Arbor Knot Privacy Policy

1. Introduction

1.1. Arbor Knot Holdings Pty Ltd ACN 684 908 736 including all of its subsidiaries listed in Section 1.2 below (**Arbor Knot**, **we**, **us**, or **our**) is dedicated to protecting your privacy and handling your personal information and personal data (**personal data**) with the utmost care and respect. This commitment is integral to our operations, from our Board members to our employees and contractors.

1.2. The purpose of this Privacy Policy (**Policy**) is to outline the arrangements, procedures, and measures that each of Arbor Knot Holdings Pty Ltd ACN 684 908 736 (incorporated in Australia) and its subsidiaries which include:

(a) Arbor Knot Ltd (incorporated in Israel);

(b) subsidiaries incorporated in Australia:

(i) AKCP Holdings Pty Ltd ACN 644 137 735;

(ii) AKCP Management Pty Ltd ACN 650 955 721;

(iii) AKCP Management 2 Pty Ltd ACN 688 219 418;

(iv) AKCP Nominees Pty Ltd ACN 650 955 703;

(v) AKCP Nominees 2 Pty Ltd ACN 650 952 882;

(vi) AKCP Nominees 3 Pty Ltd ACN 684 177 884;

(c) subsidiaries incorporated in Australia:

(i) Arbor Knot Inc;

(ii) ArborKnot Management Inc;

(iii) AKCP LLC; and

(d) Arbor Knot Gmbh (incorporated in Germany).

1.3. This Policy explains how Arbor Knot handles your personal data in accordance with the:

(a) for Spanish individuals, the Spanish Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights and the General Data Protection Regulation (EU) (2016/679) (**GDPR**);

(b) for Australian individuals, the Privacy Act 1988 (Cth) (**Privacy Act**), the Australian Privacy Principles and the Privacy Regulations 2013;

(c) for Israeli individuals, the Privacy Protection Law, 1981; and

(d) for United States individuals residing in:

(i) California: the California Consumer Privacy Act, as amended by the California Privacy Rights Act and the California Consumer Privacy Act regulations;

(ii) Colorado: the Colorado Privacy Act and the Colorado Privacy Act rules;

(iii) Connecticut: the Connecticut Data Privacy Act;

(iv) Delaware: the Delaware Personal Data Privacy Act;

(v) Indiana: Indiana Consumer Data Protection Act;

(vi) Iowa: the Iowa Consumer Data Protection Act;

(vii) Kentucky: the Kentucky Consumer Data Protection Act;

(viii) Maryland: the Maryland Online Data Privacy Act;

(ix) Minnesota: the Minnesota Consumer Data Privacy Act;

(x) Montana: the Montana Consumer Data Privacy Act;

(xi) Nebraska: the Nebraska Data Privacy Act;

(xii) New Hampshire: the New Hampshire Senate Bill 255;

(xiii) New Jersey: the New Jersey Senate Bill 332;

(xiv) Oregon: the Oregon Consumer Privacy Act;

(xv) Rhode Island: the Rhode Island Data Transparency and Privacy Protection Act;

(xvi) Tennessee: the Tennessee Information Protection Act;

(xvii) Texas: the Texas Data Privacy and Security Act;

(xviii) Utah: the Utah Consumer Privacy Act; and

(xix) Virginia: the Virginia Consumer Data Protection Act; and

(e) any other relevant privacy and credit codes applicable with respect of the above-mentioned jurisdictions,

together and each to be referred to as the **Privacy Laws**.

1.4. We are committed to safeguarding your privacy and ensuring that you understand how your personal data is collected, used, and shared.

1.5. This Policy applies whenever you visit our website, any mobile applications that we make available, access to any of our APIs, or us providing you with any of our products and services, including collecting on receivables or other amounts you may owe, providing a platform to manage payment of receivables and other similar amounts and providing services and assistance to help manage your ability to pay your debts and other liabilities, if you become an employee, contractor, agent, vendor or service provider to us or where you otherwise interact or deal with us, including by contacting us, communicating with us or submitting information to us (collectively, the **Services**).

