

Generali Central Insurance Company Limited

Data Privacy Policy

DOCUMENT SUMMARY

Title	Data Privacy Policy
Doc Classification	Internal
Document code	GCI/IT/20-21/32
Approved by	Board of Directors
Effective date	June 05 2020
Accountable Function	Information Security
Key contact	NL.ITSecurity@generalicentral.com

CHANGE / HISTORY LOG

Version No.	Rollout Date	Changed by	Approved by	Purpose of revision
1.0	June 05, 2020	CISO	Board of Directors	First Issue
1.1	May 12, 2021	CISO	Board of Directors	Data Privacy framework updated Policy format updated
1.2	May 05, 2022	CISO	Board of Directors	Policy reviewed
1.3	February 07, 2023	CISO	Board of Directors	Changes made as per 'DATA PROTECTION AND PRIVACY/ 2022 IN002 6290 E' audit
1.4	April 28, 2025	CISO	Board of Directors	Aligned with ASIA Data Privacy Framework, Information Technology Act, 2000 and Rules framed thereunder & Digital Personal Data Protection Act, 2023
1.5	August 14 2025	CISO	ISRMC	Rebranding of Document: Company name changed from " Future Generali India Insurance company " to "Generali Central Insurance Company" and logo updated

REGULATORY REFERENCES

- Digital Personal Data Protection Act, 2023 ("DPDP Act 2023")
- The Information technology Act 2000 and Rules framed thereunder ("IT Act 2000" or Information technology Act)
- Prevention of Money Laundering Act, 2002 (PMLA)

Contents

1. Glossary.....	5
2. Purpose	9
3. Scope.....	9
4. Implementation and Communication Plan	10
5. Data Privacy Framework	10
6. Data Privacy Protocols	11
7. Data Privacy Requirements.....	11
8. Data Privacy Policy Components	13
9. Data Protection Impact Assessments (DPIAs).....	31
10. Policy Compliance	32
11. Dispute Resolution and Resources	32
12. Data Classification Policy	32
13. Roles and Responsibilities (Business Functions & Employees).....	33
14. Data Privacy Policy Owner	33
15. Breach Reporting	33

1. Glossary

#	Term	Description
1	Accessibility	Data and information systems are accessible when required.
2	Administrative controls	Control that comes down through policies, procedures, and guidelines.
3	Asset	An asset is any data, device, or other component of the environment that supports organization-related activities.
4	Business as usual (BAU)	The normal execution of standard functional operations within an organization.
5	Confidentiality	Maintaining the secrecy of the information and preventing its unauthorized access
6	Confidentiality agreement	Contract between two or more parties where the subject of the agreement is a promise that information conveyed will be maintained in secrecy.
7	Data Custodian	An Employee/Team under which customer/user data is getting collected/processed/stored
8	Data Event Loss	Any data privacy violation shall be considered as a data event loss
9	Data Owner	Business Heads of respective business/es for which customer/user data is getting collected/processed/stored
10	Data Processor	Someone who provide service to client and process personal data on behalf of data controller
11	Incident Management	Activities of an organization to identify, analyse, and correct hazards to prevent a future re-occurrence.
12	Individual	Individuals, for this purpose, include prospective, current, and former customers, employees and others with whom the entity has a relationship.
13	Integrity	Preventing unauthorized modifications and ensuring that information maintains its consistency, accuracy, and trustworthiness over its entire life cycle.
14	Organization	Shall mean Generali Central Insurance Co Ltd. (GCI)

15	Personal Information (PI) / Personally Identifiable Information (PII)	Personal information (sometimes referred to as personally identifiable information) is information that is about, or can be related to, a natural person, which either directly or indirectly, is capable of identifying such a person Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual. Examples for PI or PII: Name, Gender, DOB, Place of Birth, Details of Family Members, Contact details of self and close relatives, Religion, Educational & Employment information, Marital Status, Race/Caste, Disability information, Government ID number (Driving License, Aadhaar No, PAN).
16	Retention policy	Policy that identifies the duration of time for which the information should be maintained or "retained," irrespective of format (paper, electronic, or other).
17	Sensitive Personal Data or Information (SPDI)	In accordance with the IT (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Sensitive personal data or information of a person means such personal information which consists of information relating to;— (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under 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 shall not be regarded as sensitive personal data or information for the purposes of these rules. Sensitive Personal Data has been defined under the IT Act to include certain specific personal information. However, the definition of what is considered as sensitive may vary depending on jurisdiction, prevailing regulations and also policies of an organization. In general, sensitive data elements will require additional privacy and security limitations. .

		Examples for SPDI: Password, Financial Information, Physical, physiological and mental health condition, Sexual orientation, Medical records and history, Biometric information, any such detail provided to body corporate for providing services, processing and storage. However, this definition does not apply to information available in public domain or furnished under the Right to Information Act 2005 or any other law.
18	Technical Controls	Controls implemented through technology. They may be deterrent, preventive, detective, or compensating and include such things as firewalls, IDS, IPS, and other such controls.
19	Data Privacy Officer (DPO)	Data Privacy Officer who is responsible for and has appropriate authority to ensure compliance with this Policy and is an ultimate contact person for any Data Privacy issues. GCI shall ensure that all roles and responsibilities stated below are achieved either solely through its Data Privacy Officer or divide them between its Data privacy Officer and IT Legal, Compliance and/or HR functions. The Data Privacy Officer empowered to ensure compliance of this policy and related business activities across all functional areas. Executive management of GCI will ensure that adequate funding and other necessary support is available to support the compliance with both its regulatory requirements and additional requirements within group and local privacy policies.
20	Data Subject/Data Principal	An individual whose personal data is being collected, held, or processed.
21	Personal Data	Any information relating to an identified or identifiable natural person (data subject).
22	Sensitive Personal Data or Sensitive Personal Information (SPI)	Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning a person's sex life or sexual orientation. • Password, • Physical, physiological, and mental health condition, • Sexual orientation, • Genetic or biometric information, • Racial and ethical origin, • Political opinions, • Religious or philosophical beliefs. • Trade union membership. • Internet browsing history or cookies. • Biometric details

