PERSONAL DATA PROTECTION POLICY

AMORN VISION(BANGKOK) COMPANY LIMITED

Amorn Vision (Bangkok) Co., Ltd. (**"the Company"**) is a Thailand-based organization providing creative digital media production and publication services. The Company offers consultancy services, media production, and online program development, including content relating to automotive diversity. It also operates as a media agency responsible for media planning and advertising procurement, media strategy development, market analysis, and coordination to ensure that clients' content effectively reaches their target audiences. In addition, the Company provides training services, recreational activities, academic seminars across various disciplines, modern communication and technology knowledge, legal, finance and accounting, taxation, and fire-safety training. The Company also organizes and manages events. These services are collectively referred to as the **"Services"**

In the course of providing the Services, the Company may need to collect personal data of service users (**"Service Users"** or **"you"**).

The Company recognizes its responsibility to safeguard the security of the information under its control and is committed to managing such data in a secure and trustworthy manner. Acknowledging the importance of your privacy, the Company has established this Personal Data Protection Policy (**"Policy"**), which describes the details regarding the processing, collection, use, and disclosure (**"Processing"**) of personal data. This Policy forms part of the terms and conditions of the Services and outlines the Company's practices in handling information it receives directly and/or indirectly from Service Users, including through the Company's website at https://amvsbangkok.com/ which may contain links to third-party websites that may have different data management practices.

To ensure that you clearly understand the practices of such websites and any related differences, the Company encourages you to carefully read this Policy as well as the privacy policies of any third-party websites. By accessing or using the Services, you are deemed to have read, acknowledged, and accepted the terms and details of this Policy as set out below.

1. DEFINITIONS

"Company" means Amorn Vision (Bangkok) Co., Ltd., which operates training programs, recreational activities, and academic seminars across all fields, including modern communication technology, law, finance and accounting, taxation, and fire-safety training. The Company also provides creative digital media production and publication services, consultancy services, and the production of digital content and online programs, such as content relating to automotive diversity. In addition, the Company acts as a media agency specializing in media planning and media buying management, media strategy development, market analysis, and coordination to ensure that clients' content effectively reaches their target audiences.

"Anonymization" means a process that renders the risk of identifying a data subject so minimal that such risk can be considered negligible.

"Pseudonymization" means the processing of personal data in a manner that the data cannot be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data cannot be attributed to an identifiable natural person.

“Processing” means any operation or set of operations performed on personal data or a set of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, alteration or modification, retrieval, consultation, use, disclosure by transmission or dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

“Sensitive Personal Data” means personal data of an inherently private nature that is highly sensitive and poses a risk of unfair discrimination if misused. Such data requires special care and protection. This includes racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or any other information of a similar nature as may be prescribed by the Personal Data Protection Committee.

“Personal Data” means any information relating to an individual that enables the identification of that person, whether directly or indirectly. Examples include: title, first name, last name, nickname, address, telephone number, national identification number, passport number, social security number, driver’s license number, taxpayer identification number, bank account number, credit card number, email address, vehicle registration, land title deed, IP address, Cookie ID, voice data, and other similar information.
However, the following are not considered personal data: information of deceased persons; information of legal entities; business contact information that does not identify an individual (e.g., company name, company address, corporate registration number, office telephone number, work email address, or corporate group email); anonymous data; or pseudonymous data that can no longer identify a person by technical means.

“Personal Data Breach” means a breach of security measures leading to the loss, damage, alteration, unauthorized disclosure, or unauthorized access to personal data.

“Pseudonymous Data” means data that has undergone pseudonymization.

“Anonymous Data” means personal data that has been processed to the extent that the data subject cannot be identified. Such data is no longer considered personal data. However, the anonymization process itself constitutes a form of data processing and must therefore have a lawful basis and use methods or measures that ensure the data cannot be re-identified.

“Data Subject” means a natural person to whom the data relates. It does not refer to ownership of the data or the person who created or collected the data. The term also includes legal guardians acting on behalf of persons who lack legal capacity or quasi-incompetent persons. This definition does not include legal entities established under law, such as companies, associations, foundations, or other organizations.

“Data Controller” means a natural or juristic person, governmental agency, authority, or organization that determines the purposes and means of the processing of personal data.

“Data Processor” means a natural or juristic person, governmental agency, authority, or organization that processes personal data on behalf of the Data Controller.

“Data Protection Officer (DPO)” means a person or committee appointed by the Company to perform duties in accordance with the Personal Data Protection Act B.E. 2562 (2019).

