▪ BUs will not use Personal Data unless consent is given by the Data Subject ▪ The kind of Personal Data to be used ▪ The classes of marketing subjects	▪ Intention to provide Personal Data to others for use in direct marketing ▪ Data User will not provide the Personal Data unless consent is given by the Data Subject ▪ Whether the Personal Data is to be provided for gain ▪ The kind of Personal Data to be provided ▪ The classes of persons to be provided with Personal Data ▪ The classes of marketing subjects

	Use of Personal Data in Direct Marketing by BUs that collected the Personal Data	Provision of Personal Data for use in Direct Marketing (to other BUs or third parties)
Formality Requirements	▪ Easy to read and understandable ▪ Either orally or in writing ▪ If it is given orally, written confirmation to be sent within 14 days (or a period as stipulated in local regulations)	▪ Easy to read and understandable ▪ In writing
Consent of Data Subject	Required (orally or in writing)	Required (in writing)
Consent Revocable	Yes	Yes
Response Channel	Required	Required (in writing)
Grandfathering Arrangement (subject to local law)	Applicable	Not Applicable

4.1.2.9. Security of Personal Data (DPP 7)

Personal Data should be protected against unauthorised or unlawful processing and against accidental loss, access, processing, interception by unauthorised third parties, erasure, destruction, or damage.

You must follow the security controls set out in the relevant AIA Group Security Policies and Standards. These include:

- Implement procedural, physical and logical access controls.
- Maintain documents containing Personal Data in a secure environment in accordance with AIA Group Physical Security Standards.
- Adopt adequate IT security measures and access control on Personal Data stored electronically in computer or portable devices.
- Keep Personal Data confidential – all BUs, employees and Processors are subject to contractual confidentiality obligations at all times, including after the business relationship has terminated.
- Put in place sufficient data security obligations in contracts with Data Processors, supporting by regular monitoring/audit.

Contact IT Department, Corporate Services/Security Department, Legal Department or your Department Head for further information.

Handling of Biometric Data

- If biometric data is to be collected, the relevant BUs should conduct a specific PIA to assess: the need for collecting biometric data; whose biometric data should and could be collected; and the extent of the biometric data to be collected. The BUs should also provide Data Subjects with free and informed choice to allow the collection of their biometric data, together with explanation of the rationale of collecting such data.
- BUs may collect biometric data just for confirming the identities of individuals and as such they should choose verification biometric systems to minimise the number of biometric features to be collected.
- Strong controls for access to, use and transfer of biometric data should be established. Procedures should be devised to ensure the proper use of biometric data collected, and to prevent unnecessary linkage between the biometric database and with other IT systems that may result in the transfer or change of use of the biometric data inadvertently.
- Regularly and frequently purge biometric data which is no longer required for the purpose for which it was collected.
- The system used to store and process the biometric data should be regularly evaluated to ensure that adequate effective security and privacy protective measures are in place.
- Encrypt the biometric data while it is being store or transmitted.
- Data access is restricted to authorised persons on a need-to-know basis and is protected by strong passwords, while all such accesses are recorded for review.

4.1.2.10. Data Subject Requests (DPP 8)

Data Subjects have rights to make certain requests regarding their Personal Data. These vary under local Data Protection laws and regulations, and may include rights to:

☑ Access their Personal Data	☑ Object to processing or profiling (in certain circumstances)
☑ Verify or request a copy of their Personal Data	☑ Withdraw consent
☑ Correct their Personal Data	☑ Select preferences about automated decision making
☑ Erase their Personal Data	☑ Be forgotten
☑ Restrict processing of their Personal Data	☑ Data portability

Response to Data Subject Requests

Customers may make requests via the website or by contacting the relevant person listed in the privacy notice given with their policy information. Where this is the case the relevant nominated contact will redirect the request to the appropriate department. Group Employees, Contractors and BUs should respond to requests as outlined below.

Date Subject Request recipients should note the following:	
Refer	Contact your Department Head immediately. The Department Head will be responsible for ensuring the Data Subjects request is forwarded to the correct department for proper handling.
Do Not Ignore	Do not ignore a request – in certain jurisdictions the relevant BU has an obligation to provide a response within a short time frame. For example, within 40 calendar days in Hong Kong.
Do Not Respond on Your Own	Do not reply to the request on your own (or any further correspondence) or disclose documents to the Data Subject. Forward any communications to the relevant department which handles data requests.

Considerations on handling Data Subject Requests:	
Respond	Once received, the BU must respond to the request even where the requested Personal Data is not in AIA's possession or has been destroyed. Exemptions to responding are rare (see below). Consider notifying the requested Data Subject on the status of their request. An appropriate identification verification process must be put in place to ascertain the identity of the requestor before responding to their requests. If the request cannot be fulfilled, the requested Data Subject should be notified of the reasons.
Redact	Personal Data not relating to the requested Data Subject must be redacted (e.g. if the Personal Data relates to another individual). Consult BU Compliance or BU Legal regarding any proposed redaction if necessary.
Consider Exemptions	In some situations, BU may be allowed to refuse a request if certain exemptions apply, e.g. it the request may prejudice an ongoing investigation or where the Data Subject is vexatious. These exemptions should only be relied upon if BU Compliance or BU Legal have been consulted.
Do Not Share with Third Parties	Unless the Data Subject has expressly consented to, or authorised, a third party in writing to access or obtain a copy of their requested Personal Data, no data should be provided to any third parties.
Caution regarding Charging a Fee	Unless permitted by local Personal Data Protection laws and regulations (e.g. in Hong Kong, a fee that is not excessive is permissible), a fee should not be charged. There are strict rules on how much can be charged.

Consideration on Data Subject Requests from EU/EEA residents

- If a customer, who is a resident in an EU/EEA country, requests for accessing their data (for example, request for deletion), process those requests in accordance to any local regulatory requirements.
- Process the request from a resident in an EU/EEA country as soon as possible and within one month of receipt. Do notify the requester (and your BU's Compliance) promptly,

certainly within the first month, if in an extraordinary case the process will take longer. Do complete all extended requests no later than three months of receipt.

4.1.2.11. Personal Data Breach Reporting and Notification (DPP 9)

a. Reporting, Escalation and Notification

The below steps set out what to do if there is or you suspect a breach or security incident affecting Personal Data has occurred.

Step 1

If you believe there has been a suspected or actual breach involving Personal Data, notify your direct manager and/or the relevant Compliance team. For privacy-related cyber incident, please also contact your IT helpdesk, Technology Risk Team, or email group-csirt@aia.com immediately.

Step 2

The Head of BU Compliance must record any Personal Data Breaches notified to them on the Compliance database as soon as possible and no later than 36 hours. Any potential major Personal Data Breaches must be escalated to relevant BU Exco members and Head of Group Compliance immediately. Head of Group Compliance will assess if there is a need to escalated to relevant Group Exco members.

Step 3

If there is a confirmed or suspected Personal Data Breach with potential significant impact, the Group Incident Management Process should be activated. Otherwise, the CRO / Head of BU Compliance should lead the incident management with the support from relevant business functions including IT, Security, Legal and Corporate Communications. Human Resources and Agency Distribution should be included in the event the breach involves Personal Data of employees and agents.

Step 4

Assess the likely impact and scope of the actual or suspected Personal Data Breach, including:

- Identifying and assessing the events that lead to the breach
- Identifying any key legal issues or requirements as a result of the breach
- Assessing possible risks and extent of harm faced by the Data Subject, the business impact and required remedial actions to contain and recover the breach
- Coordinating the investigation of the breach and ensuring progress of additional reporting or remedial actions
- Having regard to the nature of the breach and impact on the affected Data Subjects and applicable laws and regulations, deciding on the required or recommended notifications to be sent to relevant regulators, affected Data Subjects and other relevant recipients

Step 5

Coordinate any required or recommended notification and reporting requirements, to the affected Data Subjects or relevant regulators in accordance with local laws and regulations.

- In some jurisdictions, BUs must notify the regulator and impacted individuals if a Personal Data Breach has occurred, and within a specific timeframe. In some cases, BUs can assess if

notification is required if the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of the Data Subjects.

- Where Personal Data Breach notification is not mandatory, BU management or Incident Management Team should assess if breach notification is required. The following should be considered:
  - Whether the leaked Personal Data may be used for identity fraud.
  - Whether it is likely to result in a risk to the rights and freedoms of the Data Subjects.
- Notifications to regulators should include at least:
  - Details about the nature of the breach;
  - The number and categories of individuals and records affected;
  - Consequences of the breach;
  - Remedial actions taken; and
  - Details of the contact person.
- Consider notifying law enforcement agencies if it will help with assisting investigation and containment of the Personal Data Breach
- If the Personal Data Breach is likely to result in a high risk to the rights and freedoms of the Data Subjects, they should be notified of the incident and remedial actions taken
- Data subject notification may not be required if any of the following conditions are met:
  - Appropriate technical and organisational protection measures have been implemented, and the measures were applied to the Personal Data impacted by the breach, in particular those that render the Personal Data unintelligible to any person who is not authorised to access it, such as encryption
  - Subsequent measures have been taken to ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialise;
  - Disproportionate effort will be involved. In such a case, BUs shall instead consider issuing a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner
- In case the impacted individuals are Corporate Solutions' members, BUs must notify the respective corporate clients

b. Additional Notification Requirements (Please note that these should subject to any local regulatory reporting/notification requirements)

- Some regulators have strict timeframes to notify a Personal Data Breach. Most regulators will first allow data controllers (in this case AIA) to investigate whether a breach has occurred and gather evidence and details before having to notify provided, once it has been established with a reasonable degree of certainty that the breach has occurred, the regulator is notified without undue delay.
- Notification is generally not required if the Personal Data Breach is unlikely to result in a risk to the rights of the Data Subjects.