1.6. Acceptance of any of our Services in writing, orally or electronic means will be deemed as giving consent to the disclosures detailed herein.

1.7. Our website uses cookies to enhance your experience. For cookies that are not strictly necessary, we will ask for your consent when you first visit our website.

1.8. You can manage your privacy preferences through the controls available on our website, including your choice to receive or decline any of our marketing communications.

2. Your Rights

2.1. This section outlines your rights under the Privacy Laws, including rights to access, rectify, or erase your personal data.

2.2. Your rights include:

(a) requesting details of personal data we hold about you;

(b) accessing your personal data;

(c) requesting corrections or updates;

(d) requesting erasure of your personal data (*subject to exceptions*);

(e) restricting or objecting to processing;

(f) complaining to a supervisory authority; and

(g) withdrawing consent where applicable.

2.3. You can request confirmation of whether your personal data is being processed and can obtain access to your data (subject to a reasonable fee for multiple copies).

2.4. Inaccuracies in your personal data can be rectified, and you can request completion of incomplete information.

2.5. Access may be denied in specific circumstances, such as safety threats, unlawful access, or frivolous requests.

2.6. If access or rectification is refused, we will provide reasons unless unreasonable to do so.

2.7. You have the right to request erasure of your personal data under certain conditions, but exclusions apply (e.g., compliance with legal obligations or service delivery).

2.8. You may object to direct marketing purposes, and upon objection, processing for this purpose will cease.

3. What Personal Data We Collect

3.1. Personal data is any information or opinion that identifies you or can reasonably identify you. The information or opinion is still defined as personal data even if it is untrue or whether there is a record of it.

3.2. We have provided a list below of the personal data that may be provided to us by our clients for their customers that we service or we may collect from you or your representatives:

Personal and Contact Information:	Name, date of birth, address, phone number, email, social media username or membership in any company or trust.

Government Identifiers:	Passport, driver's license, citizenship, birth certificate, Medicare details, or tax identification numbers or any other identity documents.
Document Verification Service (DVS) gateway service provider (DVS Checks)	We may use Government related identifiers and identity documents for verifying your identity and checking with the document issuer or official record holder via a Document Verification Service (DVS) gateway service providers and third party systems for the purpose of confirming your identity. Your personal data with respect of DVS Checks will only be used by Arbor Knot for verification of your identity and not for any other purpose. If you do not provide your consent we will need to use alternative methods to verify your identity.
Financial & Personal Circumstances Information:	Occupation, place of work, bank account details, transaction data, income, assets, financial liabilities, financial changes and life events, bank account details, credit card details, credit history, credit capacity, ability to be provided with credit or credit worthiness.
Socio-Demographic Information:	Citizenship, age, gender, nationality, relationship status, occupation, dependents and place of work.
Digital Information:	IP address, device details, browsing activity, location data (if enabled), signature, photograph, video or audio recording.
Sensitive Information:	Biometric data (e.g., fingerprint for authentication), and information about life events. Please note other than what is outlined above, we generally do not collect *'sensitive information*' as defined under the Privacy Laws and we further restrict collection of such sensitive information to circumstances where we have either obtained your express consent or a permitted general situation exists.
Other Information:	Any details shared during your interactions with us, including call recordings and publicly available information.

4. What Happens If You Do Not Provide Your Information?

4.1. If you do not provide the personal data we request, we may not be able to offer our Services, verify your identity, or protect you from fraud.

5. Remaining Anonymous or Using a Pseudonym

5.1. You may choose to remain anonymous or use a pseudonym when making general inquiries. However, to provide most of our Services, we need to verify your identity.

