

India Digital Personal Data Protection Notice

Effective Date: September 18, 2026

This Privacy Notice ("Notice") applies only to individuals who are located in India and whose digital personal data is processed by Everise, including customers, members and end users of our clients, users of our website, visitors to our facilities and events, employees, contractors, job applicants, vendors, suppliers and business partners ("Data Principals" or "you"). For the purposes of this Notice, "Everise", "we", "us" and "our" mean Everise (India) BPO Services Pvt. Ltd. and, where applicable, its affiliates and group companies that process personal data in connection with the activities described in this Notice. Depending on the circumstances, Everise may act either as a Data Fiduciary or a Data Processor under applicable law.

We adopt this Notice to comply with the Digital Personal Data Protection Act, 2023 (Act 22 of 2023) ("DPDP Act"), the Digital Personal Data Protection Rules, 2025 notified vide G.S.R. 846(E) dated November 13, 2025 ("DPDP Rules") and other applicable Indian data protection laws, rules and regulations ("Applicable Privacy Laws"). Terms defined in the DPDP Act shall have the same meaning when used in this Notice.

Statutory Status and Commencement

The DPDP Act received the assent of the President on August 11, 2023. By notification G.S.R. 843(E) dated November 13, 2025, the Central Government appointed the commencement dates of the provisions of the DPDP Act in a phased manner, as follows:

- With effect from November 13, 2025: section 1(2), section 2, sections 18 to 26, sections 35, 38, 39, 40, 41, 42 and 43, and sections 44(1) and 44(3), which principally establish the Data Protection Board of India and the rule making powers of the Central Government.
- With effect from November 13, 2026: section 6(9) and section 27(1)(d), which relate to Consent Managers.
- With effect from May 13, 2027: sections 3 to 5, sections 6(1) to 6(8) and 6(10), sections 7 to 17, section 27 other than clause (d) of sub-section (1), sections 28 to 34, sections 36 and 37, and section 44(2), being the substantive obligations of Data Fiduciaries and the rights of Data Principals.

Rule 1 of the DPDP Rules provides a corresponding phased commencement. Rules 1, 2 and 17 to 21 came into force on November 13, 2025. Rule 4, on the registration and obligations of Consent Managers, comes into force on November 13, 2026. Rules 3, 5 to 16, 22 and 23 come into force on May 13, 2027.

Everise is publishing this Notice in advance of the commencement of the substantive obligations so that Data Principals in India understand how their personal data is collected and processed. Where this Notice describes an obligation that takes effect on May 13, 2027, Everise is undertaking preparations and implementing controls, policies and processes, on a phased basis during the transition period to support compliance with the DPDP Act and the DPDP Rules."

This Notice will be reviewed and updated before that date and on the issuance of any further notification, order, standard or direction under the DPDP Act or the DPDP Rules.

Disclaimer

.

The rights described in this section apply to the extent Everise acts as a Data Fiduciary in relation to the relevant personal data. Where Everise processes personal data solely on behalf of a client as a Data Processor, the relevant client will generally be responsible for responding to and fulfilling requests made

under the DPDP Act. If Everise receives a request relating to personal data processed on behalf of a client, Everise may redirect the request to the relevant client or assist the client in responding in accordance with applicable contractual and legal requirements.

In respect of the personal data of customers, members and end users of our clients, Everise does not alone, or in conjunction with other persons, determine the purpose and means of processing. Everise processes that personal data as a Data Processor, on behalf of and in accordance with the documented instructions of the relevant client, which is the Data Fiduciary. In respect of personal data that Everise collects and uses for its own purposes, such as personal data collected through our website, our facilities and events, our marketing activities and our employment and procurement relationships, Everise determines the purpose and means of processing. Everise commits to maintain transparency by responding to legitimate requests from Data Principals in India through proper channels and in consonance with Everise data privacy policies. Where a request relates to personal data that Everise processes on behalf of a client, Everise will refer the request to that client and will assist the client in responding, as required by our contract with that client.

Information We Collect and How We Use the Information

Rule 3 of the DPDP Rules requires that the notice given to a Data Principal be presented and be understandable independently of any other information, be in clear and plain language, and contain at the minimum an itemized description of the personal data processed and the specified purpose or purposes of, and a specific description of the goods or services to be provided or uses to be enabled by, the processing. This section is given in compliance with that requirement.