“Personal Data Protection Law” means the Personal Data Protection Act B.E. 2562 (2019), including all related laws, regulations, and subordinate legislation.

2. PURPOSES OF PROCESSING PERSONAL DATA

2.1 General Business Purposes

(1) To take steps at your request prior to entering into a contract or to perform contractual obligations, including serving as supporting evidence for verification, identity confirmation, assessment, and approval of service requests, contract execution, transactions, contract renewals, and service applications with the Company, as well as conducting satisfaction assessments for service improvement purposes.

(2) To provide services, including processing purchase orders, receiving payments, and performing other transactions on the Company's website or application; coordinating, communicating, public relations activities, or providing necessary service-related information under the contract or upon your request.

(3) To establish, comply with, exercise, or defend legal claims, or to fulfill legal obligations, including law enforcement compliance.

(4) To report or disclose information to governmental authorities as required by law, such as the Bank of Thailand or the Revenue Department, or upon receipt of summonses, seizure orders, or other lawful requests from the police, government agencies, or the courts.

(5) To carry out the Company's internal processes, including receiving or sending documents between you and the Company, disclosing information to agents, contractors, subcontractors, and service providers for operational purposes, as well as risk management, auditing, corporate governance, and internal administration, including fulfilling contractual obligations between you and the Company.

2.2 Marketing Purposes

The Company may use analytical data, which may be combined with non-identifiable behavioral data obtained from third parties, to design and enhance the Company's overall marketing activities. This includes, but is not limited to, the following marketing purposes:

(1) To collect and analyze your service usage in order to improve the quality of services, deliver advertising and promotional materials, and present services that may be of interest to you, including providing recommendations regarding the Company's services. You may choose to opt out of certain types of marketing communications by following the instructions provided.

(2) To organize promotional, marketing, or service-awareness activities, as well as other similar events.

(3) To send coupons, rewards, complimentary gifts, special discounts, and other relevant information regarding training courses, promotions, or Company activities.

(4) To communicate marketing-related information concerning the Company's services, including those of the Company's partners, and to use data for lawful commercial purposes.

(5) For public relations purposes, including the publication and dissemination of photographs and video recordings taken during your participation in Company-organized activities through all channels, such as website broadcasts or communications via various media platforms.

2.3 Statistical Purposes

(1) The Company periodically collects data for analytical purposes, including research, strategic analysis for development, improvement of website or application functionalities, and enhancement of the Company's services.

(2) To support planning, reporting, statistical compilation, business forecasting and estimation, and customer relationship management. This may include activities such as customer satisfaction assessments for the purpose of improving the Company's services.

3. PERSONAL DATA COLLECTED

3.1 Personal Data refers to any information that identifies, or can be used to identify, a Data Subject directly or indirectly. The ability to identify a Data Subject typically falls into at least three categories:

(1) **Distinguishability:** Information that can distinguish one individual from another.

(2) **Traceability:** Information that can be used to track an individual's behavior or activities.

(3) **Link ability:** Information that can be linked together to identify an individual. This category includes two scenarios:

1) **Linked Data:** Information that, when combined with related data already available, can directly identify an individual.

2) **Linkable Data:** Information that, when used together with other data not yet present in the system, or data available on the internet or elsewhere, could enable the identification of an individual.

3.2 Such information may take any form, whether or not it is intelligible to you, provided that it is data that can be automatically accessed by computers or devices, or is arranged in a structured manner to allow access for the purposes of:

(1) collection for processing by such computers or devices, or for inclusion in an information system for such processing; and

(2) processing by such computers or devices in accordance with prescribed instructions or programmed commands.

3.3 Personal Data therefore refers to any information that can be used to identify the data subject, including:

(1) information that may exist in paper format or any other form but is intended to be processed subsequently;

(2) information which, on its own, may not identify an individual but, when combined with other data or information, can identify a specific person, regardless of whether such other data or information is held together; and

(3) information irrespective of whether it is accurate or inaccurate.

3.4 Personal Data Collected by the Company

(1) **Identity Information:** Information that identifies the Data Subject, including government-issued documents or unique identifiers, such as title, first name, last name, national ID number, professional license number (for each profession), license number, social security number, passport number, ID card, passport, house registration, immigration

entry/exit records, work permit, driver's license, vehicle registration book, other licenses, and any other information capable of identifying an individual. This also includes marital status, military service status, language, behavioral information, bankruptcy status, minor status, and legal incapacity status.

