

Document Name	RHDFCL Data Privacy Policy
---------------	----------------------------

1. Introduction

This document outlines Religare’s approach to accomplish fundamental principles and guidelines for handling personal data and confidential information obtained from employees, clients, and external parties of Religare. By adhering to this policy, Religare ensures the privacy and security of the information entrusted to the organization. This Policy supports and builds upon Religare Information Security Policy’s section titled “Data Privacy policy”, regarding respecting and protecting confidential information.

2. Scope and Applicability

This policy applies to all users, including employees, contractors, temporary workers, and any other individuals who have access to personal data and confidential information as part of their roles or responsibilities at Religare. It encompasses all stages of information handling, from collection to storage, usage, disclosure, and eventual disposal.

All information pertaining to Religare, including client information, must be handled with utmost confidentiality, and should not be shared or distributed unless in compliance with this policy. If in doubt as to which category the information may fall into, consult with Legal and Information Security Group before sharing any such privileged information.

3. Legal and Regulatory Compliance

Religare is dedicated to adhering to all relevant data protection laws, regulations, and industry standards that apply to operations in India. The Data privacy policy is based primarily on the requirements of the Digital Personal Data Protection Act, 2023 of India (DPDPA), ensuring the protection and lawful processing of personal data for Religare users.

4. User Obligations of Religare

The following section captures the Users obligations and responsibility while handling Religare’s confidential information.

4.1 Handling of Religare Data

All Religare users have a responsibility to protect Religare's information based on their specific roles. It is crucial to note that personal information can only be shared internally or externally in accordance with the provisions of DPDPA—

- (a) for which the Data Principal has given her consent; or
- (b) for certain legitimate or lawful purposes or uses

- i. Religare users should seek guidance from leadership before sharing Religare business information internally or externally with explicit consent. Religare users must only distribute such information to authorized individuals and when it is necessary to accomplish a specific objective, such as directly providing services to a client.

4.2 Personal Data

All categories of personal data processed at Religare must be treated as per the requirements of DPDPA. Religare users must limit the sharing and access of personal data to individuals who genuinely require it to fulfil their job responsibilities

4.3 Direct marketing requirements

Religare users must not send direct marketing communications to individuals who have opted out of receiving them unless they have received specific consent to do so.

4.4 Sharing Client Information

Religare users must only share and/or grant access to client personal information with explicit consent or in line with certain legitimate or lawful purposes wherever deemed necessary.

- (i) The client has provided the explicit consent (including privacy notice) to; or
- (ii) Applicable law requires the distribution of such client personal information.

4.5 Data Minimization

Religare must implement data minimization practices, ensuring that the collection, use, and retention of personal data are limited to what is necessary for a specific purpose.

4.6 Incident Management

Religare users must refer to the Religare incident management policy for guidance and procedures regarding incident handling.

- If Religare users suspect or otherwise become aware of any event where personal data is involved and that may be defined as an Incident, they must

promptly (as soon as possible), notify their respective functional leader and their Information Security Group or CISO before taking any other action.

- If an Incident is confirmed, the responsible teams are required to determine appropriate remedial action. Remedial action may include internal and/or external communications depending on relevant obligations Religare has to clients and/or regulators for the protection of such Religare personal information.

4.7 Training and Awareness

Religare users must complete data privacy and confidentiality training assigned to them.

4.8 Further requirements

Religare users must comply with any additional data protection obligations, confidentiality obligations required by local Applicable Law and/or Professional Standards.

5. Data Principal Rights and Data Protection

All Religare users are required to establish procedures that uphold the minimum standards for safeguarding Religare Information as outlined in this Policy, along with other relevant policies, legal agreements, applicable laws, and professional standards. The below mentioned sub-section delve further into ensuring that there is compliance with the policy and procedure.

5.1 Notice and Consent

Religare to provide a clear and understandable privacy notice or statement to individuals whose personal data is being processed before the data is collected. This notice will inform them about how their personal data is being used and protected. The notices as minimum should include the following information :

- (i) the personal data and the purpose for which the same is proposed to be processed;
- (ii) the manner in which an individual may exercise their rights
- (iii) the manner in which the Data Principal may make a complaint to the Data Protection Board, in such manner and as may be prescribed.