		• PAN or AADHAR card • Driving License or other government ID/ address proof
23	Personal Health Information (PHI)	PHI is any information about an individual (the Data Principal) which can be medical records and history.
24	Critical Personal Information (CPI)	CPI is any information about an individual (the Data Principal) as below but not limited to. 1. Financial information such as bank account or credit card or debit card or other payment instrument details. 2. Internet/ Mobile banking related information. 3. Passbooks/ Bank statement. 4. Cheque scan copies
25	Data Controller	The entity that determines the purposes and means of processing personal data.
26	Data Processor	The entity that processes personal data on behalf of the data controller
27	Consent	A freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data.
28	Data Breach	A security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.
29	Data Minimization	The principle that personal data collected should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
30	Data Portability	The right of a data subject to receive their personal data in a structured, commonly used, and machine-readable format and to transmit those data to another controller.
31	Data Protection Impact Assessment (DPIA)	A process to help identify and minimize the data protection risks of a project.
30	Encryption	The process of converting information or data into a code to prevent unauthorized access
31	Anonymization	The process of removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.
32	Pseudonymization	The processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information.
33	Right to Access	The right of data subjects to obtain confirmation as to whether or not personal data concerning them is

		being processed, and, where that is the case, access to the personal data.
34	Right to Rectification	The right of data subjects to have inaccurate personal data corrected or completed if it is incomplete
35	Right to Erasure (Right to be Forgotten):	The right of data subjects to have their personal data erased under certain conditions.
36	Right to Restriction of Processing	The right of data subjects to restrict the processing of their personal data under certain conditions.
37	Right to Object	The right of data subjects to object to the processing of their personal data under certain conditions.
38	Data Inventory	A comprehensive list of data assets within an organization, detailing the types of data collected, stored, and processed.
39	Data Flow Diagram	A graphical representation of the flow of data within an organization, showing how data is processed and transferred between different systems and stakeholders.
40	Data Privacy Impact Assessment (DPIA)	A tool used to identify and mitigate risks to data privacy and protection in projects that involve the processing of personal data.
41	GCI	Generali Central Insurance Co Ltd.

2. Purpose

To implement an effective data privacy policy to maintain Confidentiality, Integrity and Accessibility of data collected/generated, processed, and stored at GCI (hereinafter referred to as “Organization”). It can be achieved by:

- Identifying data/information which includes personal Identifiable Information (PII) and Sensitive Personal Data or Information (SPDI).
- Ensuring effective controls are in place to protect PII and SPDI.
- To comply with regulatory data privacy requirements.

3. Scope

This policy applies to all GCI employees (permanent/temporary/trainee), consultants, contractors, vendors other third parties and auditors who may receive sensitive information, have access to such information collected or processed, or who provide information to the organization (hereinafter referred to as “Associates”). This policy document must be read in

conjunction with Information and Cyber Security policy and all other relevant policies as necessary.

All vendors, consultants, contractors working with GCI, and who have or may have access to personal information, will be expected to have read, understood, and ensure compliance with this policy. No such third party may access any sensitive information held by the organization unless entered into a confidentiality agreement.

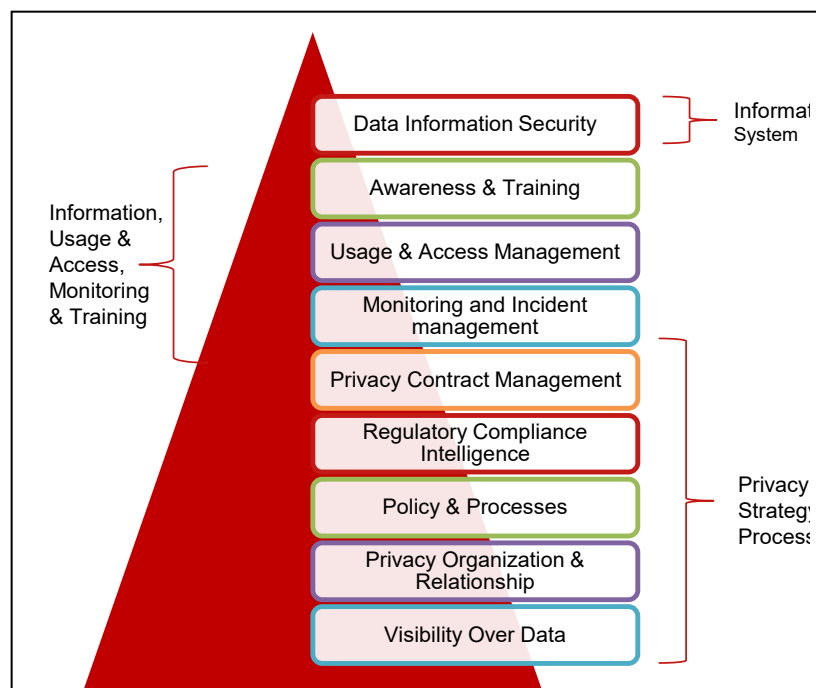
4. Implementation and Communication Plan

- The policy will be available to all employees at GCI intranet portal
- The policy will be communicated to employees during awareness sessions
- The policy will be communicated to applicable external parties on requirement

5. Data Privacy Framework

To protect customer information from unauthorized use, disclosure, modification, or misuse, Will be adopting the Privacy Framework which is based on the global privacy best practices and frameworks.

To safeguard customer information against unauthorized access, disclosure, alteration, or misuse, we will implement the Privacy Framework, which aligns with global best practices and standards in privacy protection.



6. Data Privacy Protocols

The organization including its Associates shall follow the data privacy protocols as follows:

- Obtain and process information fairly, by informing everyone about “**what and how**” the data is being collected, utilized, retained, and disclosed. The individuals are to be made aware of their rights as per the prevailing laws.
- Personal data shall be processed for one or more specified, explicit, and lawful purposes upon the consent of an individual.
- Maintain the accuracy of the data, keep data secure and erase the data once its purpose has been fulfilled or as specified in the organization data retention policy.
- Ensure it is adequate and relevant but not excessive.
- Ensure the fulfilment of individual rights such as the right to the correction, completion, updating, nominate and erasure of personal data for which prior consent was obtained.
- The organization shall obtain **verifiable consent** from the legal guardian before processing the personal data of a child (under age 18).
- Process must be established to verify the age of everyone signing up for the services.
- The organization shall prohibit processing of personal data of a child to ensure compliance with applicable privacy regulations.
- Identify and classify data based on its sensitivity and importance.
- Encrypt data at rest and in transit to protect it from unauthorized access.
- Implement role-based access controls (RBAC) to restrict access to data based on the user's role within the organization.
- Grievance Officer/DPO appointed to address the discrepancies and grievances raised by individuals.