6. How We Use Your Personal Data

6.1. We use your personal data for the following purposes:

Providing Services:	We may process your personal information for the following purposes: ▪ **Debt and Receivables Management**: To facilitate the collection of outstanding receivables or other amounts you may owe, and to provide a platform for managing payments and related financial obligations. ▪ **Financial Assistance Services**: To offer support and services that help you manage your ability to meet financial commitments, including debts and liabilities. ▪ **Representatives**: To work with your authorised representatives, including agents or legal proxies, in relation to your account or services. ▪ **Customer and Partner Engagement**: To service our mutual customers, interact with you as an appointed service provider, and deliver our services effectively. ▪ **Third-Party Collaboration**: We may also share and process data with our appointed vendors, contractors, and service providers who assist in delivering, maintaining, or improving our Services. ▪ **Service Improvement and Personalisation**: To enhance user experience, improve our Services, and tailor our offerings to better meet your needs. ▪ **Marketing and Communications**: To market and promote relevant products and services, and to communicate with you or your authorised representatives regarding updates, offers, and Service-related information.
Business Operations:	To handle transactions, respond to inquiries and complaints, arranging for services to be provided by third parties appointed by us, manage risks, to comply with our contractual obligations, facilitating our internal business operations, such as record keeping, data analytics, reporting, quality assurance, auditing, internal governance, training and including the fulfilment of any of our legal and regulatory requirements.
Security and Fraud Prevention:	To prevent and investigate fraud, cyberattacks, and unauthorised access.
Improving Services:	To review feedback, test new features, and develop better products and services.
Compliance with Laws:	To meet our clients or our legal and regulatory responsibilities, such as verifying identity or sharing data with law enforcement.

6.2. We may combine your information with other data to understand trends, improve services, and assess risks more effectively.

7. De-Identified Information

7.1. We may remove identifying details from your personal data for research or analysis purposes. This Policy and Privacy Laws will generally not apply to our use of de-identified information. However, we will continue to safeguard this de-identified information.

7.2. If this information is later combined with other data that identifies you, it will be treated as personal data.

8. Collecting or Sharing Your Personal Data

8.1. From time to time, in order for us to perform the functions and/or activities described above we may collect or share personal data about you with third parties or organisations as described below:

Group Companies or our Affiliates:	Subsidiaries our related entities and other organisations with whom we have affiliations (if any) to facilitate our and their internal business processes for operational purposes.
Other Organisations	Other organisations, who jointly with us, provide products or services to you or with whom we partner to provide products or services to you.
Joint account holders and Guarantors	Joint account holders or guarantors.
To your Authorised Representatives	Where we have been notified of your Authorised Representative, we will disclose your details to them (including your legal adviser, lender, financial adviser, insurer, executor, administrator, guardian, trustee, or attorney).
Service Providers:	Contractors, financial institutions, third party service providers who assist us in operating our business (including but not limited to credit reporting bodies, insurers and technology service providers) and these service providers may not comply or be required to comply with our Policy that we provide the Services with.
Authorities:	Government agencies, regulatory bodies when required by law, government registries, law enforcement bodies in any jurisdiction, credit reporting bodies and public information in public registers.
Third Parties:	Our financial advisers, legal advisers, auditors or organisations involved in a corporate re-organisation or involved in a transfer of all or part of the assets or business of our organisation. Organisations involved in the payments systems including financial institutions, merchants and payment organisations. Organisations required to assist us discharge our legal requirements (for e.g. the 'know your client' requirements under applicable Anti- Money Laundering and Counter Terrorism laws and identification requirements). We may use or disclose your information to comply with our legislative or regulatory requirements in any jurisdiction and to prevent fraud, criminal or other activity that may cause you, us or others harm including in relation to our products or Services.

Document Verification Service (DVS) gateway service provider	We may use verification of identity service provider to simplify our customer on-boarding and to verify your identity. With your consent, your personal data will be checked with the document issuer or official record holder via a Document Verification Service (DVS) gateway service provider and third party systems for the purpose of confirming your identity. Your personal data will only be used by Arbor Knot for verification of identity and not for any other purpose.
Other Circumstances	Where required or authorised by law or we have a public duty to do so, with your express consent, where your consent may be reasonably inferred from the circumstances, or where it is permitted under the Privacy Laws. We may also use or disclose your personal data for a secondary purpose where the use or disclosure is required or authorised by or under law or a court/tribunal order, or if a permitted general situation applies.

