PRIVACY POLICY

AMG INSURE BROKER COMPANY LIMITED

Company Registration Number 0105558151560

Register office: 60 Amorn Building 5th Floor, Soi Chalermsuk (Ratchadapisek 42), Chandrakasem, Chatuchak, Bangkok 10900 Thailand

Tel: +66 (0) 2-009-5955. Website: www.amgib.com

CONTENT

PRIVACY POLICY

AMG INSURE BROKER COMPANY LIMITED

AMG Insurance Broker Company Limited (the **"Company"**), which provides services as a general insurance agent and broker, including other insurance-related operations and associated activities (the **"Services"**), places a high priority on the privacy of its clients. Accordingly, the Company has developed this Personal Data Protection Policy to inform its clients of the Company's policy and guidelines regarding the protection of rights in relation to the collection, use and disclosure (the **"Processing"**) of personal data of natural persons (hereinafter referred to as **"you"**), received by the Company in both document and electronic formats. Such personal data is considered an integral part of the Company's Service terms and conditions, in compliance with the Personal Data Protection Act B.E. 2562 (2019) (**"Personal Data Protection Act"**) and relevant laws and regulations.

This Privacy Policy informs you of the methods by which the Company collects, uses, or discloses your personal data, including the types of data collected, the purposes of such processing, and the retention periods. It also provides details regarding the disclosure of personal data to third parties, your rights in relation to your personal data, measures for the confidentiality and security of your personal data, and the procedures by which you may contact the Company.

The Company recommends that you thoroughly read and understand this Policy, whether directly or indirectly, via various channels such as the Company's website at www.amgib.com, the internet, applications, and all related services or tools. Links to other relevant websites may also be provided to inform you of the Company's personal data protection practices. Each instance of your use of the services shall constitute full acceptance and acknowledgment of the terms set forth in this Policy.

SCOPE OF THIS POLICY

(1) This Personal Data Protection Policy governs the Company's activities concerning the collection, use or disclosure of personal data of data subjects. Such personal data must be identifiable and may include, but is not limited to, the following: full name, age, gender, nationality, identification number, passport number, address, telephone number, or email address. It should be noted that this information must not be generally available to the public.

(2) This Personal Data Protection Policy has been approved by the Company's Board of Directors and applies to directors, executives, employees, insurance agents, insurance brokers, as well as contractors, partners, and individuals, including service users or visitors to the Company's website, applications, or other communication channels. All parties involved are required to comply strictly with this Policy.

DEFINITIONS

"Company"	refers to AMG Insurance Broker Company Limited, a legal entity engaged in the business of providing non-life insurance agency and brokerage services, as well as other insurance-related activities and operations. The Company shall comply with all applicable laws and regulations to fulfill its business objectives.

“Personal Data”	means information about an individual that can identify that person directly or indirectly, including, but not limited to, title, full name, nickname, address, telephone number, national identification number, passport number, social security number, driver’s license number, tax identification number, bank account number, credit card number, email address, vehicle registration number, land deed number, IP address, Cookie ID, and audio recordings. However, publicly available information, corporate data, general business contact information (e.g., company name, company address, corporate registration number, office phone number, and business email address), anonymous data, and pseudonymized data that cannot be reidentified do not constitute Personal Data.
“Data Subject”	refers to an individual to whom the data relates, either as the individual directly associated with the data or as one who has rights and interest in the data, but does not imply legal ownership of or control over the data. The term **“Data Subject”** also includes guardians or legal representatives authorized to act on behalf of an incapacitated or quasi-incapacitated individual. This Policy does not apply to entities established by law, such as corporations, associations, foundations, or other legal organizations.
“Data Controller”	means an individual, legal entity, governmental authority, or organization responsible for determining the purposes and means of processing Personal Data. This responsibility includes the collection, use or disclosure of Personal Data, which may be determined solely or jointly with others.
“Data Processor”	means an individual, legal entity, governmental authority, or organization that processes Personal Data on behalf of a Data Controller and following its instructions. The Data Processor does not have the authority to determine the purposes and means of processing.
“Document Format”	refers to any written or printed material, including letters, numbers, diagrams, or other representations, which serve as evidence of meaning and may be used as a lawful record for Personal Data processing
“Electronic Data Format”	means information created, sent, received, stored, or processed electronically, including data exchanged via electronic data interchange, email, telegraph, telex, or fax. This data must be subject to personal data control and protection according to relevant standards and legal requirements.
“Anonymization”	refers to a process that reduces the risk of identifying a Data Subject to an insignificant level. Once anonymized, the data

	cannot identify an individual, thereby protecting Personal Data in compliance with established standards and legal requirements.
“Anonymous Data”	means Personal Data that has been processed to render it non-identifiable. Such data is no longer considered Personal Data. The anonymization process, while a form of data is no longer considered Personal Data. The anonymization process, while a form of data processing, must be legally authorized and capable of ensuring that the data cannot be re-identified.
“Pseudonymization”	refers to processing Personal Data in a way that the data cannot be attributed to a Data Subject without additional information. This additional information must be stored separately and be subject to appropriate technical and organizational safeguards to prevent re-identification, enhancing data security and privacy according to data protection law.
“Pseudonymous Breach”	refers to pseudonymized Personal Data that, while not directly identifying the Data Subject, could be used for re-identification with additional data. Unauthorized access to such data proses risks to the rights and freedoms of the Data Subject.
“Processing”	means any operation or set of operations performed on Personal Data or sets of Personal Data, whether by automated means or not, including but not limited to collection, recording, organization, structuring, storage, alteration, retrieval, consultation, use, disclosure, transmissions, dissemination, or otherwise making available, alignment, combination, restriction, erasure, or destruction, conducted per legal standards for Personal Data protection.
“Sensitive Personal Data”	means inherently private information prone to misuse or discrimination and requires special handling. This data includes but is not limited to race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health data, disabilities, union membership, genetic data, biometric data, or other similar sensitive data as defined by the Data Protection Committee.
“Personal Data Breach”	means any security breach leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to Personal Data that may impact the rights and freedoms of the Data Subject, potentially causing financial loss or damage to the Company’s reputation.
“Data Protection Officer (DPO)”	means an individual or committee appointed by the Company to oversee compliance with the Personal Data

	Protection Act B.E. 2562 (PDPA). The DPO's core duties include advising on legal data protection compliance, assessing risks to Personal Data, and collaborating with relevant departments to ensure appropriate safeguards are in place.
"Personal Data Protection Law"	refers to the Personal Data Protection Act B.E. 2562, including other related laws designed to safeguard the rights and freedoms of Data Subjects, setting guidelines for the lawful handling of Personal Data, including its collection, use, disclosure, and processing to prevent privacy infringements.

