Privacy Policy

CONVERSE MOBILE

Content

1. PURPOSE

Converse Mobile is committed to protect the privacy, confidentiality, and security of the personal data it collects, processes, and stores during its business operations.

This Privacy Policy outlines how the organization collects, uses, shares, retains, and protects personal data, and explains the rights of individuals whose data we process. It reflects our compliance obligations under applicable data protection laws, including but not limited to the:

- General Data Protection Regulation (GDPR) – UK, European Union
- Digital Personal Data Protection (DPDP) Act
- Any other local privacy regulations that may apply to specific jurisdictions

We recognize the importance of individual privacy and believe that transparency in our data practices builds trust with our customers, employees, partners, and users. We are committed to processing personal data responsibly, lawfully, and in a manner that respects individual rights.

2. Scope

This Privacy Policy governs the collection, processing, storage, sharing, and disposal of personal data , across all products, services, platforms, and business functions where personal data is involved.

This policy applies to:

- All personal data collected and processed in physical and digital formats
- All business units, departments, employees, contractors, and third parties act on behalf of the organization.
- Data subjects including customers, website visitors, job applicants, employees, and vendors

3. Types of Personal Data Covered

This policy applies to all forms of personal data, including but not limited to:

- **Identity Information** – Full name, date of birth, government-issued ID numbers
- **Contact Information** – Phone numbers, email addresses, postal addresses
- **Demographic Information** – Gender, nationality, language preferences
- **Financial Information** – Bank account details, payment card information (where applicable)
- **Authentication Data** – Usernames, passwords, security questions
- **Location Data** – IP addresses, GPS data, geolocation (if enabled)
- **Behavioral Data** – Browsing activity, system usage logs, preferences

- **Biometric or Sensitive Data** – Only where legally permitted and explicitly consented

4. Individuals Covered

This policy applies to the personal data of:

- Customers and end-users of the organization of products or services
- Employees, interns, and job applicants
- Business partners, vendors, and service providers
- Website visitors and platform users
- Any other individuals whose data is processed by or on behalf of the organization.

5. Jurisdictional Applicability

This policy applies to all personal data processed in:

- **UK & European Union**, in accordance with the **GDPR**
- Any other jurisdiction where the organization operates or handles personal data, subject to local data protection laws

3. TERMS AND DEFINITIONS

Term	Definition
Personal Data	Any data that relates to an identified or identifiable natural person (data subject). This includes names, contact details, identification numbers, IP addresses, or any factor specific to that person's identity.
Sensitive Personal Data	A special category of personal data that may include financial information, health data, biometric identifiers, sexual orientation, or any information classified as sensitive under applicable law.
Data Subject	The individual whose personal data is being collected, held, or processed.
Processing	Any operation performed on personal data, whether automated or manual, including collection, storage, use, alteration, sharing, or deletion.
Data Controller	The natural or legal person who determines the purposes and means of processing personal data. [ORG NAME] typically acts as a Data Controller.
Data Processor	A third party or service provider that processes personal data on behalf of the Data Controller.
Consent	A clear, affirmative act that signifies a data subject's agreement to the processing of their personal data for specific purposes. Consent must be freely given, informed, specific, and revocable.
Anonymization	The process of removing all personal identifiers from data so that individuals cannot be identified, directly or indirectly.
Pseudonymization	The process of replacing identifying fields within a data record with artificial identifiers (pseudonyms), still allowing data analysis but limiting identification.
Third Party	Any person or organization other than the data subject, data controller, or processor, authorized to access or process personal data.
Cross-Border Transfer	Transmission of personal data outside the jurisdiction in which it was originally collected, especially to countries without equivalent data protection laws.