- Always consider whether any other notifications may be expedient (e.g. notifying Internet companies such as Google and Yahoo! may assist to remove the cached information/link from their search engine; notifying law enforcement agencies may assist to investigate the incident).
- If the Personal Data Breach does not impact policyholders/customers, the most appropriate personnel or department should communicate the breach to the affected individuals. For instance, in general the Human Resources Department and the Agency Distribution Department when a breach involves employees and agents respectively.
- Ensure there are contractual arrangements in place with Processors, to notify the BUs without undue delay in the event the Processor is aware of an actual or suspected Personal Data Breach. Such contract should also ensure that the Processor will support and provide necessary information to the BU where required.
- Remember to contact BU Legal before any communications are sent to regulators or affected individuals. Certain jurisdictions have particular requirements as to the content and format of the notices.
- Refer to the AIA Group Incident Management Standards for additional requirement as regards to the investigation, reporting and escalation of incidents, including Personal Data Breaches.

4.1.2.12. Privacy Impact Assessment (DPP 10)

Privacy Impact Assessment ("PIA"), or a similar privacy risk assessment process, should be used to evaluate BU's processing activities in terms of its impact upon Data Privacy, so as to avoid or minimise adverse impacts and ensure appropriate safeguards are put in place.

PIA is a tool which helps to identify an effective way to comply with data protection obligations and meet Data Subjects' expectations of Data Privacy. A template is included in Appendix F.

A PIA should be conducted prior to the following activities, and it can be conducted in conjunction with the Third Party Security Assessment:

- commencing any new business initiative or project that might have impact on Personal Data;
- implementing privacy-intrusive technologies;
- making any major changes in organisational practices involving Personal Data;
- any actions that may result in increased volumes or broader scope of Personal Data being collected, processed or shared; or
- conducting any automated decision making or processing any Sensitive Personal Data.

For activities which do not involve Personal Data, e.g., IT infrastructure change, PIA is not required under most circumstances.

Project Sponsor/Manager, BU Compliance / DPO (or equivalent) and BU Legal have specific roles conducting the PIA. Their responsibilities are outlined below:

- Project Sponsor/Manager should inform BU Compliance / DPO (or equivalent) for any new business initiative or project that might have impact on Data Privacy, and complete the assessment.
- BU Compliance / DPO (or equivalent) should review the appropriateness of the PIA.
- If required, BU Legal should assist BU Compliance to determine whether a project has significant privacy impact on Personal Data or if a tailored PIA is required and obtain support from other relevant departments (e.g. IT, HR) as appropriate.

4.1.3. Compliance Controls (DPP 11)

4.1.3.1. Privacy Policy Statement

Data protection laws and regulations in many jurisdictions require openness and transparency about how organisations process Personal Data. At Group level, we do this by publishing a Privacy Policy Statement on our website and by making a copy available to Data Subjects on request. An example of Privacy Policy Statement is in Appendix E.

Each BU should do the same in their local language to the extent required to meet specific applicable local law requirements.

The Privacy Policy Statement should be reviewed annually or whenever there is any significant change on the local regulatory requirements.

4.1.3.2. Education and Awareness

All employees can access the Policy and local Policies issued by each AIA BU, if any.

Head of BU Compliance should provide or arrange local training for all relevant employees as required, preferably at least on a biennial basis. Attendance records of those training sessions should be maintained in the HR system or by BU Compliance.

Training for Data Processors / agents shall be conducted in accordance with the terms of the contract between the applicable BU and such third parties.

4.1.3.3. Monitoring and Testing

Periodic monitoring activities and testing may be conducted by the Head of Compliance or Group Compliance to monitor compliance with the Policy and the effectiveness of the relevant controls. The results of the assessments must be reported in accordance with the relevant guidelines on compliance review.

Group Compliance may perform monitoring or testing of the control procedures based on the results of any risk assessment. Independent assurance will be provided by GIA as part of its risk based audit programme.

Such monitoring and testing activities should also be extended to Processors. These can be conducted by the concerned business function, BU Compliance or GIA as part of its risk based audit programme, as appropriate.

4.2. Roles and Responsibilities

Roles and responsibilities for covering the requirements of this Policy are set out by the DPP principles, in section 3 and each respective section. Roles and responsibilities in relation to this document are provided within the table below:

Table 1: Roles and responsibilities in relation to this document

Stakeholder	Role
Group Board	Responsible for approving the Policy
Group Board Risk Committee ("BRC")	Responsible for recommending approval of the Policy to the Board
Group Executive Risk Committees ("ERC")	Responsible for endorsing the Policy prior to submission to Group BRC
BU ERCs	Acknowledges the Policy and is responsible for making local amendments in line with requirements of the CPG Standard
First Line	Executes the provisions of the Policy, ensuring risk taking remains with Risk Appetite
Second Line	Proposes and reviews this Policy to ensure its ongoing appropriateness for the Group. Also provides oversight of the First Line to ensure that Risk Management is carried out appropriately
Third Line	Testing and independent verification that the Policy remains fit-for-purpose, in terms of both its design and execution

4.3. Exemptions

Exemptions to this Policy should be requested only in special circumstances, for example whereby it is required by a BU in order to meet requirements of their respective jurisdictions. Exemptions are considered to be either Policy exemptions or transactional exemptions, as defined by the CPG Standard.

For Policy exemptions and transactional exemptions, an escalation must be made to the Group CRO (the Policy Owner for this Policy) and be supported by a rationale from the BU CRO and other BU Executives as appropriate. Approval for the proposed standard exemptions or transactional exemptions should be received explicitly from the Group CRO before the exemption is treated as authorised.

4.4. Breach Management and Escalation

Where a Group function or BU breaks or fails to observe a requirement of this Policy without prior authorisation (as per the established exemptions criteria) this will be deemed as a breach. Breaches should be escalated to the BU CRO (where applicable) and Group CRO, who will further notify any parties as deemed appropriate.

Breaches to Group Compliance Policies and Compliance Standards should be notified and reported via incident reporting as per the Group Operational Risk Incident Procedure. Consultation with Group CRO and BU CRO is advised for exceptions that may not have yet reached the reporting threshold as mandated by the Group Operational Risk Incident Procedure.

Breaches to this Policy not previously authorised in line with the exemptions requirements (section 4.3) may also be managed in accordance with the Group's disciplinary procedures.

4.5. Monitoring, Review and Amendments

BU Risk and Compliance functions are responsible for monitoring compliance with this Policy on an ongoing basis and documenting the results of monitoring activity for their respective business on at least a biennial basis. Instances of non-compliance should be reported to the Group CRO.

This Policy should be reviewed on at least biennially in line with the review, endorsement, and approval procedures outlined by the CPG Standard.

Material amendments must be subject to the full review, endorsement, and approval procedures prior to being authorised and implemented across the Group. The Policy Owner also retains discretion to deem any other suggested amendment as material.

Administrative changes to this Policy, i.e. those not considered material, may be approved and implemented immediately (or in another appropriate timescale) by the Policy Owner.

4.6. Delegation of Authority and Other Administrative Matters

Group Risk & Compliance is responsible for the administration and revision of this Policy. This Policy will be reviewed at least biennially. Group Risk & Compliance is responsible for communicating the Policy to employees.

In line with the Group's principle of 'empowerment within a framework', the Group CRO delegates authority for implementing the requirements of this Policy within each BU to the relevant BU CRO. Each BU CRO is further empowered to delegate authority to their direct reports, or as otherwise deemed appropriate. BU CROs are responsible for reporting any matters to the Group CRO as they would reasonably expect to be made aware of, including but not limited to any exemptions and breaches to this Policy.

Notwithstanding the above, responsibility for the overall design and execution of this Policy sits with the Group CRO, whilst ultimate accountability and oversight is retained by the Group Board.

The latest effective version of this Policy shall reside on the CPP as per the CPG Standard. Any inquiries of this Policy shall be made to the primary Policy contact person as listed in the CPP and stated in the document details section of this Policy.

5. Approvals

This Policy is approved by the Group Board.

A. Appendix A – Summary of Data Privacy Policy Standards

The table below collates all requirements (indicated by DPP references) of this Policy.

