Privacy Policy

Last updated August 4, 2022

Version 2.0 | Effective 5 June 2026

1. Introduction and Scope

Entity: AUDC Pty Ltd
ACN: 637 164 722
AFSL Number: 700123
Registered Address: Level 3, 461 Bourke Street, Melbourne VIC 3000, Australia
Privacy Officer Email: privacy.officer@audd.digital
Website: https://www.audd.digital

(AUDC, we, us, our) holds Australian Financial Services Licence No. 700123 granted by the Australian Securities and Investments Commission (ASIC). We provide financial services as authorised under that licence, and we also operate the website audd.digital.

We are committed to protecting the privacy and confidentiality of the personal information we collect and hold. This Privacy Policy explains how we collect, use, disclose, store, and protect personal information about individuals who interact with us, including clients, prospective clients, website visitors, job applicants, and other individuals.

This Policy applies to all personal information we handle in connection with our business activities, whether collected through our website, in person, by telephone, by email, or in the course of providing financial services.

This Policy is made in accordance with the Privacy Act 1988 (Cth), the 13 Australian Privacy Principles (APPs) set out in Schedule 1 to that Act, the Privacy and Other Legislation Amendment Act 2024 (Cth), and our obligations as an AFSL holder under the Corporations Act 2001 (Cth).

1.1 Who This Policy Applies To

This Policy applies to all individuals whose personal information we hold, including:

- current, former, and prospective financial services clients;
- users of our digital asset or financial technology platform services;
- visitors to our website at audd.digital;
- job applicants and prospective employees;
- representatives of our business partners, platform partners, merchants, service providers, and contractors; and
- any other individual who contacts us or provides us with personal information.

1.2 Related Documents

This Policy should be read in conjunction with our Financial Services Guide (FSG), our Terms of Use, and any specific collection notices we provide to you at the time we collect your personal information. In the event of any inconsistency between this Policy and a specific collection notice, the collection notice will prevail to the extent of that inconsistency.

2. What Personal Information We Collect

‘Personal information’ means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not the information or opinion is true, and whether or not it is recorded in a material form. This includes information that could be used, alone or in combination with other information, to identify you — including certain digital identifiers such as blockchain wallet addresses.

We only collect personal information that is reasonably necessary for one or more of our business functions and activities.

2.1 Website and General Enquiries

- • Name, title, and contact details (email address, telephone number, postal address).
• Technical data collected automatically when you visit our website, including your IP address, browser type, pages visited, and the time and date of your visit. This information is generally statistical and may not be personally identifiable.
• Any other information you voluntarily provide through our website contact forms or by email.

2.2 Financial Services Clients

In the course of providing financial services, we may collect a broader range of personal information, including:
• Full legal name, date of birth, residential and postal address.
• Contact details including telephone numbers and email addresses.
• Identity verification documents (e.g. passport, driver's licence) as required by law.
• Tax File Number (TFN) and other tax-related information, where required by law for the provision of financial services.
• Financial information, including income, assets, liabilities, account details, and investment objectives.
• Employment status and occupation.
• Information about your financial needs, goals, and risk tolerance.
• Transaction records and records of financial services provided to you.
• Any other information necessary to provide you with the relevant financial service or to meet our legal obligations.

2.3 Job Applicants

- • Name, contact details, and employment history contained in resumes or CVs.
• Qualifications, education history, and professional references.
• Right to work status and identity documentation.
• Sensitive information provided voluntarily in the context of recruitment (see section 2.5 below).

2.4 Digital Asset and Blockchain Information

Where we provide services involving digital assets or operate in connection with blockchain networks, we may collect the following categories of information. Where any of this information identifies, or can reasonably be linked to, an identifiable individual, we treat it as personal information and all Australian Privacy Principles apply to it:
• Blockchain wallet addresses and public keys.
• Blockchain transaction hashes, transaction history, and on-chain metadata.
• Network information relating to blockchain interactions.
• Blockchain analytics information, including risk scores and wallet attribution data generated by third-party blockchain analytics providers.
• Sanctions screening results and watchlist match data.
• Fraud prevention information and compliance monitoring data generated in connection with your transactions or account activity.
Collection of this information is required for the purposes of AML/CTF compliance, sanctions screening, fraud prevention, and customer due diligence under the AML/CTF Act and our obligations to AUSTRAC. Some collection is voluntary (for example, you providing a wallet address to initiate a transaction) and some is generated automatically as a result of your activity on our platform or on public blockchain networks.

