Tech Mahindra GDPR Data Privacy Compliance Statement

Dated 06-Jun-2018

V1.1

Table of Contents

1. OUR COMMITMENT TO DATA PRIVACY

Tech Mahindra is committed to place high priority on protecting and managing data in accordance with accepted standards including ISO 27001, NIST framework and PCI-DSS. The company has compliance with applicable EU GDPR regulations, including as a data processor, while also working closely with our customers and partners to meet contractual obligations for our procedures, products and services.

Tech Mahindra is committed to safeguard the personal information we collect, process, and store on behalf of our clients and business partners. In particular, we are committed to ensuring that any personal information entrusted to us is safeguarded an appropriate level of security protection and is only used in a way that our clients' customers and employees would reasonably expect.

2. HOW WE MANAGE DATA PRIVACY: SUMMARY AND HIGHLIGHTS

We take data privacy seriously. We have developed Data Privacy, and Protection framework to ensure that our organization and services are compliant with applicable data privacy laws and that wider data privacy risks are effectively managed.

Our approach:

1. Starts with our Data Privacy and Protection Policy and Framework, which sets out senior management commitment to comply with data privacy laws in all the jurisdictions in which we do business and the standards of behavior expected of our people when working with each other, our clients, and our business partners;
2. The Processes are underpinned and supported by appropriate standards, and standard operating procedures that have been specifically designed to ensure that data privacy risks are effectively managed across our businesses; Focuses on establishing a sustainable data privacy control framework, which places sufficient emphasis on the implementation and continual improvement of effective data privacy control.
3. **Governance**- Driven by Steering Committee of CISO (Chief Information Security Officer), CIO, Legal Officer, and DPO (Data Privacy Officer) who are responsible for promoting compliance and awareness of applicable data privacy laws, advising on the implementation of our data privacy policies and standards, and monitoring compliance in jurisdictions across the globe Governance which includes Data Protection Officers among others, coordination with privacy lawyers, Legal Function, security and cybersecurity professionals at Corporate and Delivery Units for customer engagement dedicated to ensuring deployment of the data privacy as per GDPR
4. **Awareness** -Privacy and security awareness training for associates through e- learning and test, including account-specific privacy and security training as per customer engagements
5. **Security** Compliance with security standards' best practices
6. **Incident Management** -Security incident response process and client-specific incident response plans as Tech Mahindra takes all security incidents very seriously
7. **Polices and Processes** -Update and implementation of privacy and security policies, guidelines, and tools for GDPR compliance to integrate privacy-by-design, data minimization, third-party due diligence
8. **Data Subject Rights** -Update of data subject rights policies to GDPR
9. **Assurance and Audits**- Regular maturity assessments, bench markings and audits with results communicated to the highest level of management with mandatory remediation plans.

3. DETAILS OF APPROACH FOR DATA PROTECTION COMPLIANCE

3.1 STRATEGY & GOVERNANCE

1. We have established DPO who reports to Vice Chairman as well as to Executive Steering Committee.
2. CISO Function comprises a number of full-time privacy professionals. We nominate compliance officers for functions and delivery units who are responsible for implementing Tech Mahindra Data privacy program, designing and developing data privacy compliance solutions.

3. These compliance officers across our businesses are responsible for ensuring that our data privacy policies, standards and procedures are implemented across our business areas and are operating effectively.

3.2 INFORMATION SECURITY AND DATA PROTECTION

1. Our strategic data security approach is to build controls to protect, detect, respond to, and recover from adverse cyber and information security events. We maintain a suite of data and cyber security policies that set out our commitment and expectations for the protection and security of personal information.
2. Data at rest, data in motion are encrypted and access to data are controlled as appropriate
3. We implement a security, data privacy awareness and training program to raise our colleagues' awareness of their responsibilities for the protection of personal data.
4. We operate a global security operations center to monitor, detect, manage and respond to security incidents, including any cyber threats to our network and systems.

3.3 DATA LIFECYCLE MANAGEMENT

1. We maintain as per customer inputs, appropriate ROP (records of processing activities) involving personal information, which will provide us with a view of where we collect, use, retain, and disclose personal information across our business globally. These processing records have been designed to enable us to meet our data privacy legal and regulatory obligations GDPR etc.).
2. We have implemented appropriate procedures to ensure our processing records are reviewed periodically by customers. We have processes in place to help us determine our legal basis for processing (e.g., legitimate interests; consent):
3. We leverage our data inventory to document our view of our processing;
4. We take steps to ensure we have the corresponding notice and consent tracking actions in place where required.