4. ROLES AND RESPONSIBILITIES

The protection of personal data is a shared responsibility across all levels of the organization. The following roles have specific responsibilities to ensure privacy is embedded into business processes, technology, and culture.

a) Board of Directors

- Provide strategic oversight and endorse the organization's privacy and data protection posture
- Ensure privacy risks are addressed as part of enterprise risk management
- Allocate sufficient resources for compliance with applicable privacy laws
- Review and approve major policy changes related to personal data governance

b) Chief Executive Officer (CEO)

- Act as the executive sponsor for the organization's data privacy strategy
- Championship of a culture of privacy and ethical data handling
- Ensure that data protection is considered in all major business decisions
- Hold senior leadership accountable for privacy compliance in their respective functions

c) Data Protection Officer (DPO) / Privacy Officer

- Serve as the primary point of contact for privacy-related matters within the organization and with data protection authorities
- Monitor compliance with privacy laws and internal policies
- Conduct Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs)
- Maintain the Record of Processing Activities (RoPA)
- Respond to data subject requests and coordinate breach notifications
- Advise on lawful bases for data processing and data sharing practices

d) Business Unit Heads / Functional Leaders

- Ensure privacy risks are identified and addressed within their business functions
- Ensure personal data collected and used within the unit is necessary, lawful, and aligned with this policy
- Participating in Privacy by Design and impact assessments for new processes or tools
- Ensure teams are trained in data protection responsibilities

e) Application Owners / Product Managers

- Maintain an inventory of personal data processed by their applications
- Ensure data collection forms and flows align with privacy policies and consent requirements
- Implement and document role-based access controls
- Work with DPO to support privacy impact assessments for new features or data use cases

f) Information Technology (IT) Team

- Implement appropriate technical controls to ensure confidentiality, integrity, and availability of personal data
- Maintain audit trails, access logs, and encryption systems
- Support the secure deletion and retention of personal data in line with policy

- Assist in incident detection and response processes for data breaches
- Embed security and privacy best practices into system design, build, deployment, and monitoring (Privacy by Design)
- Ensure secure configuration of cloud platforms and infrastructure hosting personal data
- Enforce infrastructure-level access restrictions and logging
- Manage vulnerabilities

g) End Users / Employees

- Handle personal data responsibly and only for authorized purposes
- Follow the organization's privacy, acceptable use, and information security policies
- Report suspected data breaches, unauthorized access, or loss of personal data immediately
- Participating in mandatory privacy and data protection training

h) Human Resources (HR)

- Ensure employee data is collected and used in accordance with privacy regulations
- Incorporate privacy notices and consent mechanisms into onboarding/offboarding
- Collaborate with DPO in managing data subject requests from employees or former staff

i) Legal and Compliance Team

- Interpret and track evolving global privacy laws and regulations
- Review data processing agreements (DPAs) and third-party contracts for privacy clauses
- Assist in regulatory reporting, audits, and legal aspects of data breach response
- Support DPIAs, RoPA documentation, and consent model design

j) Information Security Team

- Oversee the implementation of security measures protecting personal data
- Monitor access, detect anomalies, and enforce incident response plans
- Work with DPO to classify personal data and enforce tiered data protection requirements
- Participate in root cause analysis for privacy-related incidents

5. CATEGORIES OF PERSONAL DATA COLLECTED

The organization may collect and process the following categories of personal data, depending on the nature of your interaction with us and the services you use:

a) Identification and Contact Information

- Full name
- Email address
- Phone number
- Postal address

- Government-issued ID (where legally required)

b) Demographic Information

- Date of birth
- Gender
- Nationality
- Language preferences

c) Employment and Professional Information

- Job title and designation
- Employer/company name
- Work contact information
- Resume/CV and educational background (for applicants or employees)

d) Financial and Transactional Data

- Bank account or payment information (only where necessary)
- Tax identification numbers
- Billing and invoicing data
- Transaction history

e) Authentication and Access Data

- Login credentials (usernames, hashed passwords)
- Role-based access rights
- System or application activity logs

f) Device and Technical Information

- IP address
- Browser type and version
- Operating system
- Device identifiers
- Log files and usage analytics

g) Location and Behavioral Data

- Geographic location (when enabled or inferred via IP)
- Website navigation patterns
- Clickstream data
- Communication preferences

h) Sensitive Personal Data (collected only with explicit consent and where lawful)

- Health-related information (if provided voluntarily or as part of employment)
- Biometric identifiers (e.g., fingerprints or facial recognition used for secure authentication)
- Financial credentials
- Any information defined as "sensitive" under local privacy laws

We only collect personal data that is necessary for specific, legitimate business purposes, and ensure that appropriate legal bases are established for each type of data collected.