8.2. We will ensure these parties comply with the applicable Privacy Laws and maintain the security of your personal data and information.

9. Retaining and Deleting your Personal Data

9.1. We retain your personal data only for as long as necessary to fulfill its purpose or meet legal requirements. Once no longer needed, we securely destroy or de-identify the data.

10. Security of your Personal Data

10.1. Much of the information we hold about you will be stored electronically. We store some of your information in secure data centres that are located in Australia. We also store information in data centres of our contracted service providers (including cloud storage providers), and some of these data centres may be located outside of Australia. Some information we hold about you will be stored in paper files. We use a range of physical, electronic and other security measures to protect the security, confidentiality and integrity of the personal data we hold both in Australia and overseas.

10.2. We use technical and organisational measures to protect your personal data. This includes:

(a) storing data in secure locations (both physical and digital);

(b) limiting access to authorised individuals and having in place identity and access management controls;

(c) employees and our contracted service providers are bound by internal information security policies and are required to keep information secure;

(d) regular training for employees on privacy and security practices;

(e) we regularly monitor and review our compliance with internal policies and industry best practice.

10.3. The security of your personal data is important to us. We take reasonable measures to ensure that your personal data is stored safely to protect it from misuse, loss, unauthorised access, modification or disclosure, including electronic and physical security measures

10.4. Despite our precautions, sending unencrypted data online carries risks. You are responsible for keeping your passwords secure.

10.5. We cannot ensure the security of any information that you transmit to us over the internet and you do so at your own risk. Our website links to external websites and we take no responsibility for the privacy practices or the content of these other sites.

10.6. We will not sell your personal data to other companies or organisations without your prior consent.

11. Sharing Information with Overseas Recipients

11.1. We may share your information with trusted service providers located overseas. Before sharing, we take steps to ensure these providers comply with the applicable Privacy Laws and secure your data.

11.2. Prior to disclosing your personal data to an overseas recipient, unless a permitted general situation applies, we will take all reasonable steps to ensure that:

(a) the overseas recipient does not breach the Privacy Laws;

(b) the overseas recipient is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way the Privacy Laws protect the information; or

(c) you have consented to us making the disclosure.

11.3. Currently we are handling, storing, and processing personal information in the following locations where Arbor Knot provides Services including in Australia, Europe, Israel, United Kingdom and the United States of America. The locations where we handle, store and process your personal information may change as our business needs change and we appoint other service providers from time to time. We will update this Policy to reflect any material changes to the jurisdictions in which we handle, store and process your personal information.

11.4. When we make onwards transfers of your personal information outside the European Economic Area, we ensure it benefits from an adequate level of data protection by:

(a) relying on European Commission adequacy decisions under Article 45 of the GDPR, finding that the third country to which the information is being transferred offers an adequate level of protection; or

(b) using European Commission approved standard contractual clauses under Article 46(2) of the GDPR for the information to all other third countries.

11.5. For further information on international data transfer and the mechanisms we adopted to safeguard your personal information, please contact us by using the contact details disclosed in this Policy.

12. Automated Decision Making

12.1. Arbor Knot does not engage in automated processing for decision-making purposes. This means that we do not make decisions based solely on automated processing, including profiling, that would significantly impact your legal rights or similarly affect you.

12.2. All significant decisions involving your data are reviewed and made by our team to ensure transparency, fairness, and accountability in our processes.

13. AI and Data Privacy

13.1. Arbor Knot may use AI and Large Language Models (LLMs), and includes AI and LLMs in its Privacy Impact Assessment process to fully understand the risks and data usage involved in these systems.

13.2. Where AI systems process personal data, Arbor Knot restricts AI use to systems governed by strict agreements, ensuring that any AI data processing involving personal data is not shared with other customers or third parties and is not used to train models outside the organisation's control, and remains within the control of Arbor Knot at all times.

14. Data Breach Notification Obligations

14.1. We are committed to protecting personal information and complying with applicable data protection laws in the jurisdictions where we operate. In the event of a data breach involving personal information, we will assess the nature and impact of the breach and, where required by law, notify the relevant authorities and affected individuals.