PURPOSE OF COLLECTION, USE, AND DISCLOSURE OF PERSONAL DATA BY THE COMPANY

The Company, operating in the field of insurance agency and brokerage, inclusive of all general and other insurance activities as well as related business operations, finds it necessary to collect, use, and disclose personal data for the following purposes:

1. **Execution of Client Requests:** The Company collects, uses, and discloses personal data to fulfil client requests prior to or in accordance with a contractual agreement. The objective is to verify or identify the client's identity when accessing the Company's platform, products, and/or services, as well as to facilitate account management, membership, delivery, financial matters, and any associated tasks required for the client to receive requested products and/or services.

2. **Advertising and Marketing Management:** The Company's objective includes advertising, conducting marketing campaigns, analyzing and developing products, and engaging with clients to provide guidance or introduce products and services. This may involve handling media and advertisements, where, in some instances, the client may appear as a presenter or feature within the Company's promotional media.

3. **Operations and After-Sales Client Care:** The Company intends to review and analyze personal data to enhance online service channels, ensuring clients receive the highest quality of service in terms of speed and convenience. Additionally, the Company prioritizes the efficient management and monitoring of client accounts to prevent unauthorized access and to continually improve service delivery.

4. **Information Technology Management:** The Company aims to establish and develop information systems for data collection and processing, with data connectivity between clients and agents, to support technology-related services. This includes processing data from website usage, applications, and various social media platforms (e.g., Facebook, LinkedIn, Twitter, YouTube, and Line) to ensure the system operates effectively and supports the Company's business activities.

5. **Business Development and Operation:** The Company pursues activities to enhance business performance, including managing products and/or services, fraud detection and prevention, customer relationship management, as well as evaluating and measuring the effectiveness of marketing and advertising policies across different channels. This is to ensure efficient operations and to foster business growth.

6. **Management of Complaints, Disputes, and Legal Proceedings:** The Company is committed to handling complaints, disputes, and legal proceedings, including risk management by reviewing, investigating, and taking measures to exercise rights under contracts and relevant laws. This is aimed at resolving disputes or conflicts that may arise between the Company and Clients in connection with the Company's services.

7. **Risk Assessment:** The Company collects and processes personal data for the purpose of evaluating and analyzing risks associated with insurance activities. This encompasses calculating insurance premiums and tailoring proposals suitable for clients, ensuring the Company's operations align with acceptable risk standards and meet client's needs appropriately.

8. **Service Improvement:** The Company aims to analyze data and conduct research on insurance services to continuously enhance the quality and efficiency of services provided to clients. The goal is to respond to client needs and increase satisfaction by implementing improvements based on data-driven insights and market trend analyzes to maintain service relevance and optimal performance.

9. **Customer Relationship Management:** The Company is committed to fostering long-term client relationships by ensuring high-quality post-sales service that fully meets client's needs. Additionally, the Company values client feedback to refine and develop service offerings, aiming to build client satisfaction and trust through clear and open communication.

10. **Fraud Prevention:** The Company uses personal data to detect and prevent potential fraud in business processes. The Company has implemented strict procedures and measures to prevent and examine fraudulent behavior. Additionally, the Company is dedicated to safeguarding personal data from unauthorized access or misuse by employing appropriate security technologies and systems, thereby assuring clients of the safety of their personal data.

PERSONAL DATA COLLECTED

Personal data refers to any information that can be used to identify the data subject, either directly or indirectly. This identification is characterized by at least three key features as follows:

- **Distinction** refers to the capacity of the data to differentiate between individuals, allowing it to clearly point to a specific person.

- **Tracking** refers to the ability of the data to monitor the behavior or activities of an individual. This data may be utilized to analyze and assess the individual's conduct.

- **Linkage** refers to the capability of the data to be connected with other information in such a way that it identifies an individual. This can be further divided into two scenarios:

    - **Linked Data:** Refers to instances where information, when combined with related data, can clearly identify an individual.

    - **Potentially Linked Data:** Refer to situations where a dataset, when combined with other data, may identify an individual; however, the additional data required for such identification may not be within the system or could be located on the internet or other external sources.

The data may consist of any information that can be used to identify the data subject, either directly or indirectly. Such data may be understood or not, and may be in a form that is accessible by computers or other devices automatically, or stored in an organized manner for easy access. The purpose of such data processing is as follows:

- **Collection for Processing:** Data may be collected for processing by computers or devices, or as part of a data system used for data processing.

- **Processing on Command:** Data may be processed by computers or devices following specific instructions or programs, which may include data analysis, data management, or the transmission of data of data to other parts of the system.

Personal data is any data that can be used to identify an individual, whether in paper form or other formats, and is intended for future processing. Even if the data itself may not directly identify an individual at the time, when combined with other data or information, it may enable such identification. Furthermore, personal data need not be combined with other data to identify an individual, nor is its identification dependent on the veracity of the data.

The Company has collected personal data of its clients only to the extent necessary for the purpose of using the data, as will be notified to the data subject, and has classified the types of personal data as follows:

1. **Identity Data:** Refers to data that can be used to identify the data subject, including data related to specific names or official documents, with the following details:

   (1) **Name Identification:** Title, First Name, Surname.

   (2) **Identification Numbers:** Nation ID number, professional license number (for each profession), business registration number, social security number, passport number.

   (3) **Official Documents:** National ID card, passport, house registration, work permit, driving license, vehicle registration book, and other documents that can be used to identify an individual.

   (4) **Status Information:** Marital status, military service status.

   (5) **Other Personal Data:** Language, behavioral data, bankruptcy status, information about minors, persons with disabilities, and persons similarly deemed incapacitated.

2. **Contact Data:** Refers to data used for communication with the data subject, including data related to addresses and other communication channels, as follows:

   (1) **Address:** Current address, registered address, postal address.