#	DPP Requirement	Applicable
1	**DPP 1 – Notice/Purpose** Specific information must be communicated in a clear, easy to understand format to Data Subjects by way of a notice when collecting personal data from them. Process personal data only for the purposes notified.	Group/BU
2	**DPP 2 – Consent** Determine whether (explicit) consent from Data Subjects is required. Where required, ensure consent is informed, specific and freely given. Express consent is usually required for direct marketing and when sensitive personal data is involved.	Group/BU
3	**DPP 3 – Accuracy/Storage/Retention** Keep personal data accurate and only for as long as is necessary to fulfil the purpose for which it was collected. Personal data should be deleted or disposed of when it is no longer necessary for any business or legal purposes.	Group/BU
4	**DPP 4 – Transfers/Processing** Personal data may only be transferred and processed when Data Subjects are informed, and consent may be required. Appropriate safeguards should be put in place when transferring or disclosing personal data to third parties.	Group/BU
5	**DPP 5 – Overseas Transfers/Processing** Ensure special conditions enabling cross-border transfers/processing are met. Assess any potential regulatory implications for cross-border data transfers/processing activities.	Group/BU
6	**DPP 6 – Direct Marketing** Provide sufficient notices and obtain requisite consents from Data Subjects for direct marketing. Direct marketing must not be conducted outside the scope of notice/consent. Ensure Data Subjects are provided with a specific channel to opt out.	Group/BU
7	**DPP 7 – Security** Ensure appropriate measures are implemented to maintain security and protect against unauthorised access, loss or use of personal data. Follow guidelines set out in relevant information security policies.	Group/BU
8	**DPP 8 – Data Subject Requests** The Data Subject may have certain individual rights such as access to and correction of personal data. Data Subject requests should be directed to the relevant managers to ensure proper handling.	Group/BU
9	**DPP 9 – Breach Notification** Any suspected or actual personal data breach must be reported to the relevant managers immediately. Notification to local regulators and (in some cases) data subjects may be required.	Group/BU
10	**DPP 10 – Privacy Impact Assessment** Conduct privacy impact assessment where necessary prior to processing personal data that is likely to present higher privacy risks due to its nature or the scope of the processing operation. Minimise identified privacy risks.	Group/BU
	DPP 11 – Compliance Controls Privacy Policy Statement should be established. Adequate education and awareness, and monitoring and testing activities should be put in place.	Group/BU

B. Appendix B – One Page Policy Summary

WHAT YOU SHOULD KNOW

Rationale for this Policy

At AIA Group we respect the privacy of our customers, employees and business partners. Among our most important assets is the trust and confidence that are placed in AIA Group to properly handle personal information. Legal obligations also require us to deal with personal data confidentially and securely.

This Policy provides guidance on the applicable AIA Group standards for how personal data should be collected, accessed, used, stored, transferred, and disposed of by AIA Group.

If local applicable laws and regulations require higher compliance standards than this Policy, then AIA Group Business Entities in those jurisdictions must meet those higher standards.

Policy Scope

This Policy applies to AIA Group, its subsidiaries and each of their individual employees. Third parties authorised to collect, access, store, transfer use and dispose personal data on behalf of AIA Group should be required to comply with this Policy through contractual means.

Implications of Breaches

Breaches of this Policy by any employees of AIA Group or its subsidiaries may result in disciplinary action. Breaches of this Policy by authorised business partners may result in contractual liability.

Resources

The AIA Group Data Privacy Policy set out roles and responsibilities and required procedural controls.

What is Personal Data?

Personal data is any information which (alone or when used in combination with other information) relates directly or indirectly to an individual, from which it is practicable to identify the individual, and which is in a form where it is practicable to access or process the data. Examples include (individually or together): name, address, gender, national identification numbers, medical records, employment records and email addresses. Be aware that what constitutes personal data may vary in different jurisdictions, and in some jurisdictions additional protections apply for sensitive personal data (e.g. health records and biometric data).

Our statement of values

It is the policy of AIA Group to operate its business to the highest ethical standards and to comply with data privacy and security laws and regulations. Personal data must be collected, accessed, stored, transferred, used and disposed of in a way that protects the concerned individuals and enhances AIA Group's business operations.

WHAT YOU SHOULD DO (OR NOT DO)

DO

- Remember that data privacy is everyone's responsibility.
- Understand your responsibilities under the AIA Group Data Privacy Compliance Guidelines and any local guidelines and procedures and how these apply to your specific role and daily responsibilities.
- Ask your manager or Compliance if you are unsure how the AIA Group Data Privacy Compliance Guidelines apply to you.
- Be particularly mindful when dealing with sensitive personal data such as health records and biometric data.
- Encrypt personal data and reconfirm the correct recipient before sending it to an authorised party outside of AIA's network.
- Keep all personal data secure and confidential. Only allow authorised employees to access on a "need to know" basis.
- Dispose personal data in a secure manner or irreversibly de-identified it when it is no longer required according to the Records Retention Schedule.
- Regularly review personal data kept in your work computer to ensure it is not kept longer than needed and where it is needed, that the personal data is still accurate.
- Remember, AIA Group is committed to protecting persons who raise matters in good faith. Report any suspected data privacy breaches (e.g. leakage of personal data to unauthorised party) immediately to your supervisor, Human Resources or Compliance. You may also report suspected breaches anonymously via the AIA Ethics Hotline at www.aiaethicsline.com. (Refer to AIA Group Whistleblower Protection Policy for further details).

DON'T

- Do not disclose any personal data either internally or externally unless you are authorised to do so.
- Do not use personal data for new purposes without confirming with Legal and Compliance that the new use is consistent with consents previously obtained.
- Do not leave personal data unattended on your desk, printers or in meeting rooms.
- Do not take personal data outside of AIA premises without permission from your manager. Sending personal data to your personal email account is strictly prohibited.
- Do not retain personal data for a period longer than as specified in the Records Retention Schedule.

WHAT YOU SHOULD WATCH OUT FOR

- Many jurisdictions in which AIA Group operates have local data protection laws and regulations. You should understand and comply with them.
- Be aware that there may be restrictions in your jurisdiction on transferring personal data overseas. Ensure you seek advice from Legal and Compliance.
- Refer to relevant AIA Group Information Security Policy and Standard, Physical Security Standard, AIA Group Records Management Policy and Guidelines for other relevant mandatory controls of personal data.

C. Appendix C – Cookie Policy Template

COOKIE POLICY

AIA Company Limited and its subsidiaries ("AIA", "we", "us" and "our") operate this website. This website uses cookies and other tools to help distinguish you from other users of the website. This helps us to provide you with a good experience when you use the website and also allows us to improve the website. By continuing to use the website, you are agreeing to us placing cookies on your computer.

WHAT ARE COOKIES

Cookies are small text containing small amounts of information which are downloaded and may be stored on any of your web browsers or internet enabled devices (e.g. your computer, smartphone or tablet) that can later be read by the server - like a memory for a web page.

This means we automatically collect and store the following information about your visit:

- the internet domain and IP address from where you access the website;
- the type of browser software and configuration and operating system used to access the website;
- the date and time you access the website;
- if you linked to the website from another website, the address of that website; and
- the pages you enter, visit and exit the website from, content viewed and duration of visits.

Our Privacy Statement *[insert link to privacy statement]* sets out full details of the other information we collect and how we use your personal information.

USE OF COOKIES

The types of cookies we use and why we use them, includes but is not limited to the following:

- **Strictly necessary cookies.** These are cookies that are required for the operation of the website, and include, for example, cookies that enable you to log into secure areas of the website;

- **Analytical/performance cookies**. These cookies allow us to recognise and count the number of visitors and to see how visitors move around and use our website. These cookies are used for web enhancement and optimisation purposes and to aggregate statistics on how our visitors reach and browse our websites. This helps us to improve the way our website works, for example, by ensuring that users are finding what they are looking for easily and to help us understand what interests our users, and measure how effective our advertising is;

- **Functionality cookies**. These are used to recognise you when you return to the website. This enables us to personalise our content for you, tailor the website for your needs and remember your preferences, for example, your choice of language or region, browsing font size;

- **Targeting cookies**. These cookies record your visit to the website, the pages you have visited and the links you have followed. We will use this information to make our website and any material displayed on it more relevant to your interests. We may also share this information with third parties for this purpose; and

- **Advertising cookies.** These cookies will remember your preferences, and in general, that your used the website, to tailor advertising to you that are as relevant to you as possible, e.g. by selecting interest-based advertisements for you, or preventing or limit the number of times you see the same advisement to help measure the effectiveness of advertisements.

Please note that some cookies on the website are managed by third parties, including, for example, advertising networks, features such as videos, maps and social media, and providers of external websites like web traffic analysis services. These cookies are likely to be analytical/performance cookies or targeting cookies. You should refer to the third parties' own cookie and privacy policies for information about how they may use your information.

MANAGING COOKIE SETTINGS

You can block cookies by activating the setting within your browser that allows you to refuse the setting of all or some cookies. Please be aware if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of our website.

If you wish to withdraw your agreement at any time, you will need to delete your cookies using your browser settings for each browser you use.

For more information about how to do this, please follow the 'Help' option in your internet browser for more details.

D. Appendix D – Consent Statements Template

POLICY HOLDER PICS/CONSENT - LONG FORM

AIA PERSONAL INFORMATION COLLECTION STATEMENT

[Insert name of relevant AIA entity that is the data controller for this privacy statement] ("**AIA**", "**we**", "**us**", "**our**") recognise our responsibilities in relation to the collection, use, disclosure and other processing and storage of personal data.

Among the most important assets of the AIA Group Limited group of companies ("**AIA Group**") is the trust and confidence placed to properly handle information. Customers expect us to maintain their information accurately, protected against manipulation and errors, secure from theft and free from unwarranted disclosure.

This personal information collection statement ("**privacy statement**") provides you with notice as to why your personal data is collected, how your personal data is collected, how it is intended to be used, to whom your personal data may be disclosed and how to access, amend and otherwise exercise your rights in respect of your personal data.

What personal data do we collect, and how do we collect it?

