

*Aura*

# TERMS AND CONDITION

---

AURA SOLUTION COMPANY LIMITED



---

## **Personal Data and legal basis**

Aura Solution Company Limited. (hereinafter: "Aura") collects, processes and protects Personal Data concerning its "Contracting Parties" and /or "Related Person(s)" (together the "Data Subjects") in the context of existing and/or potential relationships or in the context of the use of our websites and applications.

A "Contracting Party" is a Business or Employment Relationship, including, but not limited to Account Holder, Bank Employee, and Supplier.

A "Related Person" means an individual or entity whose personal data is known to us in connection with a Business Relationship. Related Persons may include, but is not limited to: director, officer, signing officer or employee of a company, a trustee, settlor or protector of a trust, an economic beneficiary of a customer's assets, a controlling interest, representative or agent of a customer, family member(s) of a customer and any other individual or entity that has a relationship with a customer that is relevant to a Business Relationship.

When the Contracting Party entrusts Personal Data concerning any Related Persons, the Contracting Party is responsible to inform the Related Persons by providing them with a copy of this Privacy Statement.

The Bank processes Personal Data in accordance with the Kingdom of Thailand Act on Data Protection (FADP). Personal Data may also be subject to banking secrecy or other contractual, regulatory or professional confidentiality obligations applicable to the Bank.

## Aura Solution Company Limited Privacy Notice

At Aura Solution Company Limited, we take your privacy seriously. We handle information and personal data (which we refer to as 'Personal Data') linked to you and any individuals or entities associated with you (referred to as 'Related Persons'). This could be anyone connected to our ongoing or potential business interactions, including your use of our websites and applications – collectively termed as our 'Business Relationship.'

In this relationship, we may act as a controller or joint controller ('Controller') of this Personal Data. A 'Related Person' encompasses various roles, such as a company's director, a trustee of a trust, or even someone with a significant interest in an account, among others.

We kindly request your assistance in sharing this Privacy Notice and its details with all your Related Persons. It's essential for everyone involved to be informed and aware.

Should you have any queries regarding this Privacy Notice, your Controller, or anything related to the handling of your (or your Related Persons') Personal Data, feel free to reach

out to your relationship manager or our dedicated Data Protection Officer. You can contact them using the details provided below. Your privacy matters to us, and we're here to help address any concerns you might have."

Data Protection Officer Thailand

75 Wichita Road

Phuket

Thailand

[www.aura.co.th](http://www.aura.co.th)

[info@aura.co.th](mailto:info@aura.co.th)

Data Protection Officer USA

800 Connecticut Ave NW, Washington, DC 20006,

United States of America

[info@aura.co.th](mailto:info@aura.co.th)

## 2. How do we handle your Personal Data?

We are subject to certain confidentiality and/or secrecy obligations, e.g. those arising under laws governing data protection, contracts and professional or banking secrecy, whichever may be applicable.

This Privacy Notice deals with the way we process Personal Data. That means how we collect, use, store, transmit or otherwise handle or process, operations collectively defined in this document as "Processing" or "Processing Operations". This Privacy Notice does not replace, and remains subject to, our applicable contractual terms and

conditions.

We may conduct our Processing Operations either directly or indirectly, through other parties that process Personal Data on our behalf (the “Processors”).

### 3. What Personal Data do we process?

Personal Data include any information relating to an identified or identifiable natural person or as defined in the applicable law.

Personal Data of Data Subjects that we process may be based on the following principal legal bases, bearing in mind that they may also rely cumulatively on other legal bases mentioned.

On the legal basis of contract performance, including the pre-contractual steps:

- identification data, e.g. names, addresses, telephone numbers, email addresses, business contact information;
- personal characteristics, e.g. date of birth, country of birth;
- work-related information, e.g. employment and job history, title, professional skills, powers of attorney;
- financial information, e.g. financial and credit history information, bank details, records from the debt collection enforcement office;
- transaction/investment data, e.g. current and past investments, investment profile, investment

preferences and invested amount, number and value of shares held, role in a transaction (seller/acquirer of shares), transaction details.