6. PURPOSE OF DATA COLLECTION

The organization collects and processes personal data only for legitimate, specific, and clearly defined purposes. We ensure that data is not used in a manner incompatible with these purposes, and that all processing is supported by an appropriate legal basis under applicable data protection laws.

a) Legal Basis for Processing

Depending on the context, we process personal data based on one or more of the following legal grounds:

- **Consent**: Where the data subject has given explicit, informed consent for processing
- **Contractual Necessity**: To enter or fulfil a contract with the data subject
- **Legal Obligation**: To comply with applicable laws and regulatory requirements Legitimate
- **Interest**: To pursue the organization's legitimate business interests, balanced against the rights of individuals
- **Vital Interests**: To protect the life or safety of an individual (in exceptional situations)
- **Public Task**: If applicable under statutory mandates

b) Primary Purposes of Data Processing

Purpose	Description
Customer Relationship Management	To communicate with customers, respond to inquiries, and manage support tickets
User Registration and Access Control	To authenticate users, assign access rights, and manage system security
Human Resources and Payroll	To recruit, onboard, manage, and compensate employees
Legal and Regulatory Compliance	To meet obligations under labor laws, financial regulations, tax laws, and data protection statutes
Service Delivery	To provide contracted services, customize user experiences, and ensure platform functionality
Marketing and Communications	To send newsletters, promotional content, event invitations, and conduct surveys (only with consent)
Analytics and Business Intelligence	To analyze system usage, optimize operations, and support strategic decision-making
Fraud Prevention and Security	To detect, investigate, and respond to security threats, unauthorized access, or abuse
Contract and Vendor Management	To evaluate, engage, and manage third-party providers and partners

c) Change of Purpose

If we intend to use personal data for any purpose not originally disclosed at the time of collection, we will:

- Evaluate whether the new purpose is compatible with the original one
- Notify the data subject (where required)
- Obtain additional consent, if the legal basis requires it

7. DATA COLLECTION METHODS

The organization collects personal data through various means; direct, automated, and third party; to support its business operations, comply with legal obligations, and enhance user experience. We apply the principles of data minimization, accuracy, and fairness at every stage of the data collection process.

a) Direct Collection from Data Subjects

We collect personal data directly when an individual voluntarily interacts with us through the following means:

i. Digital Interfaces

- Registration forms on websites and mobile apps
- Online surveys, event registrations, webinar sign-ups
- Customer service forms, chatbot inputs, contact forms
- Newsletter or marketing opt-in forms
- Feedback and satisfaction surveys

ii. Verbal and Written Communication

- Phone calls, video calls, or face-to-face meetings
- Email, instant messaging, or internal collaboration platforms
- Customer support or sales-related conversations (recorded with consent, where applicable)

iii. Employment & HR Processes

- Job application forms, resumes, and supporting documents
- Employee onboarding forms (ID proofs, tax documents, medical declarations)
- Performance appraisals, leave applications, and exit forms

b) Automated Collection Methods

Certain data is collected automatically when individuals interact with our digital systems and infrastructure. This may include:

i. Website and Application Usage

- IP address, browser type and version, device type, and screen resolution
- URLs visited, pages viewed, session duration, and referring pages

- Language preferences, time zone settings

ii. Cookies and Tracking Technologies

- First party and third-party cookies
- Web beacons, pixels, and scripts embedded in websites and emails
- Preference and personalization settings
- Behavioral profiling (subject to consent, where required)

iii. Mobile Applications

- Device ID (e.g., Android ID, IDFA)
- App usage logs and crash reports
- Push notification preferences
- Geolocation data (if enabled by the user)

iv. Internal Systems Monitoring

- System login/logoff time stamps
- Access control logs and audit trails
- Network activity monitoring (per company policy) Note: Cookie usage is further detailed in Section 12.

