Objective:

This policy statement seeks to:

1. inform all members of GIA of the main databases currently managed by GIA and
2. set out the collection, usage, disclosure and sharing of the personal data of individuals (claimants, policyholders, applicants, insurance agents and/or any other individuals) whose personal data are submitted by GIA members and/or on their behalf by their appointed authorised agents to the various databases managed by GIA and/or its appointed third party service providers.

Collection of Data:

1. There are 3 main databases managed by GIA. They are:
   i. GIA Record Management Centre ("GIARMC")
   ii. Fraud Management System ("FMS")
   iii. Agents Registration and CPD Management ("ARCM")

***GIARMC*:**

2. This database collects personal data of policy holders, claimants and/or other individuals involved in a motor accident from motor insurance policies and Singapore Accident statements through its members and/or their authorised personnel and/or their authorised workshops/agents who will upload these data into an E-filing system. The data will then be transferred to the GIARMC. The GIARMC is a centralised database which holds data and personal information of policyholders and claimants. GIA and their appointed third party service provider collects and will have access to these data for the purpose of carrying out their operations.

3. In addition GIA's members will also get access to personal data and information of policyholders and claimants who are not their insured persons as the GIARMC is able to pick up data and send it to the relevant insurer once an accident report is lodged at the reporting centre. An illustration is when drivers involved in an accident lodge their accident reports at different reporting centres, the system is able to pick up the personal information and data of the drivers and send these data over to the respective insurers involved.

***FMS*:**

4. GIA's IT service providers upload data collected in the GIARMC database to the FMS system for the analysis of fraudulent motor claims. Members also upload data from their own databases to the FMS for fraud analysis and detection. The FMS is managed by GIA and/or their appointed service providers and data uploaded onto it are used for fraud investigation and management.

5. FMS also deals with fraud analysis and detection for travel insurance. These data are uploaded by members to the system in order for fraud analysis and detection to be carried out.

***ARCM*:**

6. This is a system where members' key in personal data of their general insurance agents and/or applicants who wish to apply to be an insurance agent. These data will be assessed by GIA and the Agents' Registration Board to determine whether their application is approved.

7. ARCM is also a system where GIA is able to track registered insurance agents' Continuing Professional Development (CPD) hours. Registered insurance agents are also able to access this system and check on their own professional development hours.

Usage, disclosure and sharing of data

1. GIA will now set out the purposes of the data collection and under what circumstances will the data collected be used, disclosed or shared.

***GIARMC*:**

2. The data collected from the GIARMC is used for the settlement of motor accident claims and to support the *No Claims Discount Enquiry* and the *FMS* which are managed and operated by GIA and/or GIA's authorised third party providers.

3. Aside from the above mentioned operations, data collected may be used and disclosed for the following purposes (including but not limited to):
    a. consider whether to provide a person with insurance coverage with respect to his/her profile and claims history and other underwriting factors
    b. process their application for insurance
    c. administer and/or manage their relationship, account and/or policy with the various insurers
    d. verify the NCD entitlement of a policyholder and/or potential policyholder
    e. carry out the necessary due diligence or other screening activities in accordance with legal or regulatory obligations or risk management procedure that may be required by law
    f. investigate fraud, misconduct, and unlawful action or omission relating to a person's application or his policy

***FMS*:**

4. Data collected will be used for the following purposes:
    a. create a claims history of the policyholders and/or claimants based on the information provided by members
    b. analyse the claims history and personal data of policyholders and claimants for suspected inflated and/or fraudulent claims

c. detect and highlight claims and/or claimants where there are possible indicators of suspected inflated and/or fraudulent claims
d. disclose the claims information and personal data of specific policyholders and/or claimants for evaluating, investigating, controlling or managing fraud

5. These data may be disclosed for the following purposes:
    a. To GIA members, parties that assist in evaluating, investigating, controlling or managing fraud, regulators, law enforcement and government agencies as reasonably required for the purposes stated
    b. For complying with requirements under any regulations, laws or court orders

ARCM:

6. ARCM is the information repository to store and process information relating to general insurance agents and nominee agents.