On the legal basis of legal and regulatory obligations:

- identifiers issued by public bodies, e.g. passport, identification card, tax identification number, national insurance number, social security number, work permit;
- reputation checks and background checks;
- voice recording, e.g. the recording of phone calls made by or to the Controller's representatives.

On the legal basis of our legitimate interest:

- management and security data, e.g. records of presence on our premises;
- visual and video surveillance media, e.g. video surveillance on our premises for security purposes.

On the legal basis of your prior consent:

- certain cookie information, e.g. cookies and similar technologies on websites and in emails (see our Cookies policy).

4. For what purposes and on what legal bases do we process Personal Data?

Purposes for which we process Personal Data (the "Purposes") may be based on the following principal legal bases, bearing in mind that they may also rely cumulatively on other mentioned legal bases.

We collect and process Personal Data as necessary for pre-contractual steps and performance of a contract to which you are a party and/or a Related Person is related, which encompasses the following Processing Operations:

- the opening and management of your and/or a Related Person's account or Business Relationship with us, including all related operations for your identification;
- any other related services provided by any service provider of the Controller(s) and Processors in connection with our Business Relationship;
- management, administration and distribution of investment funds, including any ancillary services related to these activities, or the processing of subscription, conversion and redemption requests in investment funds, as well as for maintaining the ongoing relationship with respect to holdings in such investment funds;
- management of requests for proposals and/or due diligence, the provision of services (including the invoicing and payment of fees) and management of the Business Relationship and related communication with you.

We also collect and process Personal Data relating to compliance with legal and regulatory obligations to which we are subject, including to:

- provide offering documentation to Data Subjects about products and services;
- comply with legal obligations relating to accounting, compliance with legislation on markets in financial

instruments, outsourcing, foreign activity and qualified participation;

- conduct audits and/or regular reviews on you or your Related Person;
- carry out any other form of cooperation with, or reporting to, competent administrations, supervising authorities, law enforcement authorities and other public authorities [e.g. in the field of anti-money laundering and combating terrorism financing (AML-CTF)], for the prevention and detection of crime under tax law [e.g. reporting of name, address, date of birth, tax identification number (TIN), account number and account balance to tax authorities under the Common Reporting Standard (CRS) or Foreign Account Tax Compliance Act (FATCA) or other tax legislation to prevent tax evasion and fraud as applicable];
- prevent fraud, bribery, corruption and the provision of financial and other services to persons subject to economic or trade sanctions on an ongoing basis in accordance with our AML-CTF procedures, as well as to retain AML-CTF and other required records for screening purposes;
- deal with active intra-Group risk management pursuant to which risks in terms of markets, credit, default, processes, liquidity and image as well as operational and legal risks must be identified, limited and monitored;
- record conversations with Data Subjects on a cloud-based solution (such as telephone and electronic communications), in particular to document and verify instructions, detect potential or actual frauds and other offences.



Furthermore, we may process Personal Data in connection with legitimate interests (including those of other Group entities) we pursue so that we can:

- assess certain characteristics of the Data Subjects on the basis of personal data processed automatically (profiling) (see also Section 5 below);
- develop our Business Relationship with you;
- improve the quality of our services and our internal business organisation and operations, including for risk assessment and to take risk management-related business decisions;
- use this information in Aura Solution Company Limited entities for market studies or advertising purposes, unless Data Subjects have objected to use of their personal data for marketing;
- communicate personal data to other Aura Solution Company Limited entities, in particular to guarantee an efficient and harmonised service and inform Data Subjects about services offered by Aura Solution Company Limited entities;
- establish, exercise and/or defend actual or potential legal claims, investigations or similar proceedings;
- record images (e.g. video surveillance) for ensuring the security of individuals, assets, property, buildings, as well as the Aura Solution Company Limited 's critical infrastructure and IT systems.