(2) **Contact Information:** Examples include current address, address as per house registration, postal address, email address, telephone number, fax number, and other contact information provided when registering on the Company's website or application, or when participating in events, exhibitions, or seminars. This also includes Line ID, MS Teams ID, Facebook ID, Instagram ID, and other social media identifiers, as well as similar information.

(3) **Account Information:** Examples include username, password, and security questions and answers for authentication purposes.

(4) **Financial Information:** Such as bank account numbers, credit/debit card numbers, payment history, income and sources of income, payment methods, PromptPay information, receipts (e.g., amounts), payment details (to and from the Data Subject), payment dates and/or times, payment cards, deposit slips/payment slips, amounts paid, refund details, check information, credit records, financial instruments, deposit details, taxes, balances, outstanding debts, financial statements, company certificates, shareholder lists, and other payment or financial information when you agree to use the Company's services.

(5) **Employment Information:** Such as job position, company/organization name, work history, income from employment, and performance evaluation data.

(6) **Education Information:** Such as educational history, degrees/certificates, institution names, and grades or scores.

(7) **Health Information:** Such as medical history, information regarding illnesses or health conditions, and information about treatments or medications.

(8) **Biometric Information:** Such as fingerprints, facial photographs, voice data, signatures, height, weight, and photographs.

(9) **Usage Information:** Such as login information, website/application usage history, tracking/location data, information received from promotional media, service usage history, and social media handles.

(10) **Preferences and Interests:** Such as personal likes, preferences, interests, subscription/marketing settings, participation in promotional activities, and any special privileges. This may include information you provide to the Company or its partners during marketing activities, and is not limited to the examples above.

(11) **Survey or Feedback Information:** Such as responses to questionnaires, opinions or suggestions submitted via the website or application, survey data, satisfaction assessments, or other similar items.

(12) **Subscription or Membership Information:** Such as membership registration information, participation in groups/activities, completion of various application forms, participation in events or campaigns, service types, and history of service subscriptions.

(13) **Transaction Information:** Such as details of purchases or sales, order numbers, transaction history, service dates and locations, delivery addresses/dates and times, service request forms, acknowledgment receipts, recipient signatures, invoices,

transaction status and location, purchase behavior, product and service details, complaints and claims, desired purchase timing, and outstanding balances.

(14) **Communication Information:** Such as personal data you provide when communicating with the Company via messages, records of communications, emails sent/received, or inquiries.

(15) **Multimedia Information:** Such as audio, still images, or videos, including data from CCTV and recordings of participation in events or campaigns organized by the Company.

(16) **Automatically Collected Information through System Tracking:** The Company may use automated technologies to collect personal data when you access the website or application via computers or mobile devices. These technologies may include cookies, pixels, tags, and other similar tracking technologies, as follows:

1) Personal data provided via the Company's website or application, including name, address, telephone number, and social media handles.

2) Personal data collected during marketing activities on other websites, applications, or social media platforms when participating in promotions, campaigns, or similar activities, for record-keeping purposes.

3) Personal data automatically collected via system tracking, such as IP address, browser type, operating system, visited web pages, and referring websites.

4) Data related to precise location, including real-time geographic coordinates from mobile devices or computers, and location-based services using GPS, Bluetooth signals, IP addresses combined with public Wi-Fi hotspots, cell towers, or other technologies to estimate the device's location (where feasible).

(17) **Personal Data of Third Parties Provided by You:** Such as name prefix, first name, last name, address, telephone number, relationship with you, occupation, executive positions, authorized representatives of a legal entity, proxies of a legal entity, directors, shareholders, employees, co-owners, or other personal data of any individual that you have assured the Company you obtained consent from the individual to disclose to the Company. This includes consent for the Company to process such personal data for the purposes notified to you by the Company.

(18) **Social Relationship Information:** Information regarding the social relationships of the Data Subject, such as political status, political positions, board memberships, relationships with Company personnel, contractual relationships with the Company, or interests in businesses dealing with the Company.

(19) **Other Information:** Information collected, used, or disclosed by the Company related to the relationship between the Company and the Data Subject, such as contract details (contract number, contract type, data retention period), application forms, or survey forms.