To support your use of this website, your visits to an Everise facility or event, your relationship with Everise, your employment or engagement by Everise, or your use or consideration of our products and services, we may collect and disclose, for the purposes described below, personal data in the following categories and for the following purposes:

1. For data collection when you visit the Everise website, facilities or events

When you visit www.weareeverise.com, we will generally collect the following website data that results from your usage of the website: browser type and version, operating system used, website from which you are visiting us (referral URL), date and time of accessing our website, and internet protocol (IP) address. This information, including your IP address, will be used to enable your access to our website and to safeguard and maintain the security and functionality of our website and related services. We also collect information about your activities during your visit in order to personalize your website experience, such as recording your preferences and settings, and to collect and use your information on an aggregated and anonymized basis to help us improve and further develop our website and to improve the products and services of Everise and its affiliates. When you register to visit an Everise facility or event we will generally collect information similar to the information we collect when you visit our website, such as your name, email address, phone number, company and, if applicable, the name of the Everise employee you are visiting, in order to confirm your purpose for accessing the facility or event and to enforce the Everise security, safety and facilities policies. We also use closed circuit television to monitor our facilities for security and safety purposes.

2. For marketing and requests for information about Everise and its products and services

With regard to certain content on the Everise website, and its products and services, such as brochures, case studies, fact sheets, guides, videos, webinars, infographics and other information, we may request certain information pertaining to you before you can access such content. If you send us such a request or otherwise contact us through the Data Subject Request Form, we may collect and process the following

personal data about you: name, company, job title, email address and phone number, details of the services or products you are interested in, and any further information you choose to provide to us in a comments field, or in an email or similar communication to Everise. We may use this information to correspond with you, to provide you with the requested information or to process an order. Note that this information may also be transferred to the appropriate recipients described in the section below captioned “Disclosure of Personal Data”. You can also consent to receive marketing information. You may choose to opt out of receiving future email or mailings by following the Everise unsubscribe procedure, or by withdrawing your consent as described in the section captioned “Withdrawal of Consent”. When you register for a webinar or other event, we may collect information, online or offline, in relation to the event and during an event, such as participation in sessions and survey results. We combine the personal data we collect to develop aggregate information that provides analysis and business intelligence for conducting our business and for marketing purposes. You can choose to receive information by email or telephone about our products and services, or sign up for subscriptions.

3. For our clients’ customers

As a business process outsourcing company, Everise provides customer management solution services on an outsourced basis. When you interact with Everise in that capacity, whether by voice, chat, email, messaging or any other channel, we process the personal data that you provide and that the client makes available to us, on the documented instructions of that client and for the purposes of the services that the client has engaged us to perform. This may include verifying your identity, retrieving account information, processing payment, responding to your enquiry, resolving your complaint, and recording and monitoring interactions for quality assurance, training and regulatory compliance purposes. We do not determine the purpose or the means of that processing and we do not use that personal data for our own purposes.

4. For employees, contractors and job applicants

Where you are an employee, an individual contractor, an intern or a job applicant of Everise in India, we process your personal data for the purposes of recruitment, assessment and selection, onboarding, payroll and benefits administration, tax and statutory compliance, performance and talent management, learning and development, workforce planning and scheduling, workplace health and safety, information and physical security, investigations and disciplinary proceedings, management of grievances and of the prevention of sexual harassment process, and the establishment, exercise or defense of legal claims. This may include your identity and contact details, date of birth, photograph, educational and employment history, references, results of background verification carried out in accordance with applicable law, statutory identifiers required for payroll, tax and statutory benefit compliance, bank account details, compensation and benefits data, attendance and productivity data, information relating to your health where necessary for the administration of insurance, statutory benefits or workplace accommodation, and details of your nominees and dependants where you provide them.

Everise relies on the legitimate use for employment purposes recognised in section 7(i) of the DPDP Act where applicable, and on your consent where consent is the appropriate basis. Personal data relating to employment is also addressed in the Everise Data Privacy Statement for Employees and in the applicable human resources policies, which should be read together with this Notice.

5. For vendors, suppliers and business partners

Where you are a vendor, supplier, service provider, channel partner or a representative of any of them, we process your name, business contact details, job title, credentials and qualifications, bank and tax details necessary for payment, and records of our dealings with you, for the purposes of onboarding and due

diligence, contract management, procurement, payment, sanctions and anti bribery screening, security clearance for access to our facilities and systems, and the establishment, exercise or defense of legal claims.

Itemised Description of the Personal Data We Process

The personal data we process falls within the following categories. Not every category applies to every Data Principal. The categories that apply to you depend on the nature of your relationship with Everise and, where we act as a Data Processor, on the instructions of our client.