5.2 Data Principal Rights

Religare must establish mechanisms to respond to data principal requests, including addressing questions, complaints, and managing requests to exercise their rights under applicable laws. Data Principal. The process should include:

- a. Guidelines on how to:
 - i. address questions or complaints from individuals relating to how Religare has processed their Personal Data; and
 - ii. Manage requests from Data Principals to exercise their individual rights under applicable law.
 - iii. Identify the information that has been requested,
 - iv. Before disclosing information, confirm the identity of the requestor.
 - v. If applicable, redact certain information that would breach privacy of others.
- b. Mechanisms for informing the respective individual when the request involves:
 - i. Right to access information about personal data
 - ii. Right to nominate
 - iii. Right to correction and erasure of personal data
 - iv. Right of grievance redressal.

The Information Security Group and legal team should guide the business heads for handling Data Principal requests and propose improvements for managing personal data, like ensuring its encrypted at rest and in motion, conducting regular privacy audits, and ensure compliance with the policy.

5.3 Risk Assessments: Third Party due Diligence and PIAs

Religare must conduct data privacy risk and compliance assessments on systems and third parties handling Religare personal data:

Third Party Due Diligence

- Religare should conduct data privacy risk and compliance assessments on third parties that handle Religare personal information including suppliers, acquisition targets and alliance partners.
- Third party due diligence should include an evaluation of data protection and confidentiality risks as part of the on boarding process for new suppliers or when there is a change in the processing of Religare personal information.

In case of third-party handling Religare personal data; third-party must be evaluated based on the risk that they present. Clauses like indemnification, LOL and insurance must be incorporated to accord legal protection to Data controller.

5.4 Fiduciary or Processor Determination

Religare should determine whether it is acting as the Fiduciary or processor with respect to each Processing activity.

5.5 Sharing Client Information

Religare must ensure that Religare users keep client personal information confidential and only share such information strictly in accordance with this policy. In addition, Religare must not enable sharing of client information with other Religare and other

third parties including third-party service providers or sub-contractors unless all the following requirements are met:

- a) There is an established business purpose for sharing the client personal information with each recipient.
- b) The client has provided the necessary consent for such sharing of client personal information or applicable law requires the distribution of such client personal information.

5.6 Cross-Border Personal Data Transfers

Religare should define and regulate cross-border transfers of personal data based on applicable laws. Religare shall ensure transfer is based on applicable laws and standards.

5.7 Annual Confirmation of Compliance

Religare users must confirm annual compliance with their obligations under this policy through the following process:

- a) Reviewing the policy annually
- b) Reporting any compliance exceptions to their business heads
- c) Taking appropriate steps to remediate or otherwise address relevant exceptions

5.8 Information Security

Religare users must maintain applicable technical, administrative, physical, and organizational security measures to protect Religare personal information as informed by the Information Security function.

5.9 Further requirements

Religare should monitor and implement any other additional local data privacy and protection requirements and the obligation to keep personal information confidential through formal training or other methods of awareness communication.

6. Data Storage, Retention and Deletion

Religare will ensure that the controls are in place and follow the below steps:

6.1 Data Retention and Storage

Religare will retain personal data only for as long as necessary to fulfil its intended purpose and in accordance with applicable laws and regulations. The retention period may vary based on the type of personal data and the purpose of processing. Religare will store personal data in a secure manner to prevent unauthorized access, loss, or misuse.

6.2 Data Deletion

Upon reaching the end of the retention period or when personal data is no longer necessary for the intended purposes, Religare will take appropriate measures to securely delete or anonymize the data. This applies to both electronic and physical records, ensuring that they are no longer accessible or recoverable.

6.3 Exceptions to Data Deletion

In some cases, Religare may be required to retain certain personal data for longer periods due to legal or regulatory obligations. In such instances, Religare will ensure that the data is protected and only retained for the necessary duration as mandated by the applicable laws.

6.4 Data Storage and Security

Religare will employ reasonable technical and organizational measures to safeguard personal data during its storage. This includes implementing appropriate access controls, encryption, and regular security assessments to maintain the confidentiality, integrity, and availability of the data.

6.5 Data Backup and Disaster Recovery

To ensure the resilience of personal data, Religare may perform routine data backups and maintain disaster recovery mechanisms. These measures are in place to protect against data loss or damage caused by unforeseen events such as system failures, natural disasters, or cyber incidents.

