Girikon Solutions Private Limited

(Subsidiaries of Girikon, Inc)

(www.girikon.com)

Version 1.9 Dated 4th April, 2025

DATA PRIVACY & PROTECTION POLICY

Document Version Control

Document Controller

Date	Document Released By	Version	Change Reference
11th April, 2018	*Mr. Sanatan Dey, Operations Manager*	*1.1*	*First release, document has been created*
24th Feb, 2019	*Mr. Sanatan Dey, Operations Manager*	*1.2*	*Second release, no changes required*
15th Jan, 2020	*Mr. Sanatan Dey, Operations Manager*	*1.3*	*Third release, no changes required*
18th Jan, 2021	*Mr. Sanatan Dey, Operations Manager*	*1.4*	*Fourth release, no changes required*
28nd March, 2022	*Mr. Sanatan Dey, Operations Manager*	*1.5*	*Fifth release, no changes required*
20th April, 2023	*Mr. Sanatan Dey, Operations Manager*	*1.6*	*Sixth release, no changes required.*
10th April, 2024	*Mr.* Sanatan Dey, Director - Delivery & Compliance	*1.7*	*Seventh release, Designation changes for Sanatan Dey, Awanish Shukla, Rajni Sharma Nath, Ravi Verma, Yoginder Singh & Shailendra Jha*
27th August, 2024	*Mr. Sanatan Dey, Director - Delivery & Compliance*	*1.8*	*Eight release, one pointer has been added under the heading of "Sensitive Personal Data "*
4th April, 2025	*Mr. Sanatan Dey, Director - Delivery & Compliance*	*1.9*	*Nineth release, Designation changes for Ravi Verma*

Reviewers

Name	Position	Role
Ms. Kalpana Singh	HR Manager	Human Resource Security
Mr. Ravi Shankar Verma	IT Manager	IT Infrastructure
Mr. Shailendra Jha	Finance Manager	Physical & Environment security & Security in supplier delivered services
Mr. Yonder Singh	Business Development-Head	Information Security in Customer Relationship
Mr. Awanish Shukla	Director - Solutions Architecture	Project Management
Ms. Rajni Sharma Nath	Director Delivery	Software Development & Support
Mr. Sanatan Dey	Director - Delivery & Compliance	Incident Management & Business Continuity& Compliances & Project Management
Mr. Ashok Anibha	CEO	ISMS Policy, Risk management, Security organization & Compliances

Approver(s)

Name	Position	Organization
Mr. Ashok Anibha	CEO	Girikon Solutions Private Limited

Authorized Users

S. No	Authorized users	Location
1	*All Employees (Permanent, Probation & Contractual)*	*India & US*

Contents

Policy Statement

The objective of this Policy is to cultivate organization-wide privacy culture to protect the rights and privacy of individuals & Customer data; to comply with applicable privacy and data protection legislations by implementing privacy principles and controls in cooperation with the Information Security Management System.
All employees should adhere and comply with this Policy and additionally, specific privacy practices that may be adopted by Girikon.

Overview

It is Girikon' s policy to comply with the privacy legislation within each jurisdiction in which aGirikon entity operates. The privacy legislation and/or an individual's right to privacy are different from one jurisdiction to another. Specific privacy practices may be adopted by Girikon to address the privacy requirements of particular jurisdictions (for e.g. HIPAA, GDPR, etc.).

This Privacy Policy of Girikon ("Policy") sets out the rules and procedures relating to the processing of Personal Data & Customer Data.

Girikon' s commitment to establishing and maintaining high standards across all the officesof Girikon for the transfer and processing of Personal Data & Customer Data. Girikon entities in India & USA are committed to adhere to the Privacy & Protection policy set by the Organization.

In addition, Girikon is implementing a global security and cyber security program to align security practices within the entire Group through the mandatory implementation of security baselines across all its business organizations.

Definitions

Personal Data means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

Processing refers to any action performed on Personal Data, such as collecting, recording, organizing, storing, transferring, modifying, using, disclosing, uploading or deleting.

Sensitive Personal Data of a person, under the Indian Information Technology Rules 2011, means such Personal Data which consists of information relating to:

- Password.
- Financial Information such as bank account or credit card or debit card or other payment instrument details;
- Physical, physiological and mental health condition;
- Sexual orientation;
- Medical records and history;
- Biometric Information;
- Any other details relating to the above mentioned, provided by any person to Girikon for providing services;
- Any Information received pursuant to the above mentioned by Girikon for processing, or storing such Information under a lawful contract or otherwise.
- Provided that any Information that is freely available or accessible in public domain or furnished under the Right to Information Act 2005 or any other law for the time being in force will not be considered to be Sensitive Personal Data.
- No mobile information will be sold or shared with third parties for promotional or marketing purposes.

