Privacy Policy

Scope

This Data Privacy Policy sets out the requirements for ensuring that Armour Capital Private Limited (“ACPL”, “we”, “us”) collects, uses, retains, and discloses personal information in a fair, transparent, and secure manner.

This Data Privacy Policy applies to the personal information, including sensitive personal data or information, of:

- ACPL customers;
- users of ACPL’s website, mobile applications (if any), and social media accounts;
- employees and temporary staff;
- contractors;
- third-party vendors; and
- any other persons associated with ACPL in connection with business-related transactions or communications.

This Data Privacy Policy does not apply to independent data held by third parties. However, it shall continue to apply to:

- personal information collected or processed by third parties on behalf of ACPL; and
- personal information of third parties collected by ACPL.

By accessing or using this website or any services provided by ACPL, you agree to be bound by the terms stated herein, together with all terms incorporated by reference. If you do not agree to these terms, you must not use this website or the services provided by ACPL.

Objective

This Data Privacy Policy provides guidance on the collection, use, retention, storage, access, and disclosure of personal information by ACPL, as may be necessary from time to time.

ACPL is committed to respecting an individual’s privacy rights and expectations, and to protecting personal information collected by ACPL from unauthorized access, use, retention, storage, and disclosure. Compliance with this commitment is a primary management objective and a shared responsibility of all ACPL employees and all third parties conducting business with or on behalf of ACPL.

Responsibility for Compliance

The Data Privacy Policy set out in this document applies to information and information systems, including software, hardware, firmware, storage media, transmission media, and computer networks, collectively referred to as “Information Assets,” used by ACPL.

All ACPL employees, senior professionals, and third-party vendors, contractors, and other service providers shall ensure compliance with the obligations set out in this policy document. Compliance with this Data Privacy Policy shall be ensured by:

- all ACPL employees and temporary staff who have access to personal information in the course of their business activities;
- senior professionals, who are responsible for ensuring that appropriate privacy controls are implemented within their business functions; and

- third-party vendors, contractors, and outsourcing partners who perform services for or on behalf of ACPL and who are expected to follow standards of conduct consistent with the principles of this Data Privacy Policy.

Consequence Management and Non-Compliance

Any breach of this Data Privacy Policy may result in disciplinary action. The nature of the disciplinary action will depend on the nature and seriousness of the violation. Such violations shall be dealt with in accordance with the existing HR processes and may result in consequences ranging from a verbal reprimand to termination of employment or contract, and/or legal action.

Where a department or function is unable to comply with any requirement of this Data Privacy Policy, an exception must be obtained. Any such exception shall be documented, together with the reasons for the exception and the associated risks.

Policy Statement

All ACPL employees shall comply with the DPDP Act 2023 along with the DPDP rules 2025 and Indian Information Technology Act, 2000, including the IT Amendment Act, 2008 and the IT Rules, 2011, in relation to the privacy and protection of personal information and sensitive personal data or information of customers, employees, contractors, third-party vendors, and any other persons or entities associated with ACPL for any business-related transactions or communications, whether verbal or implied.

Key Data Privacy Principles

This Data Privacy Policy establishes the minimum standards adopted by ACPL in relation to data privacy. It is aligned with, and in certain cases exceeds, the requirements of applicable laws and regulations, including the DPDP Act 2023 and the DPDP rules 2025, the Indian IT Act, 2000, the IT Amendment Act, 2008, and the IT Rules, 2011.

Personal information means any information relating to a natural person which, either directly or indirectly, and either alone or together with other information available to ACPL or likely to be available to ACPL, can identify such person. Personal information includes sensitive personal data or information.

The personal information, including sensitive personal data or information, collected by ACPL may include:

- Name;
- PAN card number;
- driver’s licence number;
- bank account number;
- passport number;
- e-mail address;
- Aadhaar card details;
- account statement; and
- any other personal information, including sensitive personal data or information, received by ACPL for processing, or stored or processed by ACPL under a lawful contract or arrangement.

ACPL values the personal information entrusted to it and is committed to collecting, using, retaining, and disclosing such information in a fair, transparent, and secure manner by following the principles below.

Collection Limitation

Personal information shall be collected by fair, lawful, and transparent means. ACPL shall be transparent with individuals regarding how their personal information will be used, with whom it will be shared, and where it may be transferred.

Consent shall be obtained in writing or electronically from the provider of sensitive personal data or information before such information is collected, and the purpose of use shall be disclosed.

When collecting personal information directly from the concerned individual, ACPL shall take reasonable steps to ensure that the provider of the information is aware of the following:

- that personal information is being collected;
- the purpose for which it is being collected;
- the intended recipients of the information; and
- the name and address of the entities collecting and retaining the information.

The provider of information shall at any time, whether while availing the services or otherwise, have the option to withdraw the consent earlier given to ACPL. Such withdrawal shall be made in writing to ACPL at its communication address at 616-617, Anam -2 Ambli T Junction, Iscon Ambli Road, Ahmedabad, Gujarat - 380058, or by e-mail to grievance@armourcapital.in.