c) Indirect Collection via Third Parties

We may receive personal data about individuals from trusted third-party sources, such as:

i. Affiliates and Subsidiaries

- Intra-group data sharing for HR management, payroll, and system access
- Shared CRM systems for unified customer service delivery

ii. Service Providers and Processors

- Background verification agencies, payroll processors, and tax consultants
- Marketing platforms, analytics providers, and customer support vendors
- Cloud hosting, infrastructure, and SaaS solution providers

iii. Business Partners and Clients

- Contact information from business partners or referral programs
- User account details shared for integrated service provisioning
- Vendor due diligence or KYC information from partner portals

iv. Public and Open Sources

- Publicly available profiles (e.g., LinkedIn, professional forums)
- News media, regulatory disclosures, or open government databases

7.1 Data Collection Principles

- **Lawfulness**: Data is collected only when there is a valid legal basis

- **Fairness and Transparency**: Individuals are informed through privacy notices, banners, and consent forms
- **Accuracy**: Efforts are made to ensure data is up-to-date and correct
- **Data Minimization**: Only the data necessary for each purpose is collected
- **Security**: Data collection mechanisms are secured using encryption, access controls, and input validation

8. DATA SHARING AND DISCLOSURE

The organization does not sell personal data. We only share or disclose personal data with third parties where it is legally justified, contractually protected, and necessary for legitimate business or compliance purposes. All data sharing is governed by the principles of **purpose limitation**, **data minimization**, and **accountability**.

8.1 Categories of Third Parties with Whom We May Share Personal Data

Recipient Category	Purpose of Disclosure
Affiliates/Subsidiaries	For shared HR systems, unified customer support, IT operations, or internal compliance
Service Providers / Vendors	To perform functions on our behalf under a Data Processing Agreement (e.g., cloud hosting, payroll, IT support)
Business Partners	For joint product delivery, technical integration, or sales/referral collaborations
Payment Gateways / Banks	For processing financial transactions securely
Government Authorities / Regulators	To comply with legal obligations, tax audits, court orders, or law enforcement requests
Auditors / Legal Advisors	For statutory audits, investigations, or legal defense
Recruitment Partners	For candidate screening, interview scheduling, and background verification

8.2 Conditions for Data Sharing

We ensure that any personal data shared with third parties is:

8.2.1 Limited to the minimum necessary to fulfil the stated purpose

- Based on valid legal grounds, such as contractual necessity, consent, or legal obligation
- Governed by contracts (Data Processing Agreements or equivalent) requiring:
    - Confidentiality
    - Use limitations
    - Security controls
    - Sub-processor obligations
    - Subject to ongoing oversight, such as periodic audits or security assessments

8.2.2 Cross-Border Data Transfers

We may transfer personal data to jurisdictions outside the country of collection, especially where our cloud service providers, support teams, or business units operate globally.

Cross-border transfers are conducted only when:

- The destination country has been recognized as having **adequate data protection laws**
- Appropriate safeguards are in place, such as:
    - Standard Contractual Clauses (SCCs) approved by authorities o Data Transfer Agreements with audit rights and confidentiality clauses
    - Binding Corporate Rules (BCRs) (where applicable)
- The data subject has provided **explicit informed consent** (if required by law)

8.2.3 No Unauthorized Disclosure

- The organization does not rent, sell, or share personal data with third parties for their own marketing or profiling purposes
- Unauthorized disclosure of personal data by any employee, vendor, or third party is a violation of this policy and subject to disciplinary or contractual consequences

9. DATA RETENTION AND DISPOSAL

The organization is committed to ensuring that personal data is not retained longer than necessary for the purposes for which it was collected. We apply robust data lifecycle management practices to ensure compliance with legal, regulatory, operational, and contractual obligations, and to minimize privacy and security risks.