We will collect and store your personal data either:

- directly when you provide such information to us (for example, when you fill in policy application or claim forms; or when you send us enquiries or communications);
- indirectly through your use of our websites, apps or social media platforms; or
- where you have provided it to us through any other means.

We may obtain lawfully collected personal or non-personal data about you from affiliated entities, business partners and other independent third party's sources. We may also collect some information about your computer or other devices used when you visit our websites or apps [or social media platforms].

The personal data we collect (which includes sensitive personal data as defined under relevant applicable laws and regulations), includes the following:

- information you provide when you apply for, renew or make a claim under a policy and/or you correspond with us, including: your name, address and other contact details, date of birth, bank account or credit card details, passport/identity card number, information about your dependants and health records; and
- technical information collected when you use our websites and apps [and social media platforms]: such as IP address, browser type and version, time zone settings, browser plugin types, operating systems and platform, device information (including where mobile device the IMEI number, wireless networks and general network information).

The provision of your personal data is voluntary. You may choose not to provide us with the requested data, but failure to do so may inhibit our ability to do business with you or to respond to your enquiries. We will usually identify any information which is mandatory (i.e. information required for policy administration) when we collect the information from you. [In certain jurisdictions, and where required by law, AIA will not collect personal data without your consent.]

Why we collect your personal data and how it may be used?

Personal data is collected for the following purposes:

- processing, administering, implementing and effecting the requests or transactions contemplated in this document or any other documents you may submit to us from time to time, including without

limitation processing policy applications; administering your policy; collecting premiums and outstanding amounts from you; investigating, analysing, processing and paying claims made under your policy; and renewals, variations and cancellations or reinsurance of your policy;

- exercising any right under your policy including right of subrogation, if applicable;
- designing new or enhancing existing products and services;
- to communicate with you, including to send you administrative and other communications about any policy or account you may have with us, to provide technical support as regards our websites and apps, or about future changes to this privacy statement;
- for advanced data analytics, and for statistical or actuarial research undertaken by the AIA Group, the financial services industry or our respective regulators;
- for our data matching, internal business (including corporate reorganisation) and administrative purposes;
- to provide you with access to the content on our websites or apps [or social media platforms];
- to monitor your use of our websites and apps [and social media platforms], and conduct analysis of the use of them in order to personalise, operate, evaluate and improve them and our services, understand your preferences and troubleshoot any problems;
- to assist in law enforcement purposes, investigations by police or other government or regulatory authorities in any jurisdiction and to meet reporting obligations and requirements imposed by law or agreed to with government or regulatory authorities in any jurisdiction; and
- other purposes directly relating to any of the above.

Unless otherwise permitted by applicable laws and regulations, we will obtain consent from you if we wish to use your personal data for purposes other than those stated in this privacy statement or a directly related purpose.

For our policy on using your personal data for promotional or marketing purposes, please see the section entitled "**Use of Personal Data for Direct Marketing Purposes**" below.

Who may be provided with your personal data?

Personal data will be kept confidential but may, where permitted by applicable law or where such disclosure is necessary to satisfy the purpose or a directly related purpose for which the personal data was collected, provide such personal data to the following parties:

- any person authorised to act as an agent of AIA [or another AIA Group company] for the distribution of products and services offered by us [or that AIA Group company];
- any agent, contractor or third-party service provider (within or outside AIA Group) who provides administration, data processing, telecommunications, computer, payment, debt collection or securities clearing, technology outsourcing, cloud, call centre, mailing and printing services in connection with the operation of AIA's business and provision of our services to you;
- any member of the AIA Group;
- agents, contractors or third-party service providers (within or outside the AIA Group) including companies to help deliver our services, such as reinsurance companies, investment management companies, claims investigation companies, industry associations or federations;
- other companies who help gather your information or communicate with you, such as research companies and ratings agencies, in order to enhance the services we provide to you; and
- government or regulatory bodies in any jurisdiction or any person to whom AIA [or another member of the AIA Group] must disclose data: (a) under a legal and/or regulatory obligation in that or any

other jurisdiction applicable to that particular AIA company; or (b) pursuant to an agreement between the AIA company and the relevant government, regulatory body or other person.

For our policy on sharing of your personal data for promotional and marketing purposes, please see the section entitled "**Use of Personal Data for Direct Marketing Purposes**".

[For AIA Hong Kong only] In relation to any personal data collected by us whilst providing any services in respect of our mandatory provident fund master trust schemes, such personal data would only be transferred to the above persons for the purpose of providing any mandatory provident fund related services.

From time to time, we may purchase a business or sell one or more of our businesses (or portions thereof) and your personal data may be transferred or disclosed as a part of the purchase or sale or a proposed purchase or sale. In the event that we purchase a business, the personal data received with that business would be treated in accordance with this privacy statement, if it is practicable and permissible to do so. In the event that we sell a business, we will include provisions in the selling contract requiring the purchaser to treat your personal data in the same manner required by this privacy statement.

Your personal data may be transferred to, stored or otherwise processed by AIA, or provided to any of the above persons who may be located or from which they provide services, in or outside the jurisdiction or territory in which you are resident or located. Where required under relevant law, we may seek your consent to the transfer of such information outside your jurisdiction to our facilities or to those third parties with whom we share it as described above. Your personal data will only be transferred to other locations, where we are satisfied that adequate levels of protection exist to protect the integrity and security of your personal data, which as minimum are comparable to the jurisdiction or territory in which you provided such personal data.

Security and Retention of Personal Data

AIA applies reasonable security measures to prevent unauthorised or accidental access, processing, erasure, loss or use.

AIA may retain your personal data for as long as necessary to fulfil the purpose(s) for which it is collected or as otherwise required to ensure compliance with applicable laws and regulations. Reasonable steps will be taken to delete or destroy your personal data when it is no longer necessary for any of the purpose above.

Access Rights to Personal Data and Contact Us

You may have the right in accordance with applicable laws and regulations to:

- verify whether AIA holds any personal data about you, to access or obtain a copy of any such data, and/or to access information about how AIA used or disclosed your personal data;
- require AIA to correct any personal data relating to you which is inaccurate;
- request deletion of your personal data under certain circumstances;
- withdraw your consent or request a change to your scope of consent;
- request deregistration or deletion of your registered account (if any);
- make a complaint about AIA's data handling; and
- enquire about AIA's policies and practices in relation to personal data.

Requests for access, correction, complaints or other queries relating to your personal data should be addressed to:

[Name / Position]

[Address]

[Email]

Under applicable laws and regulations we may have the right to charge costs for the processing of the above personal data requests.

You also have the right to lodge a complaint with a supervisory authority in certain jurisdictions if you consider that the processing of your personal data infringes applicable law.

Consequences of consent withdrawal

You may withdraw your consent to collect, use or disclose your personal data as set out in this privacy statement by giving us reasonable notice.

If you withdraw your consent for us to collect, use or disclose your personal data for non-marketing reasons, we will be unable to process, administer and/or manage your policy, relationship and/or account with us. In such event, you may be required to surrender or terminate all your policies or accounts or withdraw from any programmes in which you are participating. This may be to your disadvantage, as you may be losing valuable benefits from your policies or programmes, incur surrender charges or it may not be possible for you to obtain a similar level of protection on the same terms in the future.

If you do not want to receive any direct marketing communications, you may withdraw your consent at any time. Please note that such withdrawal of your consent will not affect our ability to provide you with the products and services for which you have requested or to which you have applied, subscribed or are participating with us.

Amendments to this Privacy Statement

AIA reserves the right, at any time and without notice, to add to, change, update or modify this privacy statement, simply by notifying you of such change, update or modification. If we decide to change our personal data policy, those changes will be notified to you either on our website or in writing so that you are always aware of what information we collect, how we use the information and under what circumstances the information is disclosed. Any such change, update or modification will be effective immediately upon posting. Where required by applicable law, we may also notify you in the event of material changes to this privacy statement and, where required, seek your consent to those changes.

Use of Cookies

AIA may use cookies on various websites we maintain, for example, to collect and compile aggregate statistics on how you reach and browse our websites to help us understand how we can improve your experience on it. For details on the types of cookies we collect and what they are used for, please refer our Cookie Policy [*Insert link*]

Additional Information

Should you have any questions on any part of this privacy statement or would like additional information regarding AIA's data privacy practices, please do not hesitate to contact us (see the section entitled "**Access Rights to Personal Data and Contact Us**" above).

Consent

By [clicking] ***OR*** [signing] below you acknowledge and agree to the collection, use and disclosure of your personal data (including sensitive personal data where applicable, and overseas transfers of your personal data) as set out in our privacy statement [above] ***OR*** [*insert hyperlink*].

I AGREE/SUBMIT/SIGNATURE BOX (amend as applicable)

****

Use of Personal Data for Direct Marketing purposes

To provide you with information about our products and services, *[insert relevant AIA entity name]* ("**we**", "**us**", "**our**") would like use your name and [the email address,] [[mobile] telephone number, and] [postal address] you provide to us ("**contact details**") to send you promotional materials and direct marketing communications about the following products, services, advice and subjects: insurance, annuities; MPF/ORSO; wealth management; investment; banking; financial services; credit cards; medical/health treatment; educational; recruitment; training; reward/loyalty/privilege programmes; charitable/non-profitable causes ("**Classes of Marketing Subjects**"), but we cannot do so without your consent.