   (2) **Electronic Contact Information:** Email address, phone number, fax number, Line ID, MS Teams ID, Facebook ID, Instagram ID.

(3) **Other Contact Information:** Contact information provided when the data subject registers on websites or applications, participates in activities, exhibitions, and seminars, or other similar information.

3. **User Account Data:** Refers to information necessary for the creation and access of user accounts within the Company's system, including the following details:

   (1) **Username:** The name chosen by the data subject for identification within the system.

   (2) **Password:** The password used for accessing the user account, which must be kept confidential.

   (3) **Security Questions and Answers:** Information used to verify identity for password resets or for account security.

4. **Financial Information:** Refers to data related to the financial status and transactions of the data subject, including key information such as bank account numbers, credit/debit card numbers, payment history, income and sources of income, payment methods and forms, PromptPay data, receipts, payment details, cheque information, credit data records, financial instrument details, deposit records, tax amounts, outstanding balances, financial statements, and company certifications and shareholder lists.

5. **Employment Information:** Refers to data regarding the employment status and employment details of the data subject, including the following:

   (1) **Job Title:** Information about the position or role the data subject holds within an organization.

   (2) **Company/Organization Name:** The name of the company or organization where the data subject is or has been employed.

   (3) **Employment History:** Information regarding past employment, including tenure in various positions and relevant organizations.

   (4) **Employment Income:** Data on income derived from employment, including salary, wages, special allowances, or other benefits.

   (5) **Performance Evaluation Data:** Information on performance evaluations received from employers or assessors, such as assessment scores, feedback, or development recommendations.

6. **Educational Information:** Refers to data regarding the educational background and qualifications of the data subject, with details as follows:

   (1) **Educational History:** Information on the education previously received by the data subject, including education levels and courses attended.

   (2) **Degrees/Certificates:** Data on academic qualifications obtained, such as a Bachelor's degree, Master's degree, Doctoral degree, or relevant certifications.

(3) **Name of Educational Institution:** The name of the educational institution from which the data subject graduated, whether domestic or international.

(4) **Grades or Scores:** Information on academic results, Grade Point Average (GPA), or grades received during studies.

7. **Health Information:** Refers to data about the physical and mental health conditions of the data subject, which may include sensitive information, such as:

(1) **Medical History:** Information on past illnesses, medical diagnoses, and treatments received.

(2) **Information on Health Conditions:** Data related to chronic illnesses, diagnosed health conditions such as mental health issues, or other health conditions that may impact life or work.

(3) **Treatment or Medication Information:** Information on treatments previously received, medications taken, or other medical therapies such as surgeries, physical therapies, medication usage, and ongoing medical care.

8. **Biometric Data:** Refers to data related to unique physical or behavioral characteristics that can be used to specifically identity an individual, including:

(1) **Fingerprints:** Information concerning the ridge patterns on an individual's fingertips, used for identity verification or authentication.

(2) **Facial Photographs:** Images of an individual's face, which may be used for identification via facial recognition technology.

(3) **Voice Data:** Information about distinctive aspects of an individual's voice, such as pronunciation, voice patterns, or accent, which can be used to confirm identity.

(4) **Signatures:** Information regarding the individual's signature, which is unique to that person.

(5) **Height and Weight:** Physical characteristics, such as height and weight, which in certain circumstances may aid in identification.

(6) **Photographs:** General photographs showing an individual's appearance, including body shape, skin color, attire, or any uniquely worn items.

9. **System Usage Data:** Refers to data related to an individual's usage of computer systems or electronic devices, including access to the company's online services. This data may be used to analyze usage and enhance the user experience, comprising:

(1) **Login Data:** Information on the time and location of user logins, including login history and usage of the company's platform.

(2) **Website/Application Usage History:** Records of site visits, clicks, content viewing, purchases, or other activities on the company's websites or applications.

(3) **Location Tracking Data:** Information logging the user's location, such as GPS data or device-tracking information.

(4) **Marketing Communication Engagement Data:** Information regarding receipt of marketing communications, offers, or promotional activities via various channels, such as email or advertisements.

(5) **Service Usage History:** Detail on services previously used or currently in use by the user, including feedback, comments, or complaints regarding such service.

(6) **Social Media Usage Data:** Information related to social media accounts linked to the company's services, including Facebook, Instagram, Twitter, or other platforms.

10. **Preferences and Interests Data:** Refers to information regarding personal preferences and interests of the data subject, which may influence their interactions with the company. This data may be utilized to enhance customer service experience and personalize communications, including:

(1) **Personal Preferences and Interests:** Information on individual preferences, such as types of products or services of interest, as well as favorite content or activities, which the company uses to refine services and marketing offers.

(2) **Marketing Communication Preferences:** Information regarding the data subject's desire to receive news, promotions, or marketing campaigns via various channels, such as email, messaging, or social media.

(3) **Promotional Activity Participation:** Data related to participation in promotional events, receipt of special offers, or other promotional activities organized by the company or its partners.

(4) **Information Sharing Decisions with the Company or Partners:** Personal data voluntarily provided by the data subject through marketing or promotional events.

11. **Survey or Feedback Data:** Refers to information provided by the data subject through survey responses or feedback, which the company uses to improve its services and products, and to enhance customer experience, including:

(1) **Survey Responses:** Information provided in response to surveys, such as feedback or marketing-related data on preferences or interests.

(2) **Comments or Feedback:** Comments or suggestions provided on the company's website, applications, or other platforms, which may be used to improve services or address product or service issues.

(3) **Survey Data:** Data collected from surveys, including statistical information gathered from survey or group assessment.

(4) **Satisfaction Assessments:** Information regarding satisfaction levels with products or services, used to evaluated product or service effectiveness and suitability.

(5) **Other Similar Data:** Additional information related to surveys, assessments, or feedback provided by the data subject in other forms.

12. **Membership or Participation Data:** Refers to data related to membership subscriptions, registration to participate in activities, completion of request forms, or participation in groups or campaigns. This data may include:

    (1) **Membership Information:** Information provided by the data subject upon becoming a company member, such as name, address, email, phone number, or other identification and account details.

    (2) **Group or Event Participation Information:** Information provided by the data subject when joining groups or events organized by the company or its affiliates, such as seminars, conferences, competitions, or public activities.

