



01 — SCOPE AND PURPOSE

This Data Privacy & Protection Policy sets out the principles and practices that guide Aura Solution Company Limited (“Aura”, “we”, “us” or “our”) in relation to the collection, use, processing, storage, disclosure, protection and retention of personal information. The Policy applies to personal information collected or processed by Aura in connection with our websites, digital platforms, professional services, communications, enquiries, business relationships, publications, events and other activities to which this Policy applies. It is intended to provide clients, business partners, visitors, colleagues and other stakeholders with a clear understanding of how Aura approaches personal information and the standards we seek to maintain when information is entrusted to us. The Policy describes, among other matters, the categories of information Aura may collect, the circumstances in which information may be obtained, the purposes for which it may be used, the circumstances in which it may be disclosed, the safeguards applied to it, the manner in which it may be retained and the rights that may be available to individuals under applicable law. Aura recognises that personal information can be private, sensitive and, in certain circumstances, commercially significant. Our approach is therefore founded upon the principles of purpose, proportionality, confidentiality, security and responsible stewardship.

This Policy applies to information processed by Aura in the course of our legitimate activities. The precise nature and extent of processing may vary depending upon the relationship involved, the services provided, the jurisdiction concerned and the applicable legal and regulatory framework. This Policy does not necessarily apply to websites, applications, platforms, products or services operated independently by third parties, even where those services may be accessible through links appearing on Aura’s websites or digital platforms.

Third-party services operate independently and may be governed by their own privacy policies, terms of use and information-management practices. Aura does not control the privacy practices of independent third parties and cannot assume responsibility for how they collect, use, retain or disclose personal information. Where you choose to access a third-party service, we encourage you to review its applicable privacy policy and terms before providing personal information.



Nothing in this Policy is intended to replace, restrict or remove any rights or protections that may be available to individuals under applicable law. Where specific legal, regulatory or contractual requirements apply to a particular relationship or activity, those requirements may take precedence over the general principles described in this Policy.

Our approach is guided by a simple principle: INFORMATION ENTRUSTED TO AURA SHOULD BE HANDLED WITH PURPOSE, DISCRETION AND RESPONSIBILITY.

02 — INFORMATION WE COLLECT

The information Aura collects depends on the nature of your interaction with us. Where appropriate, this may include your name, address, email address, telephone number, professional position, organisation, country of residence and other contact or identification information that you voluntarily provide. Where a business or professional relationship exists, we may also process information necessary to establish, maintain and administer that relationship. Depending on the circumstances, this may include contractual, financial, professional, transactional or correspondence information. When you interact with our digital platforms, certain technical information may also be collected automatically. This may include your IP address, browser type, device information, operating system, pages accessed, dates and times of visits, referring websites, session information and other information concerning your interaction with our platforms. We seek to ensure that the information collected is relevant and proportionate to the purpose for which it is obtained.

03 — HOW INFORMATION IS COLLECTED

Aura may receive information directly from you, from individuals or organisations acting on your behalf, or from other legitimate sources connected with our business activities.

Information may be provided when you contact Aura, submit an enquiry, request information, communicate with our representatives, enter into a business relationship,



participate in an event, subscribe to communications or otherwise interact with our services. We may also receive information from professional advisers, counterparties, service providers, business partners or other parties where such information may lawfully be shared with us. Certain technical information may be collected automatically through your interaction with our websites and digital platforms. Where personal information is received from a third party, Aura expects that the information has been collected and transferred in accordance with applicable requirements.

04 — HOW WE USE INFORMATION

Aura may process personal information where there is a legitimate business, contractual, operational, legal, regulatory or professional purpose for doing so. The information entrusted to us may be used to establish, develop and maintain professional and business relationships, understand the nature of those relationships and provide an appropriate level of service and communication.

