DATA PROTECTION POLICY

Ver 4.0

Document Control:

Document Name	Data Protection Policy
Document ID	TMF-POL-009
Security Classification	Internal

Authorization:

Document Owner	Reviewed by	Authorized by
Chief Information Security Officer	CTO	Management

Version Control:

Version	Modification Date	Brief description of the change
1.0	04-Mar-2020	Document Creation
2.0	21-Dec-2021	Annual Review
3.0	25 Jan 2023	Annual Review
4.0	25 Jan 2024	Annual Review

Table of Contents

1. Introduction....4
2. Scope....4
3. Objective....4
4. Roles and Responsibilities....5
5. Definitions....6
   5.1. Data Protection....6
   5.2. Personal Data....6
   5.3. Non-Personal Data....6
   5.4. Data Portability....7
6. Data Protection Policy....7
   6.1. Data Protection Risks....8
   6.2. Data Processing....8
   6.3. Data Protection Incident Management....8
   6.4. Data Storage....9
   6.5. Data Use....9
   6.6. Business Continuity Planning....10
   6.7. Data Classification & Disposal....10
   6.8. Third Party Compliance....10
   6.9. Awareness, Culture, and Communication....10
   6.10. Privacy by Design....11
   6.11. Data Protection Impact Assessment (DPIA)....11
   6.12. Rights of Data Principals....11
   6.13. PII Data Disclosure....11
   6.14. Data Accuracy....12
7. Compliance....13
   7.1. Policy Review, Revision and Communication....13
   7.2. Disclosing data for other reasons....13
   7.3. Subject access requests....13
   7.4. General Staff Guidelines....13

1. Introduction

Tata Motors Finance (TMF) is committed to national and international compliance with data protection laws. This Data Protection Policy applies worldwide to the TMF and subsidiaries, and is based on globally accepted, basic principles on data protection. Ensuring data protection is foundation of trustworthy business relationships and the reputation of the TMF as an attractive employer.

The Data Protection Policy provides one of the necessary frameworks with conditions for safeguarding data in the enterprise and in cross-border data transmission. It ensures enablement of adequate level of protection as prescribed by the national laws for security in storage / at-rest, and in transmission, including countries that may not yet have adequate data protection laws.

The importance of data protection increases as the amount of data created and stored in the course of business operations, continues to grow at unprecedented rates. This is especially so as TMF has to manage the risk of non-personal (business) data and personal information (PII) collected during the course of business operations.

Consequently, a large part of the strategy is in protecting data from compromise and ensuring data privacy and other key components of data protection, ensuring the confidentiality, integrity and availability through quick restoration after any corruption or loss.

The effective enablement of this Policy will foster a culture of data protection across the organization resulting from overall confidence from secure processing of personal and non-personal data. The organization will also benefit from regulatory compliance which usually result in reduced risk of penalties and reputational damage non-compliance.

2. Scope

This policy applies to all subsidiaries of Tata Motors Finance Holding Limited (TMFHL) namely Tata Motors Finance Limited (TMF) and Tata Motors Finance Solutions Limited (TMFSL), collectively referred to as TMF in this document

This Policy covers all employees of TMF and its subsidiaries, contractors, consultants, partners and any other external entities.

Generally, the Policy will also apply to anyone who collaborates with or acts on behalf of TMF and may need access to TMF data.

3. Objective

The purpose of this policy is to provide the direction to ensure the security of and to protect all the business data in the enterprise, including personal information of employees, contractors, vendors, interns and customers.

While providing the direction for data protection, the policy will seek to include fundamental provisions for enabling of privacy controls for data security.

4. Roles and Responsibilities

All users at TMF are responsible for ensuring data is collected, stored and handled appropriately. Each team that handles personal or non-personal data must ensure that it is handled and processed in line with this policy and data protection principles. All employees are responsible for ensuring that they meet the requirements of the regulation. They should familiarize themselves with this policy and related documents.

The following persons, in the organization, are identified to have key responsibility:

Data Protection Officer
Has overall responsibility for privacy compliance and protection of personal / non-personal data as a data controller and data processor with applicable regulations.

Data Protection Officer - will have responsibility for the following, but not be limited to:

- Keeping the Board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data TMF holds about them (also called 'Subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the TMF's sensitive data.