    (3) **Request Form Information:** Information provided by the data subject when completing request forms for services or special privileges, such as requests for additional information or benefits.

    (4) **Campaign Registration Data:** Data associated with registration for marketing campaigns or promotional events, such as sales campaigns or competitions.

    (5) **Service Type Data:** History of subscriptions or selections of company services, including details on the types of services subscribed to.

    (6) **Service Subscription History:** Data related to subscription history for services or participation in company activities, including membership renewal or cancellation records.

13. **Transaction Data:** Refers to data relating to transactions for the purchase and sale of goods and services, including transactions between the data subject and the company, comprising:

    (1) **Sales Details:** Information on goods and services purchased, such as product or service specifications.

    (2) **Order Number:** The reference number for the data subject's order, which can be used to track order processing or delivery.

    (3) **Transaction History:** Information about past transactions, including transaction dates, service locations, or delivery points.

    (4) **Delivery Address/Date and Time of Receipt:** Data on the delivery address and the scheduled date and time for receipt or delivery.

    (5) **Service Request Forms:** Information from forms completed by the data subject to request services, including special or requested benefits.

    (6) **Acknowledgment and Recipient Signature:** Information on confirmation of goods or service receipt, including recipient signature.

(7) **Invoices:** Information related to invoices or payment documentation associated with transactions.

(8) **Transaction Location and Status:** Information on the transaction location or its current status.

(9) **Purchase Behavior:** Information on purchase patterns, including preferred purchase times, product selection behaviors, and buying trends.

(10) **Complaints and Claims:** Information on complaints or claims related to goods and services.

(11) **Outstanding Debt:** Information on outstanding amounts or items related to financial transactions.

14. **Communication Data:** Personal data provided by the data subject to the company when using services or engaging in communications with the company, including information on interactions, communication records, emails sent or received, and inquiries made by the data subject.

15. **Multimedia Data:** Refers to data related to audio, still images, or moving images, including information obtained from CCTV cameras used to monitor activities within or around the company. Multimedia data also includes recordings made during participation in events or campaigns organized by the company.

16. **Data Automatically Collected through Computer System Monitoring:** The company may use automated technology to collect personal data when the data subject uses the company's website or applications, either via computer or mobile device. Such technology may include cookies, pixels, tags, and similar tracking technologies. The data that may be collected includes:

(1) **Personal Data Provided by the Data Subject:** Information specified by the data subject via the company's website or applications, such as name, address, phone number, and social media usage data.

(2) **Marketing Activity Data:** Personal data collected during marketing activities on other websites, applications, or social media platforms, particularly when the data subject participates in promotional events or campaigns.

(3) **Automatically Collected Data:** Information collected through computer system monitoring, such as IP addresses, browser used, operating system, pages visited, and referral websites that directed users to the company's site.

(4) **Precise Location Data:** Information on precise location, potentially including real-time geographic coordinates from mobile devices or computers. The company may use GPS signals, Bluetooth, IP address, Wi-Fi hotspots, and mobile cell towers to approximate the device's location.

17. **Third-Party Personal Data Provided by the Data Subject:** The company may collect personal data of third parties provided by the data subject. This data may include titles, names, surnames, addresses, phone numbers, relationships with the data subject, occupation, executive status, authorized representative roles, directorships,

shareholdings, employment, ownership, co-ownership, or any other personal data subject assures the company that they have obtained the necessary consent from such third parties to disclose their data to the company and to allow the company to process the personal data for the purpose communicated to the data subject.

18. **Social Relationship Data:** The company may collect data related to the social relationships of the personal data subject, which may include political affiliations, positions in organizations, relationships with company personnel, employment status with the company, and involvement in company-related business.

19. **Other Data:** The company may collect, use, or disclose other data related to the relationship between the company and data subject, which may include:

    (1) Contractual Data: Contract numbers, types, and retention periods for data.

    (2) Application Forms or Questionnaires: Forms completed by the data subject to provide additional information to the company.

SOURCES OF PERSONAL DATA

The Company may receive your personal data from various parties involved in the personal data protection process. These parties encompass four main categories: the data subject, the data controller, the data processor, and third parties. The relationships between these parties are outlined in four distinct channels as follows:

1. **Personal Data Obtained Directly from You**

   The Company may receive your personal data directly from you, through affiliated companies, or from existing data held by the Company resulting from your use of or engagement with Company services. This may occur through digital channels, websites, authorized representatives, or other communication channels. The Company collects your personal data through the following service processes:

   (1) Direct Provision of Personal Data by the Data Subject: The data subject may provide personal data to the data controller in various instances, such as service applications with the Company, membership or package registrations, contract signings, form submissions, and documentation required for transactions with the Company. This also includes instances where you voluntarily submit data, such as participating in surveys, email or telephone exchanges, and other forms of communication between the Company and yourself, opinion surveys, or data collection from the Company's website via browser cookies, user identity verification, training sessions, activities, or similar engagements.

   (2) Provision of Personal Data to the Data Processor: The data subject may submit personal data to the data processor as part of operational tasks performed on behalf of the data controller.

   (3) Provision of Personal Data from the Data Processor to the Data Subject: The data controller may provide personal data to the data subject upon request, such as in the processing of submitted requests by the data subject.

(4) **Provision of Personal Data from the Data Processor to the Data Subject:** The data processor may deliver personal data to the data subject as per the instructions or guidance provided by the data controller.

2. Personal Data Received from Third Parties

The Company may receive your personal data from third parties in the following circumstances:

(1) **Provision of Personal Data from the Data Controller to the Data Processor:** The data controller may provide personal data to the data processor under an outsourcing agreement related to data processing operations.

(2) **Provision of Personal Data from the Data Processor to the Data Controller:** The data processor may provide personal data to the data controller upon the completion of processing activities as per the agreement.

(3) **Provision of Personal Data from the Data Controller to Third Parties:** The data controller may provide personal data to third parties when necessary to fulfil business agreements or conduct relevant activities.

(4) **Provision of Personal Data from the Data Processor to Third Parties:** The data processor may deliver personal data to third parties in accordance with the instructions or guidance provided by the data controller.

(5) **Personal Data Obtained from Third Parties:** The Company may obtain personal data from third parties, including but not limited to the Company's business partners, clients, data controllers, data processors, or other parties that the Company reasonably believes have a lawful right to process the personal data of the data subject and to disclose such data to the Company.