9.1 Retention Policy Objectives

- Comply with applicable data protection laws (e.g., GDPR Art. 5(1)(e), DPDP obligations)
- Reduce risks of unauthorized access, outdated records, and over-retention
- Support the organization's internal audit, legal defense, and operational continuity
- Enable secure and auditable disposal practices for both electronic and physical data

9.2 Data Classification and Retention Mapping

Each category of personal data is assigned a retention period based on:

- Purpose of collection
- Regulatory requirements
- Industry-specific obligations

- Contractual commitments
- Organizational risk tolerance

The organization maintains a detailed **Data Retention Schedule** that maps:

Data Category	Source / Owner	Retention Period	Applicable Law / Standard
Employee HR files	HR Department	3 years postseparation	Labor law, taxation, audit
Financial and tax data	Finance Department	3 years	Income Tax Act, Companies Act
Customer contracts and records	Sales / Legal	3 years after end of service	Limitation Act, contractual auditability
Applicant and recruitment data	HR / Talent Acquisition	3 years (if not hired)	Business continuity (with consent)
Marketing and lead generation	Marketing	3 years	GDPR/DPDP (consent based processing)
System logs and user analytics	IT / Security / DevOps	6 months	IT governance, incident forensics
Email communications	All departments	3 years	Legal hold, corporate records policy
Backup data	IT / Infrastructure	As per backup rotation cycle	BCP, DR, operational needs (access controlled)

9.3 Data Retention Enforcement Mechanisms

- Periodic review of stored data across systems, applications, databases, and repositories
- Integration of retention rules into DLP tools, cloud policies, and document management systems
- Departmental responsibilities for declaring when records can be archived or deleted
- Privacy Office audits of compliance with the Data Retention Schedule

9.4 Secure Disposal of Personal Data

When personal data reaches the end of its retention period; or when the data subject requests erasure where applicable; the organization follows secure disposal practices based on the medium:

For Digital Data:

- Secure file deletion using certified erasure tools
- Cryptographic wiping of disks
- Database truncation and schema cleaning

- Cloud provider deletion confirmations (where applicable) **For Physical Records:**
- Shredding or incineration by certified vendors
- Use of locked bins and security destruction workflows
- Documentation of disposal (date, method, authorized personnel)

9.5 Backup and Archival Data

- Backups are encrypted, access-restricted, and stored in secure data centers
- Retained solely for business continuity and disaster recovery
- Data from backups will not be restored unless justified and approved
- Upon end-of-life, backups are destroyed by secure decommissioning procedures

9.6 Anonymization and Aggregation

Where business value remains and legal obligations permit, data may be **anonymized or aggregated**, removing any personally identifiable attributes. Such data is:

- Exempt from retention limits under most privacy laws
- Used for analytics, research, or statistical purposes
- Reviewed to ensure irreversibility of identification

9.7 Exceptions and Legal Holds

Retention periods may be extended beyond standard timelines in the following cases:

- Legal hold or pending litigation
- Ongoing internal or external investigation
- Regulatory instructions or audit
- Data subject consent for prolonged retention (with justification)

Such exceptions are reviewed by the **Legal**, **DPO**, or **Compliance** team and documented with clear rationale.

9.8 Accountability and Oversight

Role	Responsibility
Department Heads	Enforce data retention rules within their function
IT & Infrastructure	Implement automated purging mechanisms and secure disposal
DPO / Privacy Office	Maintain Data Retention Schedule; approve exceptions and audits
Employees & Data Handlers	Follow retention guidelines; report outdated or orphaned records

10. DATA SUBJECT RIGHTS

As part of the organization commitment to lawful and transparent processing of personal data, we ensure that all individuals (data subjects) whose data we process are powered to exercise their rights under applicable privacy regulations including the **GDPR**, and **DPDP Act**

We maintain streamlined processes, verified access controls, and documented responses to facilitate the fulfilment of these rights in a timely and auditable manner.