IT Manager / CIO / CTO
Will have responsibility for the following, but not be limited to:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services that TMF is considering using to store or process data. For instance, cloud computing services.

IS Manager / CISO
Will have responsibility for the following, but not be limited to:

- Enablement and management of data protection / security controls and procedures.
- Review and audit of people, processes and technologies enabled in TMF and related to data protection.
- Responding to any incidents of data breach / loss / leak / compromise.
- Conducting awareness and training programs for TMF users along with the DPO.

- Approving any exceptions from the Data Protection Policy.
- Addressing any data protection queries from journalists or media outlets like newspapers.

5. Definitions

5.1. Data Protection

Refers to the process of ensuring / enabling safeguards and security of enterprise information from breach, loss, leak, corruption or compromise? Data protection controls should be enabled to provide the protection during all data states, and this included data-at-rest, data-in-transit.

5.2. Personal Data

Data protection regulations and laws have identified elements of personal information that must be protected and this is termed as Personally Identifiable Information (PII). Such information relates to a person and includes, but is not limited to the following:

- Password(s);
- Phone, Address etc. which can be used to identify a person;
- Financial information of the individual;
- Physical, physiological and mental health condition;
- Sexual orientation;
- Medical records and history;
- Biometric information;

5.3. Non-Personal Data

Present day regulation identifies non-personal data as a distinct separate information asset in the organization. The law also has set a different set of regulations for such data assets. Such information relates to the organization and includes, but is not limited to the following:

- Business information held in emails, files, other forms of communication
- Financial information and reports
- Internal performance information
- Payroll information
- Sales and marketing plans
- Audit reports etc

5.4. Data Portability

The ability to move data among different application programs, computing environments or cloud services.

6. Data Protection Policy

During the course of business, TMF needs to gather, produce and use certain information that is confidential or private, and may be personal or non-personal in nature. The security of such information is important for TMF to maintain business leadership and as per industry best practices or regulatory requirements.

This policy provides the guidance for the collection, management and protection of data in TMF to meet data protection laws / regulations and adhere to best practices. This is to be achieved through effective controls and procedures to prevent data breach, loss, leak or compromise.

TMF collects information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available, it is important to ensure the following:

That data will be:
- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the TMF within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

That data will not be:
- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the TMF has direct obligations towards people to whom the data belongs. Specifically, we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

To exercise data protection TMF is committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures

- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.

6.1. Data Protection Risks

Data in an organization comprises personal and non-personal information which can be confidential, or sensitive requires adequate safeguards, to protect it as well as TMF from some very real risks and threats, including, but not limited to:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Loss of Business**. Customers / associated may terminate business relations in event of a data breach / leak loss.
- **Regulatory penalties.** In event of non-compliance or due to an incident leading to data breach/loss/leak.
- **Reputational damage**. For instance, the TMF could suffer if hackers successfully gained access to sensitive data.

6.2. Data Processing

Personal data of customers / employees and non-personal data (relating to TMF business) will be securely stored, in electronic form, and in accordance with the provisions of TMF policies for Information Security, the IT Act and any other applicable laws for Privacy.

In addition, data collected for a specific purpose, product or service may be stored at TMF with other information relating to an individual, and only in accordance with the data protection principles mentioned in this Policy.

6.3. Data Protection Incident Management

Any incident or event of data breach / compromise / loss / leak, or a violation of the guidelines set in this policy must be reported immediately to the IS Manager / CISO and respective service line leaders so that the exposure can be contained.

The procedures and guidance as set in the TMF Incident Response & Management Policy will be invoked and followed.

Incidents should be followed up with appropriate response and mitigated. Upon closure TMF team will carry out a forensic investigation and conduct a root cause analysis to understand the causes, and update the internal procedures accordingly.

6.4. Data Storage

When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the TMF's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

6.5. Data Use

TMF collects personal data in the course of business operations and should ensure the security of the same during the lifecycle. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, breach or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally. In particular, sharing via email should be in a secure manner, as this form of communication is easily breached.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorized external contacts.
- Personal data should never be transferred outside of the organization.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

6.6. Business Continuity Planning

The key principles of data protection are to safeguard and make available data under all circumstances. As such data protection strategy should be included and planned along with the TMF BCP/DR and Backup team.