Where the provider of information withdraws his or her consent in relation to personal information, ACPL shall evaluate the request and take appropriate action. If an individual does not provide the required personal information, or later withdraws consent in relation to such information, ACPL may choose not to provide the services for which the information was sought. ACPL may retain certain data to comply with its obligations under applicable law.

Data Minimization

Only such personal information as is required for authorized business activities shall be collected from the provider of information. Personal information shall not be made available to any person, including internal staff, who is not authorized or does not have a business need to know such information.

Purpose of Collection

As required by regulation, ACPL collects personal information for purposes including KYC verification of customers. Bank account statements are collected to assess the customer's creditworthiness, and bank account details are collected for the collection of dues and repayment of loans. Personal information of employees is collected for purposes such as background verification, salary payment, insurance, and related employment requirements.

Use Limitation

Personal information shall be used only for the purpose for which it was collected. Privacy risks shall be considered before any collection, use, retention, or disclosure of personal information, including in connection with a new system or project.

Security

Adequate safeguards shall be maintained for personal information collected, used, retained, or disclosed in support of ACPL's business activities, through relevant usage, technical, organizational, and physical policies, standards, and processes.

ACPL has a comprehensive documented information security program and information security policies that include managerial, technical, operational, and physical security control measures.

However, ACPL shall not be responsible for any loss, unauthorized access, or harm caused to the information provider through misuse of his or her personal information, except where such loss, access, or harm is the direct and foreseeable result of ACPL's negligence and failure to comply with this policy. The information provider acknowledges that ACPL shall not be responsible, in particular, for any act of a third party or any act on the part of the information provider that results in loss, damage, or harm to such information provider or any other person.

Access, Correction, and Update

Processes shall be established to enable providers of information, upon request, to review the information they have provided and to ensure that any personal information or sensitive personal data or information found to be inaccurate or incomplete is corrected or amended, as feasible.

ACPL shall not be responsible for the authenticity of any personal information or sensitive personal data or information supplied by the provider of information. ACPL shall ensure that customer data is verified through document verification in accordance with the process laid down in the AML / KYC Policy.

To review, correct, or update their personal information, customers may write to us at grievance@ratnaafin.com or contact us at our communication address at 616-617, Anam -2 Ambli T Junction, Iscon Ambli Road, Ahmedabad, Gujarat - 380058.

Retention

Sensitive personal data or information shall be retained only for as long as necessary to support a specific business activity or to comply with any legal or regulatory requirement.

Disclosure

Personal information, including sensitive personal data or information, collected or stored by ACPL may be disclosed where required to comply with applicable law, directions issued by Government agencies empowered under law for the prevention and investigation of offences, or pursuant to an order of a competent court.

Transfer of Personal Information to Third Parties

Appropriate protection mechanisms shall be provided for personal information where such information is transferred outside ACPL's network.

ACPL may transfer sensitive personal data or information to any entity or person located in India or in any other country that provides the same level of data protection as that followed by ACPL under the DPDP Rules 2025 and IT Rules, 2011. Such transfer shall be permitted only where it is necessary for the performance of a lawful contract entered into between

ACPL, or any person acting on its behalf, and the information provider, or where the information provider has consented to such transfer.

Personal information, including sensitive personal data or information, may be disclosed or transferred to insurers, credit bureaus, verification agencies, collection partners, regulatory and legal authorities, including credit information agencies, law enforcement agencies, and judicial agencies, as well as affiliates and business partners.

Reasonable due diligence shall be conducted to ensure that the third party has adequate security and privacy controls in place before any personal information, including sensitive personal data or information, is shared.

Marketing and Promotional Activities

Marketing and promotional communications shall be sent to providers of information or customers only after obtaining the required consent, in accordance with obligations under applicable law.

Grievance Officer

Any grievance or discrepancy raised by the provider of information regarding the processing of personal information shall be addressed in a time-bound manner by the designated Grievance Officer.

Customers may write to us at grievance@ratnaafin.com or contact us at the communication address at 616-617, Anam -2 Ambli T Junction, Iscon Ambli Road, Ahmedabad, Gujarat - 380058.

Grievance Officer Details: Mr. Harshit Maniyar
Communication Address: 616-617, Anam -2 Ambli T Junction, Iscon Ambli Road, Ahmedabad, Gujarat - 380058
Email: grievance@armourcapital.in

Third Party Websites and Services

ACPL's website and services may contain links to third-party services and may enable users to access third-party websites, products, and services. Customers or borrowers access and use such third-party websites or services entirely at their own risk. ACPL shall not be liable for any outcome, loss, or harm arising from such use of third-party websites or services. Users are advised to review the privacy policies of any third party before using its websites, products, or services.

Changes to this Data Privacy Policy

ACPL may revise or update this Data Privacy Policy from time to time. Continued use of ACPL's website and/or services after the effective date of the revised Data Privacy Policy shall constitute acceptance of the revised policy. If the user does not agree with any revised terms, the user should refrain from using ACPL's website and/or services.