- Identity and contact data, such as name, postal address, email address and telephone number.
- Online identifiers and website usage data, such as IP address, cookie and device identifiers, browser type and version, operating system, referral URL, and date and time of access.
- Electronic, visual and audio data, such as closed circuit television footage of individuals in our facilities, call recordings, chat transcripts and screen recordings created for quality assurance and regulatory compliance.
- Professional data, such as the name of your employer, your job title and your business role.
- Account, transaction and service data processed on behalf of a client, such as account identifiers, service history, entitlement and payment status, to the extent the client makes such data available to us.
- Employment and engagement data, as described in the section captioned “For employees, contractors and job applicants”.
- Health related data, where necessary for the administration of insurance and statutory benefits, for workplace accommodation, or for responding to a medical emergency.
- Inferences drawn from the above that reflect your preferences and interests.

The DPDP Act does not create a separate category of sensitive personal data and applies a single standard of protection to all digital personal data. Everise nevertheless applies enhanced controls, including restricted access and additional security safeguards, to categories of personal data that carry a higher risk of harm, such as financial data, health related data, government issued identifiers and the personal data of children.

Personal Data Not Covered by This Notice

Under the DPDP Act, personal data does not include:

- i. personal data that you have made or caused to be made publicly available, or personal data that is made publicly available by any other person who is under an obligation under any law in force in India to make such personal data publicly available;
- ii. personal data processed in a non-automated manner that is not in digital form and is not intended to be digitised;
- iii. personal data processed by an individual for any personal or domestic purpose; and
- iv. data that has been de-identified or aggregated such that it no longer relates to an identifiable individual.

The DPDP Act applies to the processing of digital personal data within the territory of India, and to processing outside India where the processing is in connection with any activity related to the offering of goods or services to Data Principals within the territory of India.

Legal Basis for Processing

We process your personal data on the basis of your consent given under section 6 of the DPDP Act, or where a legitimate use recognized in section 7 of the DPDP Act applies. Where we rely on consent, your consent shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action,

shall signify your agreement to the processing of your personal data for the specified purpose, and shall be limited to such personal data as is necessary for that specified purpose. The legitimate uses on which we may rely include:

- processing for the specified purpose for which you have voluntarily provided your personal data and in respect of which you have not indicated to us that you do not consent to the use of your personal data;
- processing for the purposes of employment, or those related to safeguarding the employer from loss or liability, such as the prevention of corporate espionage, the maintenance of confidentiality of trade secrets, intellectual property or classified information, or the provision of any service or benefit sought by a Data Principal who is an employee;
- compliance with any judgment, decree or order issued under any law in force in India;
- responding to a medical emergency involving a threat to the life or an immediate threat to the health of you or of any other individual; and
- taking measures to ensure safety of, or to provide assistance or services to, individuals during any disaster or any breakdown of public order.

Where you gave consent to the processing of your personal data before the commencement of the DPDP Act, we will, as soon as it is reasonably practicable, give you a notice containing the information required by section 5 of the DPDP Act, and your personal data may continue to be processed until you withdraw your consent.

Purposes for Which We Use or Disclose Personal Data

We may use or disclose the personal data we collect for one or more of the following purposes:

1. To fulfil or meet the reason for which the information is provided. For example, as part of the services that Everise offers to its clients, when you provide us with personal data as part of a transaction or enquiry, we will use that information to verify identity, retrieve account information, process payment or respond to your enquiry;
2. To carry out our obligations and enforce our rights arising from any client contract;
3. For quality assurance, training and regulatory compliance;
4. As necessary or appropriate to protect the rights, property or safety of Everise, our clients, our personnel or others;
5. To respond to legitimate law enforcement requests and as required by applicable law and issuances, lawful court order or government regulation;
6. As described to you when collecting your personal data or as otherwise permitted under Applicable Privacy Laws; and
7. To evaluate or conduct a merger, divestiture, restructuring, reorganisation, dissolution or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation or a similar proceeding, in which personal data held by us is among the assets transferred.

Sources of Personal Data

We obtain the categories of personal data listed above from the following categories of sources:

- directly from you;
- indirectly from you, from our clients or from their agents, for example through information we collect from our clients in the course of providing services to them;

- directly and indirectly from your activity on our website, computer resources and telephony systems, for example from submissions through our website portal or website usage details collected automatically;
- from recruitment agencies, referees and background verification agencies, where permitted by applicable law and, where required, with your consent; and
- from publicly available sources and from your professional networking profiles.

Disclosure of Personal Data

As a business process outsourcing company, Everise provides customer management solution services on an outsourced basis. In this regard, we may disclose the above-referenced categories of personal data to our affiliates and subsidiaries, service providers, contractors and subcontractors, or to other third parties, only as directed by the Everise client in connection with the account Everise has with that client, to further the services Everise provides to the customers or members of that client, and to website users and guests visiting our sites. When we disclose personal data, we enter into a contract that describes the purpose and requires the recipient to keep that personal data confidential, to process it only for the purpose of the contract, and to implement reasonable security safeguards. Section 8(2) of the DPDP Act permits a Data Fiduciary to engage, appoint, use or otherwise involve a Data Processor to process personal data on its behalf, for any activity related to the offering of goods or services to Data Principals, only under a valid contract.