Depending on the circumstances, this may include:

- establishing and maintaining professional, commercial and business relationships;
- responding to enquiries, requests, correspondence and other communications;
- providing services, information, materials or assistance requested by you;
- administering agreements, mandates, engagements and other commercial arrangements;
- maintaining appropriate records relating to our relationships and activities;
- managing communications and correspondence with clients, partners, advisers and other stakeholders;
- operating, maintaining, securing and improving Aura's websites, digital platforms and technology infrastructure;



- understanding how our digital platforms are used and identifying opportunities to improve their functionality, performance and user experience;
- maintaining information-security, cybersecurity and technology controls;
- managing operational, financial, commercial, compliance and business risks;
- preventing, identifying and investigating fraud, misuse, security incidents or other unlawful or inappropriate activity;
- complying with applicable legal, regulatory, accounting, professional and other obligations;
- responding to lawful requests or requirements from courts, regulators, governmental authorities or other competent bodies;
- protecting Aura's rights, property, systems, confidential information and legitimate business interests; and
- establishing, exercising, managing or defending legal claims and proceedings.

Where appropriate and permitted by applicable requirements, information may also be used to communicate with clients and other stakeholders concerning Aura's services, publications, research, insights, market perspectives, institutional activities and other relevant content. Such communications are intended to be relevant to the nature of the relationship and may be subject to applicable preferences, permissions and legal requirements. Aura seeks to ensure that personal information is not used indiscriminately. The manner in which information is processed should remain connected to the purpose for which it was collected, the nature of the relationship concerned and the legal basis upon which the processing takes place. Where circumstances change and a new purpose for processing arises, Aura may assess whether that purpose is compatible with the original purpose, whether additional information or notice is required and whether another legal basis is necessary. Our approach is guided by a straightforward principle: information should have a purpose, and that purpose should be legitimate, proportionate and understood.



05 — THE BASIS FOR PROCESSING

Aura seeks to process personal information on a lawful and appropriate basis. Depending on the circumstances, the nature of the relationship, the information involved and the jurisdiction concerned, Aura may rely upon one or more legal bases for processing personal information.

LEGITIMATE INTERESTS

Aura may process personal information where such processing is reasonably necessary for our legitimate business, operational, administrative, security, risk-management or organisational interests. This may include managing relationships, protecting our systems and information, improving our services, maintaining appropriate records, managing operational risks or conducting activities necessary for the responsible operation of Aura. Where legitimate interests are relied upon, Aura seeks to consider whether the relevant interests are balanced appropriately against the rights, freedoms and reasonable expectations of the individuals concerned.

CONTRACTUAL NECESSITY

Personal information may be processed where it is necessary to establish, perform, administer or manage a contractual or professional relationship. This may include information required to provide services, communicate with clients or counterparties, administer an agreement, fulfil agreed responsibilities or take steps requested before entering into a relationship. The information processed for these purposes will depend upon the nature and requirements of the relevant engagement.

CONSENT

In certain circumstances, Aura may request and rely upon your consent before processing personal information for a particular purpose. Where consent is the applicable basis, the request will be made in a manner intended to allow you to understand what you are consenting to. Where applicable, you may have the right to withdraw your consent.



Withdrawal of consent does not necessarily affect the lawfulness of processing undertaken before the withdrawal, and Aura may continue to process information where another lawful basis applies or where retention or processing is otherwise required or permitted by law.

LEGAL AND REGULATORY OBLIGATIONS

Aura may process personal information where such processing is necessary to comply with applicable laws, regulations, regulatory requirements, court orders, governmental requirements or legitimate requests from competent authorities. These obligations may arise from the jurisdictions in which Aura operates, the nature of a particular relationship, the services provided or the activities undertaken. Such processing may include maintaining records, responding to regulatory enquiries, fulfilling reporting obligations, supporting compliance procedures, preventing unlawful activity or meeting other mandatory requirements.

OTHER LAWFUL BASES

Depending on the jurisdiction concerned, applicable law may provide additional legal bases for processing personal information. Aura may rely upon such bases where appropriate and where the relevant requirements are satisfied. The applicable legal basis may therefore differ according to the nature of the information, the purpose of the processing, the relationship involved and the jurisdiction in which the processing takes place. Aura seeks to ensure that personal information is processed on an appropriate legal basis and that the purpose, scope and manner of processing remain proportionate to the circumstances.

06 — CONFIDENTIALITY AND RESPONSIBLE ACCESS

Confidentiality is central to Aura's approach to information and forms an important part of the trust placed in us by our clients, business partners, colleagues and other stakeholders.



