



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

DATA PRIVACY & PERSONAL DATA PROTECTION POLICY

Document Classification	Public
Document Owner	Infini Systems Limited (Formerly Known As Infini Systems Private Limited)
Approved By	Board of Directors
Version	1.0
Effective Date	01.08.2026
Review Frequency	At least annually or upon material regulatory, legal, technological or business change

1. PURPOSE

Infini is committed to protecting the privacy, confidentiality, integrity and security of information entrusted to it by customers, regulated entities, lending partners, financial institutions, business partners and other stakeholders.

This Data Privacy & Personal Data Protection Policy ("Policy") establishes the principles and practices governing the collection, access, processing, use, transmission, storage, retention and deletion of personal data, credit information and other confidential information processed by Infini in connection with its products and services.

Where Infini provides technology, verification, assessment, AML, PEP, KYC, compliance, analytics or related services to a bank, NBFC, financial institution or other regulated entity ("RE"), Infini generally processes information on behalf of and under the instructions of the relevant RE, subject to applicable law, regulatory requirements and/or contractual obligations/rights.

2. SCOPE

This Policy applies to:

- Personal data, credit information and confidential information processed through Infini's services;
- Information received from or on behalf of regulated entities, lending partners, customers and business partners; and
- Information processed for verification, assessment, KYC, AML, PEP, sanctions, compliance and related use cases.

3. REGULATORY AND LEGAL FRAMEWORK

Infini shall comply with applicable privacy, data protection, information security, cybersecurity and sector-specific laws, regulations and regulatory directions applicable to its business and contractual engagements.



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

Depending on the nature of the service and the relevant regulated entity, this may include:

- Digital Personal Data Protection Act, 2023;
- Digital Personal Data Protection Rules, 2025, as and when applicable;
- Information Technology Act, 2000 and applicable rules;
- applicable Reserve Bank of India ("RBI") directions and circulars;
- applicable SEBI, IRDAI, PFRDA, NPCI, UIDAI, PMLA and other regulatory requirements, where relevant;
- applicable credit information and credit reporting requirements;
- applicable cybersecurity and outsourcing requirements;
- contractual requirements imposed by regulated entities; and
- other applicable laws, regulatory directions, notifications and binding instructions.

4. DEFINITIONS

4.1 Personal Data

"Personal Data" means data relating to an identifiable individual, as defined under applicable data protection law.

4.2 Data Principal

The individual to whom personal data relates.

4.3 Regulated Entity / RE

A bank, NBFC, financial institution, insurer, payment entity or other entity regulated by a competent regulatory authority.

4.4 Customer Information

Information relating to an individual or entity that is received or processed in connection with the provision of Infini's services.

4.5 Credit Information

Information relating to an individual's or entity's credit history, creditworthiness, financial obligations, credit facilities, repayment behaviour or other information obtained from a credit information company, lending partner, regulated entity or other authorised source.

4.6 Processing

Any operation performed on information, including collection, recording, structuring, alteration, retrieval, validation, matching, analysis, transformation, transmission, use, storage, deletion or destruction.

4.7 Audit Logs

System-generated records relating to access, processing, transactions, system activity, administrative actions, security events and other activities maintained for security, audit, regulatory or operational purposes.



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

5. INFINI'S DATA PROCESSING MODEL

5.1 No Permanent Customer Data Repository

Infini does **not ordinarily maintain a permanent repository of customer information or customer documents** received for limited verification, assessment or related processing.

Information required to perform a particular service is processed only for the authorised purpose and for the period necessary to complete such processing.

Certain information may, however, be processed or retained where necessary to:

- execute the contracted service;
- maintain system security and integrity;
- comply with applicable law or regulatory requirements;
- maintain audit records;
- investigate a security or operational incident;
- comply with a lawful instruction from an RE or Data Principal;
- support a specific use case expressly authorised by the relevant RE;
- develop, test, improve or maintain Infini's products, services, systems, models, algorithms and technology;
- conduct analytics, quality assurance, service optimisation, benchmarking, research and development;
- prevent, detect and investigate fraud, misuse, security incidents and other unauthorised or unlawful activities;
- generate aggregated, statistical, anonymised or de-identified information for lawful business, analytical, operational or product development purposes; and/or
- support other lawful business or operational purposes permitted under applicable law.