Categories of Recipients of Personal Data	Purpose of Sharing or Disclosure
Service Providers for Business Operations	For implementation of business process outsourcing operations-related processing activities including, but not limited to, software and technology solutions for contact center and customer experience solutions, sales management, and solutions for enterprise telephony, call recording, workforce management and back-office operations
Service Providers and Partners for Support Function	For implementation of support-related processing activities including, but not limited to, advertising and marketing, hiring and recruitment, background checking, pre-employment requirements, employment benefits, payroll and statutory benefit administration, contracts management, physical and cyber security, and maintenance of legal claims
Other Everise group companies	1. To conduct the various aspects of the business operations of Everise; 2. To store personal data in connection with the performance of services of Everise to its clients
Everise clients, being the Data Fiduciaries in respect of their customers, members and end users	To perform the services that the client has engaged Everise to provide, and to return, transfer or erase personal data on the instructions of that client
Government entities, regulators, law enforcement agencies and the Data Protection Board of India	To comply with a legal obligation, to respond to a lawful request, requisition, summons or order, and to intimate a personal data breach

Professional advisers, auditors, insurers and independent data auditors	To obtain legal, accounting, audit, insurance and assurance services, and to carry out the audits and assessments required under Applicable Privacy Laws
---	--

No Sale of Personal Data; Cookies and Similar Technologies

The DPDP Act does not use the concepts of the “sale” or the “sharing” of personal data, and it does not provide a right to opt out of a sale. Everise does not sell personal data for any purpose whatsoever.

When you use the Everise website, certain service providers and contractors may be authorized to use cookies and similar technologies for purposes including website functionality, analytics and advertising. Where required by applicable law, Everise seeks to ensure that consent for the use of non-essential cookies and similar technologies is obtained through appropriate consent management mechanisms before such technologies are activated. The availability and functionality of cookie preference controls may vary by website, platform or service.

Where consent is relied upon, Everise will provide Data Principals with a reasonable means to review, manage or withdraw their cookie preferences in accordance with applicable law. Cookies and similar technologies that are strictly necessary for the operation, functionality and security of the website may continue to be used where permitted by applicable law.

Personal Data of Children and of Persons with Disability

Under section 2(f) of the DPDP Act, a child is an individual who has not completed eighteen years of age. In relation to a child, the Data Principal includes the parents or lawful guardian of that child, and in relation to a person with disability who has a lawful guardian, the Data Principal includes that lawful guardian.

Everise does not knowingly process the personal data of a child, or of a person with disability who has a lawful guardian, without obtaining verifiable consent as required by section 9(1) of the DPDP Act read with Rules 10 and 11 of the DPDP Rules. Everise does not undertake tracking or behavioural monitoring of children and does not direct targeted advertising at children. Everise does not undertake any processing of personal data that is likely to cause any detrimental effect on the well-being of a child.

Where verifiable parental consent is required, we will adopt appropriate technical and organizational measures and observe due diligence to check that the individual identifying herself as the parent is an adult who is identifiable, where required in connection with compliance with any law in force in India, by reference to reliable details of identity and age available with us, or to details of identity and age voluntarily provided by that individual, including through a virtual token mapped to such details issued by an entity entrusted by law or by the Government with the issuance of such details, or made available and verified by a Digital Locker service provider. Where consent is to be obtained from the lawful guardian of a person with disability, we will observe due diligence to verify that the guardian has been appointed by a court of law, by a designated authority under section 15 of the Rights of Persons with Disabilities Act, 2016, or by a local level committee under section 13 of the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999.

Where Everise processes the personal data of a child on behalf of a client, it does so only on the documented instructions of that client and on the basis of the verifiable parental consent obtained by that client. Rule 12 of the DPDP Rules, read with the Fourth Schedule to the DPDP Rules, exempts certain classes of Data Fiduciaries and certain purposes from sections 9(1) and 9(3) of the DPDP Act, subject to the conditions

specified in that Schedule. The prohibition in section 9(2) against processing that is likely to cause a detrimental effect on the well-being of a child is not exempted.

Everise may process health-related personal data where reasonably necessary for employment administration, insurance and benefit programs, workplace accommodations, occupational health and safety requirements, medical emergencies, legal compliance, or other purposes permitted under applicable law. Such processing will be limited to the personal data reasonably necessary for the relevant purpose and access will be restricted to authorized personnel, service providers, advisors or government authorities who have a legitimate need to know such information.