Personal information entrusted to Aura is not intended to be made available indiscriminately. Access to information within Aura is intended to be limited to individuals who have a legitimate business, professional, operational, contractual, compliance or legal reason to access the information concerned. This principle applies throughout the information lifecycle, from collection and use through to storage, disclosure, retention and eventual disposal. Where information is sensitive, commercially confidential or otherwise subject to heightened expectations of discretion, Aura may apply additional access restrictions and safeguards appropriate to its nature and importance. Access permissions may be structured according to responsibilities, seniority, role, operational requirements and the specific information involved. Where appropriate, access may also be monitored or reviewed as part of Aura's information-security, risk-management and governance practices.

Employees, representatives, advisers and approved service providers may be subject to confidentiality obligations appropriate to the information they handle and the responsibilities they undertake. Aura seeks to ensure that information remains available to those who legitimately need it while maintaining appropriate barriers against unauthorised access, use, copying or disclosure. Confidentiality does not mean that information can never be shared. Where information must legitimately be disclosed for contractual, legal, regulatory, operational or other appropriate purposes, Aura seeks to ensure that disclosure remains proportionate and appropriately controlled.

Our objective is simple:

THE RIGHT INFORMATION SHOULD REACH THE RIGHT PERSON FOR THE RIGHT PURPOSE — AND NO FURTHER.

07 — DISCLOSURE TO THIRD PARTIES



Aura may disclose personal information where there is a legitimate purpose for doing so and where the disclosure is permitted, necessary or required under applicable law. Disclosure may occur as part of the ordinary operation of our business, the administration of professional relationships, the provision of services, the management of technology infrastructure or the fulfilment of legal and regulatory responsibilities. Depending upon the circumstances, recipients may include companies within the Aura organisation, professional advisers, auditors, insurers, consultants, legal advisers, technology providers, communications providers, administrative service providers, financial institutions, counterparties and other trusted providers supporting Aura's activities. Certain information may also be disclosed to courts, regulators, governmental authorities, tax authorities, law-enforcement bodies or other competent authorities where Aura is required or permitted to do so.

In some circumstances, Aura may engage third-party service providers to perform specific functions on our behalf. These providers may require access to certain information in order to perform their responsibilities. Where third parties process personal information on behalf of Aura, we seek to establish appropriate contractual, organisational and technical safeguards concerning the use, confidentiality, security, retention and protection of that information. Third-party access is intended to remain proportionate to the purpose for which the information is provided. Aura seeks not to provide third parties with unrestricted access to personal information where such access is unnecessary. Where appropriate, access may be limited to particular information, systems, periods or functions. In circumstances involving professional advisers, counterparties or other parties acting independently from Aura, information may be shared where necessary to support a legitimate business, contractual, professional or legal purpose.

Aura may also disclose information where necessary to protect our rights, property, systems, personnel, clients or other stakeholders, or to establish, exercise or defend legal claims.

Where disclosure is required by law or by a competent authority, Aura will seek to comply with the relevant requirement while maintaining appropriate confidentiality and information-security safeguards.



Aura does not seek to sell personal information indiscriminately or disclose personal information for purposes unrelated to legitimate business, professional, contractual, legal or regulatory activities.

The guiding principle is one of restraint: information should be shared only where there is a legitimate reason, with the appropriate party, and to the extent reasonably necessary for that purpose.

08 — INTERNATIONAL DATA TRANSFERS

Aura operates in an increasingly interconnected environment and may maintain relationships with clients, counterparties, professional advisers, technology providers, financial institutions and other service providers across multiple jurisdictions. As a result, personal information may, where appropriate and legally permitted, be transferred to, accessed from or processed in a jurisdiction other than the country in which the information was originally collected. Such transfers may be necessary to support the effective operation of Aura's business, provide requested services, administer professional and commercial relationships, maintain technology and information infrastructure, communicate with clients and stakeholders, engage specialist service providers, manage operational requirements or comply with applicable legal and regulatory obligations.

Aura recognises that different jurisdictions may apply different standards to the protection of personal information. Where information is transferred internationally, we therefore seek to apply safeguards appropriate to the nature and sensitivity of the information, the purpose of the transfer, the countries involved and the requirements of applicable data-protection law.