4. SOURCES OF PERSONAL DATA (DATA PROLIFERATION)

The Company may receive your personal data from various parties involved in processes related to personal data protection, consisting of four types of individuals/entities: Data Subjects, Data Controllers, Data Processors, and Third Parties. The relationships among these parties can be divided into the following three channels:

4.1 **Personal Data Directly from You:** The Company collects personal data directly from you, via affiliated companies, or from interactions with the Company through services, communications, visits, searches, whether via digital channels, websites, authorized personnel, or other means. Personal data may be collected in the course of providing services as follows:

(1) The Data Subject provides personal data to the Data Controller, e.g., during service registration, membership sign-up, package subscriptions, contract signing, form submissions, submission of supporting documents for transactions, claims, or exercise of rights. This also includes voluntary participation in surveys, email/phone/other communications with the Company, feedback, website activity via cookies, identity verification, participation in training, events, campaigns, or other similar activities.

(2) The Data Subject provides personal data to the Data Processor, as part of operations on behalf of the Data Controller.

(3) The Data Controller provides personal data to the Data Subject, e.g., in response to the Data Subject's request.

(4) The Data Processor provides personal data to the Data Subject, e.g., as instructed by the Data Controller.

4.2 **Personal Data from Third Parties:** The Company may receive personal data from third parties as follows:

(1) The Data Controller provides personal data to the Data Processor, e.g., under outsourcing agreements.

(2) The Data Processor provides personal data to the Data Controller, e.g., upon completion of assigned work.

(3) The Data Controller provides personal data to Third Parties, e.g., under business agreements.

(4) The Data Processor provides personal data to Third Parties, e.g., as instructed by the Data Controller.

(5) Personal data received by the Company from third parties, business partners, customers, Data Controllers, Data Processors, or any other party that the Company reasonably believes has the lawful right to process and disclose the Data Subject's personal data to the Company.

4.3 **Personal Data from Other Sources:** Personal data obtained or accessed from sources other than directly from you, e.g., organizations using the Company's services, government agencies, financial service providers, data providers, or other entities authorized or obligated to disclose such information. The Company will collect data from such sources only when obtaining your consent as required by law, except when legally permitted without consent.

4.4 **Personal Data Provided by Data Subjects Regarding Third Parties:** This also includes cases where the Data Subject provides personal data of third parties to the Company. In such cases, the Data Subject is responsible for informing the third party of the details in accordance with this Policy or any applicable service announcement, and for obtaining the third party's consent if required for disclosing their personal data to the Company.

5. LEGAL BASES FOR PERSONAL DATA PROCESSING

The Company may process your personal data based on the following legal bases:

5.1 **Contractual Basis (Contract):** The Company processes your personal data to provide services or perform obligations under a contract, or when it is necessary to collect your personal data to execute the contract, respond to inquiries, verify your identity in relation to services between you and the Company, or between you and the Company's partners. Failure to provide personal data may prevent the contract or related legal actions from being fully effective under the law.

5.2 **Consent Basis (Consent):** You give consent to the Company to collect, use, manage, store, and disclose your personal data as outlined in this Policy, the Privacy Notice, and relevant terms and conditions of each service. The Company may use your personal data to present products, services, or advertisements tailored to your interests, provide offers, privileges, recommendations, and news. Such data may be obtained through your consent to the Company, its partners, representatives, brokers, distributors, or business affiliates.

5.3 **Vital Interest Basis (Vital Interest):** The Company may process your personal data to protect or prevent harm to life or physical safety in situations where you cannot provide consent, such as health monitoring during pandemics, initial medical care, or emergency situations requiring hospital transfer.

5.4 **Legal Obligation Basis (Legal Obligation):** The Company may process and disclose your personal data to comply with legal obligations, including securities and exchange laws, tax laws, anti-money laundering laws, computer laws, bankruptcy laws, and other applicable laws in Thailand and abroad. Data may be disclosed to competent authorities such as the Revenue Department, Consumer Protection Board, Police, Public Prosecutor, Courts, or other relevant authorities.

5.5 **Legitimate Interest Basis (Legitimate Interest):** The Company may process your personal data for purposes aligned with its legitimate interests, such as research, statistical analysis, service improvement, marketing communications, necessary cookie usage, call center recordings, multimedia publicity, CCTV recording, access control, complaint handling, customer satisfaction evaluation, customer care alerts or service offerings, risk management, internal audits, intra-group sharing, anonymization of personal data, cyber threat mitigation, and other operational or promotional activities that do not infringe your rights.

5.6 **Archive/Research/Statistics Basis (Archive/Research/Statistics Repository):**

(1) **Archive Databases:** Storing historically or academically valuable data, often used for research and education.

(2) **Research Databases:** Collecting data for studies in medicine, social sciences, technology, or other fields, which may include personal data.