Everise implements appropriate technical, organizational and administrative safeguards designed to protect health-related personal data against unauthorized access, use, disclosure, alteration or loss. Health-related personal data will be retained only for as long as necessary to fulfil the applicable purpose, meet legal or regulatory requirements, establish, exercise or defend legal claims, or as otherwise permitted or required by law.

Where Everise is required to process the personal data of a child or of a person with disability who has a lawful guardian, Everise will take reasonable steps to obtain and verify the consent or authorization required under applicable law before undertaking such processing.

Everise does not knowingly engage in tracking, behavioural monitoring, targeted advertising, or any processing activity that is prohibited by applicable law in relation to children. Where Everise processes such personal data on behalf of a client, Everise does so solely in accordance with the documented instructions of the relevant client and applicable contractual and legal requirements.

Everise will implement appropriate safeguards designed to protect the personal data of children and persons with disability and will process such data only for the purposes for which it was collected or as otherwise permitted by applicable law.

Transfer of Personal Data Outside India

Everise operates through a global network of affiliates, clients, service providers, contractors and business partners. Accordingly, personal data collected in India may be accessed, transferred, stored or otherwise processed in jurisdictions outside India where Everise, its affiliates, clients or service providers operate, solely for the purposes described in this Notice.

Under section 16(1) of the DPDP Act, the Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified. Rule 15 of the DPDP Rules, which comes into force on May 13, 2027, permits personal data processed under the DPDP Act to be transferred outside the territory of India subject to the restriction that the Data Fiduciary must meet such requirements as the Central Government may, by general or special order, specify in respect of making such personal data available to any foreign State, or to any person or entity under the control of or any agency of such a State.

Section 16(2) of the DPDP Act provides that section 16 does not restrict the applicability of any other law in force in India that provides for a higher degree of protection for, or a restriction on, the transfer of personal data outside India. Sectoral requirements, including directions issued by the Reserve Bank of India, the Insurance Regulatory and Development Authority of India and the Telecom Regulatory Authority of India, may therefore continue to apply to particular categories of personal data. Where such a requirement applies to a client, Everise processes that client's personal data in accordance with the

instructions given by the client to meet that requirement. Every transfer is subject to contractual commitments requiring confidentiality, purpose limitation and reasonable security safeguards.

Everise will ensure that any such cross-border transfer is carried out in accordance with the DPDP Act, the DPDP Rules and any restrictions, conditions or requirements that may be prescribed by the Government of India from time to time. Where required, Everise will implement appropriate contractual, technical and organizational measures to protect personal data and ensure that recipients process such personal data only for authorized purposes and subject to appropriate confidentiality, security and access controls.

Everise may transfer personal data to its affiliates, clients, cloud service providers, technology vendors, payroll providers, recruitment partners, professional advisors, and other authorized service providers located outside India where such transfer is necessary for business operations, employment administration, provision of services, legal compliance, security management or other legitimate business purposes described in this Notice.

Notwithstanding the foregoing, Everise will comply with any applicable law, regulatory direction, sector-specific requirement, contractual restriction, or governmental order that imposes additional conditions on the transfer, storage, access or processing of personal data outside India. Where a client is subject to specific localization or transfer restrictions, Everise will process personal data in accordance with the instructions of that client and the applicable legal requirements.

By providing personal data to Everise, and where consent is the lawful basis for processing, you acknowledge that your personal data may be transferred, accessed, stored or processed outside India in accordance with this Notice and applicable law

How Long Do We Retain Your Personal Data

We will keep the personal data we collect about you for as long as necessary to carry out the purposes set forth in this Notice or in any other notice provided at the time of data collection, but no longer than as required or permitted under applicable law, under our contract with the relevant client, or under internal Everise policy. We dispose of the personal data we collect in accordance with the Everise retention policies and procedures and, where we act as a Data Processor, in accordance with the instructions of our client.

Rule 8(1) of the DPDP Rules, which comes into force on May 13, 2027, prescribes the period after which a specified purpose is deemed no longer to be served, for the classes of Data Fiduciaries listed in the Third Schedule to the DPDP Rules. Everise does not presently fall within any of those classes. Where Everise processes personal data on behalf of a client that falls within one of the classes, Everise will give effect to that client's erasure instructions.

Under Rule 8(2), at least forty-eight hours before the completion of the period for erasure, the Data Fiduciary must inform the Data Principal that the personal data will be erased on completion of that period unless she logs into her user account or otherwise initiates contact for the performance of the specified purpose, or exercises her rights in relation to the processing.