3.4 PRIVACY BY DESIGN (PBD)

1. We conduct and maintain PIA (Privacy Impact Assessment) for the processes, projects, accounts and functions. We carry out RA (Risk Assessment) and Gap Assessment to address risks and gaps to mitigate them. We maintain PIA procedures to ensure projects involving personal information undergo review prior to implementation to ensure data privacy risks posed to data are identified and effectively managed.
2. Privacy by Design control concepts in Software, Application design are practiced by Solution Architects, Solution Designers
3. Data Minimisation: We have mechanisms to help ensure personal information we collect from our clients is restricted to the minimum we need to provide our services. Data Retention: We adopt data retention standards and schedules establishing the limits on retaining client data. Data Destruction: We have processes to securely erase data in accordance with our retention standards

3.5 PRIVACY INCIDENT MANAGEMENT

1. We take a multidisciplinary; inter function coordinated holistic incident response approach communicated to the stakeholders.
2. This approach is reviewed and updated on a regular basis to help ensure that it incorporates changes in applicable laws and regulations (e.g., GDPR).
3. We have robust processes in place to ensure that incidents are identified and responded to effectively.
4. We track and monitor potential incidents and undertake root cause analyses to help minimise the risk of similar potential issues occurring in the future.

3.6 REGULATORY CHANGE

1. Legal team keep abreast of updates in the data privacy legal and regulatory landscape, particularly where there may be changes that affect our global businesses.
2. We undertake impact assessments to determine what impact those changes may have on our personal information processing activities.

3.7 DATA PROCESSOR AND SUPPLIER ACCOUNTABILITY

1. Pre-Contract: We undertake supplier due diligence of third parties with whom we engage to ensure that their privacy environment meets our expectations in line with our legal, regulatory and contractual commitments and obligations.
2. Contract: We adopt a supplier, sub processor contractual framework methodology with appropriate privacy clauses in line with applicable legal requirements.
3. On-going assurance: We have an ongoing assurance programme which assesses third party vendors against our data privacy and security requirements

3.8 RISK AND CONTROL

1. We have appropriate processes in place to identify data privacy risks commensurate with our legal and regulatory obligations. We design, develop, and implement risk-justified controls to ensure data privacy risks are effectively managed.
2. We carry out RA (Risk Assessment) and Gap Assessment to address risks and gaps to mitigate them.

3.9 TRAINING AND AWARENESS

1. Our associates are required to complete global privacy training and exam, which sets out Tech Mahindra and its customer's expectations and requirements in the handling of personal information.
2. We require certain colleagues to complete role specific or country specific training if there are specific actions we expect them to undertake.
3. We conduct regular awareness campaigns and ad-hoc training roadshows to reinforce key training messages.

3.10 POLICY MANAGEMENT

1. We have in place a published Corporate Privacy Policy to provide a clear framework for setting data privacy objectives across our business and to set the minimum standards and internal controls that must be adhered to by our colleagues when handling personal information.
2. Our Corporate Privacy Policy is communicated to colleagues as part of their data privacy training and within our Code of Business Conduct, which is reaffirmed and refreshed by associates on an annual basis.
3. Our externally facing privacy statements provide transparency of our data processing activities.

3.11 INDIVIDUAL RIGHTS PROCESSING

1. Data Subject Rights: We have in place standard operating procedures to ensure we take a consistent and rigorous approach, in line with our legal and contractual obligations, to managing requests from individuals to exercise their rights under data protection laws (including, for example, rights of access, rectification, erasure and objection to processing).

3.12 CROSS-BORDER DATA STRATEGY

1. We implement appropriate agreements with our customers, suppliers and group legal entities which incorporate EU standard and model contractual clauses where appropriate to legitimise the processing of personal information undertaken across Tech Mahindra globally.
2. We review all of our global processes and apply a consistent and rigorous approach to the management of how personal data is used and stored globally.

3.13 ASSESSMENTS, AUDITS AND MONITORING

1. At the core of our approach to data privacy is the need to undertake ongoing and sustainable monitoring of our processes and procedures to help ensure that the activities which we undertake are appropriately addressed through regular assessments, bench markings, audits and monitoring
2. Where issues are identified we have processes in place to report, respond to, remediate, and document those issues.

4. CONTACT INFORMATION

Tech Mahindra's Data Protection Officer who can be contacted at DPO@techmahindra.com.