(3) **Statistical Databases:** Used for analysis and reporting, potentially containing personal data that requires protection.

6. PERSONAL DATA PROCESSING

6.1 **Material Scope of Processing:** Any processing of personal data must comply with the Personal Data Protection Act B.E. 2562 (PDPA) without exception. However, the following cases are exempt from requiring consent:

(1) Collection of personal data for the individual's own benefit or for purely personal or household activities.

(2) Operations of government agencies tasked with national security, including financial security, public safety, anti-money laundering, forensic work, or cybersecurity.

(3) Activities in journalism, artistic works, or literature conducted ethically or for public benefit.

(4) Activities in accordance with the duties and powers of the House of Representatives, the Senate, Parliament, or committees appointed thereby.

(5) Judicial proceedings, court operations, enforcement of judgments, asset attachment, and criminal justice processes.

(6) Processing of data by credit information companies and members under the Credit Information Business Act.

6.2 Territorial Scope of Processing: Processing of personal data must comply with the PDPA in the following circumstances:

(1) Operators with a company or branch established in Thailand, regardless of whether the processing occurs within Thailand.

(2) Operators without a company or branch in Thailand but:

1) Offer goods or services to data subjects in Thailand, whether payment is required or not; or

2) Track and collect data about the behavior of data subjects in Thailand, as long as such behavior occurs within Thailand.

6.3 Processing of Personal Data

Once personal data is obtained from any source, the Company will process your personal data under appropriate security measures to protect confidentiality and prevent loss, unauthorized access, destruction, use, modification, or disclosure. Processing may be conducted by the Company or authorized third parties under the following conditions:

(1) Collection of Personal Data

1) The Company collects personal data you provide in document or electronic form, stored in access-restricted locations, using lawful and fair methods. Collection is limited to what is necessary for providing services under the purposes specified by the Company. Prior to processing, the Company will notify you and obtain your electronic consent in a brief message or according to the Company's procedures.

   • If personal data is necessary for legal compliance or contract performance, the Company may not be able to provide services, in whole or in part, if such data is not provided.

2) The Company may collect personal data regarding your interests and used services. Consent will be obtained beforehand unless exempted as described above.

(2) Use of Personal Data

1) The Company will use and disclose personal data only for the purposes you have provided. If the Company intends to collect, use, or disclose data for additional purposes or change the purposes, it will notify you prior to processing, except where permitted or required by law.

2) The Company will use personal data appropriately, maintaining security, and controlling access, use, and disclosure. Employees or agents are prohibited from using or disclosing personal data beyond the stated purposes or to third parties, unless required or permitted by law.

3) The Company may use external IT service providers for personal data management. These providers must have security measures in place and may not collect, use, or disclose personal data beyond the Company's instructions.

(3) Disclosure of Personal Data

The Company may disclose personal data currently held or collected in the future to partners, business affiliates, or other individuals or entities as follows:

1) Shared with recipients to support Company operations under contractual conditions. Recipients must use the data only for the stated purpose and destroy or return data when no longer needed.

2) Disclosure may occur in the event of a business sale or acquisition; personal data may be considered an asset and transferred to the buyer.

3) Disclosure may occur in compliance with legal requirements, court orders, law enforcement, regulatory investigations, or other legally mandated situations. Only the necessary amount of data will be disclosed to protect national security, public interest, or enforce laws and agreements.

4) The Company may comply with international data disclosure standards through standard contractual clauses or other legally approved mechanisms for global personal data transfers.

5) The Company may disclose personal data to universities, business partners, customers, IT service providers, payment service providers, and third parties acting on behalf of the Company for payment processing, data analysis, marketing, surveys, or other purposes stated in this policy. These third parties are required to protect personal data in the same manner as the Company.

Third Parties with Access to Personal Data Include:

- Employees, contractors, and service providers processing data on behalf of the Company.
- Data controllers, processors, affiliated organizations, or third parties requested by the data subject to share data.
- Global partners, affiliates, and business partners using data for services requested by you.
- Service providers, supporting contractors, auditors, lawyers, and other consultants of the Company.
- Government agencies and authorities with legal access to personal data, including police, public prosecutors, courts, and other authorized state officials.