Under Rule 8(3), a Data Fiduciary must retain personal data, associated traffic data and other logs of the processing for a minimum period of one year from the date of such processing, for the purposes specified in the Seventh Schedule to the DPDP Rules, after which those records must be erased unless further retention is required for compliance with any other law in force, Everise policies, or as notified by the Government. Retention obligations under other laws, including the Information Technology Act, 2000 and the rules and directions made under it, the Companies Act, 2013, tax and labour legislation, and any sectoral requirement applicable to a client, continue to apply.

Security Safeguards

We implement reasonable security safeguards to prevent a personal data breach, including in respect of any processing undertaken on our behalf by a Data Processor. Consistent with Rule 6 of the DPDP Rules, those safeguards include, at a minimum:

- appropriate data security measures, such as securing personal data through encryption, obfuscation or masking, or the use of virtual tokens mapped to that personal data;
- appropriate measures to control access to the computer resources used by Everise and by our Data Processors;
- visibility on the accessing of personal data, through appropriate logs, monitoring and review, to enable the detection of unauthorised access, its investigation and its remediation so as to prevent recurrence;
- reasonable measures for continued processing in the event that the confidentiality, integrity or availability of personal data is compromised, including by way of data backups;
- retention of logs and personal data for a period of one year for the purposes of detection, investigation, remediation and continued processing, unless compliance with any law in force requires otherwise;
- contractual obligations on our Data Processors to implement reasonable security safeguards; and
- appropriate technical and organisational measures to ensure the effective observance of security safeguards.

Personal Data Breach

On becoming aware of any personal data breach, we will, to the best of our knowledge, intimate each affected Data Principal, in a concise, clear and plain manner and without delay, through her user account or any mode of communication registered with us, and will provide a description of the breach including its nature, extent and the timing of its occurrence, the consequences relevant to her that are likely to arise from the breach, the mitigation measures implemented and being implemented, the safety measures that she may take to protect her interests, and the business contact information of a person who is able to respond on our behalf to her queries.

We will also intimate the Data Protection Board of India without delay, with a description of the breach including its nature, extent, timing and location of occurrence and the likely impact, and will furnish to the Board, within the period allowed by the DPDP Act, upon becoming aware of the breach or within such longer period as the Board may allow on a written request, an updated and detailed description of the breach, the broad facts relating to the events, circumstances and reasons leading to the breach, the mitigation measures implemented or proposed, any findings regarding the person who caused the breach, the remedial measures taken to prevent recurrence, and a report of the intimations given to affected Data Principals.

Where the personal data affected by a breach is processed by Everise on behalf of a client, Everise will notify that client without undue delay and will support that client in discharging its obligations as Data Fiduciary. Reporting obligations to the Indian Computer Emergency Response Team under section 70B of

the Information Technology Act, 2000 and the directions issued under it apply in addition to, and not in substitution for, the obligations described in this section.

Everise's role as Data Fiduciary and Data Processor

1. Everise processes personal data in different capacities depending on the nature of its relationship with the individual and the purpose of processing.
2. Where Everise collects and processes personal data for its own business purposes, including in relation to its employees, job applicants, contractors, vendors, suppliers, website visitors and event attendees, Everise acts as the Data Fiduciary and is responsible for compliance with applicable obligations under the DPDP Act.
3. Where Everise processes personal data on behalf of its clients in connection with outsourced customer experience, contact center, back-office, or other business process services, Everise acts as a Data Processor and processes such personal data solely on the documented instructions of the relevant client acting as the Data Fiduciary.
4. In such cases, rights under the DPDP Act are generally exercisable against the relevant client as Data Fiduciary. If Everise receives a request relating to personal data processed solely on behalf of a client, Everise may redirect the request to the relevant client or assist the client in responding in accordance with the applicable service agreement and legal requirements.
5. The rights described in this section apply only to the extent Everise acts as a Data Fiduciary in relation to the relevant personal data. Where Everise acts solely as a Data Processor on behalf of a client, the relevant client will generally be responsible for responding to and fulfilling such requests.

Your Rights and Choices

Although Everise is not a "Data Fiduciary" as defined under the DPDP Act in respect of the personal data of customers, members and end users of our clients, it will attempt to provide responses to legitimate and verified written requests made under the DPDP Act. The DPDP Act provides Data Principals with specific rights in relation to their personal data. This section describes those rights and explains how to exercise them. Where a right is exercisable only against the Data Fiduciary, and Everise processes your personal data on behalf of a client, we will refer your request to that client and assist the client in responding.