2.5 Sensitive Information

'Sensitive information' is a category of personal information attracting a higher level of protection under the Privacy Act. It includes information about a person's racial or ethnic origin, political opinions, religious beliefs, health information, sexual orientation, and criminal record. We do not seek to collect sensitive information unless it is reasonably necessary for our

functions and we have your consent, or we are required or authorised by law to collect it. Where sensitive information is relevant to a recruitment application and you provide it voluntarily, we will take your submission as consent to our use of that information solely for recruitment purposes. We will not use sensitive information for any other purpose.
If you provide sensitive information that we did not request and do not require, we will destroy or de-identify that information as soon as practicable in accordance with APP 4.

3. How We Collect Personal Information

We collect personal information in the following ways:

- Directly from you, when you provide it to us through our website, by email, by telephone, in person, or in the course of completing forms or agreements.
- From third parties authorised by you, such as your accountant, financial adviser, or legal representative acting on your behalf.
- From publicly available sources, where relevant to our functions (for example, ASIC registers, property records, or publicly available financial information).
- Automatically through our website and platform, using cookies and similar technologies (see section 8 below), and through automated monitoring of platform and API activity (see section 4.4 below).
- From our service providers, where those providers have collected information on our behalf.
- From platform partners, merchants, and integrated services, as described in section 3.1 below.

3.1 Collection Through Platform Partners, Merchants and Integrated Services

AUDC may provide services through merchants, platform partners, promoters, distributors, and integrated technology providers (collectively, Platform Partners). Personal information about you may be collected:

- directly by AUDC through our own onboarding and service delivery processes;
- by a Platform Partner acting as our agent or service provider, on our behalf and subject to our instructions; or
- by a Platform Partner in the first instance for its own purposes, and then provided to AUDC for the purposes of onboarding, AML/CTF compliance, settlement, compliance, and service delivery.

Where a Platform Partner collects personal information and subsequently provides it to us, we require that the Platform Partner’s collection notice (provided to individuals at the time of collection) informs individuals that their information may be shared with AUDC and the purposes for which AUDC will use it. All Platform Partners are required by written agreement to handle personal information in a manner consistent with the Australian Privacy Principles, to implement appropriate data security measures, and to notify us promptly of any data breach affecting information they hold on our behalf.

Where personal information is collected jointly by AUDC and a Platform Partner — that is, where both entities determine the purpose and means of collection — each entity holds independent obligations under the Privacy Act. AUDC is accountable for its own handling of that information regardless of the Platform Partner’s conduct.

We will always take reasonable steps to notify you of the key matters relating to our collection of your personal information at or before the time of collection, or as soon as practicable afterwards, in accordance with APP 5. Collection notices will identify: who we are; the purpose of collection; whether collection is required or authorised by law; any third parties to whom we may disclose the information; and how you can access and correct the information we hold.

4. Why We Collect and Use Personal Information

4.1 Primary Purposes

- Providing financial services to you under our AFSL, including providing financial product advice, dealing in financial products, and managing your account.

- Providing digital asset and platform-related services as authorised under our AFSL and applicable law.
- Complying with our obligations as an AFSL holder under the Corporations Act 2001, including record-keeping, disclosure, and anti-hawking obligations.
- Complying with AML/CTF obligations under the AML/CTF Act, including customer identification and verification (KYC), customer due diligence (CDD), and enhanced due diligence (EDD).
- Sanctions screening and complying with obligations under Australian and applicable international sanctions regimes.
- Fraud detection and prevention.
- Managing our website and responding to your enquiries.
- Recruiting and assessing job applicants.

4.2 Secondary Purposes

We may also use your personal information for the following secondary purposes, where we are permitted to do so under APP 6:

- Improving our products, services, and website.
- Direct marketing of our financial services to you, where you have consented or where we are permitted to do so under APP 7 (see section 7 below).
- Complying with any applicable law, court order, or regulatory requirement.
- Protecting and enforcing our legal rights.