Where required, appropriate contractual, technical and organisational measures may be implemented to support the lawful transfer and continued protection of personal



information. These measures may include contractual protections, access restrictions, information-security controls, confidentiality obligations and other safeguards appropriate to the circumstances. Where a third party processes personal information on behalf of Aura in another jurisdiction, we seek to ensure that the relevant relationship is governed by appropriate arrangements concerning confidentiality, security, permitted use and the handling of personal information. International processing does not alter the fundamental principle that information entrusted to Aura should be handled with discretion, purpose and appropriate protection wherever it is processed.

09 — INFORMATION SECURITY

Aura regards information security as an essential component of responsible information management and an important part of maintaining the confidence placed in us. We maintain organisational, technical and administrative measures designed to protect personal information against unauthorised access, misuse, alteration, disclosure, loss, destruction or other forms of inappropriate handling. The measures applied may vary according to the nature, sensitivity and volume of information concerned and the risks associated with the relevant processing. Depending on the circumstances, safeguards may include access controls, authentication procedures, encryption, system monitoring, network and platform protections, secure information-handling procedures, internal policies, incident-response processes and restrictions governing access to sensitive information.

Access to personal information is intended to operate on a need-to-know basis wherever appropriate. Individuals within Aura, and approved third parties acting on our behalf, should only have access to information to the extent reasonably necessary for their responsibilities. Our employees, representatives, advisers and approved service providers may also be subject to confidentiality, security and data-protection obligations appropriate to the nature of their role. Aura recognises that information security is not a static discipline. Technology changes, threats evolve and new forms of digital interaction introduce new considerations. We therefore seek to periodically review our security arrangements and strengthen controls where appropriate in response to evolving



technology, operational experience, emerging threats and applicable regulatory expectations.

No method of electronic transmission, communication or storage can be guaranteed to be completely secure. Nevertheless, Aura remains committed to maintaining safeguards proportionate to the risks associated with the information entrusted to us.

10 — COMMUNICATIONS OVER OPEN NETWORKS

Communications transmitted through open or public networks, including the internet, may involve risks that are outside Aura's direct control. Information transmitted through such networks may potentially be intercepted, altered, delayed, lost, misdirected or otherwise compromised despite the safeguards applied by the parties involved. This is an inherent consideration when communicating through public digital infrastructure and should be taken into account when transmitting confidential or sensitive information. Users should therefore exercise appropriate care when deciding what information to communicate through open communication channels. Where information is particularly confidential, sensitive or commercially important, Aura may, where appropriate, provide or recommend alternative communication methods or additional security measures designed to provide a higher degree of protection.

Aura may also establish specific communication procedures for certain relationships, transactions or categories of information where the circumstances warrant additional controls.

While we seek to protect communications using appropriate technical and organisational measures, users should recognise that no open network can be regarded as entirely free from risk.

The protection of sensitive information is therefore a shared responsibility between Aura, its clients, business partners and other parties participating in the communication.



11 — DATA RETENTION

Aura retains personal information for as long as reasonably necessary to fulfil the purpose for which it was collected, maintain an ongoing relationship, perform contractual obligations, administer services, protect legitimate interests or satisfy applicable legal, regulatory, accounting, professional and operational requirements. The appropriate retention period will depend upon the nature of the information, the purpose for which it is processed, the relationship concerned and the circumstances in which the information was obtained. Certain information may be retained for longer periods where required or permitted by law, where necessary to establish, exercise or defend legal claims, where required for regulatory or audit purposes, or where a continuing legitimate business requirement exists.

Retention periods may also be influenced by the nature of a particular client or business relationship and the obligations that apply to the relevant activity. Aura seeks to avoid retaining personal information indefinitely where there is no legitimate reason to do so. Where information is no longer required, Aura seeks to securely delete, destroy, anonymise or otherwise dispose of it in accordance with applicable legal and regulatory requirements and our internal information-management practices. Where immediate deletion is not technically or operationally possible, information may be securely isolated or otherwise protected until appropriate disposal can take place. Our approach to retention is therefore guided by a simple principle: information should be retained for a legitimate reason, protected for as long as it is retained and responsibly disposed of when it is no longer required.