6.7. Data Classification & Disposal

Data Protection best practices require that data, especially personal data, should only be stored for a time period necessary for its processing and thereafter, (at the end of the lifecycle) it should be securely destroyed.

Data should be classified to identify the criticality and sensitivity, as per the Data Classification Policy and shall be disposed at the end of the lifecycle accordingly. The retention, disposal and destruction procedure will be followed as per the IS Policy other internal procedural documentation.

6.8. Third Party Compliance

A number of TMF business processes depend on third party vendors and the provision of this Policy shall apply to all outsourcing contracts. Privacy, protection, disposal and other related requirements shall be included in outsourcing agreements.

Therefore, TMF need to make sure their third parties comply with privacy requirements and follow strict security policies and controls, aligned with TMF policies and controls.

6.9. Awareness, Culture, and Communication

TMF shall periodically conduct awareness programs to develop a culture of data privacy by making employees aware about the best practices to handle personal and non-personal data in the conduct of business

The provisions and expectations for this policy shall be communicated to all users.

6.10. Privacy by Design

Best practices require that new services, products, technologies or business expansion, should include data protection principles from the design and strategy stage. TMF will ensure that any processes or technologies being inducted within the organization will include requirements of data protection and privacy in the design or agreement.

6.11. Data Protection Impact Assessment (DPIA)

TMF will undertake to carry out a Data Protection Impact Assessment in respect of critical and sensitive data, whether personal or non-personal. This will help evaluate risks due to outsourcing, or internal processing.

6.12. Rights of Data Principals

The data principal is the person who has entrusted TMF with PII and has the right to access their data, right to seek correction of their data, right to portability of their data, and the right to be forgotten.

TMF is committed to respecting the rights of data principals and will enable appropriate processes and technologies to comply with any requests in a timely and efficiently. This will provision the means for consent, approval and notice as defined in the PDPB.

6.13. PII Data Disclosure

TMF shall not disclose the personal data of any individual, held by it, outside the organization except

- When TMF has express consent to do so, or in circumstances as agreed between TMF and the individual.
- When necessary, to regulatory bodies, law enforcement agencies and auditors.
- When TMF is required or permitted to do so by law.
- To fraud prevention agencies where required.

6.14. Data Accuracy

The law requires TMF to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort TMF should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- TMF will make it easy for data subjects to update the information TMF holds about them. For instance, via the TMF website.

- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the responsibility of the data owner to ensure marketing databases are checked against industry suppression files every six months.

TMF shall maintain physical, technological and procedural safeguards and security that comply with the IT Act and applicable Privacy legislations and obligations.

In addition, training procedures shall be in place for all users at TMF to ensure high standards in relation to data protection.

Some essential steps to be followed by TMF users are listed to ensure data privacy:

a. Access to sensitive data shall be provided strictly on the basis of need to know.
b. Backup should be kept in a safe and secure environment.
c. Sensitive personal data should be shared only against proper authorization.
d. Data kept in file servers, or shared servers should have proper access controls.
e. Logs of the systems should be taken periodically and reviewed to identify the user accesses for the applications and servers containing sensitive personal data.
f. Strict disciplinary actions should be taken if any breach of data protection standards is identified as per this policy.
g. Data privacy should be ensured in using TMF resources such as laptops, online applications, external storage devices, file servers, records and documents.

7. Compliance

TMF users are expected to comply with the requirements of this Policy. Failure to comply with the provisions of this policy may, at the discretion of TMF management, result in disciplinary action as per the effective rules and policies.

7.1. Policy Review, Revision and Communication

This policy shall be reviewed and updated once every year to incorporate relevant changes. All subsequent updates to the policy shall be communicated over email and made available to all employees.

7.2. Disclosing data for other reasons

In certain circumstances, TMF may allow personal data to be disclosed to law enforcement agencies without the consent, or notice, of the data subject.

Under these circumstances, TMF will disclose requested data. However, the DPO/CISO/ Management will ensure the request is legitimate, seeking assistance from the Board and from the Legal advisers as necessary.

7.3. Subject access requests

All individuals who are the subject of personal data held by TMF are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the TMF requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the DPO/CISO.

TMF will verify the identity of person making a subject access request as well as the validity of the request before handing over any information.

The TMF has a privacy statement, setting out how data relating to individuals is used by the TMF and related information.

7.4. General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.

- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **TMF will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorized people, either within the TMF or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

-EOF -