We will not use or disclose your personal information for a purpose other than the primary purpose for which it was collected (or a directly related secondary purpose) without your consent, except as required or permitted by law.

4.3 Financial Crime Compliance and Transaction Monitoring

We may collect, use, analyse, and retain personal information for the following financial crime compliance purposes, which are required or authorised by the AML/CTF Act and our AFSL obligations:

- AML/CTF compliance, including customer identification, KYC, CDD, and EDD.
- Sanctions screening against Australian and applicable international sanctions lists.
- Fraud detection, fraud prevention, and fraud investigation.
- Transaction monitoring for suspicious activity.
- Regulatory reporting, including the lodgement of Suspicious Matter Reports (SMRs) and Threshold Transaction Reports (TTRs) with AUSTRAC, and reporting to ASIC and other regulators as required.
- Blockchain analytics, including the use of third-party blockchain analytics platforms to assess the risk profile of wallet addresses and transaction histories.

Some of these activities involve the use of automated tools and systems, including blockchain analytics platforms and algorithmic risk-scoring tools. See section 4.5 below for further information about our automated decision-making practices.

4.4 Platform and Settlement Monitoring

AUDC monitors platform, API, settlement, and partner-integrated activity for the following purposes, each of which is required or authorised by our AFSL obligations, the AML/CTF Act, or our legitimate interests in operating a secure and compliant platform:

- Fraud prevention and detection.
- AML/CTF compliance and sanctions compliance monitoring.
- Dispute investigation and resolution.
- Security monitoring and incident response.
- Operational risk management and platform integrity.

Where this monitoring generates or involves personal information about an individual (for example, where a specific individual's API usage pattern or settlement activity is flagged for review), that information is handled in accordance with this Privacy Policy and all applicable Australian Privacy Principles.

Technical and operational monitoring data that does not identify, and cannot reasonably be linked to, an identifiable individual (for example, aggregate platform throughput statistics) is not personal information and is not subject to the Privacy Act.

All monitoring activities are conducted in accordance with applicable law, including the Telecommunications (Interception and Access) Act 1979 (Cth) and any other legislation governing the interception or monitoring of communications.

4.5 Automated Decision-Making

We use automated tools and systems in the course of providing our services and fulfilling our compliance obligations. These include:

- Blockchain analytics platforms (such as third-party risk-scoring tools that assess the risk profile of wallet addresses based on their transaction history and network associations).
- Algorithmic AML/CTF transaction monitoring systems that flag transactions or account activity for further review.
- Automated sanctions screening systems that match customer identity data against Australian and international sanctions lists.
- Automated onboarding and identity verification tools.

These tools may generate assessments, scores, or flags that inform decisions about whether to onboard a customer, whether to proceed with a transaction, whether to apply enhanced due diligence, or whether to file a regulatory report.

Decisions that significantly affect your interests — such as a decision to decline your onboarding application, block or delay a transaction, or apply additional identity verification requirements — are subject to human review by a member of our compliance team before a final determination is made. You have the right to request that a decision made about you that is significantly informed by automated processing be reviewed by a human. To exercise this right, please contact our Privacy Officer using the contact details at the top of this Policy.

We will update this section as additional obligations regarding automated decision-making transparency come into force under the Privacy and Other Legislation Amendment Act 2024 and any implementing regulations.

5. Disclosure of Personal Information

We do not sell your personal information to third parties.

We may disclose your personal information to the following categories of recipients, to the extent necessary for our business activities:

- ASIC, AUSTRAC, the Australian Taxation Office (ATO), and other regulatory bodies, where required by law.
- Our professional advisers, including lawyers, accountants, and auditors, under obligations of confidentiality.
- Our IT service providers, cloud hosting providers, and technology platforms that support our business operations, under contractual data security obligations.
- Product issuers, custodians, and other financial services entities where necessary to execute or facilitate a transaction or provide a financial service.
- Credit reporting bodies or agencies, where permitted by law.
- Courts and tribunals, where required by a court order or subpoena.
- Platform Partners (as described in section 3.1), for the purposes of service delivery, onboarding, AML/CTF compliance, settlement, and compliance.