3. Personal Data Obtain from Other Sources

The Company may obtain your personal data from sources other than directly from you. These sources may include but are not limited to:

(1) **Entities Engaging Company Services:** Personal data obtained from entities that are clients or service providers of the Company.

(2) **Government Agencies:** Data received from governmental agencies legally authorized and obligated to disclose such information.

(3) **Financial Service Providers:** Data obtained from financial service providers in connection with your transactions.

(4) **Data Provider:** Data obtained from data providers responsible for the collection and management of personal data.

(5) **Other Organizations or Agencies:** Data received from other organizations or agencies with the legal authority to disclose such information.

4. **Personal Data Provided by the Data Subject in Respect of Third Parties**

In case where the data subject provides personal data of third parties to the Company, the data subject is responsible for notifying the third parties in accordance with this policy or relevant service announcements. The following steps should be undertaken:

(1) **Notification:** The data subject must inform the third parties of the disclosure of their personal data to the Company, including the purposes and nature of the data usage as stipulated in the Company's data protection policy.

(2) **Obtaining Consent:** Where required by law, the data subject must obtain consent from the third parties prior to providing their personal data to the Company.

LEGAL BASES FOR PERSONAL DATA PROCESSING

The Company may process personal data of the data subject based on the legal grounds outlined below:

1. **Contractual Basis**

The Company processes your personal data to provide services or fulfill the duties and obligations stipulated in a contract. The collection of personal data is necessary to perform contractual obligations, respond to queries, and verify identities during services between you and the Company, as well as for dealings with the Company's business partners to achieve the purpose of fulfilling contractual obligations. Failure to provide personal data may render the contract or legal transactions between you and the Company legally ineffective.

2. **Consent Basis**

You consent to the Company collecting, using, managing, maintaining, and disclosing your personal data as set forth in this Data Protection Policy and Privacy Notice, as well as in the terms and conditions associated with each service. The Company may use your personal data to offer products, services, or advertisements tailored to your interests, thereby enhancing your service experience. This includes sending offers, special benefits, recommendations, and updates, which may originate from your consent given to the Company, affiliated companies, business partners, or third parties related to the Company. Should you choose to withdraw your consent in the future, the Company will adhere to relevant legal requirements in effect.

3. **Vital Interests Basis**

The Company may process your personal data to prevent or mitigate risks to life and bodily harm in situations where you are unable to provide consent, particularly in health-related scenarios such as disease prevention and control during an outbreak, or processing health data for first aid or emergency hospital transfer in life-threatening situations. The Company will implement necessary legal measures and safeguards to ensure that your personal data is protected and used strictly for such purposes.

4. **Legal Obligation Basis**

The Company may disclose your personal data to comply with the orders of legally empowered authorities or to fulfill relevant legal obligations. This includes, but is not limited to, compliance with securities and exchange law, tax regulations, anti-money laundering laws, computer crime laws, bankruptcy laws, and other laws applicable to the Company domestically or internationally. In such cases, the Company may be required to share information with government agencies legally authorized to request the Company's data, such as the Revenue Department, Office of Consumer Protection Board, Office of Insurance Commission, National Police Agency, Office of the Attorney General, and various courts, ensuring strict adherence to relevant regulations and requirements.

5. Legitimate Interest Basis

The Company may process your personal data for legitimate and lawful purposes, including conducting research, compiling statistics, improving service quality, recording call center interactions, recording CCTV footage, managing risks, communicating with customers, handling complaints, and assessing customer satisfaction. Such data processing aims to enable the Company to offer high-quality services and respond to your needs effectively, including enhancing internal procedures for the ultimate benefit of customers and the Company's operations.

6. Archival/Research/Statistical Basis

The Company may retain and use data for purposes that hold archival, research, or statistical value. This includes:

(1) **Archival Databases:** The Company maintains data of historical or academic value, often utilized for research and educational purposes. Such data supports knowledge advancement and insight across various fields.

(2) **Research Databases:** The Company maintains research databases for studies in fields such as medicine, social sciences, or technology. These databases often contribute to the development of innovative approaches or discoveries beneficial to society.

(3) **Statistical Databases:** Statistical databases are used for analysis and reporting, which may include protected personal data. Such use supports valuable analyses aimed at improving services and marking data-driven decisions.

The retention and use of such data will comply with rigorous standards and practices to safeguard the rights of the data subject and ensure compliance with relevant laws.

PROCESSING OF PERSONAL DATA

1. Material Scope of Personal Data Processing

All personal data processing shall comply fully with the standards set forth under the Personal Data Protection Act B.E. 2562 (2019), without exception. However, certain types of personal data processing are exempted from the requirement of obtaining consent, as outlined below:

(1) Processing for Personal or Family Activities
Personal data collected solely for personal benefit or activities within a family context is exempt from consent requirements.

(2) Processing by Government Authorities for National Security
Data processing undertaken by state agencies responsible for national security, including financial security of the state, public safety, anti-money laundering activities, forensic sciences, or cybersecurity measures, is exempt from consent requirements.

(3) Processing for Media, Artistic, or Literary Activities
Processing of personal data within the scope of media activities, the arts, or literature is exempt if conducted in line with professional ethics or for the public benefit.

(4) Processing by Legislative Bodies
Processing undertaken by the House of Representatives, the Senate, Parliament, or committees appointed by such bodies in the exercise of their official duties and powers is exempt from the requirement for consent.

(5) Processing within Judicial Proceedings
Data processing carried out by the courts, officials within the judicial process, enforcement officers, and those handling the seizure or attachment of assets, as well as operations in the criminal justice process, is exempt from consent requirements.

(6) Processing by Credit Information Companies
Processing of data conducted by credit information companies and their members, in accordance with credit information business laws, is exempt from the consent requirement.

2. Territorial Scope of Personal Data Processing

The processing of personal data shall adhere to the standards of the Personal Data Protection Act B.E. 2562 (2019) in the following circumstances:

(1) Entities Established in Thailand
Data processing by entities or their branches established in Thailand, regardless of whether the actual data processing takes place within or outside Thailand.