12 — COOKIES AND SIMILAR TECHNOLOGIES

Aura's websites and digital platforms may use cookies and similar technologies to support functionality, security, performance, usability and the overall digital experience. Cookies are small data files or similar technologies that may be placed on or associated with your device when you visit a website. Depending on their purpose, they may allow a website to recognise a returning visitor, remember selected preferences,



maintain certain functionality or provide information about how the website is being used. Aura may use different categories of cookies and similar technologies according to the purpose for which they are required.

ESSENTIAL COOKIES

Essential cookies support the basic operation, security and technical functionality of our websites. They may be necessary to enable certain features, maintain secure sessions, manage technical functions or support the reliable delivery of requested services. Because these technologies may be necessary for the operation of the website, they may not always be capable of being disabled through ordinary cookie-preference controls.

ANALYTICS COOKIES

Analytics cookies and similar technologies may be used to help Aura understand how visitors interact with our websites. This may include information concerning pages visited, approximate usage patterns, navigation behaviour, technical performance and other aggregated or statistical information. The purpose is to help Aura understand how our digital platforms perform and identify opportunities to improve their structure, functionality, content and usability.

PREFERENCE COOKIES

Preference cookies may be used to remember settings or choices made during a visit to our websites. Where applicable, these technologies may improve continuity and convenience by reducing the need to repeatedly enter or select the same preferences.

MARKETING AND MEASUREMENT TECHNOLOGIES



Where applicable and permitted, Aura may use certain technologies to understand engagement with communications, publications, digital content or other institutional activities.

Such technologies may assist with measuring the effectiveness and relevance of communications and improving how Aura presents information to its audiences. The use of such technologies will remain subject to applicable requirements and any controls or preferences made available to users.

MANAGING COOKIES

Depending on the technology involved, you may be able to manage certain cookie preferences through your browser settings or through controls made available on Aura's website.

You may choose to restrict, block or delete certain cookies. However, doing so may affect the availability, functionality or performance of particular features. Third-party services operating through Aura's digital platforms may also use their own cookies or similar technologies and may be subject to separate privacy policies.

13 — THIRD-PARTY SERVICES AND LINKS

Aura's websites and digital platforms may contain links to websites, applications, social-media platforms, technology services or other digital environments operated by third parties.

These links may be provided for convenience, information, reference or broader access to resources that may be relevant to our clients, visitors and stakeholders. A link to a third-party website does not necessarily constitute an endorsement, recommendation or representation by Aura concerning the organisation, service, content or practices of that third party.

Third-party platforms are generally outside Aura's direct control and are not automatically subject to this Data Privacy & Protection Policy. Accordingly, Aura cannot assume



responsibility for the privacy practices, security arrangements, data-processing activities, content, availability or policies of independent third-party services.

Where you choose to access a third-party website, application or platform, the information you provide may be collected and processed in accordance with that third party's own privacy policy, terms of use and applicable practices. We therefore recommend reviewing the relevant privacy and security information of any third-party service before providing personal information or engaging with the service.

Where Aura integrates a third-party technology or service into one of our digital platforms, we seek to assess the role and purpose of that service and, where appropriate, apply suitable contractual, technical and organisational safeguards.

14 — YOUR DATA PROTECTION RIGHTS

Aura recognises that individuals may have important rights concerning the personal information held about them. Subject to the laws applicable to you, the jurisdiction concerned and the circumstances in which your information is processed, you may have one or more of the following rights.

ACCESS

You may have the right to request information concerning the personal information Aura holds or processes about you and, where applicable, to obtain a copy of that information.

CORRECTION

You may have the right to request that inaccurate, incomplete or outdated personal information be corrected or updated. Aura may also take reasonable steps to verify the



accuracy of information where circumstances indicate that a record may require amendment.

DELETION

In certain circumstances, you may have the right to request the deletion of personal information. This right is not absolute. Aura may be entitled or required to retain certain information to comply with legal, regulatory, contractual, accounting or other legitimate obligations.

RESTRICTION OF PROCESSING

You may, in certain circumstances, have the right to request that Aura restrict or limit the processing of your personal information. Such a right may apply where the accuracy, lawfulness or necessity of processing is being challenged or where applicable law otherwise provides for such restriction.