As stated in more detail below, you can request that we:

- provide you with a summary of the personal data we process about you and the processing activities we undertake with respect to that personal data;
- provide you with the identities of all Data Fiduciaries and Data Processors with whom your personal data has been shared, along with a description of the personal data so shared;
- correct, complete or update your inaccurate or incomplete personal data;
- erase your personal data;
- redress your grievance in relation to any act or omission regarding the performance of our obligations; and
- give effect to a nomination made by you.

To exercise any of these rights, please fill out the form at the following link: <https://everise.privacy.saymine.io/Everise>.

1. Right to Access Information about Personal Data

Under section 11 of the DPDP Act, where you have previously given consent to the processing of your personal data, you have the right to obtain from us, on request, a summary of the personal data being processed by us and the processing activities undertaken by us with respect to that personal data, the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared, along with a description of the personal data so shared, and any other information related to the personal data and its processing as may be prescribed. Under section 11(2) of the DPDP Act, this right does not extend to the sharing of your personal data by us with another Data Fiduciary authorized by law to obtain it, where that sharing is pursuant to a request made in writing by that other Data Fiduciary for the purpose of the prevention, detection or investigation of offenses or cyber incidents, or for the prosecution or punishment of offences.

2. Right to Correction and Erasure of Personal Data

Under section 12 of the DPDP Act, you have the right to the correction, completion, updating and erasure of your personal data for the processing of which you have previously given consent. On receiving a request for correction, completion or updating, we will correct inaccurate or misleading personal data, complete incomplete personal data and update your personal data. On receiving a request for erasure, we will erase your personal data unless its retention is necessary for the specified purpose or for compliance with any law in force. Please be advised that Everise will generally decline a request to erase personal data if you are a current employee or customer of one of the Everise clients, or if you are a former customer of one of the Everise clients and Everise must keep the personal data pursuant to a legal obligation or pursuant to the instructions of that client. We may reach out to you and request additional information to verify any relevant information before we process your request.

3. Right of Grievance Redressal

Under section 13 of the DPDP Act, you have the right to have readily available means of registering a grievance with us in respect of any act or omission regarding the performance of our obligations in relation to your personal data or the exercise of your rights. We will respond to your grievance within the period published in our grievance redressal system, which, in accordance with Rule 14(3) of the DPDP Rules, shall be a reasonable period not exceeding ninety days, and we will implement appropriate technical and organisational measures to ensure the effectiveness of that system. Section 13(3) of the DPDP Act requires you to exhaust the opportunity of redressing your grievance with us before approaching the Data Protection Board of India.

4. Right to Nominate

Under section 14 of the DPDP Act, you have the right to nominate any other individual who shall, in the event of your death or your incapacity, exercise your rights under the DPDP Act in respect of your personal data. Incapacity, for this purpose, means the inability to exercise those rights by reason of unsoundness of mind or infirmity of body. You may make a nomination in accordance with our terms of service and applicable law, using the means and furnishing the particulars that we require.

5. Withdrawal of Consent

Under sections 6(4) to 6(6) of the DPDP Act, you have the right to withdraw your consent at any time, and the ease of doing so will be comparable to the ease with which the consent was given. The consequences of withdrawal will be borne by you. Withdrawal of consent does not affect the lawfulness of processing

carried out on the basis of that consent before its withdrawal. On receiving a withdrawal, we will, within a reasonable time, cease and cause any Data Processor engaged by us to cease processing your personal data, unless processing without your consent is required or authorized under the DPDP Act, under the rules made under it, or under any other law in force in India.

6. Means of Exercising Your Rights

In accordance with Rules 14(1) and 14(2) of the DPDP Rules, we prominently publish on our website the details of the means using which you may make a request for the exercise of your rights, and the particulars, if any, such as a username or other identifier, which may be required to identify you under our terms of service. You may make a request using the Data Subject Request Form available at <https://everise.privacy.saymine.io/Everise>, or by writing to us at dataprivacy@weareeverise.com. Only you, or an individual duly authorised by you in writing to act on your behalf, may make a request relating to your personal data. You may also make a request on behalf of your child or of a person with disability of whom you are the lawful guardian. Making a request does not require you to create an account with us. We will use the personal data provided in a request only to verify the identity or the authority of the requestor and to respond to the request.

Verification, Response Timing and Format

On receiving your request, we will need to verify your identity to determine that you are the same person about whom we hold the personal data in our systems. These verification efforts require us to ask you to provide information so that we can match it with information you have previously provided to us. To the extent possible, we will avoid requesting additional information from you for the purposes of verification. In exercising your request, we may ask you for the following information: name, address, phone number, email address, your relationship with Everise, and, where necessary, a copy of a valid proof of identity. We may request additional information necessary to verify your identity to a reasonable degree of certainty by verifying at least two to three pieces of personal data previously provided to us which we have determined to be reliable for the purpose of verifying identity. We cannot respond to your request or provide you with personal data if we cannot verify your identity or your authority to make the request and confirm that the personal data relates to you.