- Related entities, including Dexah Advisory Pty Ltd (Dexah), as described in section 5.1 below.
- Third-party blockchain analytics providers, for the purpose of AML/CTF compliance and fraud prevention (see section 4.3).
- Any other party with your express consent.

We do not share your personal information with third parties for their own marketing purposes.

5.1 Related Entities — Dexah Advisory Pty Ltd

AUDC may share personal information with Dexah Advisory Pty Ltd ACN 647 452 962 (Dexah), a wholly owned subsidiary of AUDC. Dexah provides technology and platform infrastructure services and compliance services including AML/KYC processing to AUDC.

Personal information may be shared with Dexah where required to:

- provide services to you;
- perform onboarding and identity verification processes;
- satisfy AML/CTF obligations, including customer due diligence and transaction monitoring;
- process transactions; and
- manage financial crime risk.

The disclosure of your personal information to Dexah is for the primary purpose for which it was collected (providing financial services and fulfilling compliance obligations) and accordingly does not require your additional consent under APP 6.

Dexah is bound by a written data sharing and services agreement with AUDC that requires Dexah to: handle personal information in accordance with the Australian Privacy Principles; implement appropriate technical and organisational data security measures; notify AUDC promptly of any data breach affecting AUDC client information; and use personal information only for the purposes for which it was provided.

Where Dexah stores or processes personal information outside Australia, it does so in the same jurisdictions used by AUDC’s broader service provider network — currently the United States, Singapore, the United Kingdom, and the European Union. Those disclosures are governed by the same cross-border obligations described in section 6 of this Policy, including the data processing agreements and adequacy assessments that apply to all overseas recipients.

6. Cross-Border Disclosure of Personal Information

Some of our service providers, technology platforms, and related entities are based outside Australia and may process or store your personal information overseas. The countries in which such recipients are currently located include:

Jurisdiction	Recipients / Context
United States	Cloud infrastructure providers, blockchain analytics platforms, and compliance technology providers.
Singapore	Regional technology and settlement service providers.
United Kingdom	Compliance and financial technology service providers.
European Union	Cloud service providers operating under EU data protection frameworks.
United States, Singapore, United Kingdom, European Union	Dexah Advisory Pty Ltd (ACN 647 452 962), a wholly owned subsidiary of AUDC, providing AML/KYC processing and technology platform infrastructure services. Dexah’s overseas processing occurs within the same jurisdictions and under the same contractual protections as AUDC’s direct service providers.

Other jurisdictions	We will notify you if we engage service providers in jurisdictions not listed above. Contact the Privacy Officer for the most current list.

.Before disclosing personal information to an overseas recipient, we take reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to that information, in accordance with APP 8. These steps include:

- Entering into data processing agreements with overseas service providers that require them to handle your information in accordance with the APPs or equivalent privacy standards.
- Assessing whether the laws of the recipient's country provide a level of protection substantially similar to the Privacy Act, including for jurisdictions such as the United Kingdom (UK GDPR) and the European Union (GDPR).
- Where we are unable to satisfy ourselves of equivalent protection and do not have a binding contractual arrangement, obtaining your consent to the overseas disclosure and informing you that APP 8.1 will not apply in that circumstance.

We remain accountable for the handling of your personal information by overseas recipients to whom we disclose it, except where you have provided informed consent to a specific disclosure in circumstances where we have notified you that APP 8.1 will not apply.

If the jurisdictions in which we operate change materially, we will update this section and notify affected individuals in accordance with section 15 of this Policy.

7. Direct Marketing

We may use your personal information to send you information about our financial services, updates, and other communications that we think may be of interest to you, where we are permitted to do so under APP 7 or the Spam Act 2003 (Cth).

We will only send you direct marketing communications where:

- you have consented to receiving them; or
- we have collected your contact information in the course of providing you with a financial service, and you would reasonably expect to receive marketing communications from us about similar services, and we provide you with a simple opt-out mechanism with each communication.

You may opt out of receiving direct marketing communications from us at any time by:

- clicking the 'unsubscribe' link in any marketing email we send you;
- emailing us at privacy.officer@audd.digital with the subject line 'Opt-Out'; or
- contacting our Privacy Officer by telephone or post using the details at the top of this Policy.

We will process your opt-out request promptly and within a reasonable period, and at no cost to you. We will not send you further direct marketing communications after you have opted out.