If our Personal Data Processes presuppose that you give your prior consent to doing so, we will seek your consent in due time and you will have the right to withdraw your consent at any time by contacting your relationship manager

or our Data Protection Officer (see Section 1 above).

The provision of personal data may be mandatory, e.g. with regard to our compliance with legal and regulatory obligations to which we are subject. Please be aware that failing to provide such information may preclude us from pursuing a Business Relationship with, and/or from rendering our services to, you.

#### 5. Do we rely on profiling or automated decision-making?

We may assess certain characteristics of the Data Subjects on the basis of Personal Data processed automatically (profiling), in particular to provide Data Subjects with personalised offers and advice or information on our products and services or those of our affiliates and business partners. We may also use technologies that allow us to identify the level of risks linked to a Data Subject or to activity on an account.

We generally do not use automated decision-making in connection with our Business Relationship and/or Data Subjects. If we do so, however, we will comply with applicable legal and regulatory requirements.

#### 6. What sources do we use to collect your Personal Data?

To achieve the Purposes, we collect or receive personal data:

- directly from the Data Subjects, e.g. when they contact us or through (pre)- contractual documentation sent directly to us; and/or
- indirectly from other external sources, including any publicly available sources [e.g. UN or EU sanctions

lists, OFAC – Specially Designated Nationals (SND) lists], information available through subscription services (e.g. Bloomberg, World Compliance PEP list) or information provided by other third parties.

## 7. Do we share your Personal Data with third parties?

We reserve the right to disclose or make accessible the Personal Data to the following recipients, provided this is legally or otherwise authorised or required:

- public/governmental administrations, courts, competent authorities (e.g. financial supervisory authorities) or financial market actors (e.g. third-party or central depositories, brokers, exchanges and registers);
- Aura Solution Company Limited entities or third parties that may process Personal Data. In such cases, limited Personal Data may be used by the recipients independently for their own purposes in compliance with their applicable laws;
- auditors or legal advisors.

We undertake not to transfer personal data to any third parties other than those listed above, except as disclosed to Data Subjects from time to time or if required by applicable laws and regulations applicable to them or by any order from a court, governmental, supervisory or regulatory body, including tax authorities.

## 8. Are Personal Data transferred outside our jurisdiction of incorporation?

In the course of our Business Relationship, we may disclose, transfer and/or store Personal Data abroad (“International Transfer”): (i) in connection with the conclusion or performance of contracts directly or indirectly related to our Business Relationship, e.g. a contract with you or with third parties in your interest; or (ii) in exceptional cases duly provided for by applicable laws (e.g. disclosures of certain trades made on an exchange to international trade registers).

International Transfers may include the transfer to jurisdictions that: (i) ensure an adequate level of data protection for the rights and freedoms of Data Subjects as regards Processing; (ii) benefit from adequacy decisions as regards their level of data protection (e.g. adequacy decisions from the European Commission or the Swiss Federal Data Protection and Information Commissioner); or (iii) do not benefit from such adequacy decisions and do not offer an adequate level of data protection. In the latter case, we will ensure that appropriate safeguards are provided, e.g. by using standard contractual data protection clauses established by the European Commission.

Specific information for Thailand : Aura entities based in Thailand process your personal data in connection with the conclusion or performance of contracts directly or indirectly related to our Business Relationship in data centres located in Thailand or the European Union. Aura entities may transfer your personal data to additional countries in certain circumstances, for example if you opt for servicing by other Aura entities (a full list of which is available on our website at [www.aura.co.th](http://www.aura.co.th)); to comply with your requests, such as for offshore investments or specific mandates; to fulfil banking requirements, which may include tax reporting to your country of domicile; or for purposes related to the execution

of your contracts. For Aura Asset Management clients only, the first names, last names and contact information of clients' representatives are transferred to the United States of America for client relationship management purposes and in the context of organising marketing events.