We endeavour to respond to a verified request as soon as practicable and in any event within the period published in our grievance redressal system, which shall not exceed ninety (90) days. If we require more time, we will inform you of the reason and of the extension period in writing. We will deliver our written response by post or electronically, determined by the method by which you submitted the request. The response we provide will also explain the reasons why we cannot comply with a request, if applicable. We may use other verification methods as the circumstances dictate, and we may reject requests that are unreasonably repetitive, excessive or manifestly unfounded, or that we have a good faith, reasonable and documented belief are fraudulent. If we decline a request on any of those grounds, we will notify you and provide the reasons for the denial. We generally do not charge a fee to process or respond to your request but we may charge reasonable fees, cost-proportionate administrative fees, or refuse to act on a request entirely if it is determined that the request is manifestly unfounded, excessive, or repetitive.

Duties of Data Principals

Section 15 of the DPDP Act imposes duties on Data Principals. In exercising your rights under the DPDP Act, you shall comply with the provisions of all applicable laws, you shall not impersonate another person while providing your personal data for a specified purpose, you shall not suppress any material information while providing your personal data for any document, unique identifier, proof of identity or proof of address issued by the State or any of its instrumentalities, you shall not register a false or frivolous

grievance or complaint with a Data Fiduciary or with the Data Protection Board of India, and you shall furnish only such information as is verifiably authentic while exercising the right to correction or erasure. Breach of these duties is punishable under the Schedule to the DPDP Act.

Consent Managers

Section 6(7) of the DPDP Act permits a Data Principal to give, manage, review and withdraw consent through a Consent Manager registered with the Data Protection Board of India. Rule 4 of the DPDP Rules, which comes into force on November 13, 2026, sets out the conditions for the registration and the obligations of Consent Managers. Everise will publish its position in relation to Consent Managers once the registration framework is operational and the Board has published the list of registered Consent Managers.

Data Protection Officer and Significant Data Fiduciary Obligations

Everise prominently publishes on its website, and mentions in every response to a communication for the exercise of the rights of a Data Principal, the business contact information of the person who is able to answer, on behalf of Everise, questions about the processing of personal data. That contact information is set out in the section captioned "Contact Information".

As at the Effective Date of this Notice, Everise has not been notified by the Central Government as a Significant Data Fiduciary under section 10 of the DPDP Act, and is not aware of having been included in any class of Data Fiduciaries so notified. If Everise, or any class of Data Fiduciaries in which Everise is included, is so notified, Everise Data Protection Officer based in India will represent Everise under the DPDP Act, who will be an individual responsible to the board of directors or a similar governing body, and who will be the point of contact for the grievance redressal mechanism. Everise may also appoint an independent data auditor, will undertake a Data Protection Impact Assessment and an audit once in every period of twelve months in accordance with Rule 13 of the DPDP Rules, will cause the person carrying out that assessment and audit to furnish to the Board a report containing significant observations, will observe due diligence to verify that the technical measures adopted by it, including algorithmic software used for the hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data, are not likely to pose a risk to the rights of Data Principals, and will observe any restriction specified by the Central Government under Rule 13(4) on the transfer outside the territory of India of personal data and of the traffic data pertaining to its flow.

Complaints to the Data Protection Board of India

If you are not satisfied with our response, you may register a complaint with the Data Protection Board of India in accordance with section 13(3) and section 27 of the DPDP Act, after exhausting the opportunity of redressing your grievance with us.

Changes to Our Privacy Notice

We reserve the right to amend this Notice at our discretion and at any time. Kindly visit our privacy policy page for updates. This Notice is updated as of September 18, 2026.

Contact Information

If you have any questions or comments about this Notice, our Privacy Statement, or the ways in which we collect and use your personal data, or if you wish to register a grievance, please do not hesitate to contact us at:

Website: Data Subject Request Form at <https://everise.privacy.saymine.io/Everise>

Email: dataprivacy@weareeverise.com or Legal@weareeverise.com

Grievance Officer for India: Namita Prasad | Namita.Prasad@weareeverise.com

Postal Address, India: 1/22, 2nd Floor, Asaf Ali Road, Central Delhi, Delhi- 110002

Postal Address, Global: Everise, Inc., 600 N. Pine Island Road, Suite 320, Plantation, FL 33324, USA