7. Data Privacy Requirements

- Below specified are the Data Privacy requirements in alignment to the prevailing Information Technology Act and Rules, and its applicability to the respective business/es and the data owner will be responsible for keeping the control in place.

- The data privacy standards in accordance with the current Information Technology Act and Rules are described below, along with their relevance to the relevant business or businesses. The data owner is responsible for maintaining the control.

#	Requirements	Related Actions & Checks
1	Policy for privacy and disclosure of information	Disclaimer should be available at the source from where information is being collected.
2	Collection of Information	Explicit, unambiguous & verifiable consent from customer shall be incorporated for each GCI business (customer providing PII or SPDI data)
3	Collection of information	Business owners to obtain sign off from legal team and compliance team for collection of data for lawful purpose/purposes mentioned in the consent.
4	Collection of information	What all data is considered mandatory for regulatory requirement and should not be deleted even if the consent is withdrawn by the customer? ---- [the same to be specified in the consent document obtained from the customer] What information is deemed necessary for regulatory purposes and should not be erased, even if the client withdraws their consent. The same must be stated in the customer-provided consent agreement. In case the consent is withdrawn, what are the dependencies for serving the customer? Is the data being deleted after withdrawal of consent & is a confirmation mail sent to customer after withdrawal of consent & deletion of data?
5	Collection of information	1. Is there a data retention policy? 2. What is the data retention period specified by the regulatory body? 3. If no regulatory & legal requirement is applicable, what is the data retention period defined by businesses in GCI? (If there is no data retention policy, then it needs to be drafted and shared with GCI IT Security Team by relevant data owner – business function)
6	Collection of information	1. Is individual level data available to the customer for review and updates?

		2. In case of any customer data update (PII & SPDI) confirmation communication must go to the customer. Preferably, this must be followed by a ticketing process with unique ticket No.
7	Grievance Redressal	1. What is the process to capture discrepancies and grievances in case of misuse of customer data (beyond the consent taken)? 2. Is there a grievance officer designation defined. 3. Are the details (name and contact details) published on the website? 4. How the grievances resolved within one month from the date of receipt of grievance and recorded for future ref?
8	Collection of information	Is proper parental consent taken and age verification done for GCI clients of age below 18 years.
9	Collection of information	Is proper consent/permission taken from the customer before disclosing the information to the third party as a part of initial consent?
10	Storage of information	What are the security controls implemented to ensure data security (PII & SPDI) through data life cycle.
11	Storage of information	Perform mock drills scheduled at regular intervals to ensure that business stakeholders at GCI are ready in case of an actual data breach? CCMP Tabletop Exercise
12	Transfer of Information	1. Is proper consent/permission taken from the customer before disclosing the information to the third party as a part of initial consent? 2. Is there any data transferred to other body corporates or person within India or outside without a lawful contract?

8. Data Privacy Policy Components

The various components of the Privacy Policy shall cover the following structure as defined below:

1. Governance
2. Legal Requirements
3. Regulatory Requirements
4. Policy Details

5. Privacy Policy on website

7.1 Governance

GCI shall have the governance structure as follows which establishes the roles and responsibilities of all the stakeholders in the organization.

- The Board of Directors (“Board”)
- Information Security Risk Management Committee
- Chief Information Security Officer (CISO)
- Chief Risk Officer (CRO)
- Chief Compliance Officer
- Data Privacy Officer (DPO)

7.1.1 The Board

The Board is responsible for effective evaluation, directing and monitoring the overall Privacy program.

In addition, the Board also shall:

- Appoint a Data Protection Officer (“DPO”) who would be reporting to the highest management level or Board of Directors.
- Appoint an Independent Data Auditor responsible for evaluating and ensuring compliance with provisions of the DPDP Act 2023.
- Review the privacy Incidents reported to the Board.
- Approve the Privacy Policy.
- Any subsequent modifications to the policy shall be approved and recommended by the Committee for Information Security to the Board for its approval.
- Approve the necessary budgets on an annual basis for the various Privacy related activities comprising of Operational, Technical and HR Controls which will include Human Resources Training and Education.

7.1.2 Information Security Risk Management Committee (IS RMC)

The Committee for Information Security shall oversee the privacy program of GCI on an ongoing basis. In addition, the Committee for Information Security also shall periodically

1. Review the privacy incidents, evaluate the cause, and suggest remedies to such incidents.
2. Approve the subsequent changes to the Privacy Policy.
3. Identify the privacy incidents and major changes to the Privacy policy to be presented to the Board.

7.1.3 Chief Information Security Officer (CISO)

The CISO is responsible for effective evaluation, directing and monitoring the overall Privacy program.

In addition, the CISO also shall

- Review the privacy Incidents reported to the Board.
- Implementing data encryption and masking techniques to protect sensitive information from unauthorized access and breaches.
- Setting up robust access controls and monitoring systems to ensure that only authorized personnel have access to sensitive data.
- Ensure that data privacy is integrated into the overall business strategy. This involves participating in strategic discussions and aligning cybersecurity initiatives with business goals

7.1.4 Chief Risk Officer (CRO)

- Be responsible for the overall risk management functions of the organization which shall include Information Security Risk Management in its purview.
- Obtain regular updates from the CISO regarding IS related issues / incidents, updates, new initiatives and corrective / preventive actions taken, remain involved in IS related initiatives such as IS awareness and training, IS assessments and escalation of critical IS incidents.
- The CRO, along with the CISO shall represent information security related event / issues and initiatives at the Control Management Committee.

7.1.5 Chief Compliance Officer

The Privacy Policy is a legal as well as regulatory requirement and the Head of Compliance will be responsible to the plan, build, run, and maintain the privacy program of GCI.

- Review of the Privacy Policy prepared by the Designated Officer and recommend to the IS RMC and the Board for the approval of the same, as mentioned.
- Ensure that the periodic review of the Policy is undertaken.
- Review the Privacy related incidents and recommend necessary actions. Identify the incidents and/or remedial actions to be referred to the Committee or the Board.
- Apprise the Board or the Committee of the critical privacy related incidents upon receipt of necessary details with regards to the incident from Info Sec team and IT team

7.1.6 Data Privacy Officer (DPO)

The designated officer for privacy will be responsible for the following:

- Will be the single point of contact for all external interested parties for their query related to the grievance related to Privacy Policy.
- The Name and contact details of the Grievance officer shall be published on the website of the company.
- Periodic review of the Privacy Policy and ensure that the same is up to date and not obsolete.
- To Liaise with the Data Protection Authority
- Prepare or amend the Privacy Policy in line with the Legal and Regulatory requirement.
- Ensure that the latest version of the Privacy Policy is updated and available on the website of GCI Corporate Communications
- In case of any Mobile application the privacy policy is also displayed and accepted before the permission to use the application.