6.4 Sensitive Personal Data

When necessary, the Company may process personal data considered sensitive, including but not limited to: race, ethnicity, political opinions, religious or philosophical beliefs, sexual behavior, criminal history, health information, disabilities, trade union membership, genetic data, biometric data, or other data similarly affecting the data subject, as prescribed by the Personal Data Protection Committee. The Company will make every effort to implement adequate security measures to protect your sensitive personal data. Such data will be processed only for purposes permitted by law and for purposes notified by the Company, depending on specific activities or services, and only after obtaining your written consent prior to collection, or if you voluntarily disclose the data publicly, or where personal data laws permit.

Except for specific employee-related processing, the Company generally does not intend to process sensitive personal data such as race, blood type, or religion, even if such information appears on identification cards, household registration, or other documents you voluntarily submit to the Company.

If you submit any information containing sensitive data, whether in documents or other media, you are responsible for masking such data yourself. If you do not do so, the Company will assume you have explicitly authorized it to handle the masking on your behalf. The data, once appropriately masked by the Company, is considered complete, legally valid, and may be processed under the Personal Data Protection Act B.E. 2562.

In cases where the Company cannot technically or otherwise mask sensitive information, it will store such sensitive data solely as part of identity verification documentation.

6.5 Personal Data of Minors, Persons of Limited Capacity, or Incapacitated Persons

If the Company becomes aware that personal data requiring consent for collection belongs to a minor, a person of limited capacity, or an incapacitated person, the Company will not collect such personal data until consent is obtained from a legal guardian, parent, or custodian authorized to act on behalf of the data subject, as required by law.

(1) **Minor:** In commercial or other business activities, or as an employee under a labor contract, a minor who has legal capacity equivalent to an adult may have consent provided by their legal guardian. For minors aged 10 years or younger, consent must be obtained directly from the authorized legal guardian.

(2) **Person of Limited Capacity:** Refers to an individual whom the court has declared of limited capacity due to physical disability, mental incapacity, habitual wasteful conduct, substance abuse, or similar reasons that prevent them from managing their affairs responsibly. Consent must be obtained from their legal guardian, except where law allows consent to be given without prior guardian approval.

(3) **Incapacitated Person:** Refers to an individual whom the court has declared incapacitated due to mental illness. Consent must be obtained from their custodian authorized to act on their behalf.

If the Company discovers after collection that the data subject is a minor, a person of limited capacity, or an incapacitated person and consent from the appropriate guardian, parent, or custodian was not obtained, the Company will promptly delete or destroy such personal data unless there is another lawful reason for retaining it.

7. DATA SUBJECT RIGHTS

7.1 Your Rights under the Personal Data Protection Law:

You have the following rights as provided under applicable personal data protection law:

(1) **Right to Withdraw Consent:** You may withdraw your consent for the processing of your personal data at any time while your data is held by the Company.

(2) **Right of Access:** You have the right to access your personal data and request copies of such data, including information collected without your prior consent.

(3) **Right to Rectification:** You may request correction of inaccurate or incomplete personal data.

(4) **Right to Erasure:** You may request deletion of your personal data under certain circumstances.

(5) **Right to Restriction of Processing:** You may request suspension of processing of your personal data under certain circumstances.

(6) **Right to Data Portability:** You may request transfer of your personal data provided to the Company to another data controller or to yourself under certain circumstances.

(7) **Right to Object:** You may object to the processing of your personal data under certain circumstances.

Requests to exercise the above rights are free of charge. The Company will consider and respond to your request within 30 days from the date of receipt.

7.2 **Respect for Personal Choice:** The Company respects your rights and allows you to choose the methods by which the Company contacts you or processes your data. Non-consent to certain data processing may affect the Company's ability to perform contractual obligations or provide full services.

7.3 **Submission of Requests:** All requests to exercise your rights must be made in writing via the Company's electronic system at https://amvsbangkok.com/ following the Company's procedures. The Company will use reasonable efforts to respond within a reasonable time frame not exceeding statutory limits. The Company may refuse requests if legal exemptions apply, if compliance would hinder contractual obligations, affect the provision of benefits, or cause harm to others' rights or freedoms. The Company reserves the right to charge a reasonable fee for processing such requests.

7.4 **Limitations on Exercising Rights:** If the Company processes your personal data based on contractual necessity, legitimate interest, or legal obligation, it may refuse requests to object, restrict, or erase personal data where retention is necessary under legal exemptions or compliance requirements as described in Section 6.1.

8. MARKETING AND PROMOTIONAL ACTIVITIES

8.1 **Marketing Communications:** During the use of our services, the Company may send you information regarding marketing activities, promotions, products, and services that the Company believes may be of interest to you in order to provide services effectively.