(2) Entities Not Established in Thailand
Entities without an establishment or branch in Thailand, in case where they:

(a) **Offer Goods or Services to Data Subjects in Thailand**
Offer goods or services to individuals in Thailand, irrespective of whether payment is required.

(b) **Monitor the Behavior of Data Subjects in Thailand**
Engage in the tracking and collection of behavior data of individuals in Thailand, provided that such behavior occurs within Thailand.

3. Security Measures for Personal Data Protection

Upon receiving personal data from the data source, the Company shall process such personal data with appropriate security measures, ensuring the confidentiality and integrity of the data to prevent loss, unauthorized access, destruction, use, alteration, modification, or disclosure. The Company or third parties authorized by it may process personal data under the following conditions:

(1) Personal Data Collection

The Company will collect personal data provided by individuals in either document or electronic form within restricted access locations, using lawful and fair means. The Company will collect data only as necessary for service provision in line with defined purposes. Before proceeding, the Company will inform the data subject and obtain consent electronically, using a brief notification or other methods established by the Company.
If the personal data requested is necessary for legal compliance or contract performance with the data subject, failure to provide such data may prevent the Company from delivering certain services. The Company may collect information on the data subject's interests and services used, with prior consent unless an exception applies.

(2) Personal Data Usage

The Company shall use and disclose personal data only for the purposes specified by the data subject. Should the Company wish to collect, use, or disclose data beyond the initial purpose, it will notify the data subject beforehand unless legally permitted otherwise. The Company will ensure that data usage is appropriate, with secure access controls. The Company shall monitor its staff and authorized personnel to prevent unauthorized use or disclosure, except as legally required or permitted without consent.

The Company may engage third-party information service providers for data storage. Such providers must maintain strict security measures and are prohibited from collecting, using, or disclosing data beyond the Company's instructions.

(3) Personal Data Disclosure

The Company may disclose personal data or related information to partners, affiliates, or other entities within the following limits:

(a) **Business Support Disclosure**
The Company may share data with recipients to support its business operations, under contractual conditions that limit data use to intended purposes only. Recipients must destroy or return data once no longer needed.

(b) **Legally Mandated Disclosure**
The Company may disclose data upon request, as appropriate and lawful. In case of acquisition or sale of all or part of the Company's assets, collected data may be considered transferable to the buyer.

(c) **Court or Government Orders**
The Company may disclose data under legal mandates, including court orders, subpoenas, regulatory investigations, or any process requiring disclosure by law.

(d) **Cross-Border Data Transfers**
The Company may disclose data internationally, following applicable data protection laws, by adhering to standard contractual clauses or other legally approved mechanisms.

(e) **Disclosure to Business Partners and Service Providers**
The Company may disclose data to its business partners, clients, platform providers, IT service providers, payment processors, and other third-party entities for order fulfillment, payment processing, data analysis, promotions, research, marketing, customer satisfaction surveys, and other purposes as outlined in this policy. These external parties must ensure data protection to the same standards as the Company.

External parties with access to personal data may include:

- **Employee and Contractors** responsible for data processing on behalf of the Company.
- **Data Controllers or Processors** engaged by the Company, or third parties designated by the data subject to share information.
- **Global Affiliates and Business Partners** using the data to fulfill services as requested.
- **Service Providers, Auditors, Lawyers, and Advisors** supporting the Company's operations.
- **Government Authorities,** including law enforcement and judicial bodies authorized to request personal data, such as police, public prosecutors, courts, or other empowered governmental agencies.

4. Processing of Special Categories of Sensitive Personal Data

Where necessary, the Company may process sensitive personal data such as racial or ethnic origin, political opinions, religious, philosophical beliefs, sexual behavior, criminal records, health information, disabilities, trade union membership, genetic or biometric data, or other similarly sensitive data as determined by the Personal Data Protection Committee. The Company will take all reasonable measures to implement adequate security protocols to protect such sensitive data. Processing of this data will occur only for purposes permitted by law or for specific purpose as previously notified by the Company, depending on the nature of certain activities or services. Sensitive data processing will be conducted only upon obtaining written consent from the data subject before collection, or if the data subject voluntarily makes such data public, or where permitted by law to process without consent.

The Company does not typically process sensitive personal data such as racial or ethnic origin, blood type, or religion, except as required for employee-specific purposes. While such data may appear in documents voluntarily provided to the Company, such as national identification

cards, household registration records, or other personal documents, data subjects are required to redact any sensitive data themselves before submitting these documents. If such sensitive data is not redacted, the Company will assume that the data subject has expressly consented to the Company redacting the information on their behalf. Once redaction has been completed by the Company, the document provided shall be deemed complete and fully enforceable under applicable laws. The Company may process this data in accordance with the Personal Data Protection Act B.E. 2562.

Should technical issues or other circumstances prevent the redaction of sensitive data, the Company will retain such data solely for the purpose of identity verification and will not use it for any other purpose.

5. Personal Data of Minors, Quasi-Incompetent Persons, or Incompetent Persons

In cases where the Company becomes aware that personal data requiring consent for collection pertains to data subject who is a minor, quasi-incompetent person, or incompetent person, the Company shall refrain from collecting such data until consent has been duly obtained from the person legally authorized to act on behalf of the minor, such as a parent or guardian, or from a curator or custodian, as applicable. All actions will comply with statutory requirements, as detailed below:

(1) **Minors:** In commercial or business activities appropriate to the status of a minor, the minor may provide consent for the processing of personal data when such activities are equivalent to those a legally competent adult would engage in. However, if the minor is under the age of 10, the collection of personal data shall require direct consent from the person exercising parental authority.

(2) **Quasi-Incompetent Persons:** This refers to individuals deemed by a court order to be quasi-incompetent, often due to physical disability, mental disorder, alcohol or substance dependency, or similar conditions rendering them unable to manage their own affairs or potentially leading to harm to their property or family. Any consent for data processing must be obtained from the individual's curator, who holds the legal authority to act on their behalf, unless otherwise stipulated by law in certain circumstances that permit consent without the curator's involvement.

(3) **Incompetent Persons:** This refers to individuals whom a court has declared incompetent, generally due to mental incapacity. In such cases, any consent required for data processing must be obtained from the individual's custodian with the authority to act on their behalf.