14.2. Depending on the applicable legal framework, our obligations may include:

(a) **Australia (Privacy Act 1988 & Notifiable Data Breaches Scheme)**: If a breach is likely to result in serious harm, we will notify the affected individuals and the Office of the Australian Information Commissioner (OAIC) as soon as practicable.

(b) **European Union (GDPR)**: We will notify the relevant supervisory authority within **72 hours** of becoming aware of a personal data breach, unless the breach is unlikely to result in a risk to individuals' rights and freedoms. If the breach poses a **high risk**, we will also notify affected individuals without undue delay

(c) **Israel (Protection of Privacy Law & Data Security Regulations)**: In the case of a **Severe Security Incident**, we will notify the **Israeli Privacy Protection Authority (PPA)** and, if required, the affected individuals. Notification may be required even when there is a concern about the existence of such an incident.

(d) **United States (Federal and State Laws)**: We will comply with applicable **state-specific breach notification laws**, which may require notifying affected residents and state Attorneys General.

14.3. We will provide all required information in our notifications, including the nature of the breach, the categories of affected data, potential consequences, and the measures taken to mitigate harm. Where permitted, we may issue public notices if individual notification is impracticable.

15. Your Rights

15.1. In this Section 15, we have summarised the rights that you have under the Privacy Laws. Some of the rights are complex, and not all of the details have been included in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.

15.2. The summary of your principal rights under Privacy Laws are:

(a) to request, at any time, for us to inform you of the personal data we hold about you;

(b) the right to access;

(c) the right to rectification;

(d) the right to erasure (where we have no legitimate right or business requirements to retain your personal data);

(e) the right to restrict or object to processing (where we have no legitimate right or business requirements to retain your personal data);

(f) the right to complain to a supervisory authority; and

(g) the right to withdraw your consent (where we have no legitimate right or business requirements to retain your personal data).

15.3. You have the right to confirmation as to whether or not we process your personal data and, where we do, access to the personal data, together with certain additional information. Providing the rights and freedoms of others are not affected, we will supply to you a copy of your personal data. The first copy will be provided free of charge, but additional copies may be subject to a reasonable fee.

15.4. You have the right to have any inaccurate personal data about you rectified and, taking into account the purposes of the processing, to have any incomplete personal data about you completed. If we refuse your request to correct your personal data, you also have the right to request that a statement be associated with your personal data noting that you disagree with its accuracy.

15.5. We may refuse to give you access to the personal data we hold about you if we reasonably believe that giving access would pose a serious threat to the life, health or safety of an individual, or to public health or safety, where giving access would be unlawful, where giving access would have an unreasonable impact on the privacy of other individuals, or if we consider the request to be frivolous or vexatious.

15.6. If we refuse to give you access to or to correct your personal data, we will give you a notice explaining our reasons except where it would be unreasonable to do so.

15.7. In some circumstances you have the right to the erasure of your personal data without undue delay. Those circumstances include:

(a) the personal data that is no longer necessary in relation to the purpose for which it was collected or otherwise processed;

(b) you object to the processing under certain rules of applicable Privacy Laws;

(c) the processing is for direct marketing purposes; and

(d) the personal data has been unlawfully processed.

15.8. However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary for us to provide any products or services to you, for compliance with our legal and regulatory obligations, attend to any complaints made by you or for the establishment, exercise or defence of legal claims.

15.9. You have the right to object to our processing of your personal data for direct marketing purposes (including profiling for direct marketing purposes). If you make such an objection, we will cease to process your personal data for this purpose.

15.10. Arbor Knot will not use for marketing purposes your Government related identifiers and identity documents and any results from checking your personal data with the document issuer or official record holder via a Document Verification Service (DVS) gateway service provider and third party systems for the purpose of confirming your identity.

16. Making a Privacy Complaint

16.1. If dissatisfied with how your personal data is handled, you can contact us. We can be reached on the contact details provided in Section 23 of this Policy.