We do not use sensitive information for direct marketing purposes.

We use Google AdWords remarketing to display advertisements to previous visitors to our website on third-party websites and through the Google Display Network. This service uses cookies to identify previous visitors. You may adjust your Google advertising preferences at any time by visiting Google's Ad Settings page (adssettings.google.com), or by using your browser settings to reject cookies. You may also opt out of AUDC's remarketing specifically by contacting our Privacy Officer using the details above

8. Cookies and Online Tracking

Our website uses cookies and similar tracking technologies. Cookies are small data files stored on your device by your web browser. We use the following types of cookies:

- Essential cookies: Required for the website to function correctly. These cannot be disabled without affecting core functionality.
- Analytics cookies: Help us understand how visitors use our website, including which pages are

visited most frequently, so we can improve our service. The information collected is aggregated and generally not personally identifiable.
- Marketing and tracking cookies: Used in connection with our Google AdWords remarketing service (see section 7 above) to track individual visits to our website so that we can display relevant advertisements to you on other platforms. These cookies do track your individual visits to our website.

You can control and manage cookies through your browser settings. Most browsers allow you to refuse or delete cookies. Please note that disabling some cookies may affect the functionality of our website. For more information about managing cookies, visit www.allaboutcookies.org

9. Security of Personal Information

We take the security of your personal information seriously. We implement a range of physical, electronic, and procedural safeguards to protect your personal information from misuse, loss, unauthorised access, modification, or disclosure. These include:

- Secure storage of physical records in access-controlled premises.
- Encryption of electronic records and use of secure, access-controlled IT systems.
- Restricted access to personal information on a need-to-know basis.
- Regular staff training on privacy and data security obligations.
- Contractual data security obligations imposed on all third-party service providers and Platform Partners who handle personal information on our behalf.

While we take all reasonable precautions, no data transmission over the internet or data storage system can be guaranteed as completely secure. If you have reason to believe that your interaction with us is no longer secure, please contact us immediately.

When personal information is no longer required for the purposes for which it was collected, and we are not required by law to retain it, we will take reasonable steps to destroy or permanently de-identify it. Note that as an AFSL holder we are required to retain certain client records for a minimum of 7 years under the Corporations Act 2001 (Cth). AML/CTF records must be retained for a minimum of 7 years under the AML/CTF Act.

10. Notifiable Data Breaches

We are subject to the Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act 1988 (Cth). If we become aware of a data breach that is likely to result in serious harm to any individual whose personal information is involved (an eligible data breach), we are required to:

- notify the Office of the Australian Information Commissioner (OAIC) as soon as practicable; and
- notify affected individuals as soon as practicable, either individually or (if direct notification is not practicable) by way of a public statement.

We have internal procedures in place for identifying, assessing, containing, and reporting data breaches. These procedures include a Data Breach Response Plan maintained by our Privacy Officer.

If you believe that a data breach has occurred that may affect your personal information, please contact our Privacy Officer immediately using the details at the top of this Policy.

11. Accessing and Correcting Your Personal Information

11.1 Right of Access

You have the right to request access to the personal information we hold about you. To make an access request, please contact our Privacy Officer in writing using the contact details at the top of this Policy.
We will respond to your request within 30 days of receipt. In some circumstances we may need to extend this period if the request is complex; we will notify you if an extension is required.
We will not charge a fee for making an access request. We may charge a reasonable fee for

providing access if the cost of doing so is significant (for example, locating and compiling records across multiple systems). We will advise you of any such fee before incurring it.
We may decline to provide access in certain limited circumstances permitted by the Privacy Act, for example where providing access would be unlawful or would unreasonably impact on the privacy of other individuals. If we decline to provide access, we will give you a written notice explaining our reasons and how you may complain about the decision.

11.2 Right to Correction

If you believe that personal information we hold about you is inaccurate, incomplete, out of date, or misleading, you may request that we correct it. Please contact our Privacy Officer in writing.

We will respond to correction requests within 30 days. If we correct information, we will notify any third parties to whom we have previously disclosed the inaccurate information, if it is reasonable to do so. If we decline to make a correction, we will explain our reasons and you may request that we attach a statement to the information noting your view that it is inaccurate.