5.2 Transient Processing

For verification and assessment services, the typical processing lifecycle is:

Receive → Process → Verify/Assess → Generate Output → Return Output → Purge Temporary Data

Information/documents received from the relevant RE or authorised source may be temporarily held within Infini's controlled processing environment, including transient memory or temporary processing infrastructure such as Redis, solely for the duration required to complete the authorised processing activity.

Following completion of the relevant processing and delivery of the output to the authorised recipient, temporary processing information shall be deleted, purged or otherwise rendered inaccessible in accordance with applicable system configurations, contractual requirements and retention obligations.

6. PURPOSE & LIMITATION

Infini shall process information for:

- the purpose for which the information has been provided;
- purposes authorised by the relevant RE or customer;



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

-
- purposes necessary to provide contracted services;
 - purposes required under applicable law or regulatory directions;
 - authorised KYC, AML, PEP, sanctions, fraud-risk or compliance activities;
 - information-security and operational-integrity purposes;
 - audit and regulatory compliance;
 - product, service and technology development and improvement;
 - analytics, quality assurance, service optimisation and benchmarking;
 - fraud prevention, risk management and information-security purposes;
 - research and development, including development, testing and validation of models, algorithms, rules and other technological capabilities;
 - generation and use of aggregated, statistical, anonymised or de-identified information; or
 - other lawful purposes that are reasonably necessary or incidental to Infini's business and permitted under applicable law.

Infini may generate and use information derived from the operation and use of its products and services, including verification results, match results, system-generated identifiers, technical metadata, performance information, risk indicators, analytical outputs and other information generated through Infini's systems, for providing, securing, maintaining, improving and developing its products and services and for other lawful purposes, subject to applicable law, regulatory requirements and contractual obligations.

Where Infini processes information on behalf of an RE or customer, such processing shall remain subject to the authorised purposes and instructions applicable to Infini's role as a technology or processing service provider.

7. CREDIT INFORMATION

As part of its services, **credit information, where applicable, collected or accessed by Infini shall be used and processed only for the purposes for which such information is obtained.**

Such purposes may include:

- facilitating credit assessment;
- supporting underwriting and credit decisioning;
- verification and assessment;
- services requested by or through customers;
- services requested by or on behalf of a lending partner or regulated entity;
- risk or compliance assessment where authorised; and/or
- such other purposes as may be permitted by the relevant source, lending partner, regulated entity, customer or applicable law.

Credit information may be shared with:

- the relevant customer;
- the relevant lending partner;
- the relevant regulated entity;
- authorised service providers;
- within its organisation;



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

-
- authorised personnel/representatives;
 - regulatory or governmental authorities where legally required; and/or
 - other persons where permitted or required under applicable law or regulatory directions.

Infini shall take appropriate measures to ensure that access to credit information within its organisation is restricted to authorised personnel and is provided only for legitimate and permitted purposes.

Infini does not share credit information with its group companies, subsidiaries, or affiliates, except where explicitly permitted by these terms or where required or permitted under applicable law or regulatory direction. No unauthorized access to credit information is permitted by us, and access is strictly limited for the specified purpose for which such information was collected.

8. ACCESS CONTROL

Access to personal data and credit information shall be restricted based on:

- role and responsibility;
- legitimate business requirement;
- authorised processing purpose;
- role-based access controls;
- contractual requirements; and/or
- applicable legal and regulatory requirements.

9. GROUP COMPANIES, SUBSIDIARIES AND AFFILIATES

Infini shall maintain appropriate safeguards to prevent unauthorised access to credit information by its group companies, subsidiaries or affiliate entities.

Information may be shared with such entities only where:

- there is a legitimate and documented business purpose;
- for processing such information for Infini;
- for purpose of providing service;
- such sharing is authorised;
- applicable law permits the sharing;
- appropriate contractual and confidentiality protections are in place, where applicable; or
- the sharing is consistent with the requirements of the relevant RE.