- To conduct data protection impact assessments (DPIAs) where required

7.2 Legal Requirements

The following laws related to Privacy, as amended from time to time, are applies to GCI group wherever applicable:

- The Information technology Act 2000 (“IT Act 2000”) specifically Sec 43A
- The Information technology Act (Reasonable Security practices and procedures and sensitive personal data or information) rules, 2011 specifically Rule 4 to Rule 7
- The Digital Personal Data Protection Act, 2023
- The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 (“Aadhar Act 2016”) specific sections and the following regulation
- Aadhaar (Data Security) Regulations 2016
- Aadhaar (Sharing of Information) Regulations 2016

7.2.1 Legal Basis of Processing

The organization must ensure that KYC process is performed in accordance with the applicable regulatory requirements as a part of customers onboarding journey wherever applicable. (PML act 2002 and Anti Money Laundering program, Sec 8A of Aadhaar Act 2016)

7.3 Regulatory Requirements

Regulatory Requirements of Data Privacy Policy as per the DPDP Act.

The **Digital Personal Data Protection (DPDP) Act 2023** outline comprehensive requirements for data privacy policies in India.

1. Rights of Data Principals

- Access and Correction: Data principals have the right to access their personal data and request corrections.
- Data Portability: Data principals can request their data in a structured, commonly used format.
- Right to Erasure: Data principals can request the deletion of their personal data under certain conditions.
- Right to Nominate: Data principals can nominate another individual to exercise their rights in case of incapacity or death

2. Consent Management

- Verifiable Consent: Data fiduciaries must obtain verifiable consent from data principals before processing their personal data.
- Parental Consent: For data principals under 18 or those with disabilities, verifiable consent from a parent or guardian is required

- **Withdrawal of Consent:** Data principals should be able to withdraw consent as easily as it was given

3. Data Breach Notification

- **Notification to Data Principals:** In case of a data breach, data fiduciaries must notify affected data principals and the Data Protection Board within 72 hours
- **Detailed Reporting:** Provide detailed information about the breach to the Data Protection Board

4. Data Privacy Notice

- **Transparency:** Data fiduciaries must provide a clear and itemized notice about the collection, purpose, and use of personal data.
- **Accessibility:** The notice should include a link to withdraw consent and make complaints to the Data Protection Board

5. Security Safeguards

- **Reasonable Security Measures:** Data fiduciaries must implement adequate security measures to protect personal data
- **Data Protection Impact Assessments (DPIAs):** Significant Data Fiduciaries (SDFs) must conduct annual DPIAs and data privacy audits

6. Data Retention and Deletion

- **Retention Period:** Personal data should be retained only as long as necessary for the purpose of processing.
- **Deletion of Inactive Data:** Personal data of data principals who have not interacted with the data fiduciary for three years must be deleted, with prior notification

7. Cross-Border Data Transfers

- **Government Regulations:** Data fiduciaries must adhere to requirements established by the central government regarding cross-border data transfers
- **Data Localization:** Certain categories of data must be retained within India

8. Processing of Children's Data

- **Age Verification:** Data fiduciaries must verify the age and identity of the parent or guardian when processing children's data
- **Special Provisions:** Exemptions for healthcare professionals, educational institutions, and childcare providers for specific activities

9. Consent Managers

- **Certification:** Consent managers must be Indian-incorporated companies with a net worth of at least INR 2 crore and a certified interoperable platform for managing consent

10. Data Protection Officer (DPO)

- **Appointment:** Data fiduciaries must appoint a DPO and publish their contact details

11. Processing by the State

- **Permitted Activities:** The state may process personal data for providing benefits, services, certificates, licenses, or permits as permitted by laws and policies

Compliance Considerations

- **Regular Audits:** Conduct regular audits to ensure compliance with the DPDP Act and its rules.
- **Employee Training:** Provide ongoing training to employees on data privacy policies and best practices.
- **Policy Updates:** Regularly update data privacy policies to reflect changes in regulations and business practices.

Data Protection Measures: Implement robust data protection measures, including encryption, access controls, and incident response plans.

7.4 Policy Details

7.4.1 Information that is collected and processed

7.4.1.1 Personal information collected from customers, GCI Employee & vendors:

In connection with your purchase of products & services from the organization, the organization shall collect your details, not limited to name, photograph, date of birth (DOB), address, email address, occupation country, and telephone number, etc. via our website or physical forms.

7.4.1.2 Collection of Information from third party

The organization may collect information from third parties such as credit bureaus/Digital verification services etc. based on information gathered from the prospect/client/customer.

7.4.1.3 Collection, processing and purpose of Sensitive Data

GCI collects the sensitive personal data or information wherever applicable as mentioned in **Table1** below for the following activities:

- Offering services/products to its customers.
- Providing access to office premises to GCI and its partners personnel.
- Conducting business operation and processing payments.

Table1

Information collected for given purpose.

#	Sensitive Personal Data	Collected	Purpose of Collection
1	Password	Yes	To provide the customer with digital access to the details of his/her account
2	Financial information such as bank account, credit card, debit card or other payment details	Yes	To evaluate customer's eligibility for services/products offered to customer.
3	Physical, physiological, and mental health condition	Yes	To evaluate customer's eligibility for services/products offered to customer.
4	Sexual orientation	No	Not collected by GCI presently
5	Medical records and history	Yes	To evaluate customer's eligibility for services/products offered to customer.
6	Biometric information – Fingerprints*	Yes	To be used in the event the customer decides to opt for eKYC (electronic KYC) authentication using the biometric information as provided by UIDAI.
7	Biometric information – Eye retina and irises	No	Not collected by GCI presently
8	Biometric information – Voice patterns	No	Not collected by GCI presently
9	Biometric information – Facial patterns	No	Not collected by GCI presently
10	Biometric information – Hand measurement	No	Not collected by GCI presently

7.4.2 Collection of Personal Information

Personal information may be collected online or offline. Regardless of the collection method, the same privacy protection shall apply to all personal information.