We would also like to share your name and contact details with providers (including to other entities within the AIA Group Limited group of companies ("**AIA Group**")) of any of the Classes of Marketing Subjects and call centre, marketing or research services so that they can send you promotional materials and conduct direct marketing in relation to the products and services they offer, but we also cannot do so without your written consent.

[For AIA Hong Kong only] In relation to any personal data collected by the AIA Group whilst providing any services in respect of our mandatory provident fund master trust schemes, such personal data would only be used for promoting or marketing any products or services that are directly related to AIA Group mandatory provident fund schemes.

Please indicate your consent to receive such direct marketing communications by ticking the appropriate boxes below:

[ ] from *[insert relevant AIA entity name]*

[ ] from other companies within the AIA Group as described above

[ ] from selected third parties as described above

Please indicate how you would like to receive such direct marketing communications:

[ ] email

[ ] SMS / telephone

[ ] post

If you do not want to receive any direct marketing communications, you may withdraw your consent at any time free of charge by contacting [AIA's Data Protection Officer] as follows: [insert contact details] or by using the unsubscribe function on the direct marketing messages. Any such request should clearly state details of the personal data in respect of which the request is being made.

POLICY HOLDER PICS/CONSENT - SHORT FORM

If a BU prefers just to have a short-form notice/consent, the following must be included as a minimum:

For collection and use of personal data:

- the AIA entity/ies who is/are the data controller
- types of personal data that will be collected, used or disclosed, e.g. name, contact details
- the reasons why the personal data is collected, used or disclosed
- details of with whom the personal data will be shared, e.g. group entities, services providers, third parties
- details of any transfer to other locations outside of the jurisdiction in which the BU operates/Data Subject is located
- any rights of the individual to which the personal data relates, e.g. right to request access, right to correction
- contact details of the person/role to whom an individual can make a request or compliant

For direct marketing:

- the AIA entity/ies who will be sending the direct marketing communications
- types of personal data that will be used for direct marketing purposes, e.g. name, contact details
- the types of products or services which will be marketed
- whether the personal data will be shared with third parties to carry out direct marketing
- how an individual can opt-out of receiving direct marketing materials
- separate non pre-ticked boxes to obtain consent

E. Appendix E – Privacy Policy Statement Template

PRIVACY STATEMENT

[AIA Group Limited and/or its subsidiaries] [insert name of relevant AIA entity/ies that is the data controller for this privacy statement] ("**AIA**", "**we**", "**us**", "**our**") recognise our responsibilities in relation to the collection, use, disclosure and other processing and storage of personal data.

Among the most important assets of AIA Group Limited and/or its subsidiaries (**"AIA Group**") is the trust and confidence placed to properly handle information. Customers and potential customers expect us to maintain their information accurately, protected against manipulation and errors, secure from theft and free from unwarranted disclosure. We protect data security of our customers and potential customers by complying with the all relevant data protection laws and regulations, and ensure compliance by our staff with strict standards of security and confidentiality.

This statement provides you with notice as to how and why your personal data is collected, how it is intended to be used, to whom your personal data may be transferred to, how to access, review and amend your personal data, and our policies on direct marketing and the use of cookies. You may be asked to consent to the practices and policies in this statement when you access, or interact with us via, this website. Otherwise, by using this website, you are accepting the practices and policies in this privacy statement. If you object to any practices and policies in this statement, please do not use this website to submit your personal information to AIA.

This website is for general information purpose only. While we use reasonable efforts to ensure the accuracy of the information on this website, AIA does not warrant its absolute accuracy or accept any liability for any loss or damage resulting from any inaccuracy or omission. Without prior permission from AIA, no information contained on this website may be copied, except for personal use, or redistributed.

AIA recognises its responsibilities in relation to the collection, holding, processing or use of personal data. The provision of your personal data is voluntary. You may choose not to provide us with the requested data, but failure to do so may inhibit our ability to provide information and services to you or to respond to your enquiries. AIA will not collect any information that identifies you personally through this website unless and until you use and browse the website, buy our products or services, register as a member, interact with us, sign-up to receive news about our products and services, or otherwise communicate with us (including where requesting technical support).

This website, and our social media platforms are not intended for persons in jurisdictions that restrict the distribution of information by us or use of such website or social media platforms. If this is applicable to you, we would advise you to make yourself familiar with and observe the relevant restrictions, and AIA does not accept liability in this respect.

How we collect data.

We will collect and store your personal data either:

- directly when you provide such information to us (for example, when you us enquiries or communications);
- indirectly through your use of our websites, apps or social media platforms; or
- where you have provided it to us through any other means.

We may obtain lawfully collected personal or non-personal data about you from affiliated entities, business partners and other independent third party's sources. We may also collect some information about your computer or other devices used when you visit this website, apps or social media platforms.

The personal data we collect (which includes sensitive personal data as defined under relevant applicable laws and regulations), includes the following:

- identity information – name, address, personal contact details (including email address and

telephone numbers); and
- technical information – such as IP address, browser type and version, time zone settings, browser plugin types, operating systems and platform, device information (including where mobile device the IMEI number, wireless networks and general network information).

If you make use of any social media features or platforms, either on our website, an application we provide, or otherwise through a social media provider, we may access and collect information about you via that social media provider in accordance with their policies. When using a social media feature, we may access and collect information you have chosen to make available and to include in your social media profile or account, including but not limited to your name, gender, birthday, email address, address, location etc. Our access to this information may be limited or blocked based on your privacy settings with the relevant social media provider.

We will usually identify any information which is mandatory (i.e. information required for creating an account, and to enable you to access the features of the website and receive any services) when we collect the information from you. You may choose not to provide us with the requested data, but failure to do so may inhibit our ability to do business with you or to respond to your enquiries.

Why we collect your personal data and how it may be used?

Personal data is collected for the following purposes:

- to provide you with access to the content on the website, apps or social media platforms;
- to process and administer your account, to implement and effect the requests or transactions contemplated by the forms available on our website or any other documents you may submit to us from time to time;
- to design new or enhance existing products, information and services provided by us;
- to communicate with you including to send you administrative and technical communications about any account you may have with us, to provide technical support or notify about future changes to this privacy statement;
- for statistical or actuarial research undertaken by AIA, the financial services industry or our respective regulators;
- for advances data analytics, data matching, internal business and administrative purposes;
- to monitor your use of the website, apps and social media platforms and conduct analysis of the use of the website in order to operate, evaluate and improve the website and our services, understand your preferences and troubleshoot any problems;
- to assist in law enforcement purposes, investigations by police or other government or regulatory authorities and to meet requirements imposed by applicable laws and regulations or other obligations committed to government or regulatory authorities;
- to personalise the appearance of our websites, provide recommendations of relevant products, information and services and provide targeted advertising on our website or through other channels;
- other purposes as notified at the time of collection; and
- other purposes directly relating to any of the above.

Unless permitted by applicable laws and regulations, we will obtain consent from you if we wish to use your personal data for purposes other than those stated in this privacy statement.

AIA may retain your information for as long as necessary to fulfill the purpose(s) for which it is collected or as otherwise required to ensure compliance with applicable laws and regulations. AIA applies reasonable security measures to prevent unauthorised or accidental access, processing, erasure, loss or use including limiting physical access to data within AIA's systems and encryption of sensitive data when transferring such data. Reasonable steps will be taken to delete or destroy the information when it is no longer necessary for any of the purpose above.

For our policy on use of your personal data for promotional or marketing purposes, please see the section entitled "Use of Personal Data for Direct Marketing Purposes".

Who may be provided with your personal data?

Personal data will be kept confidential but may, where permitted by law or where such disclosure is necessary to satisfy the purpose or a directly related purpose for which the personal data was collected, provide such personal data to the following parties:

- any person authorised to act as an agent of AIA [or another AIA Group company] in relation to the distribution of products and services offered by AIA [or that AIA Group company];
- any agent, contractor or third-party service provider (within or outside AIA Group Limited) who provides administration, data processing, telecommunications, computer, payment, debt collection or securities clearing, technology outsourcing, call centre services, mailing and printing services in connection with the operation of AIA's business and AIA's provision of services to you;
- any member company of AIA Group Limited in relation to the provision or marketing of insurance services;
- any agent, contractor or third-party service provider (within or outside AIA) including companies that help deliver our services, such as reinsurance companies, investment management companies, claims investigation companies, industry associations or federations;
- other companies that help gather your information or communicate with you, such as research companies and ratings agencies, in order to enhance the services we provide to you; and
- government or regulatory bodies in any jurisdiction or any person to whom an AIA company must disclose data: (a) under a legal and/or regulatory obligation in that or any other jurisdiction applicable to that particular AIA company; or (b) pursuant to an agreement between the AIA company and the relevant government, regulatory body or other person.

For our policy on sharing of your personal data for promotional and marketing purposes, please see the section entitled "**Use of Personal Data for Direct Marketing Purposes**".

From time to time, we may purchase a business or sell one or more of our businesses (or portions thereof) and your personal data may be transferred or disclosed as a part of the purchase or sale or a proposed purchase or sale. In the event that we purchase a business, the personal data received with that business would be treated in accordance with this privacy statement if it is practicable and permissible to do so.

Your personal data may be provided to any of the above persons who may be located in other jurisdictions or territories to that in which you are located. Your information may be transferred to, stored, and processed in other jurisdictions where any AIA company is located, or jurisdictions where a third-party contractor is located or from which the third-party contractor provides us services. Where required under relevant law, we may seek your consent to the transfer of such information outside your jurisdiction to our facilities or to those third parties with whom we share it as described above. Your personal data will only be transferred to other locations, where we are satisfied that adequate levels of protection exist to protect the integrity and security of your personal data, which as minimum are comparable to the jurisdiction or territory in which you provided such personal data.