10. AML, PEP AND OTHER COMPLIANCE USE CASES

For specific use cases such as:

- Anti-Money Laundering ("AML");
- Countering Financing of Terrorism ("CFT");
- Politically Exposed Person ("PEP") screening;
- sanctions screening;
- adverse-media screening;
- transaction monitoring;
- customer due diligence;



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

-
- enhanced due diligence; and
 - other regulatory compliance monitoring,

the underlying customer and case data may remain hosted within the infrastructure or designated data environment of the relevant regulated entity.

In such cases, Infini operates primarily as a **technology and processing service provider**, processing cases in accordance with the instructions and requirements of the relevant RE.

Where case information is temporarily processed within Infini's environment, it shall be subject to appropriate access controls, security measures and retention/purge controls.

Once the relevant RE has completed its processing and taken the final dataset into its designated EDMS or other authorised repository, Infini shall purge the corresponding temporary data in accordance with the agreed retention and deletion requirements.

11. DATA MINIMISATION

Infini shall, where practicable:

- minimise the volume of information processed;
- avoid retaining documents after completion of the authorised purpose;
- restrict access to information to authorised users and systems; and
- implement automated or controlled deletion wherever technically feasible.

12. DATA STORAGE

Infini distinguishes between different categories of information based on their purpose and retention requirements.

12.1 Transient Processing Data

Data temporarily required to execute a verification, assessment or other authorised service.

Such data shall be:

- processed within controlled environments;
- protected through appropriate security controls;
- accessible only to authorised systems and personnel; and
- purged following completion of the relevant processing or applicable retention period.

12.2 Regulated Entity Data

Where the relevant customer or case data is hosted within the RE's environment, Infini shall process such data according to the RE's authorised instructions and applicable contractual and regulatory requirements.

12.3 Audit and Security Logs

Infini may retain audit, security and operational logs where required for:

- regulatory compliance;
- cybersecurity;
- incident investigation;



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

-
- operational monitoring;
 - user accountability;
 - audit;
 - fraud prevention;
 - contractual obligations; or
 - legal requirements.

Such logs shall be protected against unauthorised access or illegal use.

12.4 Aggregated and De-Identified Information

Infini may create, maintain and use aggregated, statistical, anonymised or de-identified information derived from information processed through its services for analytics, benchmarking, research, product and service improvement, fraud and risk analysis, business intelligence and other lawful purposes.

Where such information is no longer capable of identifying a Data Principal, Infini may retain such information notwithstanding the deletion or purge of the underlying personal data, subject to applicable law and contractual requirements.

13. DATA RETENTION

Infini shall not retain customer information merely because it is technically possible to do so.

Temporary processing data shall be purged following completion of the authorised processing activity, subject to applicable legal, regulatory, contractual, security or audit requirements.

Longer retention may apply where:

- applicable law requires it;
- a regulatory authority requires it;
- the relevant RE instructs or authorises such retention;
- an investigation or audit requires preservation;
- litigation or a legal hold applies;
- a security investigation is ongoing; or
- retention is necessary to satisfy a specific regulatory or contractual requirement.

14. DATA DELETION AND PURGING

When information is no longer required for the authorised purpose or applicable retention requirement, Infini shall securely delete, purge or otherwise render such information inaccessible.

Depending on the applicable technology, deletion may include:

- logical deletion;
- secure purge;
- expiry of temporary memory;
- deletion of temporary files;
- deletion of cached information;
- removal of temporary database records;
- cryptographic destruction, where applicable; or
- other technically appropriate deletion mechanisms.



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

Backup and disaster-recovery data shall be managed in accordance with Infini's applicable backup and retention procedures.

15. LEGAL HOLD

Information that would otherwise be deleted may be preserved where necessary to comply with:

- legal proceedings;
- regulatory investigations;
- law-enforcement requirements;
- litigation;
- audits;
- security investigations;
- contractual disputes; or
- other legally valid preservation requirements.