If the Company is initially unaware that the data subject is a minor, quasi-incompetent person, or incompetent person and later discovers that personal data was collected without the necessary consent from the person with legal authority (e.g. a parent, curator, or custodian), the Company shall promptly delete or destroy the data unless a lawful basis, other than consent, justifies the processing of such data.

RIGHTS TO PERSONAL DATA PROTECTION OF THE DATA SUBJECT

1. Rights under the Data Protection Law

You, as the data subject, have rights as stipulated under data protection laws, including the following:

(1) **Right to Withdraw Consent:** You have the right to withdraw consent previously given to the Company for processing your personal data, at any time, as long as your data remains under the Company's control.

(2) **Right of Access:** You have the right to request access to your personal data held by the Company and to request a copy thereof. You may also request the disclosure of the source of any data acquired by the Company without your consent.

(3) **Right of Rectification:** You have the right to request that the Company correct any inaccurate personal data or complete any incomplete personal data.

(4) **Right to Erasure:** You may request that the Company delete your personal data in certain circumstances as permitted by law.

(5) **Right to Restriction of Processing:** You may request the restriction of processing of your personal data under certain legal conditions.

(6) **Right to Data Portability:** You may request the transfer of your personal data, which you have provided to the Company, to another data controller or directly to yourself, under specific conditions.

(7) **Right to Object:** You may object to the processing of your personal data in certain circumstances as permitted by law.

These rights may be exercised free of charge. The Company shall consider and inform you of the outcome within 30 days from the date of receiving your request.

2. Control and Contact by the Data Subject

The Company respects your right to privacy. You may select your preferred methods of controlling your data, and the Company will act on your request to ensure transparency and data accuracy. However, if you do not consent to data processing, the Company may be unable to fully perform the contractual obligations or fulfil the terms agreed with you.

3. Request for Rights Exercise

Request to exercise rights under clause 7.1 must be made in writing via the electronic system provided by the Company on its website, www.amgib.com, and in accordance with the procedures specified by the Company will make reasonable efforts to act within an appropriate time frame and not exceed any statutory deadlines. The Company reserves the right to decline a request if legal exemptions apply or if the request may prevent the Company from fulfilling its contractual obligation. The Company further reserves the right to charge a fee for processing requests, at the rate specified by the Company.

4. Verification of Identity

For security purposes, the Company may require you to verify your identity before exercising your rights. If there are any limitations on rights exercise, the Company will inform you if your request cannot be fulfilled.

5. **Exceptions to Rights**

If the Company processes your personal data on grounds of contractual performance, legitimate interests, or compliance with legal obligations, the Company may lawfully refuse your request to delete or restrict the use of personal data, if it falls within a legally permitted exception.

CONSEQUENCES OF NON-COMPLIANCE WITH THE DATA PROTECTION POLICY

Non-compliance with this policy may constitute an offence and may result in disciplinary action in accordance with the Company's work regulations or the terms of any data processing agreement (for data processors), as applicable to the nature of your relationship with the Company. Additionally, violations may be subject to penalties as set forth in the Personal Data Protection Act B.E. 2562 (2019), as well as other relevant laws, regulations, and directives.

MARKETING ACTIVITIES AND PROMOTIONS

1. **Distribution of Information**

During your use of the Company's services, you may receive communications about marketing activities, promotions, products, and services that the Company considers may be of interest to you, to ensure optimal service delivery.

2. **Disclosure or Transfer of Personal Data for Marketing Purposes**

The Company may disclose or transfer your personal data to external parties, both domestically and internationally, only to the extent necessary and in accordance with the data processing purposes specified in this Policy. Third-party advertising services, such as banner advertisements displayed on websites, may involve the use of cookies or other tracking technologies. These third-party activities are beyond the Company's control, and the Company has no rights to access or manage third-party operations. Third parties may cookies on your computer to track online activities and browsing behavior, enabling the display of advertisements aligned with your interests.

3. **Consent to Contact**

By providing consent to the Company, you authorize the Company to contact you via automated telephone systems or computer-controlled platforms, including sending pre-recorded messages or using other technology for lawful purposes and the offering of third-party products and services.

4. **Opting Out of Promotional Communications**

You may opt out of receiving promotional emails, newsletters, or the Company's latest information, as well as marketing phone calls, by contacting the Company through the channels specified in this Policy.

LINKING OF PERSONAL DATA WITH BUSINESS PARTNERS OR OTHER ENTITIES

1. Linking of Personal Data

Should you provide personal data directly to the Company, the Company may link your personal data with business partners or other entities. In such instances, the Company will seek your consent prior to proceeding with data linkage and will disclose the following information at a minimum:

(1) The business partners or entities with whom the Company intends to link your personal data;

(2) The purpose of linking your personal data;

(3) The method used for linking the personal data;

(4) The specific personal data to be linked;

(5) The individuals or entities entitled to access the linked personal data.

2. Disclosure of Linked Data Information

When linking personal data with business partners or other entities, the Company will clearly identify the data collector and those individuals or entities granted access to the linked data, ensuring that you are fully informed. Additionally, the Company will maintain a record of the data linkage as evidence. In cases where any changes are made to the linkage arrangement, the Company will notify you of such changes and seek your renewed consent before proceeding with any modified data linkage.

USE OF COOKIES

"Cookies" refer to small data files sent by a website and stored on the personal data subject's device upon visiting the website. Cookies assist in enabling the website to remember the preferences and usage information of the data subject, such as language preference, user profile, or other settings. Upon revisiting the website, the website can recall the user and apply these previously selected settings, unless the data subject deletes cookies.

The Company employs cookies to store your login, logout, and other information when you access the website. This is done to enhance the website's performance, improve functionality, and develop marketing and content aligned with your interests and preferences. Additionally, cookies facilitate the Company's analysis of website usage activities, such as the data, time, and specific pages accessed, as well as the referring website. Cookies are also utilized to prevent and detect unauthorized activities.

For certain services, the Company offers the option to save your username or password in a cookie to avoid re-entering these details upon future visits. The Company may also use Flash Cookies to

display content aligned with your selected interests on the website and to optimize your experience when selecting services, subscribing to updates, or completing online forms.

Data subjects have the right to manage their privacy settings by choosing to accept or decline cookies. Should you choose to decline or delete cookies, some features of the website may not function at optimal capacity, potentially resulting in slower or less convenient access and use of certain functions.