Access Rights to Personal Data

Under applicable laws and regulations, you may have the right to:

- verify whether AIA holds any personal data about you and to access any such data or information about how AIA used or disclosed your personal data;
- require AIA to correct any personal data relating to you which is inaccurate;
- request deletion of your personal data under certain circumstances;
- withdraw your consent or request a change to your scope of consent;
- request deregistration or deletion of your registered account;
- make a complaint about AIA's data handling; and
- enquire about AIA's policies and practices in relation to personal data.

Requests for access, correction, complaints, or other queries relating to your personal data should be addressed to:

The Data Protection Officer
[Address]
[Email]

Under applicable laws and regulations, AIA may the right to charge costs which are directly related to and necessary for the processing of any personal data request.

You also have the right to lodge a complaint with a supervisory authority in certain jurisdictions if you consider that the processing of your personal data infringes applicable law.

Use of Personal Data for Direct Marketing purposes

In addition to the purposes set out above, where permitted by law, AIA may use your name and contact details for promotional or marketing purposes including sending you promotional materials and conducting direct marketing in relation to the following products, services, advice and subjects: insurance; annuities; Mandatory Provident Fund/Occupational Retirement Schemes Ordinance Fund wealth management; investment; banking; financial services; credit cards; medical/health treatment; educational; recruitment; training; reward/loyalty/privilege programmes; charitable/non-profitable causes; ("**Classes of Marketing Subjects**").

For the purposes of direct marketing, we may, where permitted by law, provide your personal information to providers (whether within or outside of AIA) of any of the Classes of Marketing Subjects described above and call centre, marketing or research services so that they can send you promotional materials and conduct direct marketing in relation to the products and services they offer (these materials may be sent to you by postal mail, email or other means). Where permitted by law, we may provide your personal data to providers (whether within or outside of AIA) of any of the Classes of Marketing Subjects for gain.

Before using or providing your personal data for the purposes and to the transferees set out in this section, we may be required by law to obtain your written consent, and in such cases, only after having obtained such written consent, may we use and provide your personal data for any promotional or marketing purpose.

The types of personal data that AIA would use and provide for direct marketing purposes as described above are your name and relevant contact details, although we may possess additional personal data.

If your consent is required, and you provide such consent, you may thereafter withdraw your consent to the use and provision to a third party by AIA of your personal data for direct marketing purposes and thereafter AIA shall cease to use or provide such data for direct marketing purposes.

If you have provided consent and wish to withdraw it or if you prefer not to receive marketing communications from us in any form, please inform us by writing to the address in the section on “Access Rights to Personal Data” or sending us an email to privacy.compliance@aia.com. Any such request should clearly state details of the personal data in respect of which the request is being made.

Use of Cookies

Cookies are small text containing small amounts of information which are downloaded and may be stored on any of your web browsers or internet enabled devices (e.g. your computer, smartphone or tablet) that can later be read by the server - like a memory for a web page.

AIA may use cookies and other tools on the website. By continuing to use the website, you are agreeing to us placing cookies on your computer. The information collected (including but not limited to: your IP addresses (and domain names), browser software, types and configurations of your browser, language settings, geo-locations, operating systems, referring website, pages and content viewed, and durations of visit) will be used to ensure operation of the website and enable you to log in securely, for compiling aggregate statistics on how our visitors reach and browse our websites for web enhancement and optimisation purposes, and to help us understand how we can improve your experience on it.

The cookies also enable our website to remember you and your preferences, and tailor the website for your needs. Advertising cookies will allow us to provide advertisements on our websites that are as relevant to you as possible, e.g. by selecting interest-based advertisements for you, or preventing the same advisement from constantly reappearing to you. You can find more information on the types of

cookies we collect, what we use these for, and how to manage your cookie settings in our [insert link to Cookie Policy].

External links

If any part of this website contains links to other websites, those sites may not operate under this privacy statement. You are advised to check the privacy statements on those websites to understand their policies on the collection, usage, transferal and disclosure of personal data.

Amendments to this Privacy Statement

AIA reserves the right, at any time and without notice, to add to, change, update or modify this privacy statement, simply by notifying you of such change, update or modification. If we decide to change our personal data policy, those changes will be notified on our website so that you are always aware of what information we collect, how we use the information and under what circumstances the information is disclosed. Any such change, update or modification will be effective immediately upon posting. Where required by applicable law, we may also notify you in the event of material changes to this privacy statement and, where required, seek your consent to those changes.

Additional Information

Should you have any questions on any part of this privacy statement or would like additional information regarding AIA's data privacy practices please do not hesitate to contact us by the contact details above.

F. Appendix F – Privacy Impact Assessment Template

Privacy Impact Assessment Template

If you have any questions about the privacy impact assessment pre-screening questions or the impact assessment template, please contact your Business Entity's Compliance team.

Instructions

Privacy Impact Assessment ("PIA") should be completed when there are events that significantly change in the privacy risk landscape, the significant events include, but not limited to, the following:

- Commencing any new business initiative or project that might have impact on Personal Data.
- Implementing privacy-intrusive technologies.
- Making any major changes in organisational practices involving Personal Data.
- Any actions that may result in increased volumes or broader scope of Personal Data being collected, processed or shared.
- Conducting any automated decision making or processing any Sensitive Personal Data.

For changes in the IT System Infrastructure, at a minimum, the following triggers should be considered:

PIA Trigger	Description
Digitisation of records	Converting paper-based records to electronic systems.
Anonymous to Non-Anonymous	Operations performed on existing database change anonymous information into Personal Data.
Significant System Management Changes	New uses of existing IT systems, including application of new technologies, significantly changes how Personal Data is managed in the system. For example, when the company employs new relational database technologies or web-based processing to access multiple data stores, such additions could create a more open environment and avenues for exposure of data that previously did not exist.
Significant Merging	The company adopts or alters business processes so that databases holding Personal Data are merged, centralised, matched with other databases or otherwise significantly manipulated. For example, when databases are merged to create one central source of information, such a link may aggregate data in ways that create privacy concerns not previously an issue.
New User Access Mechanism	User-authentication technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by users (including Third Party users).
External Sources	The company systematically incorporates into existing information systems, databases of Personal Data purchased or obtained from third parties or public sources. An exception to this trigger would be merely querying such a source on an ad hoc basis using existing technology.

General Procedures in Completing Privacy Impact Assessment:

Step 1: Completion and submission of PIA Form to Compliance and/or Data Protection Officer.

The PIA form should be completed by the Project/Change/Initiative Sponsor/Manager prior to implementation. Upon completion, the form should be submitted to Compliance / DPO (or equivalent) for review and assessment.

Step 2: Initial review and assessment of the PIA Form

Compliance / DPO (or equivalent) will review the appropriateness of the completed PIA form. For the assessment of indicated risks and mitigating controls, Compliance / DPO (or equivalent) may indicate comments and ask the project/change/initiative sponsor/manager or BU Head to consult with other business functions (e.g. Corporate Security, Legal, IT) for additional assessments required. Comments and consultation discussion shall be documented in the PIA form.

Step 3: Consultation with other business functions

The PIA form will be returned to project/change/initiative sponsor/manager and consult with other business functions as indicated the review comments by Compliance / DPO (or equivalent). The comments should be addressed accordingly and consultation responses should be reflected in the PIA form. Once completed, the PIA form will be forwarded back to Compliance / DPO (or equivalent) for final review.

Step 4: Final review and approval of the PIA form

Compliance / DPO (or equivalent) will review the consultation responses and close the comments that were addressed accordingly. Once all the comments have been closed, Compliance / DPO (or equivalent) will sign-off in the PIA form. The project/change/initiative sponsor/manager will approve the PIA form and proceed with the implementation.

Section A – Pre-Screening

General Description

Company/Department:			
Name of Process/Project, Initiative or Changes:			
Date:			
PIA Drafter:			
Email:		**Contact Number:**	
Project Manager:			
Email:		**Contact Number:**	

Privacy impact assessment (PIA) screening questions

These PIA pre-screening questions should be completed for all new and changes to existing enactments, systems, acquisitions of third party providers, programmes, projects, initiatives, contracts and activities where Personal Data may be affected, collected, used or exchanged.

	Question:	Yes	No
1	Will the new or change initiative or contract involve the collection of new Personal Data about individuals?		
2	Will the new or change initiative or contract request or require individuals to provide further Personal Data about themselves?		

	Question:	Yes	No
3	Will the new or change initiative require Personal Data about individuals to be disclosed to organisations or people who have not previously had routine access to the information (including to organisations or people who may be located outside of your local business entity or outside your jurisdiction)?		
4	Will the initiative or change initiative involve a new use for Personal Data?		
5	Is it intended through this new or change initiative or contract to use information about individuals for a purpose other than its intended original use?		
6	Does the new or change initiative or contract involve direct marketing to individuals using Personal Data?		
7	Does the new or change initiative involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.		
8	Does the new or change initiative or contract involve the use of government-issued identifiers?		
9	Will the new or change initiative or contract result in you making decisions or taking action against individuals in ways that can have a significant impact on them?		
10	Is there any particular Personal Data about individuals which is likely to raise privacy concerns? For example, health records, criminal records or other information that people would consider to be private and sensitive.		
11	Will the new or change initiative or contract potentially involve contacting individuals in ways that they may find intrusive?		
12	Will the new or change initiative or contract potentially involve a new or amended requirement to store secure or retain Personal Data?		
13	Will the new or change initiative or contract potentially have any other impacts on privacy?		