- Personal information shall not be collected unless either of the following is fulfilled:
 - The Data Principal has provided valid, informed, and free consent.
 - Processing is necessary for the performance of a contract to which the Data Principal is a party or to take steps at the request of the Data Principal prior to entering a contract.
 - Processing is necessary for compliance with the organization's legal obligation.
 - Processing is necessary to protect the vital interests of the Data Principal; or
 - Processing is necessary for the performance of a task carried out in the public interest.
- Data Principals shall not be required to provide more personal information than is necessary for the provision of the product or service that Data Principal has requested or authorized. If any data not needed for providing a service or product is requested, such fields shall be clearly labelled as optional. Collection of personal information shall be avoided or limited when reasonably possible.

- Personal information shall be de-identified when the purposes of data collection can be achieved without personally identifiable information, at a reasonable cost.
- When using vendors to collect personal information on behalf of GCI, it must be ensured that the vendors comply with the privacy requirements of GCI as defined in this Policy.
- GCI shall at minimum annually review and monitor the information collected, the consent obtained and the notice / SoW / contract agreement identifying the purpose.
- The project team/support function shall obtain approval from the DPO & IT Security team before adopting the new methods for collecting personal information electronically.
- GCI shall review the privacy policies and collection methods of Third Parties before accepting personal information from Third-Party data sources.

7.4.3 Use of Personal Information

- The customer's personal information shall be used for the purposes of the services provided by the organization.
- The email address and mobile number provided by the customer may be used to validate customers whenever they visit the organization's online services.
- The organization will send periodic update and news alerts to users on the email address and mobile number provided by them as and when required.
- The customer will have the right to unsubscribe generic information, if any, provided.
- The consumer will have the option to stop receiving any generic information offered.
- The consumer will be able to opt out from receiving any generic information that is offered.
- In the case of employees, the same shall be used for specific communication as decided by the HR department from time to time.
- In the case of vendors, the same shall be used for sending the payment updates and other relevant information.

7.4.4 Collection of Data from Guardians on behalf of minors

- The products offered by GCI also cover minors. In the event a customer chooses to avail such policies, the parent or guardian of such minors would be required to provide personal information and sensitive personal data or information of such minors.
- In case the KYC is done for the child then the consent will have to be given by the parent or guardian.
- This is per Sec 8 of the Aadhaar Act 2016 and the related regulation as mentioned above.
- Minors are likewise covered by the GCI products. If a customer chooses to use these policies, the parent or legal guardian of the minor will need to provide sensitive personal data or information about the minor as well as their personal information.

7.4.5 Consequences of not Providing Personal Information

- If the prospect/client choose not to provide the Personal Information that is mandatory to process request for services of GCI it may not be possible to provide the corresponding product and/or service.
- Customers may not be able to avail themselves of the services of the organization if they choose not to provide the required personal information

7.4.6 Data Recipients and Disclosure of Personal Information

- To provide the best experience of GCI products & services, it is necessary for GCI to engage third party vendors who provide specific products & services to support GCI's business requirements. In this connection, GCI would make disclosure of sensitive personal data or information for the purposes of or in connection with activities such as – data entry, tele-calling, printing, business risk sharing, expert view, audit, legal proceeding, monetary payment, digital & physical communication, verification & collation of information, digital & physical storage.
- Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation:
- As required by the PMLA Act of 2002 and related Rules, the last four digits as well as the associated demographic data, such as name, DOB, and address, must be shared with the Central Know Your Customer Registry (CKYC) maintained by CERSAI (Central Registry of Securitization Asset Reconstruction and Security Interest of India). The same will be distributed electronically, along with the Aadhaar card image (if provided), or the output pdf/jpeg produced by the UIDAI website. The legal requirements make this a necessary necessity.
- GCI will not share this information with any other entity, other than those mentioned above, whatsoever without the explicit permission, except where the disclosure is mandated by law.
- The above will not be applicable for disclosures made
 - For compliance of legal obligation.
 - Governmental organizations required by law to collect data, including sensitive personal information, to verify identities, or to prevent, detect, investigate, including cyber incidents, prosecute, and punish offenders
 - To any third party by an order under the law for the time being in force.

7.4.7 Access Control

GCI shall establish a mechanism to enable and facilitate exercise of Data Principal's rights of access, blockage, erasure, opposition, rectification, and, where appropriate or required by applicable law, a system for giving notice of inappropriate exposure of personal information.

- Data Principals shall be entitled to obtain details about their own personal information upon a request made and set forth in writing. GCI shall provide its response to a request within 72 hours of receipt of written request.
- The Data Principals have the right to require GCI to correct or supplement erroneous, misleading, outdated, or incomplete personal information.
- Requests for access to or rectification of personal information shall be directed at the Data Principal's option, to the manager of the projects team or support function responsible for the personal information.
- The privacy coordinators shall record and document each access request as it is received, and the corresponding action taken.
- Organizational digital records (which include but no limited to PII/PHI/SPDI) for business shall be retained for a minimum period of one year (as per policy active period, it may be three years if the policy period is three years). The retention period may vary or extend depending on regulatory guideline.
- Till the time above digital records are retained with GCI, similar security and privacy controls shall be applied to ensure security and privacy.
- GCI should provide personal information to the Data Principals in a plain simple format which is understandable (not in any code format).

7.4.8 Data Integrity & Quality

GCI shall maintain data integrity and quality, as appropriate for the intended purpose of personal data collection and use and ensure data is reliable, accurate, complete, and current.

- For this purpose, the data privacy officer and privacy coordinators shall have systems and procedures in place to ensure that personal information collected is accurate and complete for the business purposes for which it is to be used.
- GCI shall perform an annual assessment on the personal information collected to check for accuracy, completeness, and relevance of the personal information.

7.4.9 Transfer of Information

- Presently, GCI does not transfer sensitive personal data or information to any other body corporate or person, whether in India except to those entities as required by Law. No Data or information is transferred outside the country. If in future, such a transfer is made, the same would be

- With the consent of the provider of sensitive personal data or information.
- Effected only if it is necessary for the performance of the contract with such a provider.
- Upon such transferee agreeing to be bound by the level of data protection prescribed under law.
- Except for such entities as required by law, GCI does not currently send sensitive personal data or information to any other body corporate or individual, whether in India. There is no movement of data or information outside of the nation. If such a transfer were to be made in the future, it would be done so
 - with the consent of the provider of sensitive personal data or information,
 - only if it was required to fulfil the terms of the contract with that provider
 - only if the transferee agreed to adhere to the level of data protection required by law.

7.4.10 Retention of data

Personal information may only be used for the purposes identified in the notice / SoW / contract agreements and only if the Data Principal has given consent.