OBJECTION

Depending upon the applicable legal framework and circumstances, you may have the right to object to particular forms of processing of your personal information. Where such an objection is made, Aura will consider the request in accordance with the applicable legal requirements and the legitimate grounds supporting the relevant processing.

DATA PORTABILITY

Where a right to data portability applies, you may have the right to request certain personal information in a structured, commonly used and machine-readable format. Where applicable, this may also include requesting that such information be transmitted to another organisation, subject to the requirements and limitations established by applicable law.



WITHDRAWAL OF CONSENT

Where Aura processes personal information on the basis of your consent, you may have the right to withdraw that consent. Withdrawal of consent does not necessarily affect the lawfulness of processing carried out before the withdrawal. In addition, Aura may continue to process certain information where another lawful basis applies or where retention or processing is required or permitted under applicable law.

OTHER RIGHTS

Depending on your jurisdiction, you may have additional rights relating to personal information, including rights concerning automated decision-making, profiling, international transfers or complaints to a competent data-protection authority. The availability, scope and conditions of these rights may differ between jurisdictions. Aura may need to verify your identity before responding to a request. This is an important safeguard intended to ensure that personal information is not disclosed to an unauthorised individual. Where permitted by law, Aura may also apply reasonable procedures to authenticate requests and protect the confidentiality of information held within our systems. If you wish to exercise a data-protection right or have a question concerning the manner in which Aura handles your personal information, please contact us through the official channels provided in this Policy.

Aura will consider requests carefully and seek to respond within the timeframe required by applicable law.

Our approach is guided by a simple principle: your information remains yours, and our responsibility is to handle it with the care, discretion and purpose that such trust requires.



Aura recognises that the quality of any relationship depends, in part, upon the accuracy and integrity of the information used to support it. We therefore seek to maintain personal information that is accurate, relevant, complete and appropriate to the purpose for which it is processed. Information may be provided directly by you or obtained through authorised representatives, professional advisers, counterparties, service providers or other legitimate sources. In each case, Aura seeks to exercise appropriate judgement regarding the reliability and relevance of the information received. Personal information may change over time. Addresses may change, professional circumstances may evolve, contact details may become outdated and other information may require correction. If you become aware that information held by Aura is inaccurate, incomplete, outdated or otherwise requires amendment, we encourage you to contact us so that the matter can be reviewed and, where appropriate, corrected. Aura may also periodically review information as part of ordinary relationship management, operational administration, compliance procedures, risk management and information-governance activities.

Where appropriate, we may seek additional information or clarification to ensure that records remain sufficiently accurate for the purpose for which they are maintained.

Our objective is not to maintain information for its own sake, but to ensure that information entrusted to Aura remains reliable, proportionate and fit for purpose throughout the relationship.

16 — CHILDREN AND MINORS

Aura's activities are principally directed towards adults, professional clients, families, businesses, investors, institutions and other stakeholders capable of engaging with our services and activities in their own capacity. Accordingly, Aura does not knowingly seek to collect personal information from children or minors where such collection is not necessary, appropriate or legally permitted in connection with the relevant activity. Where information concerning a minor may legitimately form part of a broader relationship, Aura seeks to handle that information with an appropriate degree of care and in accordance with applicable legal and regulatory requirements. If you believe that personal information



relating to a child or minor has been provided to Aura in circumstances where it should not have been collected, please contact us through our official channels.

Upon receiving such a concern, Aura may review the circumstances in which the information was obtained and determine whether the information should be removed, restricted, corrected or otherwise handled in accordance with applicable requirements. Our approach is guided by a simple principle: information relating to children deserves particular care, and should only be collected or retained where there is a legitimate and appropriate reason for doing so.

17 — SECURITY INCIDENTS AND DATA BREACHES

Aura recognises that responsible privacy management extends beyond the ordinary handling of information. It also requires preparedness for circumstances in which information security may be compromised. Aura maintains organisational, technical and procedural measures intended to identify, assess, contain, investigate and respond to information-security incidents that may affect personal information. An incident may include unauthorised access, accidental disclosure, loss, alteration, destruction, misuse or other compromise of information. Where an incident occurs, Aura will seek to assess the nature, scope and potential consequences of the event and determine the appropriate response.

Our response may include securing affected systems, restricting access, preserving relevant information, investigating the circumstances, assessing potential risks and implementing measures intended to prevent further compromise.

