Privacy Policy

Important: The printed copy of this document is not under control

Table of Contents

1. Preamble

Persistent Systems Limited, its subsidiaries and affiliates and any other directly controlled entities as may exist from time to time and their web presence created from time to time, hereinafter referred to as 'Persistent,' is committed to respect user's privacy and choices.

As a global software company, Persistent's primary internal asset impacting all aspects of its operations is its People. As a part of ongoing operations, Persistent is required to meet stringent contractual and regulatory requirements both for itself as well as those applicable to its customers, not only in geographies where Persistent operates but also in geographies where its customers are located. In its everyday business operations, Persistent makes use of variety of Privacy data about identifiable individuals, including data about:

a) Current, past, and prospective employees
b) Data placed in Persistent's control as part of a valid agreement with customer.
c) Users of its websites
d) Customer
e) Vendors
f) Partners
g) Visitors
h) other stakeholders

In collecting and using this data, Persistent is subject to a variety of legislation controlling how such activities may be conducted and the safeguards that must be put in place to protect it.

It is therefore necessary to have a privacy policy to lay down the guiding principles and responsibilities necessary to safeguard personal data at Persistent.

2. Scope

This Persistent Systems Privacy Policy (Privacy Policy) applies to Persistent Systems Limited("Persistent Systems "or "Persistent"), its subsidiaries and affiliates and any other directly controlled entities as may exist from time to time and their web presence via the domains Persistent.com, Accelerite.com and any other domains created from time to time, hereinafter referred to as 'Persistent', 'we', 'us' or 'our' is committed to respect your privacy and choices.

This Privacy Policy (herein referred to as "Privacy Policy), applies to all Personal Identifiable Data and Sensitive Personal Data or Information (collectively herein referred to as "Personal Data" processed by Persistent.

3. Objective

This Persistent Systems Privacy Policy explains the collection, use, processing, transferring and disclosure of personal data by Persistent. It applies to any personal data collected directly and from other sources, subject to local law, by Persistent.

4. Management Commitment to Privacy

The Persistent Privacy Policy delineates the company's objectives concerning privacy management and underscores management's unwavering commitment to privacy protection. The application of this policy is mandatory for all group companies, business lines, subsidiaries, and affiliates, including all operations performed on personal data. All employees and third-party entities (Suppliers, Vendors, etc.) associated with Persistent are obligated to adhere to this policy. Furthermore, the policy encompass all information systems and facilities involved in the processing and storage of personal data, encompassing not only internal systems owned by the company but also those employed in operations and projects executed on behalf of its customers.

5. Privacy Information Management Systems (PIMS)

a) The Persistent Information Management System (PIMS) seamlessly integrates policies, procedures, and innovative technologies to ensure strict adherence to regulatory mandates and industry standards. Our approach incorporates rigorous Technical & Organizational Measures (TOMs) meticulously designed to address privacy obligations and bolster security measures, in alignment with both regulatory mandates and client-specific requirements. In navigating the complex landscape of legal statutes and client obligations, PIMS goes beyond mere compliance, embracing both data controller and data processor responsibilities.

b) We steadfastly uphold the fundamental principles of data privacy, including:

/ Lawfulness, Fairness, and Transparency
/ Limitations on Purposes of Collection, Processing, and Storage
/ Data Minimization
/ Accuracy of Data
/ Data Storage Limits
/ Integrity and Confidentiality

c) The PIMS thus ensures a comprehensive compliance framework across all operational dimensions. These principles are tightly integrated with the Technical and Operational controls implemented across the data lifecycle of Privacy related data at Persistent.