8.2 **Disclosure to Third Parties:** The Company may disclose or transfer your personal data to third parties, domestically or internationally, only as necessary to fulfill the purposes and legal basis of processing described in this Policy. The Company may engage other advertising companies to display the Company's advertisements on websites. The use of third-party cookies and other tracking technologies is not governed by this Policy, and the Company has no access to or control over the actions of these third parties. Third parties may use cookies on your device to access stored cookies and track your online usage and behavioral patterns. They may use

information about your visits to the Company's websites to serve advertisements regarding products and services that may interest you and to personalize advertising content when you visit other websites.

8.3 **Consent to Contact:** By providing consent, you explicitly authorize the Company to contact you via automated telephone systems, computer-controlled systems, prerecorded messages, or other telecommunication technologies for legitimate purposes, including the promotion of third-party services.

8.4 **Opt-Out:** You may unsubscribe from receiving promotional emails, newsletters, or updates regarding the Company's services or marketing calls by contacting the Company through the channels specified in this Policy.

9. LINKING PERSONAL DATA WITH PARTNERS OR OTHER ENTITIES

9.1 **Consent for Data Linking:** If you provide personal data directly to the Company, the Company may link such personal data with partners or other entities. The Company will obtain your consent prior to linking the data, with at least the following information provided:

(1) The partners or entities involved in linking the personal data.
(2) The purpose of linking the personal data.
(3) The method of linking the personal data.
(4) The personal data to be linked.
(5) Individuals who have the right to access the personal data.

9.2 **Transparency and Record-Keeping:** When linking personal data with partners or other entities, the Company will clearly indicate the data collector and the data subject's rights. The Company will maintain records of the data linking as evidence. If there are any changes in the linked data, the Company will inform you and obtain your consent before proceeding.

10. COOKIES

Cookies are small pieces of information sent by a website to be stored on a visitor's device, helping the website remember user preferences such as language selection, login details, or other settings. When a visitor returns to the website, cookies allow the website to recognize the user and apply previous settings until the user deletes the cookies or disables them.

The Company uses cookies to store login/logout information and other data on your device when accessing the website. Cookies help improve website functionality, marketing, and content, and enable the Company to provide services tailored to your interests and preferences. Cookies allow the Company to analyze website activity, such as dates, times, visited pages, and referring websites, and to detect unauthorized actions.

For certain services, the Company may allow you to save usernames or passwords in cookies for convenience. The Company may also use Flash cookies to display content according to your browsing patterns and personalize your experience. When you register for newsletters, fill out online forms, or participate in surveys, the Company may attempt to identify your browser and combine cookie data with other information in the Company's possession.

Users may manage privacy settings by choosing to accept or reject cookies. If cookies are rejected or deleted, some services or website features may not function fully, potentially resulting in slower access or reduced convenience. You may also remove cookies through browser settings, but this may reduce the speed and usability of certain website functions.

11. PRIVACY POLICY OF OTHER WEBSITES

This privacy policy applies solely to the Company's services and the use of the Company's website. If you click on links to other websites (even through the Company's website), you must review and comply with the privacy policies of those websites separately from the Company's policy.

12. TRANSFER OR TRANSMISSION OF PERSONAL DATA ABROAD

12.1 Cross-Border Data Transfer: The Company may transfer your personal data to affiliated companies or other entities abroad when necessary for:

- Performing a contract to which you are a party, or fulfilling pre-contractual requests.
- Acting under a contract between the Company and another person or legal entity for your benefit.
- Preventing or mitigating harm to life, body, or health of you or others.
- Compliance with legal obligations.
- Performing important public interest duties.

12.2 Data Storage and Processing by Third Parties Abroad: The Company may store your personal data on servers or cloud services provided by third parties, and may use third-party software or applications to process your personal data. The Company will require such third parties to implement appropriate security measures and will not allow unrelated persons to access your personal data.

12.3 Legal Compliance and Safeguards: When transferring personal data abroad, the Company will comply with applicable data protection laws and implement appropriate safeguards to ensure that your personal data is protected and that you can exercise your rights regarding your personal data under the law. The Company will require recipients to apply adequate protective measures, process your personal data only as necessary, and prevent unauthorized access or disclosure.