16. INFORMATION SECURITY

Infini shall maintain appropriate technical and organisational measures designed to protect information against:

- unauthorised access;
- unauthorised disclosure;
- accidental loss;
- alteration;
- destruction;
- misuse;
- data leakage;
- cyberattacks; and
- other reasonably foreseeable security threats.

Depending on the applicable service and risk profile, controls may include:

- encryption;
- access control;
- authentication;
- role-based access;
- privileged-access management;
- network security;
- secure application development;
- vulnerability management;
- logging and monitoring;
- endpoint protection;
- incident response;
- backup and recovery;
- secure configuration management; and
- periodic security assessments.



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

17. THIRD-PARTY SERVICE PROVIDERS

Where Infini engages third-party service providers to support its services, Infini shall undertake appropriate due diligence proportionate to the nature and risk of the service.

Infini shall ensure that third-party processing does not result in use of customer information beyond the authorised purpose.

18. DATA SHARING AND DISCLOSURE

Infini shall not, in an illegal or unauthorised manner, sell, rent or commercially monetise personal data or credit information. For avoidance of doubt, the provision of data-enabled, verification, assessment, analytics, compliance, risk or other services by Infini for consideration shall not, by itself, constitute a sale or unauthorised commercialisation of personal data or credit information.

Information may be used or shared where:

1. required to provide the contracted service;
2. required for the purpose for which the information has been provided;
3. required under applicable law or regulatory directions;
4. required for authorised KYC, AML, PEP, sanctions, fraud-risk or compliance activities;
5. required for information-security and operational-integrity purposes;
6. required for audit and regulatory compliance;
7. authorised by the relevant RE or customer;
8. required under applicable law;
9. required by a competent regulatory or governmental authority;
10. necessary for authorised security, fraud-prevention or compliance activities; or
11. otherwise permitted under applicable law.

Information will be shared with:

1. infrastructure providers;
2. within its organisation;
3. affiliates and group companies;
4. authorised personnel/representatives;
5. auditors;
6. professional advisors;
7. authorities;
8. the relevant customer;
9. the relevant lending partner;
10. the relevant regulated entity;
11. authorised service providers;
12. regulatory or governmental authorities where legally required; and/or
13. other persons where permitted or required under applicable law or regulatory directions.



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

19. DATA PRINCIPAL RIGHTS

To the extent applicable to Infini's role and under applicable law, Infini shall support the relevant RE or data fiduciary in responding to lawful requests relating to personal data.

Such rights may include, as applicable:

- access to information;
- correction;
- updating;
- erasure;
- withdrawal of consent;
- grievance redressal; and
- other rights available under applicable law.

Where Infini processes information solely on behalf of an RE, requests relating to the individual's underlying customer relationship may appropriately be handled by the relevant RE and provide instructions to Infini to implement such request, provided it is in compliance with applicable laws.

20. CONSENT AND LAWFUL PROCESSING

Where consent is the applicable basis for processing, Infini shall process information in accordance with the relevant consent and instructions provided by the authorised data fiduciary or RE.

Infini shall not independently repurpose personal data beyond the authorised processing purpose.

Where processing is required or permitted under applicable law, regulation, contract or another legally recognised basis, Infini shall process such information only to the extent permitted by applicable requirements.

21. DATA ACCURACY AND INTEGRITY

Infini shall take reasonable measures, within the scope of its role and contracted services, to maintain the integrity of information processed through its systems.

Where information is provided by an RE, lending partner, customer, credit information company or other authorised source, the source shall remain responsible for the accuracy and completeness of the information provided.

22. CROSS-BORDER PROCESSING

Any cross-border processing or transfer of personal data, financial information or other regulated information shall be undertaken only where permitted by applicable law.

Where a regulated entity imposes specific data-localisation or geographic-storage requirements, Infini shall comply with such requirements applicable to the relevant service, consistent with applicable law.

23. DATA BREACH AND SECURITY INCIDENT MANAGEMENT

Infini shall maintain an information-security incident management process for identifying, containing, investigating, remediating and documenting security incidents and personal-data breaches caused by it.



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

Where an incident affects information processed on behalf of an RE, Infini shall notify and cooperate with the relevant RE in accordance with:

- applicable contractual requirements;
- agreed incident-response procedures;
- applicable regulatory requirements; and
- applicable law.