6.6 Secure Disposal of Data

When personal data reaches the end of its retention period and no longer serves a legitimate purpose, Religare will ensure its secure disposal. This may involve physical destruction or digital erasure to prevent unauthorized retrieval or misuse of the data.

6.7 Third-Party Data Processors

If Religare engages third-party data processors to handle personal data, it will be ensured that the third-party comply with Religare's data deletion, retention, and storage practices and adhere to applicable data protection laws and the contracts contain the necessary clauses for the same

In case Religare act as Data Processor, it shall notify all third party supporting its own processing of personal data of the deletion of personal data and shall ensure that all such third party shall either destroy or return the personal data-to-data controller, at the discretion of the data controller.

6.8 Audit and Compliance

Religare will regularly review and evaluate its data deletion, retention, and storage processes to ensure ongoing compliance with this policy and applicable legal requirements. Internal audits and assessments will be conducted to verify adherence to the defined data management practices.

For more information on the above section refer to Data Backup Policy for Religare.

7. Further Information

In case of any further information regarding the policy reach-out to the Religare information security group and legal team.

SPOC Details	Name	Email ID
Information Security SPOC	Mr. Dushyant Yadav	dushyant.yadav@religare.com
Legal SPOC	Mr. Rashid	rashid.mohd@religare.com

8. Appendix I- Definitions

For the purposes of this Policy:

- **Applicable Law:** means, with respect to a member of the RELIGARE Network or RELIGARE User, any laws, rules, regulations or directives applicable to such user.
- **Client Information:** means any information relating to the affairs of a current or former client obtained by Religare from a client or from a third party in connection with an engagement with such client.
- **Fiduciary:** means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;
- **Data Incident:** means any event that compromises the security, confidentiality, integrity or availability of any Religare Information, including any unauthorized or inappropriate disclosure, loss, use, destruction, alteration of, or access to, Religare Information.
- **Data Protection:** means the protection of Religare Information.
- **Religare Business Information:** means information Religare creates through business processes, intellectual property, Religare financial data. This includes all information that is created, collected, or modified by the Religare network and, including Material Non-Public Information and business product(s) created using public information regardless of whether the underlying data is publicly available. For example, the result of analyzing a data set of public records is a considered to be Religare proprietary.
- **Religare Information means:** (i) Personal Data; (ii) Third Party Information; (iii) Client Information; and (iv) RELIGARE Business Information.
- **Religare User** means every individual within RELIGARE including, but not limited to, partners, principals, employees, contractors, interns and other authorized Religare users. This also includes former employees subject to local confidentiality obligations that survive termination of employment.
- **Material Non-Public Information:** also known as insider information, describes the type of information Religare Personnel may not possess while trading securities. Material Non-Public Information includes anything learned because of a special relationship with a corporation or other legal entity or government entity. It includes

any information about the entity and its securities. It may also include information about other entities and their securities learned because of a special relationship with a client. For example, information that a client intends to make, or to assist in making, a tender offer for securities of a particular target company would bar RELIGARE Personnel possessing that information from trading in the target company's securities, as well as in the client's securities.

- **Personal Data:**, means any data about an individual who is identifiable by or in relation to such data

"Digital Personal Data" means personal data in digital form

- **Processor:** means the entity that processes Personal Data at the instruction, or on behalf, of the Fiduciary.

- **Process (in):** in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction

- **Privacy Notice:** it is a shorter and more concise document that provides a summary of key points of the privacy policy. It is often intended for the internal use and benefits of the Data Principals.

- **Professional Standards:** means the respective industry codes of conduct governing professional ethics and responsibilities, Bar Association rules and other standards pertaining to respecting confidentiality and maintaining protection of information.

- **Support Services Provider:** means internal support services utilized by a member of the Religare including but not limited to (a) general office support; (b) accounting and finance support; (c) network coordination; (d) IT functions including business applications, system management, and data security, storage and recovery; and (f) conflict checking, risk management and quality reviews.

- **Third Party Information:** means third party information other than Client Information disclosed (directly or indirectly) or made available to a member of the Religare Network or to any of its subcontractors or Support Services Provider under an obligation of confidentiality.