6. Personal data that we collect.

a) For the purposes of this privacy notice, 'Personal Data' is any data which relates to an individual who may be identified from that data, or from a combination of a set of data, and other information which is in possession of Persistent.

b) In general, you may browse our website without providing any personal data about yourself. However, we collect certain information such as:

i. Personal Data that you provide via our website, including information you provide through forms on this Site e.g., name, email address, designation, and company, including LinkedIn profiles/ URLs if provided.

ii. information about your computer and about your visits to and use of this Site, such as your Internet Protocol (IP) address, demographics, your computers' operating system, and browser type and information collected via cookies.
iii. Cookie related details are provided in the Cookie Policy.
iv. Personal data that you provide as part of employment application process, e.g., curriculum vitae (CV), cover letter, employment and education history, reference contact information, remuneration details, LinkedIn profile, photo, etc.
v. Personal data collected or created as part of employment, e.g. name, address, social security identification number, government identification details, records of personal and family particulars, education and qualifications, employment history, salary and allowances, terms and conditions of service, medical records, leaves, training, investments, outside employment, appraisal reports, assessment panel's comments, promotion board assessments and reports, conduct and discipline, career development, retirement and pension, re-employment or extension of service and renewal of agreement or revision of agreement terms.
vi. Customer and supplier partner details such as name, email address, contact details.
vii. Audio-Visual information such as photographs or images captured, video recordings (if enabled), when attending any of our events, webinars etc.
viii. Any correspondence including queries, feedback and comments submitted by you.

7. Use of your personal data:

Persistent respects your rights and ensures adherence to applicable laws and regulations. The basis of processing is aligned to applicable legal obligations, contractual agreements, legitimate interests, and explicit consent from you. We use your data:

i) To provide the requested information and services.
j) To enable us to better understand your requirements and get into agreements such as customer, vendor partner, employment contracts.
k) To communicate with you on your queries, feedback, or comments.
l) To enable marketing or promotional campaigns.
m) For web site performance, security, and usage/ data analysis.
n) To provide essential employment management services.

8. Data recipients, transfer, and disclosure of your personal data

We share your personal data:

a) Within Persistent and/ or with any of its subsidiaries.
b) Customers and business partners.
c) Service providers.
d) Authorized third parties.
e) Auditors.
f) Government institutions, law enforcement agencies or other bodies, where applicable to comply with legal requirements.
g) We may use the information to exercise our legal rights and to defend against legal claims.

h) We may use the information to investigate, prevent, and/ or act against any suspected fraud, illegal activities, situations leading to physical safety to any person, or as otherwise required by law.
i) We may share information in-case of any requirements arising out of Merger & Acquisitions.
j) We may transfer your data outside of the country or region of residence by ensuring reasonable security and contractual controls in-line with applicable data protection laws.

9. Technical and Organizational Measures

Persistent employs robust and effective technical and organizational measures (TOMs) to safeguard personal data against unauthorized or unlawful access, use, disclosure, alteration, or destruction. These measures are tailored to the specific context, purpose, and scope of data processing activities, encompassing the following:

a) **Robust Technology and Security controls**: Detailed descriptions of these controls are available on our Information Security page, accessible **here**.

b) **Data Protection Measures**: Within our Privacy Information Management System (PIMS) framework, we implement robust measures such as data classification, access controls, encryption protocols, and ongoing monitoring to mitigate privacy risks and safeguard personal data throughout its lifecycle.

c) **Security Protocols**: Persistent enforces stringent security protocols to ensure privacy and prevent unauthorized access or breaches. These measures include encryption protocols, encryption/de-identification techniques, access controls, vulnerability assessments, and intrusion detection systems, fortifying our defenses and minimizing the risk of data breaches.

d) **Privacy by Design and Default**: Our application development processes embed strategies, guidelines, and validations to promote responsible data-centric innovation in compliance with data privacy regulations, meeting both end-user and client expectations. Privacy enhancing technologies (PETs) such as Data Encryption at rest and in motion, Differential privacy, anonymization, data minimization and purpose limitation techniques are used to further enhance data security and privacy compliance.

e) **Lawful Basis for Processing**: As a controller of privacy data, Persistent relies on explicit consent or a legal basis for the collection and retention of personal data in accordance with our privacy policy. When acting as a processor, our customers determine the appropriate legal basis for processing activities. We retain personal data to comply with retention or statutory limitations or for contractual purposes only, safeguarding and limiting active use where technical limitations prevent deletion or anonymization. Persistent is a software development company and we do not use customer data for any other secondary purposes nor rent, sell, or provide personal data to third parties for purposes other than completing transactions/services.