13. RETENTION PERIOD OF PERSONAL DATA

13.1 Duration of Retention: The Company will retain personal data only as long as necessary for the purposes of processing as set out in this policy, as follows:

(1) Customer or Contractual Relationship: Personal data provided as a customer or contracting party will be retained as long as necessary to provide services under the contract, and for 10 (ten) years after the end of the contract or relationship. The Company may retain such data longer if required for specific purposes of each type of personal data, for processing needs, legal compliance, or as ordered by authorized officials or competent authorities.

(2) By Activity and Purpose: Personal data will be retained according to the type of activity and purpose of processing as indicated in the Privacy Notice.

(3) Membership: Personal data provided as a member will be retained as long as the individual remains a member of the Company.

(4) Application Data: Data on applications will be retained until the account is deleted.

(5) Consent-Based Data: Personal data processed based on your consent will be retained until you withdraw your consent and the Company has completed the related processing.

(6) Other Cases: The Company will retain personal data as long as reasonably necessary to fulfill the Company's obligations and achieve the purposes set in this policy. Where retention periods cannot be clearly determined, the Company will retain data according to

standard practices (e.g., general legal statute of limitations, typically up to 10 years). In the case of legal proceedings, personal data may be retained until the conclusion of such proceedings and for any additional period necessary to achieve the intended purposes. Data will then be deleted or retained as permitted by law.

13.2 Data Deletion and Anonymization: Upon expiry of the retention period, the Company will delete, destroy, anonymize, or otherwise process the personal data in accordance with applicable data protection laws to ensure effective protection of personal data. However, certain data may be retained longer if required by law, by order of authorized officials, or for lawful business purposes.

14. DATA SECURITY

The Company recognizes the importance of protecting the personal data of individuals. Accordingly, the Company has implemented appropriate measures to ensure the security and confidentiality of personal data to prevent loss, unauthorized access, destruction, use, alteration, or disclosure of personal data, as well as to prevent unauthorized use of personal data. Access to and use of personal data is restricted to authorized personnel only.

14.1 Security Measures: The Company employs appropriate technical, physical, and administrative security measures to prevent unauthorized access or disclosure of personal data. These measures align with the Company's business operations and generally recognized standards. Employees undergo training on personal data protection and data security. The Company also ensures that its service providers adopt adequate measures in processing, transferring, managing, and securing data on behalf of the Company. The Company regularly reviews and updates these measures as necessary to comply with applicable standards and regulations.

14.2 Policies and Procedures: The Company establishes clear policies and procedures to protect personal data, manage data securely, and prevent unauthorized access, including:

(1) Implementing clear policies and procedures to protect personal data and manage it safely in compliance with applicable law.

(2) Not selling or disclosing personal data to third parties outside of the Company's authorized data processors.

(3) Limiting customers' access to personal data.

(4) Preventing unauthorized access through encryption, authentication, and antivirus technologies as needed.

(5) Monitoring the compliance of business partners with applicable data protection laws and regulations, ensuring proper handling, transfer, and security of personal data.

(6) Regularly monitoring the Company's websites through agencies specializing in personal data protection and security.

(7) Providing training on personal data protection for employees, staff, and relevant teams.

(8) Regularly assessing the Company's practices regarding data protection, management, and security.

(9) Maintaining systems to delete or destroy personal data once the retention period expires or the data is no longer relevant or necessary.

(10) Continuously reviewing technical, physical, and administrative security measures to prevent unauthorized access or disclosure, and updating these measures as technology evolves to ensure effective data security.

15. USE OF PERSONAL DATA FOR ORIGINAL PURPOSE

The Company has the right to collect and use personal data that was collected prior to the enactment of the Personal Data Protection Act (PDPA) for its original purposes. If you do not wish the Company to continue collecting and using such personal data, you may withdraw your consent at any time through the channels designated by the Company.

16. CHANGES TO THE PERSONAL DATA PROTECTION POLICY

The Company will regularly review and update its privacy policy to ensure compliance with applicable practices, laws, and regulations. In the event of any changes to the privacy policy, the Company will notify you by promptly updating the information on its website. The privacy policy was last reviewed on 1 June 2022.

17. CONTACT CHANNELS

Data Controller Details:

Name:	**Amorn Vision(Bangkok) Company Limited**
Address:	Head Office: 42/7 Soi Chalermsuk, Ratchadaphisek Road, Chandrakasem Subdistrict, Chatuchak District, Bangkok 10900, Thailand
Contact Numbers:	Tel: (+66) 62-336-2655 Tel: (+66) 62-626-4256
Email:	amornvision.bangkok@gmail.com
Website:	https://amvsbangkok.com/

This Personal Data Protection Policy is effective from 28 May 2019.