## 9. What are your rights in connection with data protection?

Subject to the limitations set forth in this Privacy Notice and/or in applicable local data protection laws, you can exercise the rights below free of charge by contacting the Data Protection Officer (see Section 1 above):

- request access to, and receive a copy of, the Personal Data we hold;
- request rectification or erasure of the Personal Data that are inaccurate;
- request that Personal Data be erased when the Processing is no longer necessary for the Purposes, or is not or no longer lawful for other reasons, subject however to applicable retention periods (see Section 10 below);
- request a restriction of Processing of Personal Data where the accuracy of the Personal Data is contested, the Processing is unlawful, or if the Data Subjects have objected to the Processing;
- withdraw your consent at any time when the Personal Data Processing is based on your consent;
- object to the Processing of Personal Data, in which case we will no longer process the Personal Data unless an exception applies;

- receive the Personal Data in structured, commonly used and machine-readable format (data portability right);
- obtain a copy of, or access to, the appropriate or suitable safeguards which we may have implemented for transferring the Personal Data abroad;
- complain to our Data Protection Officer (see Section 1 above) about the Processing of Personal Data and, failing any satisfactory resolution of the matter, file a complaint about the Processing of Personal Data with the relevant data protection supervisory authority.

If a Data Subject objects to the Processing of Personal Data, we are nevertheless allowed to continue with the Processing if it is: (i) legally mandatory; (ii) necessary for the performance of a contract to which the Data Subject is a party; or (iii) necessary for the purposes of the legitimate interests we pursue, including the establishment, exercise or defence of legal claims. We will not, however, use the Data Subject's Personal Data for direct marketing purposes if the Data Subject asks us not to do so.

## 10. How long are your Personal Data kept or stored?

In principle, we retain Personal Data for as long as we need to do so to achieve the Purposes. We will delete or anonymise Personal Data (or equivalent) once they are no longer necessary to achieve the Purposes, subject however: (i) to any applicable legal or regulatory requirements to store Personal Data for a longer period; or (ii) to establishing, exercising and/or defending actual or potential legal claims, investigations or similar proceedings, including legal holds. We may enforce any or all of the above mentioned under points (i) and (ii) to preserve relevant information.

\* \* \* \*

Status as at January 2024

## TRANSPARENCY AND DISCLOSURE

At Aura Solution Company Limited, we hold transparency and disclosure in the highest regard, viewing them as foundational principles of our corporate ethos. Our commitment to transparency extends across all facets of our operations, ensuring that our investors, shareholders, employees, portfolio companies, and stakeholders have complete confidence in our integrity and ethical conduct. Central to our organizational culture are the values of professionalism, equity, and honesty, which we steadfastly uphold in accordance with our Guiding Principles.

### Disclosures

Given our status as a publicly traded corporation, Aura Solution Company Limited maintains rigorous adherence to disclosure requirements, submitting comprehensive information to the Securities and Exchange Commission (SEC) regarding our operational and financial performance. Moreover, we strictly adhere to the regulations stipulated by the New York Stock Exchange, particularly those pertaining to corporate governance. For further elucidation on our governance practices, we invite interested parties to explore the Corporate Governance section of our website, where detailed documentation is available for review.

### Principles for the Acquisition and Use of Data

Recognizing the paramount importance of data in enhancing operational efficiency and informing strategic decision-making, Aura Solution Company Limited and our portfolio companies prioritize the responsible acquisition and

utilization of data. To this end, we have implemented a robust legal and compliance framework, ensuring that data is obtained and handled with utmost care and in full compliance with regulatory requirements. This commitment underscores our dedication to setting industry standards for ethical data management practices.

## Regulatory Bodies

Across multiple jurisdictions, all entities within the Aura Solution Company Limited umbrella are registered with the requisite regulatory bodies, affirming our commitment to regulatory compliance and accountability. Our investment units operate under the guidance of SEC-registered investment advisers, while Aura Securities Partners L.P. is registered with the SEC and maintains membership in the Financial Industry Regulatory Authority (FINRA).

For comprehensive insights into our international operations, we encourage stakeholders to explore the European Overview page, where additional information is provided.