"Employee" means a Girikon current or former employee. As far as it applies to Employees, the Policy covers all stages of the employment cycle including recruitment and selection, promotion, evaluation and training.

"Relevant Individual" means an Employee, contractor and/or any other third party working on Girikon' s behalf and job applicants.

"**Employee**" means a Girikon current or former employee. As far as it applies to Employees, the Policy covers all stages of the employment cycle including recruitment and selection, promotion, evaluation and training.

"**Relevant Individual"** means an Employee, contractor and/or any other third party

working on Girikon' s behalf and job applicants.

"**Customer data** "means Client information and system entrusted to Girikon as a part of client specific projects and outsourcing arrangements as well as when client is using platforms and services that Girikon operates across multiple clients.

Scope of Coverage

This Policy is applicable to all Personal Data & Customer Data collected, received, possessed, owned, controlled, stored, dealt with or handled by Girikon in respect of a Relevant Individual.

Personal Data and Customer Information that Girikon handles for its clients in the context of providing consulting, technology and outsourcing services shall be processed according to the contractual provisions, specific privacy practices agreed upon with each client and by this policy as a guideline, as applicable. This Policy lays emphasis on the obligations of the Relevant Individuals dealing with Data in the course of performance of their duties.

Collection of Personal Data by Girikon

Throughout the course of the relationship with the Relevant Individual, Girikon needs to collect Personal & Customer Data. The type of Information that may be collected includes (but is not limited to), where relevant:

- Basic Information regarding the Relevant Individuals such as name, contact details, address, gender, birth date, marital status, children, parents details, dependent details, photos, photo id proof, pan card, passport, voter ID, Aadhar card, life insurance nominees/beneficiaries, fingerprint information, emergency contact details, citizenship, visa, work permit details;
- Recruitment, engagement or training records including cv's, applications, notes of interview, applicant references, qualifications, education records, test results (as applicable);
- Information about the Relevant Individual's medical condition – health and sickness records;
- The terms and conditions of employment/engagement, employment contracts with Girikon and/or previous employer;
- Performance, conduct and disciplinary records within Girikon and/or with previous employers; mobility records generated in the course of employment/work with

Girikon;

- Information relating to the Relevant Individual's membership with professional associations or trade unions;
- Leave records (including annual leave, sick leave and maternity leave);
- Financial Information relating to compensation, bonus, pension and benefits, salary, travel expenses, stock options, stock purchase plans, tax rates, taxation, bank account, provident fund account details;
- Information captured as result of monitoring of Girikon assets, equipment, network owned and/ or provided by Girikon;
- Any other Information as required by Girikon.
- Any customer Data received from customer for the purpose of delivering the project.

A. Purposes of collection and processing of Data

Girikon may collect, process and disclose Personal Data of the Relevant Individual for purposes connected with its business activities including the following purposes, hereinafter the "Agreed Purposes":

- Managing the Relevant Individual's employment/ work with Girikon including deployment/assignment of the individual to specific client projects;
- Record-keeping purposes; Payroll Administration, Payment of the Relevant Individual's salary or invoice; Performance Assessment and Training;
- Compliance with a legal requirement/obligation; health and safety rules and other legal obligations; Administration of benefits, including insurance, provident fund, pension plans; immigration, visa related purposes; Girikon Group reporting purposes;
- Back ground verification purposes; credit and security checks;
- Operational issues such as promotions, disciplinary activities, grievance procedure handling;
- Audits, investigations, analysis and statistics, for example of various recruitment and employee retention programs;
- IT, Security, Cyber security and Access Controls;
- Disaster recovery plan, crisis management, internal and external communications;
- For any other purposes as Girikon may deem necessary.

Girikon only collects uses and discloses Personal Data for purposes that are reasonable and legitimate. Such Personal Data shall be processed in a manner compatible with the Agreed Purposes; unless the Relevant Individuals have consented to it being processed for a different purpose or the use for a different purpose is permitted by applicable law. There may be circumstances, when the Relevant Individual may have volunteered personal information and given explicit/fully informed consent to its processing (for example by submission of a CV).

B. Limited Access to Data

Only those Employees who "need-to-know" or require access to function in their role should have access to Personal Data. Girikon will not disclose Personal Data to any person outside Girikon except for the Agreed Purposes, or with the Relevant Individuals' consent, or with a legitimate interest or legal reason for doing so, such as where Girikon reasonably considers it necessary to do so and where it is permitted by applicable law. In each instance, the disclosed Personal Data will be strictly limited to what is necessary and reasonable to carry out the Agreed Purposes.

When Girikon works with third parties which may have access to Personal Data in the course of providing their services, Girikon contractually requires third party to process Personal Data only on Girikon's instructions and consistent with Girikon's Data Privacy policies and Data Protection laws.