Cookie Preference: You may delete cookies through your browser settings and continue using the Company's website. However, this may result in slower or less convenient access and use of certain website functionalities.

PRIVACY POLICIES OF EXTERNAL WEBSITES

This Privacy Policy applies solely to the services provided by the Company and to the use of the Company's website. If you click on a link that directs you to another website (even if accessed through a link on the Company's website), your personal data will be subject to the external website's own privacy policy, which operates independently of the Company's policy. You are advised to review and adhere to the privacy policy outlined on the respective external website directly.

TRANSFER OF PERSONAL DATA OVERSEAS

The Company may transfer or disclose your personal data to affiliated companies or other parties abroad when necessary to fulfil a contract to which you are a party, or to take pre-contractual steps at your request, or for the performance of a contract between the Company and another individual or legal entity for your benefit. Furthermore, such transfers may be made to prevent or mitigate harm to your life, body, or health or that of others, or to comply with legal obligations or for reasons of significant public interest.

The Company may store your data on servers or cloud systems managed by third-party providers and may utilize third-party software or applications for processing your personal data. In these cases, the Company requires those third parties to implement appropriate security measures and ensures that no unauthorized parties gain access to your personal data.

Should the transfer of your personal data be made to foreign jurisdictions, the Company will strictly adhere to applicable data protection laws and will implement appropriate safeguards to ensure adequate protection of your data. Additionally, the Company will require recipients of your data to adopt suitable data protection measures, process only necessary data, and take steps to prevent any unauthorized use or disclosure of personal data.

RETENTION PERIOD FOR PERSONAL DATA

The Company will retain your personal data only as long as necessary for the purposes of processing as specified in this policy, detailed as follows:

(1) If you have provided data to the Company as a customer or contractual party, your data will be retained for the duration of the contractual period. Following the conclusion of the contract or relationship with you, your data will be retained for an additional ten (10)

years from the end of the contract year. The Company may retain data for a longer period if required for legal compliance or by order of a competent authority.

(2) The Company will retain your data according to specific types of activities and purposes outlined in the Privacy Policy.

(3) If you have provided data as a member, the Company will retain your data for as long as you remain a member.

(4) For data stored on applications, data will be retained until you delete your user account.

(5) Where personal data is processed on the basis of your consent, the Company will continue processing until you withdraw your consent and your request for withdrawal has been fully executed.

(6) For other cases, the Company will retain personal data only as reasonably necessary to achieve the purposes specified in this policy. Where a definitive retention period cannot be determined, the Company will retain data in accordance with anticipated durations, such as statutory limitation periods, up to a maximum of ten (10) years. In the event of legal proceedings, your personal data may be retained until such proceedings are concluded. Upon expiry of the retention period, the data will be deleted, destroyed, or anonymized in compliance with the Personal Data Protection law.

If a longer retention period is required by law or as directed by authorized officials, certain data may be retained for extended periods to meet business or legal obligations.

DATA SECURITY MEASURES

The Company recognizes the importance of maintaining the security of your personal data and has implemented appropriate measures consistent with industry standards to prevent unauthorized or unlawful loss, access, destruction, modification, or disclosure of personal data, as well as to prevent unauthorized use. The Company enforces specific access and use rights to maintain the confidentiality and security of personal data as follows:

(1) The Company employs technical, physical, and administrative security measures to prevent unauthorized access and disclosure of personal data. These measures align with industry standards, and Company employees are required to undergo training on personal data protection and security. Additionally, the Company requires its partners to implement adequate measures when processing, transferring, and safeguarding personal data on behalf of the Company. These measures are reviewed and updated as necessary to ensure compliance with relevant standards and laws.

(2) The Company has established clear policies and procedures to protect personal data and prevent unauthorized access, including:

(a) Implementing policies and procedures that comply with data protection laws and ensure secure data management.

(b) Ensuring that personal data will not be sold or transferred to any third party unrelated to the Company’s processing activities.

(c) Restricting customer access to personal data to the extent necessary.

(d) Preventing unauthorized access to personal data through encryption, identity verification, and antivirus technology.

(e) Assessing and evaluating the operational practices of the Company's partners, mandating that they comply with data protection laws and regulations.

(f) Monitoring and reviewing the Company's website through specialized data protection and security agencies.

(g) Providing training to employees and relevant parties on personal data protection.

(h) Regularly evaluating data protection practices, data management, and security measures.

(i) Implementing a system for data review, deletion, or destruction when the retention period expires or the data is no longer relevant to its original purpose.

(j) Regularly reviewing and enhancing security measures as technology evolves to optimize the security of personal data.

USE OF PERSONAL DATA FOR ORIGINAL PURPOSES

The Company reserves the right to collect and use your personal data obtained prior to the enactment of the Personal Data Protection Act for the original purposes for which you were notified. Should you no longer wish for the Company to continue collecting or using this personal data, you may withdraw your consent at any time by notifying the Company through the designated channels.

AMENDMENTS TO THE PRIVACY POLICY

The Company will periodically review and update this Privacy Policy to ensure compliance with applicable practices and legal regulations. Should there be any amendments to this Privacy Policy, the Company will promptly inform you by updating the relevant information on our website. The Privacy Policy was last reviewed on 11 November 2024.

CONTACT INFORMATION

Data Controller Details

Name: AMG Insure Broker Company Limited

Address: 60 Amorn Building, 5th Floor, Chalermsuk Alley (Ratchadapisek 42), Chan Kasem, Chatuchak, Bangkok, Thailand

Contact Information:
Tel: +66 (0) 2-009-5955
Fax: +66 (0) 2-512-1511

Email: info@amg.co.th
Website: www.amgib.com

Data Protection Officer (DPO)

The Data Protection Officer of AMG Insure Broker Company Limited

Address: 60 Amorn Building, 5th Floor, Chalermsuk Alley (Ratchadapisek 42), Chan Kasem, Chatuchak, Bangkok, Thailand

Contact Information:
Tel: +66 (0) 2-009-5955
Fax: +66 (0) 2-512-1511
Email: dpo@amg.co.th

This Privacy Policy is effective from 27 May 2019 onwards.

Name: Mr. Karnt Pumiresnawan
Title: Chief Executive Officer