Infini shall provide reasonable support to the relevant RE, where required, in investigation, containment, remediation and regulatory reporting.

24. AUDIT, LOGGING AND MONITORING

Infini may maintain appropriate audit trails and system logs to evidence:

- system access;
- administrative activity;
- processing activity;
- security events;
- system and configuration changes;
- data transfers;
- deletion or purge activities; and
- other activities required for security, audit or regulatory purposes.

Audit and security logs shall be retained for the period required by applicable law, regulatory requirements, contractual obligations or Infini's information-security requirements.

Infini's principal persistent data footprint is therefore intended to comprise operational, security and audit records rather than customer-document or customer-data repositories.

25. INFINI DATA AND INTELLECTUAL PROPERTY

Infini shall retain all rights, title and interest in and to its products, services, systems, software, technology, methodologies, models, algorithms, processes, tools, know-how, system-generated information, analytical outputs and other materials developed or owned by Infini, including any improvements, modifications or derivatives thereof, and in any information, data, datasets or other materials independently obtained, collected, generated or developed by Infini from lawful and authorised sources.

No customer, Data Principal, CIC, RE or other third party shall claim, restrict or interfere with Infini's use of such independently obtained, collected, generated or developed information, data, datasets or other materials where such person does not have any ownership or other legally enforceable rights in or to such information or data.

Nothing in this Policy shall transfer to any customer, Data Principal or other person any intellectual property rights of Infini in its products, services, systems, technology, methodologies or other proprietary materials.



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

26. EMPLOYEE CONFIDENTIALITY

Employees, contractors and authorised personnel who have access to personal data, credit information or confidential information shall be subject to appropriate confidentiality obligations.

Infini shall provide appropriate privacy and information-security awareness to relevant personnel.

27. ROLE OF THE REGULATED ENTITY

Where Infini operates as a technology or processing service provider for a regulated entity, the RE may determine, subject to applicable law, in respect of customer information provided by it:

- the purpose of processing;
- the categories of information to be processed;
- the applicable legal basis;
- customer notices and consent requirements;
- applicable retention obligations;
- final disposition of customer information; and
- processing instructions provided to Infini.

Infini shall process information within the scope of its contractual services and authorised instructions, subject to applicable law.

28. GOVERNANCE AND POLICY REVIEW

This Policy shall be reviewed periodically and whenever there is a material:

- regulatory or legislative change;
- change in technology architecture;
- change in processing activities;
- change in the nature of information processed;
- change in contractual requirements;
- significant cybersecurity incident; or
- change in Infini's operating model.

Material changes shall be reviewed and approved through Infini's applicable governance framework.

29. POLICY EXCEPTIONS

Any exception to this Policy shall be:

- documented;
- supported by a legitimate business or operational justification;
- subject to privacy and security risk assessment;
- subject to appropriate compensating controls;
- approved by the designated authority;
- assigned an appropriate review or expiry date; and
- in compliance with applicable law.

No exception shall override a mandatory legal or regulatory requirement.



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

30. PRIVACY AND GRIEVANCE CONTACT

For privacy-related queries, requests or concerns relating to information processed by Infini, individuals or authorised representatives may contact:

Data Privacy / Grievance Officer: Ashay Wakle

Email: support@infinisystem.com

Address: Global One, 2nd Floor, Office 1, CTS NO 252 252 1, OPP SBI, LBS MARG, KURLA(W), Mumbai Maharashtra, India, 400070

Where Infini processes information exclusively on behalf of a regulated entity, the individual may also be directed to the relevant RE, depending upon the nature of the request and the respective roles and responsibilities of Infini and the RE.

Document Control

Item	Details
Document	Data Privacy & Personal Data Protection Policy
Organisation	Infini Systems Limited (Formerly Known As Infini Systems Private Limited)
Version	1.0
Classification	Public
Policy Owner	INFINI SYSTEMS LIMITED
Approved By	Shubhram Singh Rathore
Effective Date	01.08.2026
Next Review Date	01.08.2027