- Personal information shall be retained for as long as necessary for business purposes identified in the notice / SoW / contract agreements at the time of collection or subsequently authorized by the Data Principals.
- When the use of personal information is no longer necessary for business purposes, a method shall be in place to ensure that the information is destroyed in a manner sufficient to prevent unauthorized access to that information or is de-identified in a manner sufficient to make the data non-personally identifiable.
- GCI shall have a documented process to communicate changes in retention periods of personal information required by the business to the Data Principals who are authorized to request those changes.
- Personal information shall be erased if their storage violates any of the data protection rules or if knowledge of the data is no longer required by GCI or for the benefit of the Data Principal. Additionally, GCI has the right to retain the personnel information for legal and regulatory purpose and as per applicable data privacy laws.
- GCI shall perform an internal audit on an annual basis to ensure that the personal information collected is used, retained and disposed off in compliance with the organization's data privacy policy.
- GCI retains data in accordance with the laws of India and has a data retention policy approved by the Board of GCI. Generally, GCI retains data for a period up to 10 (ten) years from the date of cessation of the relationship between you and GCI. In the event the prospect needs to understand the exact duration of any specific data or information that is stored by GCI, the client will have to write to the Grievance Redressal Officer at the contact details provided below and seek necessary clarification below.
- Personal data shall not be kept in a form which permits identification of the data subject

for longer than necessary for the purposes for which they were obtained or recorded.

- Personal data shall be erased when they have ceased to be necessary for the purpose for which they were obtained or recorded.
- Data may be stored for the duration of any kind of liability arising from legal relations or obligations or the execution of a contract or the application of pre-contractual measures requested by the data subject.
- On a regular basis, the procedure for data retention shall be determined by local legislation and a retention schedule must be drawn up.
- On the expiry of such liability as stated above, data may only be stored following their dissociation.

7.4.11 Reasonable Security Practices and Procedures

Information security policy and procedures shall be documented and implemented to ensure reasonable security for personal information collected, stored, used, transferred, and disposed by GCI.

- Information asset labelling and handling guidelines should include controls specific to the storage, retention and transfer of personal information.
- Management shall establish procedures that maintain the logical and physical security of personal information.
- Management shall establish procedures that ensure protection of personal information against accidental disclosure due to natural disasters and environmental hazards.
- Incident response protocols are established and maintained in order to deal with incidents concerning personal data or privacy practices.
- GCI is certified for ISO 27001:2022 and have implemented reasonable security practices & standards and have a comprehensive documented information security program and information security policies.
- The reasonable security practices of the protection of the Identity information of Aadhaar are stipulated in the Aadhaar Act and the related regulations.
- GCI shall always abide by the same. As on the date of this version of the policy the following practices shall be adopted:
 - GCI has established adequate security practices and standards, and it has a thorough, well-documented information security program and information security policies. GCI is accredited for ISO 27001:2022.
 - The Aadhaar Act and the associated regulations provide the necessary security procedures for the protection of Aadhaar identity information.
 - GCI will always follow the same rules. The following practices shall be used as of the effective date of this version of the policy:
 - The full 12-digit Aadhaar number or the 16-digit VID (Virtual ID) will be entered in the application of GCI will not be stored.
 - Neither the complete 12-digit Aadhaar number nor the 16-digit Virtual ID (Virtual ID) would be saved when input into the GCI application.
 - In case of eKYC no hard copy of Aadhaar Card obtained from the prospect.
 - In case the physical copies/ electronic copies of the same are provided by the customer it shall be ensured that the same is redacted before receiving the

same from the customer. Even if the same is received without redaction GCI will ensure that the same is redacted before storage.

- If the customer provides physical or electronic copies of the same, it must be guaranteed that they have been redacted before being received. GCI will make sure that the information is redacted before storage even if it is received in an unredacted form.
- The servers used for authentication services shall be within the territorial boundaries within India only.
 - Hardware Security Module should preferably be implemented in line with the UIDAI requirements for storage of Aadhaar numbers wherever applicable.

7.4.12 Obligations for Sub-processor

- Where a processor (vendor or 3rd party acting on behalf of GCI's data processor) engages another processor (Sub-processor) for carrying out specific processing activities on behalf of GCI (data fiduciary), the same data protection obligations as set out in the contract or other legal act between GCI and the processor shall be imposed on the Sub processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of India IT Act 2000 and other applicable data privacy law (e.g. DPDP Act). Where the Sub-processor fails to fulfil its data protection obligations, the initial processor (relevant vendor or 3rd party acting on behalf of GCI's data processor) shall remain fully liable to GCI for the performance of that Sub-processor's obligations.

7.4.13 Grievance Redressal

- GCI shall address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. For this purpose, GCI has designated a Grievance Redressal Officer, the details of the same are provided under this Privacy Policy as well as GCI website.
- GCI should address any discrepancies and grievances of their provider of the information with respect to processing of information in a time constrained manner. The GCI website and this privacy statement both include information about the Grievance Redressal Officer that has been selected for this purpose.
- All clients/employees/vendors can submit the grievances related to this privacy policy through any of the following channels:
 - Email
 - Website
 - Telephone
- The details of the Grievance Redressal Officer and other details shall be and Grievance Redressal Mechanism of GCI shall be provided as part of Data Privacy Policy published at website.

7.4.14 Choice & Consent

Choice refers to the options for the Data Principals are offered regarding the collection and use of their personal information. Consent refers to their agreement to the collection and use, often expressed by the way in which they exercise a choice option.