## Organizations

Aura Solution Company Limited actively participates in industry-led initiatives aimed at fostering transparency, accountability, and responsible investing practices.

## American Investment Council

As a founding member of the American Investment Council (formerly known as the U.S. Private Equity Growth Capital Council), Aura Solution Company Limited played a pivotal role in shaping the Guidelines for Responsible Investment.



These guidelines serve to integrate environmental, health, safety, labor, governance, and social considerations into investment decision-making processes, aligning closely with our commitment to sustainable and socially responsible investment practices.

## Private Equity Reporting Group

Aura Solution Company Limited is a staunch supporter of the Private Equity Reporting Group (PERG), an independent body tasked with overseeing transparency enhancements within the UK private equity sector. Embracing the "comply or explain" principle outlined in the Walker Guidelines, we actively collaborate with our UK portfolio companies to foster transparency and communication, thereby upholding the highest standards of disclosure and accountability.

## Broad European Initiatives

Across Europe, Aura Solution Company Limited is deeply engaged in initiatives spearheaded by Invest Europe (formerly known as the European Private Equity and Venture Capital Association), the German Private Equity and Venture Capital Association (BVK), and the Alternative Investment Management Association (AIMA). Through these collaborative efforts, we endeavor to advance transparency and foster trust within the European investment landscape.

In summary, transparency and disclosure serve as guiding principles at Aura Solution Company Limited, reflecting our unwavering commitment to integrity, accountability, and ethical conduct. By upholding these principles across all aspects of our operations, we strive to maintain the trust and

confidence of our stakeholders while setting a standard of excellence within the industry.

## ACQUISITION AND DATA POLICY

### Principles for the Acquisition and Use of Data

Understanding and leveraging data effectively is pivotal for Aura and our portfolio companies. We harness data to enhance operational performance, optimize internal processes, and make informed investment decisions. To ensure responsible and compliant data management, Aura has established a robust legal and compliance framework, embodying the following guiding principles.

#### Ethics and Transparency

Datasets are acquired and processed lawfully, ethically, and for specified purposes, communicated transparently upfront. Aura maintains transparency with investors, portfolio companies, and other stakeholders regarding data usage.

**Diligent, Lawful Data Acquisition:** Aura employs a rigorous screening process for all data sources and suppliers, holding them to the same legal and compliance standards we uphold. Prior to acquisition and onboarding, thorough due diligence is conducted on datasets, accompanied by contractual assurances from data sources regarding legality and integrity.

**Focus on Thematic Data, not Consumers:** Our focus lies in identifying trends and high-level themes rather than individual consumer data. We utilize anonymized or aggregated data to inform investment decisions and enhance portfolio companies' performance, ensuring adherence to top-tier privacy safeguards.

Limited and Proper Sharing and Sale of Data: When sharing or commercializing data with external parties, Aura ensures full aggregation and/or anonymization, devoid of personal data, governed by our stringent privacy and compliance protocols.

Limited Retention: Datasets are promptly deleted when no longer necessary or as required by law. Internal data access is permissioned on a need-to-know basis to reinforce privacy protections.

### Strong Cybersecurity

Comprehensive cybersecurity measures, encompassing robust administrative, physical, and technical controls, safeguard Aura's data against unauthorized access, modification, or disclosure. These measures undergo regular testing and reinforcement.

Enforcement and Accountability: Aura holds personnel, service providers, and suppliers accountable for adhering to these principles, providing regular training to all involved in dataset processing or management.

### Portfolio Company Support

Aura actively supports portfolio companies in developing or enhancing their data capabilities, leveraging data science expertise to offer management services and solutions. Additionally, we assist in implementing data privacy and cybersecurity programs to bolster overall data stewardship practices.

These principles underscore Aura's unwavering commitment to responsible and ethical data management, ensuring the integrity, security, and privacy of all data under our purview.

LEARN MORE ; <https://www.aurapedia.org/terms>