Disclosure and Transfer of Personal Data

Girikon may, from time to time, disclose and/or transfer the Relevant Individuals' Personal Data to third parties (including but not limited) listed below:

- Group Companies, affiliate companies and/or other business associates, Girikon's insurers and banks;
- External and internal auditors;
- Medical practitioners appointed by Girikon;
- Administrator of Girikon's mandatory provident fund scheme;
- Third parties who are involved in a merger, acquisition or due diligence exercise associated with Girikon;
- External companies or third-party service providers Girikon engages to perform Services on the Company's behalf;

- Third Parties providing certain information technology and data processing services to enable business operations;
- The applicable regulators, governmental bodies, tax authorities or other industry recognized bodies as required by any applicable law or guidelines of any applicable jurisdiction; and
- To any other party as deemed necessary by Girikon.

Notwithstanding anything contained elsewhere, any Personal or Sensitive Personal Data may be disclosed by Girikon to any third party as required by a Court of Law or any other regulatory or any other law enforcement agency established under a statute, as per the prevailing law without the Relevant Individual's consent.

As Girikon operating internationally, it may transfer Personal Data for the Agreed Purposes described above to its own operations, or to other subsidiaries or affiliated companies located in other jurisdictions. Such transfer is justified on the basis that there is a "need-to-know" and it is reasonable and legitimate to allow Girikon companies and businesses to operate effectively and competitively. Personal information is only transferred to another country, including within the Girikon office, in particular only in as far as a reasonable level of data protection is assured in the recipient country

When using external data processers or transferring personal data to external third parties, Girikon shall enter into agreements with appropriate contractual clauses for protection of Personal Data and confidentiality including requirements to process the Personal Data only in accordance with instructions from Girikon and to take appropriate technical and organizational measures to ensure that there is no unauthorized or unlawful processing or accidental loss or destruction of or damage to Personal Data.

Retention and Deletion of Data

It is Girikon's policy to retain certain Personal Data of the Relevant Individuals when they cease to be employed/ engaged by Girikon. This Personal Data may be required for Girikon's legal and business purposes, including any residual activities relating to the employment/engagement, including for example, provision of references, processing of applications for re-employment/re-engagement, matters relating to retirement benefits (if applicable) and allowing Girikon to fulfil any of its contractual or statutory obligations.

All Personal Data of the Relevant Individuals may be retained for periods as prescribed under law or as per Girikon policy from the date the Relevant Individuals cease to be employed/engaged by Girikon. The Personal Data may be retained for a longer period if there is a subsisting reason that obliges Girikon to do so, or the Personal Data is necessary for Girikon to fulfil contractual or legal obligations. Once Girikon no longer requires the Personal Data, it is destroyed appropriately and securely or anonymized in accordance with the law.

Security of Personal Data

Girikon takes reasonable security measures to protect Personal Data against loss, misuse, unauthorized or accidental access, disclosure, alteration and destruction. Girikon has implemented policies and maintains appropriate technical, physical, and organizational measures and follows industry practices and standards in adopting procedures and implementing systems designed for securing and protecting Personal Data from unauthorized access, improper use, disclosure and alteration.

Accuracy of Personal Data

Girikon aims to keep all Personal Data as accurate, correct, up-to-date, reliable and complete as possible. However, the accuracy depends to a large extent on the data the Relevant Individuals provide. An Individual may access much of his Personal Information online using various "self-service" HR applications deployed in Girikon. As such, Relevant Individuals must, agree to:

- Provide Girikon with accurate, not misleading, updated and complete Personal Data of the Relevant Individuals and/or any relevant person (including their consents to such disclosures to Girikon); and
- Up-date Girikon as and when such Personal Data provided earlier becomes incorrect or out of date, by providing new details.

Monitoring of Relevant Individuals' use of company network resources

Girikon may, from time to time, monitor the Relevant Individual's use of company premises, property and network resources (including computer systems, e-mails, phone calls, and internet) primarily for following purposes:

(i) facilitating business, securing personnel and property of Girikon; For example, some of the locations are equipped with surveillance cameras

(ii) maintaining a stable network environment for communications withinGirikon, and communications with external parties;

(iii) responding to any legal processes or to investigate any suspected breachof Relevant Individual's obligations under this Policy or other Girikon'spolicies or applicable law; and

(iv) providing information to the Girikon's management to ensure the properutilization of Girikon's resources.

This section is not meant to suggest that all employees will in fact be monitored or their actions subject to constant surveillance. It is meant to notify the fact that monitoring mayoccur and may result in the collection of personal information (e.g. through the use of company network resources). When using company equipment or resources, employees should not have any expectation of privacy with respect to their use of such equipment orresources.

Customer Data

Girikon does not store any customer data. For data migration purposes, we recommend that customers provide remote access to a secure cloud environment, such as an AWS server. Customer data will be processed and stored strictly in accordance with the terms outlined in the customer agreement.