Where personal information is affected, Aura will seek to take appropriate steps to protect that information and reduce potential harm to the individuals concerned. Where applicable law or regulation requires notification, Aura will notify the relevant competent authority and, where required, affected individuals within the applicable timeframe and in accordance with the requirements that apply. Following a material incident, Aura may



conduct a review of the circumstances, controls and procedures involved. Where appropriate, additional safeguards, processes or technical measures may be introduced.

Security is not considered a static objective. Aura seeks to continually review its information-protection practices as technology, threats, business activities and regulatory expectations evolve.

18 — CORPORATE TRANSACTIONS AND REORGANISATION

Aura's business may evolve over time. This may include corporate reorganisations, internal restructurings, acquisitions, disposals, mergers, financing arrangements, strategic partnerships, transfers of business activities or other transactions affecting the organisation or its assets. In connection with such circumstances, personal information may, where permitted by applicable law, be transferred to or made available to a successor entity, acquiring entity, professional adviser, financing institution, service provider or other party involved in the relevant transaction. Any such transfer would be considered in the context of the nature of the transaction, the information concerned and the legal and regulatory requirements applicable to the circumstances. Aura seeks to ensure that information remains subject to appropriate confidentiality and data-protection safeguards throughout such processes. Where personal information is transferred as part of a corporate transaction, Aura will seek to ensure that the information continues to be handled for legitimate purposes and in accordance with applicable requirements.

A change in ownership, structure or business organisation does not, in itself, diminish the importance Aura places on the responsible stewardship of personal information. The continuity of appropriate privacy and confidentiality standards remains an important consideration in any significant corporate development.

19 — GOVERNANCE, ACCOUNTABILITY AND COMPLIANCE



Aura considers privacy and information governance to be matters of institutional responsibility. Our approach is supported by policies, internal controls, procedures, responsibilities and operational practices intended to promote the lawful, appropriate and responsible handling of personal information throughout its lifecycle. These principles extend from the initial collection of information through its use, access, disclosure, storage, retention and eventual deletion or disposal. Aura seeks to maintain practices that reflect the legal, regulatory and professional requirements applicable to its activities and the jurisdictions in which relevant processing takes place. Where a particular jurisdiction imposes requirements that differ from or extend beyond the general principles described in this Policy, those requirements may apply to the relevant processing. The applicable framework may depend upon the nature of the information, the relationship involved, the services provided and the jurisdiction concerned. Aura also recognises that effective governance requires appropriate accountability. Access to information, decision-making responsibilities and information-management practices should be capable of being understood, reviewed and, where appropriate, challenged. Nothing in this Policy is intended to restrict, exclude or remove any rights, remedies or protections available to individuals under applicable law.

20 — CONTACT AURA

Aura welcomes questions concerning this Data Privacy & Protection Policy and requests relating to the handling of personal information. If you believe that your information has been processed incorrectly, if you wish to understand how your information is used, or if you wish to exercise a right available to you under applicable data-protection law, you may contact Aura through our official channels. When contacting us, we encourage you to provide sufficient information to enable us to understand the nature of your request and identify the relevant relationship, communication or information concerned.

Where appropriate, Aura may request reasonable additional information to verify your identity before responding. This is intended to protect personal information and prevent unauthorised persons from obtaining access to information concerning another individual. Aura will consider privacy-related requests carefully and seek to respond within the timeframe and manner required by applicable law.



Where a request cannot be fulfilled in whole or in part, Aura may explain the applicable reason or limitation, subject to any legal restrictions on the information that may be provided.

AURA SOLUTION COMPANY LIMITED

Email: info@aura.co.th

Website: www.aura.co.th

For formal privacy requests, please use the official Aura contact channels published on our website.