16.2. Complaints can be addressed to the Complaints Officer via email or the complaints page on our website at www.arborknot.com

16.3. Upon receiving a complaint, we will confirm receipt and provide details of the person managing your complaint.

16.4. We will investigate and propose a fair resolution, potentially requesting additional information.

16.5. A final response will typically be provided within 30 days.

16.6. If dissatisfied with our resolution, you can escalate the complaint to the relevant regulatory body after allowing us the required 30-day period.

16.7. For Australian residents, the Office of the Australian Information Commissioner (**OAIC**) contact details are provided for below if you wish to lodge a privacy complain:

To:	Office of the Australian Information Commissioner
Phone:	1300 363 992
Email:	enquiries@oaic.gov.au
Website:	www.oaic.gov.au
Mail:	GPO Box 5218, Sydney NSW 2001

16.8. For Spanish residents, the Spanish Data Protection Authority (Agencia Española de Protección de Datos – AEPD) is the national regulator responsible for enforcing privacy laws in Spain, including the GDPR and Spain's Organic Law 3/2018.

Contact Details for Privacy Complaints

Address:
Calle Jorge Juan, 6
28001 Madrid, Spain

Phone:
+34 901 100 099
+34 91 266 35 17

Website: www.aepd.es

You can submit complaints directly through their website or contact them for guidance on how to proceed with a privacy-related issue.

16.9. For USA residents, you can lodge your complaint to your relevant data protection supervisory authority in the State that you reside in.

16.10. For Israeli residents, the Israeli Privacy Protection Authority (PPA), which handles privacy complaints and enforcement under the Privacy Protection Law:

Privacy Protection Authority (PPA) – Israel

Address: Tel Aviv Government Complex
P.O. BOX 33503
Tel Aviv 6133401, Israel

Phone:
*3103 (from within Israel)
+972 3-7634050 (international)

Email for general privacy complaints: ppa@justice.gov.il

Submit a complaint or inquiry via https://www.gov.il/en/pages/public_inquiries_ilita

17. Third-Party Websites

17.1. The website may contain hyperlinks to third-party websites. We are not responsible for the privacy policies or practices of these third parties.

18. About Cookies

18.1. Cookies are files stored by web browsers, enabling servers to recognize browsers during visits.

18.2. Cookies can be either persistent or session-based, with different durations and purposes.

18.3. While cookies do not typically identify users, personal data stored may be linked to cookie data.

18.4. When using our website, we may use either *persistent* cookies or *session* cookies. Cookies contain a sequence of numbers that our web server transmits to your web browser, for which it is then stored. Cookies don't typically contain any personal information about you – however, the personal information we hold about you may be linked to the information stored in and retrieved from cookies. Please refer to our Cookies Policy on our website for more information.

19. Cookies We Use

19.1. Cookies are used for various purposes, such as:

(a) authentication and session management;

(b) application state maintenance;

(c) personalisation;

(d) security;

(e) advertising relevance;

(f) performance analysis; and

(g) storing cookie preferences.

20. Cookies Used by Service Providers

20.1. Service providers may use cookies on our website.

20.2. Google Analytics gathers data on website use via cookies to generate reports.

20.3. Google AdSense may track user interests for tailored advertisements, with opt-out options provided.

21. Managing Cookies

21.1. Most browsers allow users to block or delete cookies, with links provided for browser-specific guidance.

21.2. Blocking cookies may negatively impact website usability.

21.3. Certain website features may not work if cookies are blocked.

22. Amendments

22.1. We may update this Policy periodically by publishing changes on our website.

22.2. Users are advised to review this Policy regularly for updates. It can be located on our website at www.arborknot.com

23. Our Details

23.1. The website is owned and operated by Arbor Knot under New South Wales, Australia laws.

23.2. Contact can be made in writing via the contact details on our website at www.arborknot.com, or via email to the Privacy Officer at info@arborknot.io or for Australian customers, please call on 1300 397 709 or for US customers, please call on +1 (507) 461 8535.

23.3. This Policy is Version 2.0, dated 23 July 2025.