Our Client Data Protection (CDP) program governs the stewardship of client informationand systems entrusted to Girikon as part of client-specific projects and outsourcing arrangements as well as when clients are using platforms and services that Girikon operates across multiple clients.

The CDP program defines a set of required management processes and controls to protectour clients' data against a variety of information security and data privacy risks and consists of the following key elements:

- **Accountability** – Senior-level responsibility for data protection and mandatory program adoption for all engagements. Our organization limits access to confidential data strictly to personnel who have a legitimate

business need. Access is granted based on role-based permissions and regular reviews are conducted to ensure only authorized personnel retain access

- **Foundational controls** – Required controls for storing, accessing, handling,transmitting, and hosting client data.
- **Service-specific controls** – Service-specific controls tied to risks inherent in specific types of work, such as business process operations, application development, and infrastructure services, including cloud-based infrastructure.
- **Training and awareness** – Mandatory data protection training provided on aregular basis. Girikon conducts regular training and awareness programs focused on data and information security. These programs are designed to educate employees—including new hires and existing staff—on security best practices, compliance requirements, and how to recognize and respond to security threats
- **Technology** – Technology support including hard drive and USB encryption,workstation configuration scanning, web filtering, data loss prevention, vulnerability scanning, and penetration testing. Each employee across the organization is assigned separate system credentials consisting of a unique username and password managed through Active Directory. This ensures that all user activity is individually traceable, supporting accountability and compliance with organizational security policies
- **Information security and data privacy subject matter expertise** – Tools,processes, and subject matter specialist support for project teams. Girikon utilizes Multi-Factor Authentication (MFA) to enhance security. MFA is implemented for accessing critical systems, applications, remote access, and cloud-based services to ensure that only authorized users can gain access.

Data Protection Officer (Grievance Officer)

Any questions, discrepancies, and grievances of the Relevant Individuals with respect to processing of Personal Data may be made to the Girikon Data Protection Officer (GrievanceOfficer) at **compliance@girikon.com**

The Grievance Officer shall redress the grievances of the Relevant Individuals expeditiouslyand in any event within the period prescribed under law. In case of any queries regarding the content, interpretation, implications of this Policy, the Relevant Individuals may contactthe Grievance Officer.

Notwithstanding the above, Girikon reserves the right to decline to process any such request which may jeopardize the security and confidentiality of the Personal Data of others, as well as requests which are impractical or not made in good faith, or the circumstances as provided for under the law permitting Girikon to refuse such request(s).

Employees/Relevant Individuals Obligations & Consequences of Violations

Girikon Employee/Relevant Individual, who deals with or comes into contact with Personal Data regardless of its origin (EU or non-EU originated data), shall have a responsibility to comply with the applicable law concerning data privacy, this Policy andspecific privacy practices. The Employee/Relevant Individual should seek advice in the event of any ambiguity while dealing with Personal Data or in understanding this policy.

The Employee/Relevant Individual shall be diligent and extend caution while dealing with Personal Data of others, in the course of performance of his/her duties and shall also, at all times:

(i) Prevent any un-authorized person from having access to any computer systems processing Personal Data, and especially: (a) un-authorized reading, copying, alteration, deletion or removal of data; (b) un-authorized data input,

disclosure, uploading, transmission/transfer of Personal Data;

(ii) Abide by Girikon internal logical and physical security policies and procedures;

(iii) Ensure that authorized users of a data-processing system can access only the Personal Data to which their access right refers;

(iv) Keep a record of which personal data have been communicated, when and to whom; Not provide any Personal Data to any third party without first consulting with his/her manager or the Human Resources Department;

(v) Ensure that Personal Data processed on behalf of a third party (client) can be processed only in the manner prescribed by such third party;

(vi) Ensure that, during communication of Personal Data and transfer of storage media, the data cannot be read, copied or erased without authorization;

(vii) Immediately, on becoming aware report and notify any vulnerabilities and privacy related breach/security breaches (including potential risks).

(viii) Attend mandatory and voluntary trainings on security and data privacy including e-learnings and online sessions.

Failure to comply with the Policy and applicable laws may have serious consequences and can expose both Girikon and the Employee/Relevant Individual to damages, criminal fines and penalties. It is important to note that any non-compliance with this Policy is taken very seriously by Girikon and may lead to initiation of appropriate disciplinary actions including but not limited to Employee dismissal or Relevant Individual termination.

Training

Hr & Training Department will ensure the effective induction of all the new staff/ employee (Permanent and contractual). Through its induction arrangements, Hr & Training departments aims to ensure that it meets code of conduct of employee, its health and safety and other statutory obligation, and ensure that new staff become familiar with the organization, its management of risk and their roles in a timely and effective way. Local induction also ensures staff receives specific information and guidance on how to undertake them designated role in the organization.

Note:

1. Girikon reserves the right, to amend this Policy from time to time.