f) **Data Protection Impact Assessments**: These assessments are conducted for every new process or when there is a change in existing processes involving the processing of

personally identifiable information (PII) or sensitive personal information (SPI), ensuring secure and compliant processing across the delivery lifecycle.

g) **Compliance Assurance**: In adherence to regulatory mandates, Persistent maintains transparent processes for handling Data Subject Access Requests (DSARs), providing prompt and compliant responses to individuals inquiries regarding their personal data. Privacy notices are provided at the time of data collection for both internal and external data subjects, with privacy statements available publicly to external data subjects. These notices and statements are regularly updated to reflect changes in personal data processing or Data Privacy regulations.

h) **Training and Awareness**: Persistent invests in comprehensive training and awareness programs to educate employees on privacy best practices, regulatory requirements, and their roles and responsibilities in protecting personal data. Our privacy program remains adaptive and responsive to evolving requirements by monitoring emerging privacy regulations and industry trends, incorporating key learnings from incidents into privacy awareness initiatives.

i) **Third Party and Vendor Data Privacy**: Given the increasing reliance on outsourcing, including cloud service providers, for both Persistent and our customers, managing supply chain risk and vendor data privacy has become strategically significant. We have comprehensive guidelines for suppliers/vendors to adhere to strict obligations imposed under contracts and applicable laws. Technical and operational controls are established through contracts with third-party data processors and sub-processors, ensuring sufficient guarantees and obligations regarding data protection and security.

10. Robust incident management and breach handling

a) At Persistent, we maintain robust mechanisms for detecting, assessing, containing, and managing personal data breaches and incidents. Our well-defined processes and procedures ensure timely responses to breach notification obligations in accordance with applicable laws. In cases where an incident or breach is deemed to have a high impact or is mandated by law, affected data subjects and/or supervisory authorities are promptly notified. We implement well-established processes and playbooks through our 24x7x365 Security Operations Center to address such data breach incidents effectively. For more information on our cyber resilience practices, please visit our Cyber Resilience page.

b) We exercise a Zero tolerance policy with punitive and/or disciplinary actions in case of breach caused by human error. To control such errors, at Persistent we have process in place to take all personnel with exposure to personal data, go through mandatory privacy training course, accept the Acceptable Usage policy and we secure Privacy consent from all the users of the information systems and assets at Persistent.

11. Your Rights

Subject to local laws of your country, there are certain rights of a data subject/ principal, including but not limited to right to access information about personal data, obtaining information of processing, right to withdraw consent, right to correct inaccurate or incomplete personal data, erasure or restriction in processing of personal data, right to object to processing of personal data,

in some geographies the right to portability and right to complaint to Persistent's Privacy Officer (privacyofficer@persistent.com) and/ or respective data protection authority.

12. Certifications

Our commitment to safeguarding personal data remains steadfast, aligning with client expectations and regulatory mandates. This dedication is further underscored by our other certifications:

ISO 27701:2019 – Privacy Information Management System
ISO 27018:2014 – Securing Personal Data in Cloud
System and Organization Controls (SOC) 2 Type 2

Through these certifications and ongoing compliance efforts, Persistent demonstrates its unwavering commitment to transparency, integrity, and excellence in privacy and security practices. This commitment instills confidence in our stakeholders and reinforces our position as a trusted industry leader.

13. Contact Us

If you have any questions regarding our privacy practices or this privacy policy, please contact us at privacyofficer@persistent.com

Alternately you can write to us at:
Privacy Officer
Persistent Systems Ltd
Bhageerath, 402 E, Senapati Bapat Road
Pune – 411 016,
State: Maharashtra
Country: India

14. Updates to this privacy policy

Persistent may change the data privacy practices and update this privacy policy as and when the need arises, and the same will be made available on the website.