12. Government-Related Identifiers

We will not adopt, use, or disclose a government-related identifier (such as a Medicare number, driver's licence number, or passport number) as our own identifier of an individual, except as required or authorised by law.

We may collect government-related identifiers for the purpose of verifying your identity as required by the AML/CTF Act and related laws, but we will use them solely for that purpose.

13. Anonymity and Pseudonymity

Where it is lawful and practicable to do so, we will give you the option of not identifying yourself, or of using a pseudonym, when interacting with us. For example, you may make general enquiries via our website without identifying yourself.

However, we are required by law to verify the identity of individuals to whom we provide financial services. If you wish to receive financial services from us, we will need to collect sufficient personal information to comply with our legal obligations, including customer identification requirements under the AML/CTF Act. It is not practicable for us to provide financial services on an anonymous basis.

14. Privacy Complaints

14.1 Making a Complaint to Us

If you have a concern or complaint about the way we have handled your personal information, we encourage you to contact us first so that we can attempt to resolve the matter.

Please direct your complaint in writing to:

Addressee Privacy Officer, AUDC Pty Ltd
Post Level 3, 461 Bourke Street, Melbourne VIC 3000, Australia
Email privacy.officer@audd.digital

We will acknowledge your complaint within 5 business days and aim to provide a substantive response within 30 days. If we require additional time to investigate, we will inform you of this.

14.2 Escalation to the OAIC

If you are not satisfied with our response, or if we have not responded within 30 days, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC):

Website www.oaic.gov.au
Online complaint form www.oaic.gov.au/privacy/privacy-complaints
Phone 1300 363 992
Post Office of the Australian Information Commissioner, GPO Box 5218, Sydney NSW 2001

15. Updates to This Policy

We may update this Privacy Policy from time to time to reflect changes to our business practices, legal obligations, or regulatory requirements. When we update this Policy, we will publish the updated version on our website at audd.digital and update the ‘Effective’ date at the top of this document.

We encourage you to review this Policy periodically. Where a change is material, we will take reasonable steps to notify you directly (for example, by email to financial services clients).

Continued use of our services after any update constitutes your acceptance of the updated Policy.

16. Definitions and Interpretation

Term	Meaning
AFSL	Australian Financial Services Licence granted by ASIC under the Corporations Act 2001 (Cth).
AML/CTF Act	Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).
APP	Australian Privacy Principle as set out in Schedule 1 to the Privacy Act 1988 (Cth).
ASIC	Australian Securities and Investments Commission.
AUSTRAC	Australian Transaction Reports and Analysis Centre.
AUDC / we / us / our	AUDC Pty Ltd, ACN 637 164 722.
Blockchain analytics	The use of third-party software tools to analyse public blockchain transaction data and generate risk assessments or attributions in relation to wallet addresses and their associated transaction history.
CDD / EDD	Customer due diligence and enhanced due diligence, as required under the AML/CTF Act.
Dexah Advisory Pty Ltd	ACN 647 452 962. A wholly owned subsidiary of AUDC providing technology and platform infrastructure services and AML/KYC compliance services. See section 5.1.
Eligible data breach	Has the meaning given in Part IIIC of the Privacy Act 1988 (Cth).
KYC	Know Your Customer — the process of verifying the identity of a customer in accordance with AML/CTF Act requirements.
NDB scheme	The Notifiable Data Breaches scheme established under Part IIIC of the Privacy Act 1988 (Cth).
OAIC	The Office of the Australian Information Commissioner.
Personal information	Has the meaning given in the Privacy Act 1988 (Cth): information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not true and whether or not recorded in material form. Includes blockchain wallet addresses and other digital identifiers where they can be linked to an identifiable individual.

Platform Partners	Merchants, platform partners, promoters, distributors, and integrated technology providers through whom AUDC may provide services. See section 3.1.
Privacy Act	The Privacy Act 1988 (Cth), as amended from time to time.
Sensitive information	Has the meaning given in the Privacy Act 1988 (Cth), including health information, racial or ethnic origin, political opinions, religious beliefs, and similar categories.
SMR / TTR	Suspicious Matter Report and Threshold Transaction Report — regulatory reports lodged with AUSTRAC under the AML/CTF Act.