If you have answered 'yes' to any of these questions, please continue to Section B/C/D to complete the PIA template.

If there are any reasons you believe detailed PIA (Section B/C) are not necessary. Please document the rational below and signoff (Section D):

Section B – Personal Data

The project will collect, use, retain, disclose, and/or dispose the following Personal Data:
(Please check the appropriate box)

Personal Information		Yes	No
1	Name		
2	Home Address		
3	Business Address		

4	Email Address - Work		
5	Email Address - Personal		
6	Telephone Number – Work		
7	Telephone Number – Personal		
8	Photo		
9	Age		
10	Date of Birth		
11	Gender		
12	Marital Status		
13	Race or Ethnic Origin		
14	Religion (Religious beliefs or affiliations), Philosophical Beliefs/Orientation		
15	Education background		
16	Political Association		
17	Sexual life/preference/practice		
18	Medical, dental, insurance claims history, genetic data and biometric data, including any information on any individual's health, disability or disease		
19	Financial account numbers (bank account numbers, credit card numbers, and other information if that information would permit access to a financial account) or financial data such as credit rating, annual income, transactional history, etc.		
20	Criminal records (Offence committed or alleged to have been committed, the disposal of such proceedings, or the sentence of any court in such proceedings)		
21	Government-issued identification numbers (including National Identity numbers, Healthcare Identity numbers, Social Security numbers, Tax numbers, driver's license numbers, passport numbers, etc.).		
	Others, please add as many as will be collected		

Section C – Detailed impact assessment

Privacy impact assessment template

These questions will help identify where there is a risk that the project, new or change initiative, or contract needs to comply with the AIA Group Data Privacy Guidelines and the relevant local laws and regulations.

	Question	Response
1	Describe what the objectives of the new or change initiative or contract including the benefits and describe the impacts or potential impacts to the organisation, to individuals and to other parties. Please provide the estimated number of Data Subjects from who data is collected, system overview or data flow diagram.	

2	**Collection of Personal Data**
	• Please provide examples of personal and/or sensitive information that will be accessed, collected, handled or stored.
	• Please provide justifications on the collection of sensitive personal data below (including but not limited to):
	  ○ Government issued identifier (e.g. HK Identity Card number) and other personal identifier
	  ○ Medical history
	  ○ Biometric data (e.g. fingerprints)
	  ○ Do any third parties collect information on your behalf? Please provide details of the third parties. Have you reviewed their compliance with any local regulatory requirements? (If yes, the section on Data Collection from External Sources should be followed.)
	• Is the information collected deemed necessary for the initiative (i.e. no excessive Personal Data is collected)? Provide explanation.
	• How is Personal Data collected and was consent from the individual obtained?
	• How is the consent being obtained, i.e., via what channel?
	• How will individuals be made aware of the collection of their Personal Data?
	• Will the information be collected for a purpose other than the original intended use or authorised use? Provide explanation.	

	Question	Response
3	**Unsolicited Personal Data** • Are you likely to receive Personal Data that you do not ask for as part of the new or change initiative or contract? • If yes, have you assessed whether it could be collected under the Data Principle in relation to purpose and manner of collection of Personal Data? • If you determine you should not receive the information under local laws and regulations, do you destroy or de-identify it?	
4	**Use and Disclosure of Personal Data** • What types of Personal Data will be used or disclosed? • Will the Personal Data ever be used or disclosed for purposes other than its primary purpose? • How will individuals be made aware of the use and disclosure of their Personal Data? • Is it possible to de-identify information before use or disclosure? If yes, how will you ensure that Personal Data is de-identified before use or disclosure? • What is the primary purpose of processing Personal Data? • Please provide details if the Personal Data will be used for a secondary purpose. • Where the personal data will be used for a new purpose, has explicit consent been obtained from the Data Subjects? If "no", please justify. • Where personal data will be disclosed to a third party, will the third party be reminded of the use of the data and its responsibilities? If "yes", please elaborate. If no, please justify. • Where personal data will be disclosed to a third party, is the personal data disclosed to third party only necessary but not excessive? If "no", please justify.	
5.	**Third Party Processor** • Will any data processor(s) be involved? If "yes", have contractual or other means been adopted to ensure that the data processor(s) has taken appropriate data security measures? If "no", please elaborate on the justification. • If the personal data is to be transferred to any third party or data processor, will the Data Subjects be informed of the classes of persons to whom their personal data may be transferred? If "no", please provide the reason. • Has Third Party Security Assessment, or similar assessment, been conducted?	

	Question	Response
6	**Data Quality** Please identify all steps taken to ensure that all Personal Data collected, used or disclosed will be accurate, complete and up to date. For example, • Information was obtained from a reputable source such as government agency • the system is regularly tested for accuracy • periodic reviews of the information • a retention schedule in place that deletes information that is over a certain period • staff are trained and receive periodic updates • reviews of audit trails are undertaken regularly • independent oversight • incidents are reviewed for lessons learnt and systems / processes updated appropriately.	
7	**Direct Marketing** • Do you intend to use Personal Data for direct marketing? • Has the individual consented to the use of their Personal Data for direct marketing? • Is a free and functional unsubscribe or opt-out option/ facility provided to individuals who receive direct marketing?	
8	**Cross Border Disclosure** • Do you intend to disclose Personal Data to overseas storage / entities? Please list them. • What types of Personal Data will be disclosed to overseas storage / entities? • What steps will be taken to ensure that the overseas recipient does not breach the Data Privacy Principles in relation to the information? • Have you considered if there is any regulatory restriction prohibits such cross-border transfer and the utilisation of cloud storage for personal data?	
9	**Adoption, Use or Disclosure of Government-issued Identifiers** • Are any government-issued identifiers used? • If yes, what is the purpose? • What measures are in place to ensure appropriate use and disclosure of government-issued identifiers?	

	Question	Response
10	**Security of Personal Data** • Please describe the security measures that will be in place to protect Personal Data from misuse, interference and loss • Please describe the security measures that will be in place to protect Personal Data from unauthorised access, modification or disclosure • How will the Personal Data be stored? • Will the Personal Data be transferred in a secure manner? • Will encryption (or other secure method of transfer) for data at rest and data in transit be used? • What is the process for de-identifying or destroying information that is no longer required?	
11	**Access and Correction of Personal Data** • What options are provided to individuals who wish to access/correct their Personal Data? • How soon and how will access/correction be granted to individuals who have requested it? • Is access/correction ever refused? If yes, is written notice provided to the requestor detailing ground for refusal and a mechanism to complain? • How are third parties who have received the Personal Data, notified of the correction?	
12	**Records Retention** • What is the retention period of the Personal Data collected? • How is the retention period of the Personal Data defined? • What are the steps to be taken destroyed or de-identified Personal Data if it is no longer needed for any purpose? • If there are any third parties holding such Personal Data, how are they informed about the retention requirement? • Are there any measures in place to ensure that personal data is not kept longer than necessary to fulfil the purpose of using the data? If yes, what are the measures? If no, please justify.	

<table>
<tr><th></th><th>Question</th><th>Response</th></tr>
<tr><td>13</td><td colspan="2">From the above questions, identify the key privacy concerns, the associated risks, and the mitigating controls
<table>
<tr><th>Key Privacy Concerns</th><th>Associated risks</th><th>Mitigating Controls / Actions</th></tr>
<tr><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>14</td><td colspan="2">Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork or monitoring the third party or contract? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?
<table>
<tr><th>Mitigating actions to be taken</th><th>Target completion date</th><th>Responsible by</th></tr>
<tr><td></td><td></td><td></td></tr>
</table>
<table>
<tr><th>Contact point for future privacy concerns</th></tr>
<tr><td></td></tr>
</table></td></tr>
</table>

Section D – Signoff

Completed by:	**Date**
Reviewed by:	**Date**
Approved by:	**Date**

Note: *The PIA should be reviewed by Compliance / DPO (or equivalent), and approved by the Project Sponsor (Business Function Head)*

Note:

- The person responsible for the PIA should examine the purpose and rationale behind the project in deciding whether it is necessary to collect the type, amount and extent of Personal Data contemplated by the Data User, and explore whether less privacy intrusive alternatives could be adopted.

- The assessment is to identify, focus on and address the key areas of data privacy concern, having considered relevant factors including:
  - Functions and activities of the Data User.
  - Nature of the Personal Data involved.
  - Number of individuals concerned.
  - Significance of harm that may impact the Data Subject should their Personal Data be improperly handled.
  - Privacy requirements prescribed under the local laws and regulations.

- Adopt a "privacy by design" approach to implement from the outset measures to protect the Personal Data against indiscriminate or unauthorised access, processing, erasure, loss or use as it is practicable to do so. For example:
  - Reduce the amount of personal data to be collected to the extent that is necessary to fulfil the project objective but not excessive.
  - Safely delete, erase or dispose Personal Data when no longer required for the purpose.
  - Define clearly and limit the number of persons who can access and use the Personal Data on a “need-to-know” basis.
  - Incorporate appropriate level of system security measures.