7. Personal data uploaded there will be used for the purposes:
    a. decide on the approval of an agent's or nominee agent's registration
    b. display the registration status of insurance agents and nominee agents to the public
    c. generate reports and statistics
    d. track the agents' CPD hours
    e. any other administrative and inquiry purposes relevant to the carrying out the Agents' Registration Board or Registrar's roles for the registration, sanctioning, auditing and administration of agents and nominee agents

<u>Access to the data collected</u>

***GIARMC*:**

a. Access to the GIARMC is through a User ID and Password. Members have to submit personal particulars of their staff who they want access to be granted to. Thereafter GIA's IT service provider will issue a User ID and Password to these personnel.
b. The names of these persons must be submitted to GIA for their approval before they are given access to the system.
c. Access to the system is limited only to people who are involved in the collection of data process, for example, authorised staff of members, the reporting centres and/or approved workshops.

FMS:

a. For maintenance of security of the FMS, only staff who are assigned by GIA members with responsibility for evaluating, investigating, controlling or managing suspected fraud will be granted access by means of designated user account and password upon registration and approval by GIA. All users must abide by this privacy policy and use the information for the purposes stated only.

b. Access to the FMS is contained within the members' office premises. Granting of or sharing of the designated account with unauthorised parties or gaining access to the FMS outside of office premises is strictly prohibited and constitutes a breach of the terms of usage of the FMS. GIA will have the sole discretion of terminating the access of users. All users must accept full responsibility for all activities that occur under the designated account and password assigned to them.

ARCM:

a. Access to the ARCM is through a User ID and Password. Members have to submit personal particulars of their staff who they want access to be granted to. Thereafter GIA's IT service provider will issue a User ID and Password to these personnel.

b. The names of these persons must be submitted to GIA for their approval before they are given access to the system.

Data Security and Protection

1. GIA and or its appointed third party service providers shall take reasonable precautions to safeguard all data, personal information transferred and/or submitted to the GIARMC, FMS and ARCM against unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks.

2. In this regard, GIA has in place multiple security safeguards to ensure that the personal data collected will not be easily accessed by external parties. GIA's IT service providers are contractually obliged to observe all PDPA obligations as a data intermediary as well as to adhere to the Technology Risk Management guidelines by the Monetary Authority of Singapore to ensure that personal data is properly protected.

3. To ensure compliance with the above, GIA has taken steps to get auditors to audit the IT provider's system periodically, to provide assurance that reasonable controls have been put in place to protect and secure data collected.

Obligations of GIA Members

1. As part of GIA's daily operations would require the collection, usage, disclosure and sharing of personal data, GIA would like to ensure that all its members are aware of GIA's systems and the data it would collect, use, disclose and share from the GIARMC, FMS and ARCM in order to carry out its functions.

2. GIA would thus require all its members to make clear to their policyholders and/or potential policyholders, claimants, agents and/or any individuals that may be required to provide their personal data that their personal data and claims information would be collected and disclosed to GIA for the purposes and uses set out in this policy. This personal data information may subsequently be disclosed to and shared with third parties as and when the need arises and/or required by laws.

3. Members are to ensure that they comply with their obligations under the PDPA to inform and obtain consent from all their policyholders and/or potential policyholders, claimants, agents and/or any individual that may be required to provide his personal data regarding the collection, use, disclosure, sharing of the data with GIA and that these may be disclosed to third parties for the purposes and uses set out in this policy. Members should also inform the general insurance agents under them with regard to their personal data being stored in the ARCM system and obtain their consent for their personal data to be used and/or disclosed by GIA.

4. GIA will not be responsible for any lapses in its members' obligations to inform and obtain consent nor will GIA be liable for any claims made by any third party as a result of its members' failure to inform and obtain consent or for any breach under the Personal Data Protection Act ("PDPA") by its members and/or their authorised agents.