21. WIKIPEDIA AND THIRD-PARTY REPRESENTATION

Aura Solution Company Limited has deliberately chosen not to establish or maintain a Wikipedia page. This is a conscious institutional decision and reflects Aura's approach to the protection, accuracy, and integrity of its corporate information. As an international asset management company, Aura considers its corporate identity and institutional information to be matters of importance. Information concerning an asset management organization can influence how clients, counterparties, institutions, investors, regulators, and other stakeholders understand the organization. For this reason, Aura does not believe that its official corporate information should be placed on a platform where third parties can independently alter, reinterpret, remove, or add information without Aura having direct control over the final published record. Wikipedia operates through an open, community-edited model. Articles may be created and modified by independent contributors, and information can change over time as a result of editorial decisions, disputes between contributors, interpretation of sources, or changes in the available references. Although this model can be useful for general public knowledge, Aura does not consider it an appropriate authoritative platform for maintaining its institutional record.

Aura's concern is not simply whether an individual statement is correct at a particular



moment. It is also who has the ability to alter that information, how those alterations are evaluated, and whether the company can ensure that its corporate history and activities continue to be represented accurately and with appropriate context. These considerations have become increasingly relevant as public criticism of Wikipedia's editorial and governance structure has grown. On 8 August 2026, RT reported comments by Wikipedia co-founder Larry Sanger, who criticized the platform's governance, alleged that ideological viewpoints can influence its content, and raised concerns about the anonymity of contributors and the potential effect of Wikipedia's content on AI systems that use it as a reference. RT also reported Sanger's statements concerning historical edits attributed to government organizations. These are reported allegations and criticisms, rather than claims that Aura independently verifies, but they illustrate the broader concerns surrounding third-party editorial control. For Aura, this is particularly significant because the company does not want an external party to have the ability to modify its institutional information and thereby potentially create an inaccurate, incomplete, outdated, or misleading representation of the organization. Aura therefore maintains its authoritative corporate information through channels under its institutional control, including its official websites, corporate publications, official documentation, and applicable public or governmental records. Independent sources may also provide information about Aura, but such sources remain separate from Aura's own authoritative corporate record.

This policy does not represent a rejection of public knowledge or independent journalism. Aura recognizes the value of independent sources and welcomes factual reporting based on reliable evidence. The distinction is that independent reporting and an editable institutional profile are not the same thing.

Aura's position is straightforward:

- The identity and institutional record of an asset management company should be based on verifiable facts and authoritative sources—not on an externally controlled, continuously editable profile.
- Accordingly, Aura's absence from Wikipedia is intentional.
- It is not an omission, nor does it indicate a lack of information or recognition.



Aura simply chooses not to place its institutional identity under third-party editorial control.

EVIDENCE

22 — CHANGES TO THIS POLICY

Aura operates in an environment in which technology, business practices, regulatory expectations and legal requirements continue to develop. Accordingly, Aura may review and update this Data Privacy & Protection Policy from time to time to reflect changes in our services, digital platforms, information practices, internal standards, legal obligations or regulatory requirements.

Where material changes are made, the updated version may be published on the Aura website together with an updated effective or revision date.

The version published on the Aura website represents the current version of this Policy and supersedes previous versions, unless otherwise stated.

We encourage clients, visitors, business partners and other stakeholders to review this page periodically to remain informed about Aura's approach to privacy and the responsible management of personal information. Your continued interaction with Aura following an update does not, by itself, establish consent where consent is required under applicable law. The applicable legal basis for processing will continue to depend upon the circumstances concerned.

LAST UPDATED: AUGUST 2026

OUR PRINCIPLE



INFORMATION ENTRUSTED TO AURA IS A RESPONSIBILITY.

Privacy is not simply a matter of technology, administration or regulatory compliance. At Aura, we regard it as a matter of trust.

Every piece of personal information entrusted to us represents a degree of confidence placed in Aura — whether by an individual, a family, an entrepreneur, a business, an institution or a professional relationship.

That confidence carries a responsibility.

We therefore seek to approach information with the same discretion and discipline that define our broader relationships. We collect information with purpose, use it with restraint, protect it with appropriate safeguards and retain it only where there is a legitimate reason to do so. We believe that responsible information management should be measured not only by the systems used to protect data, but also by the judgement applied when deciding what information is necessary, who should have access to it, how it should be used and when it should no longer be retained.

Our commitment is enduring: to treat information entrusted to Aura with care, to maintain appropriate standards of confidentiality and to continually strengthen the principles and practices through which that trust is protected.

AURA SOLUTION COMPANY LIMITED

PRIVATE BY PRINCIPLE. RESPONSIBLE BY DESIGN.