- GCI shall establish systems for the collection and documentation of Data Principal consents to the collection, processing, and/or transfer of personal data.
- Data Principals should be informed about the choices available to them with respect to the collection, use, and disclosure of personal information.
- Consent shall be obtained (in writing or electronically) from the Data Principals before or at the time of collecting personal information or as soon as practical thereafter.
- The changes to the Data Principal's preferences shall be managed and documented. Consent or withdrawal of consent shall be documented appropriately.
- The choices shall be implemented in a timely fashion and respected. If personal information is to be used for purposes not identified in the notice / SoW / contract agreements at the time of collection, the new purpose shall be documented, the Data Principal shall be notified, and consent shall be obtained prior to such new use or purpose.
- The Data Principal shall be notified if the data collected is used for marketing purposes, advertisements, etc.
- GCI shall review the privacy policies of the Third Parties and types of consent of Third Parties before accepting personal information from Third-Party data sources.
- In the event the prospect/ client has decided to share the information as requested, after going through the details provided to him as above, shall give specific consent related to collection. The consent shall be preferably through the electronic mode, even though the law permits obtaining such consent through a written letter, fax, or email.
- The consent provided must be verifiable.
- After carefully reviewing the facts presented to the Data Principal as above and making a decision to share the information as required, the prospect or client must offer a particular consent connected to collection. Even though the law authorizes receiving such consent via a written letter, fax, or email, it is preferable to do it electronically.
- The consent shall be in a standard format prescribed by DPO.
- In case the eKYC is done of child then the consent will have to be given by the parent or guardian.
- Withdrawal of consent or abstinence from providing such information will adversely affect the products & services offered by GCI, including GCI having the option of not providing goods or services for which the said information was sought.
- The products and services provided by GCI would suffer if consent is withheld; GCI may also choose not to provide the goods or services for which the above-mentioned information was requested.
- The logs of the consent shall be stored by GCI. The logs will contain the time stamp, the text and a version of the consent and any other additional details as required.
- GCI is required to keep the consent logs on file. The time stamp, the wording and version of the consent, as well as any other relevant information, will all be included in the logs.

7.4.15 Storage of Sensitive Data

- All sensitive data including PII/SPDI should be labelled and handled as per GCI's Information and Cyber Security Procedure.
- The organization's sensitive data in physical form should be stored in lock and key cabinets. The organization's sensitive data stored/processed in electronic form should be adequately encrypted and stored on a controlled database on secured servers, access to which is password protected and strictly limited.
- Sensitive information about the organization that is physically present should be kept in lock-and-key cabinets. Sensitive information about the company that is processed or stored electronically should be adequately encrypted and kept in a regulated database on secured servers with password protection.

7.4.16 Data Transfer

- Organization's data must be protected from leakage or misuse during transfer.
- The data fiduciaries may transmit data outside of India, but only under the approved terms and conditions and to countries that are legally permitted to receive such transfers.
 - Organization should not disclose an individual's personally identifiable data outside BAU, except when it has obtained express consent to do so.
 - When necessary to be disclosed to regulatory bodies and auditors
 - When organization is required or permitted to do so by law

7.4.17 Security Incident Management for Data Loss Event

- Any data loss event shall be followed by GCI Security Incident management process and must be reported immediately to the concerned authorities so that the exposure can be contained.
- Data privacy breach impact assessment shall be conducted by GCI and respective stakeholders to help identify and minimize the data privacy risks due to Data Loss Event.
- Refer "IT & Cyber Security Procedure" document

7.4.18 Privacy of PII/SPDI

- Implement privacy safeguards and consistent enforcement of information security controls to address personally identifiable data and sensitive personal data & information.
- To deal with personally identifiable information and sensitive personal data & information, implement privacy safeguards and consistent implementation of information security rules.
- GCI shall implement controls on collection, processing, and disseminating of PII.
- The security controls will address:

- I. Mechanisms for ensuring that information is obtained and processed fairly, lawfully, and properly.
 - II. Ensuring confidentiality and integrity of the information is maintained throughout the lifecycle.
 - III. Following of retention policy for secure data disposal whenever data is no more required.
 - IV. List of databases, which stores and processes personal information subject to privacy regulations will be maintained by GCI team.
 - V. Compliance with the relevant data privacy/privacy regulations. The Policy will be reviewed periodically.
- GCI will, at its discretion, monitor usage of its information assets as per applicable laws and terms and condition of employment agreed upon by the Organization and the employee as per the confidentiality agreement. This may include logging and reviewing of user activity such as telephone numbers dialled, web sites visited from GCI owned assets, electronic communications exchanged through Organization information processing facilities, etc.
 - In accordance with applicable laws and the terms and conditions of employment established by the Organization and the Employee pursuant to the Confidentiality Agreement, GCI shall, at its discretion, monitor usage of its information assets. This may involve recording and examining user activity, including phone numbers called, websites viewed from GCI-owned property, electronic communications exchanged through organisation information processing facilities, etc.
 - Appropriate technical and administrative controls will be identified and implemented to protect personal information pertaining to users and customers.
 - To safeguard user and client personal information, appropriate technical and administrative procedures shall be found and implemented.
 - Controls will be implemented to prevent employees and Third-Party staff having unauthorized access of the information, information systems and/ or facilities.
 - Controls will be put in place to prevent personnel from the company and third parties from gaining unauthorized access to the data, computer systems, or facilities.
 - Identified PII shall be classified and handled as per information classification and data privacy procedure.
 - Access to the sensitive data should be provided strictly based on need to know.
 - Personal records shall be maintained and stored securely, and users of the personal records will be liable to ensure the secure storage, retention and disposal of the information.
 - Users of personal records are responsible for ensuring the safe maintenance, storage, and destruction of the data, and personal records must be maintained and stored securely.
 - Backup on a removable storage media should be kept in safe and secure environment.
 - Appropriate disciplinary actions will be taken in case of breach of privacy and privacy of Organization's data or personally identifiable information
 - If there is a breach of the privacy of the Organization's data or personally identifiable information, appropriate disciplinary measures will be taken.
 - Disclaimer should be available at the source from where information is being collected.

- Explicit and unambiguous consent from customer shall be incorporated for each GCI business (customer providing PII or SPDI data)
- Business owners shall obtain sign off from legal team and compliance team on collection of data for lawful purpose/purpose mentioned in the consent.
- Company owners must obtain approval from the legal and compliance teams before collecting data for a legal purpose or a purpose specified in the consent.
- A provision should be provided to the customer to withdraw the consent in case the organization is storing SPDI data of the customer.
- If an organization is keeping a client's SPDI data, the customer should have the option to revoke their consent.
- Customer data should be deleted after the withdrawal of consent in accordance with the regulatory requirements.
- Upon the withdrawal of consent, customer data should be erased in compliance with the law.
- An explicit consent/ permission shall be taken from the customer before disclosing the information to the third party.
- Before revealing the information to a third party, the customer's express consent or authorization must be obtained.
- Lawful contract should be signed between the organization and body corporate or person to transfer customer data.
- To transmit customer data, a valid contract must be made between the company and the body corporate or individual.
- Mock drills shall be scheduled & performed at regular intervals to ensure that business stakeholders at GCI are ready in case of an actual data breach.
- To make sure that business stakeholders at GCI are prepared in the event of a real data breach, mock exercises must be arranged and carried out on a regular basis.