G. Appendix G – Glossary of Terms

A glossary of terms used in this Policy is provided below for reference. Terms are capitalised throughout the document.

Affiliate means, with respect to the Company, a body corporate which the Company controls;

Board means the board of directors of the Group or an Affiliate;

Board Risk Committee ("BRC") means a Risk committee established by resolution of the Group or Affiliate Board;

Business Objectives means the measurable steps the Group takes to achieve its Strategy;

Business Unit ("BU") means one or more Affiliates (or parts of Affiliates) of AIA Group;

Chief Executive Officer ("CEO") means the Chief Executive of the Group or the BU appointed by the Group Board or an RCE respectively;

Chief Risk Officer ("CRO") means the senior officer of the Group or BU, as appointed by the Group or BU CEO from time to time, responsible for the Group Risk & Compliance function;

Company means AIA Group Limited;

Data Owner is the individual or business function within a BU who is responsible for the accuracy, integrity, and privacy of Personal Data under their responsibility, and to ensure adequate controls are implemented to protect Personal Data from leakage or misuse. Data Owner makes decisions regarding the handling of data in accordance with AIA Group's Information Security Policies, Standards and Procedures, and in Compliance with all local laws and regulations. Data Owner is responsible for reviewing requests for access to Personal Data under their responsibility. Other major responsibilities include:

- Responding to requests for access to Personal Data. Before approving access, the Data Owner must confirm that the requestor has a legitimate business reason for accessing the data.
- Approving the minimum access or authorisation necessary for the requestor's needs.
- Support and enable the implementation of required security measures as outlined in AIA Group's Information Security Policies, Standards and Procedures. Data Owner may consult with IT and Compliance to determine appropriate controls.
- Ensuring that reviews are conducted regularly to ensure all approved access is still valid and appropriate; all data under their ownership is appropriately stored, retained or destroyed.

Data Privacy is the relationship between collection and circulation of Personal Data and associated regulatory/legal issues. Privacy concerns exist wherever Personal Data is collected, used, stored, transferred or disposed. The protection of Personal Data relies on various business functions actively coordinating with each other, such as Information Technology, Distribution, Marketing, Legal, Compliance and Human Resources;

Data Processor is a person who (a) Processes Personal Data on behalf of another person; and (b) does not process the data for any of the person's own purposes;

Data Protection Officer ("DPO") means a role in an organisation which oversees the implementation of data privacy framework;

Data Subject is the individual who is the subject of the Personal Data;

Data User is any person (e.g. a BU or individual) who controls the collection, holding, processing or use of Personal Data;

Executive(s) refers to an individual comprising part of Executive Management who is also a member of the ExCo;

Executive Committee ("ExCo") means the Management Committee of Executives of the Group or BU appointed by the Group or BU CEO to assist them (him/her) in the fulfilment of their (his/her) duties;

Executive Risk Committee ("ERC") means the Risk Committee(s) established by the Group BRC or BU ExCo chaired by the Group or BU CEO to oversee Risk Management;

Executive Management means any persons discharging an executive management role within the Group, or acting under delegated authority by an Executive;

First Line is made up of the business decision-takers who are responsible for ensuring that effective and appropriate processes are in place at all times to effectively identify, assess and manage risk in a manner consistent with the RMF;

Group means the Company and its controlled Affiliates;

Internal Control means a process, effected by the Group or BU Board, Executive Management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and Compliance;

Policy(ies) are documents pertaining to rights retained and matters governed by the Group or Affiliate Board, as set out in the Group or Affiliate Board Charter, or in accordance with the TOR of any committees established by the Group or Affiliate Board;

Policy Owner refers to the individual with overall accountability for a Policy or Standard including its substance, communication, effectiveness and appropriate adherence;

Personal Data is also known as Personally Identifiable Information ("PII"), is recorded data relating to a Data Subject which identifies that individual either on its own or by reference to other information. It can include statements of opinion about a person. This includes data relating to AIA Group clients (or the clients of AIA Group business partners), agents, contractors, employees and business contacts.

Examples include (individually or together):

- Identification numbers (e.g. passport, driver licence, national ID, healthcare ID, etc.);
- Contact information (e.g. telephone numbers, addresses and email address);
- Account/credit card numbers and transactional history;

- Employment records including employee performance evaluation;
- Employee/visitor registration records;
- CCTV recordings, telephone recordings and emails in relation to employees' business activities;
- Individual name, age, gender, birth date, marital status, occupation;
- Medical/dental history & pharmaceutical information;
- Financial data (e.g. credit rating, income, etc.); and
- Racial, religious, political creed, union affiliation, place of birth, sexual preference, criminal history.

The above is not an exhaustive list of Personal Data and each BU can determine what are considered as Personal Data in the respective environment;

Personal Data Breach is a breach of security or other incident leading to the accidental, unauthorised or unlawful destruction, use, loss, change or disclosure of, or access to, Personal Data that is with the control or possession of a BU.

Examples include:

- Stolen or lost computers, storage devices and paper files containing Personal Data, including where passwords to access Personal Data are stored on the device.
- Employees or contractors gaining access to files containing Personal Data without business need or authorisation.
- Security of systems, computers or storage devices containing Personal Data being compromised, for example through a virus, malware, ransomware or other cyber-attack.
- Mail or email containing Personal Data sent to the wrong recipient.
- Disclosure of Personal Data to a third party who obtained it by deception.
- Unauthorised or inappropriate use of file-sharing software (e.g. Office 365) resulting in Personal Data leakage.

Privacy Impact Assessment is a tool which helps to identify an effective way to comply with data protection obligations and meet Data Subjects' expectations of Data Privacy.

Privacy Policy Statement / Privacy Statement means a document sets out the policies and practices of an organisation's commitment to protecting personal data privacy;

Procedure(s) are detailed instructions or guidance on how to implement or comply with the requirements usually stemming from a Policy or Standard, or recommendations to users when specific Policies and Standards do not apply. By nature, should be open to interpretation;

Processing means any operation or set of operations which is performed on Personal Data, whether or not by automated means. It means any way in which Personal Data is handled, for example: collection, use, recording, organisation, structuring, storage, adaption, alteration, retrieval, disclosure, erasure, deletion or destruction. Therefore, Processing covers everything that a BU and its Processors do with Personal Data;

Processors mean third parties who have access to or otherwise collect, use or disclose Personal Data on behalf of the Group;

Regional Chief Executive ("RCE") means members of the Group ExCo with overall responsibility for BUs;

Risk Appetite means the types and amount of risk, on a broad level, that the Group is willing to accept in order to achieve its Strategy and Business Objectives;

Risk Committees mean committees which are charged with direct Risk Management responsibilities to support the Boards and Executive Management of Group and BUs;

Risk Management means coordinated activities to direct and control an organisation with regard to risks;

Second Line consists of the Group and BU Risk & Compliance functions. These functions are independent of the First Line (with a direct reporting line to the Group CRO who reports direct to the Group CEO) but work closely with the First Line to ensure that risks are being managed appropriately within the Group's Risk Appetite;

Sensitive Personal Data is a subset of Personal Data. It means Personal Data which, due to its nature, has been classified as requiring additional privacy and security protections.

Data protection laws and regulations in some countries specifically define what types of data are Sensitive Personal Data and prescribe additional mandatory safeguards for Sensitive Personal Data. Other data protection laws and regulations define it by reference to the risk of harm that would be caused if there were a data breach. Sensitive Personal Data includes data relating to AIA Group clients (or the clients of AIA Group business partners), agents, contractors, employees and business contacts.

Examples of Sensitive Personal Data:

- Government-issued ID numbers (including National Identity numbers, Healthcare Identity numbers, Social Security numbers, Tax numbers, drivers licence numbers, passport numbers, etc.);
- Financial account numbers (bank account numbers, credit card numbers, and other information if that information would permit access to a financial account) and financial data such as credit rating, annual income, transactional history, etc.;
- Reports of individual background or credit checks;
- Medical, dental, insurance claims history, genetic data and biometric data1, including any information on any individual's health, disability or disease; and

[1] Biometric data is one category of Sensitive Personal Data and includes (i) the physiological data with which individuals are born and (ii) behavioural data which are the characteristics developed by an individual after birth. It often contains an individual's intimate information relating to health, mental condition or racial origin.

- Data elements revealing racial or ethnic origin, sexual orientation, political opinions, religious beliefs, trade union membership, criminal records, histories of prosecutions or convictions or allegations of crimes.

Standard(s) are documents pertaining to the rights retained and matters governed by the Group or BU ExCo, as delegated by the Group Board to the Group CEO or by an RCE to a BU CEO. Standards set out requirements for implementing principles such as those set out by a Policy or mandatory actions or rules that give Policies support and direction. Further, pursuant to the Group or Affiliate Board Charter, Standards are developed to govern management of the Group or BU and profit performance, including all operational and administrative matters except for those specifically retained by the Group or Affiliate Board and/or committees of the Group or Affiliate Board and delegated to the Group CEO;

Third Line is Group Internal Audit ("**GIA**"), which reports to the Group BAC. GIA is responsible for providing independent assurance over the effectiveness of key Internal Controls and makes recommendations based on the audit findings;

Third Party Security Assessment ("TPSA") means a Group IT process to assess the security controls of any third party which is entrusted with AIA's data.

AIA Group

Data Privacy Policy

Version 3.0