7.5 Privacy Policy on website

Introduction

Generali Central India Insurance Co Ltd ("we", "us", "our") is committed to protecting your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you visit our website www.generalicentral.com and use our services.

Information Collection

We may collect personal data such as your name, contact details, policy information, health information, financial information, and other relevant data necessary for providing insurance services.

Methods of Collection

- **Directly from You:** Through forms, applications, and other interactions.
- **Automatically:** Via cookies, web beacons, and other tracking technologies.

- **From Third Parties:** Such as medical professionals, financial institutions, and other service providers.

Information that may be provided by you directly, such as:

- Identification Information: Name, gender, residential/communication address, contact number, date of birth, marital status, email address or any other contact information.
- PAN, KYC, Signature and Photograph.
- Bank account or other payment instrument details.
- Any other detail which may be required by Us for providing such services.

Use of Information

We use your personal data for the following purposes:

- **Providing Insurance Services:** Processing applications, underwriting, claims management, and customer support.
- **Compliance:** Adhering to legal and regulatory requirements.
- **Marketing:** Sending promotional materials and offers, with your consent.
- **Improvement:** Enhancing our services and user experience.

Legal Basis for Processing

Our processing of your personal data is based on:

- **Consent:** When you provide explicit consent.
- **Contractual Necessity:** To fulfil our contractual obligations.
- **Legal Obligations:** To comply with legal requirements.
- **Legitimate Interests:** For business operations and fraud prevention.

Data Sharing and Disclosure

We may share your data with:

- **Service Providers:** For processing claims, underwriting, and other services.
- **Regulatory Authorities:** To comply with legal obligations.
- **Affiliates and Partners:** For joint marketing initiatives, with your consent.

Data Security

We implement reasonable security measures to protect your data, including encryption, access controls, and regular security audits.

Data Retention

We retain your data only as long as necessary for the purposes outlined in this policy or as required by law. Personal data of inactive users will be deleted after three years, with prior notification

User Rights

You have the following rights regarding your personal data:

- **Access and Correction:** Request access to and correction of your data.
- **Erasure:** Request deletion of your data under certain conditions.
- **Restriction:** Request restriction of data processing.
- **Portability:** Request a copy of your data in a structured format.
- **Withdrawal of Consent:** Withdraw your consent at any time.

Cookies and Tracking Technologies

We use cookies to enhance your experience on our website. You can manage your cookie preferences through your browser settings.

International Data Transfers

We may transfer your data to countries outside India, ensuring adequate protection through Standard Contractual Clauses or equivalent mechanisms

Children's Privacy

Our services are not intended for children under 18. We do not knowingly collect data from children without parental consent.

Changes to the Privacy Policy

We may update this policy from time to time. We will notify you of any significant changes by posting the new policy on our website.

Contact Information

If you have any questions or concerns about this Privacy Policy, please contact us at gcicare@generalicentralinsurance.com

9. Data Protection Impact Assessments (DPIAs)

A DPIA is a process for identifying and mitigating risks to the privacy and security of personal data. DPIAs are required for processing activities that are likely to result in a high risk to the rights and freedoms of data subjects, such as large-scale processing of sensitive personal data.

GCI shall conduct data protection impact assessments (DPIAs) once a year wherever applicable.

DPIAs shall be directed and monitored by the DPO or a designated member of the data protection team. The DPIA will include:

- A description of the processing activity and the personal data involved.
- An assessment of the necessity and proportionality of the processing.

- An assessment of the risks to the rights and freedoms of individuals.
- A description of the measures in place to mitigate those risks.

The results of the DPIA will be documented and retained for future reference.

10. Policy Compliance

- All Compliance to the data privacy policy shall be reviewed on an annual basis by DPO along with CISO to ensure continuous compliance monitoring through the implementation of compliance measurements and periodic review processes.
- The CISO is authorized to define operating process and guidelines for implementation and compliance of this policy and mandate the operating function to act accordingly.
- In cases where non-compliance is identified, the DPO shall review the reasons for such non-compliance along with a plan for remediation and report them to Information Security Steering Risk Management Committee (IS RMC).
- Depending on the conclusions of the review, need for a revision to the policy may be identified.
- In instances of persistent non-compliance by the individuals concerned, they shall be subject to action in accordance with the GCI Disciplinary Policy.

11. Dispute Resolution and Resources

Dispute Resolution and Escalation Process for Employees

- Employees with inquiries or complaints about the processing of their personal information shall first discuss the matter with their immediate supervisor. If the employee does not wish to raise an inquiry or complaint with an immediate manager, or if the manager and employee are unable to reach a satisfactory resolution of the issues raised, the employee shall bring the issue to the attention of the Data Privacy Grievance Authority. (Emailing at privacy.governance@generaliceutral.com)

Dispute Resolution and Escalation Process for Customer/ Third Party

- Customers / Third Party with inquiries or complaints about the processing of their personal information shall bring the matter to the attention of the Grievance Officer in writing. Any disputes concerning the processing of the personal information of non-employees shall be resolved through arbitration (Emailing at privacy.governance@generalicentral.com)

12. Data Classification Policy

Refer “*Information and Data Classification Policy*”

13. Roles and Responsibilities (Business Functions & Employees)

- **Data Stewards:** Assign data stewards responsible for managing data within their domains.
- **Employees:** Define the responsibilities of all employees in protecting data privacy.

14. Data Privacy Policy Owner

- DPO and CISO are owners of the Data Privacy Policy

15. Breach Reporting

- A “Data Privacy breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
- Usually, a Data Privacy breach happens when Personal Data (for example of clients or employees) is disseminated without authorization, e.g. stolen, lost or mistakenly disclosed.
- GCI would operate a Data Privacy breach reporting process to ensure that each incident is managed appropriately. This reporting process can leverage already existing reporting processes (for example the Compliance Reporting processes).
- GCI as required by local law and regulations would promptly notify affected individuals and/or the respective regulator and maybe the media when privacy is breached and the breach affects a predetermined number of individuals and/or meets certain other criteria.

Under this Policy, GCI is required to report breaches:

- to the DPO (subject to materiality thresholds as defined by data privacy policy)
- to the local Legal, Compliance or Risk Committee (subject to materiality thresholds as defined by data privacy policy)
- Reporting to the Senior and Business Management, the DPO, the local CEO, should be made within 5 working days of the discovery of the breach. Reporting to the local Legal, Compliance or Risk Committee should be made at the next possible occasion.