10.1 Summary of Rights

Right	Explanation
Right to Access	Obtain confirmation of whether we process your personal data, and receive a copy of such data along with details of purpose, recipients, and retention.
Right to Rectification	Request correction or completion of inaccurate, outdated, or incomplete personal data maintained by us.
Right to Erasure (Right to be Forgotten)	Request deletion of personal data where there is no lawful reason to retain it (e.g., consent withdrawn, data no longer needed).
Right to Restrict Processing	Ask us to temporarily stop processing your data while a dispute or verification is underway.
Right to Data Portability	Receive your personal data in a structured, commonly used, machine-readable format, and request its transmission to another service provider.
Right to Object	Object to processing carried out under legitimate interests (including profiling), or for direct marketing.
Right to Withdraw Consent	Withdraw your consent at any time, without affecting the lawfulness of prior processing based on that consent.
Right to Lodge a Complaint	File a complaint with the Data Protection Authority or our internal grievance officer, depending on jurisdiction.
Right to Be Informed	Be clearly informed, at the time of data collection, about how your data will be used, shared, and retained.
Right to Nominate	Appoint a nominee to exercise your rights in case of incapacity or death.
Right to Opt-Out	Opt-out of the sale or sharing of your personal data, or from targeted advertising.

10.2 How to Exercise Your Rights

Data subjects can exercise their rights by submitting a request through any of the following secure channels:

- **Email**: info@conversemobile.com
- **Online Portal**: https://www.conversemobile.com/
- **Postal Mail**: Attn: Data Protection Officer,
    - To ensure the request is lawful and verified, we may require:
        - Identity verification (e.g., government-issued ID, OTP verification, or employee ID)
        - Specification of the data or processing activity in question
        - Additional authorization if the request is submitted by a nominee or representative

10.3 Verification and Authentication Process

We verify identity to prevent unauthorized access to personal data. Verification methods may include:

- One-time password (OTP) via registered email or phone
- Employee or customer ID validation (if applicable)
- Legal documentation for guardians or nominees

Requests submitted without sufficient verification may be rejected with justification.

10.4 Processing and Timelines

Action	Timeframe
Acknowledgment of request	Within **7 business days**
Fulfilment or formal response	Within **30 calendar days**
Extensions (if needed)	Up to an additional **30 days**, with justification provided
Escalation or complaints	Addressed as per internal grievance handling timeline

In case of complexity or volume, we may require additional time and will inform the data subject accordingly.

10.5 Limitations and Exceptions

While the organization will make all reasonable efforts to honor valid requests, we may restrict or deny a request where:

- Fulfilling the request would infringe on the rights or freedoms of others
- We are legally obligated to retain the data (e.g., for tax, fraud prevention, or regulatory purposes)
- The data is held in backup or archival systems and restoration is not technically feasible
- The request is repetitive, manifestly unfounded, or abusive

10.6 Children's Data and Rights of Guardians

For data subjects who are minors (as defined by local law, e.g., under 18 under DPDP):

- Requests must be submitted by a **parent or legal guardian**
- Proof of guardianship will be required
- For educational, healthcare, or service environments involving children, special provisions apply and are communicated separately

10.7 Nomination and Posthumous Rights

Individuals may **nominate a representative** to exercise their rights in case of incapacity or death. Such nominations must be:

- Recorded in writing
- Supported with legal documentation for validation

Posthumous requests will be honored in accordance with applicable legal frameworks and the availability of relevant data.

11. DATA SECURITY MEASURES

The organization implements a comprehensive set of technical, administrative, and organizational measures to protect personal data from unauthorized access, loss, alteration, disclosure, or destruction. These safeguards are based on industry standards such as **ISO/IEC 27001**, **ISO/IEC 27701**, and applicable data protection regulations.

11.1 Information Security Management System (ISMS)

The organization operates a centralized Information Security Management System (ISMS) that governs:

- Risk-based security control selection

- Periodic risk assessments and treatment plans
- Incident response, monitoring, and forensic analysis
- Continuous improvement of controls and awareness

The ISMS is reviewed annually and updated based on evolving threats, audit findings, and regulatory requirements.

11.2 Technical Security Controls

Control Area	Examples of Measures Implemented
Access Control	Role-based access, least privilege, password policies, MFA, SSO
Network Security	Firewalls, intrusion detection/prevention (IDS/IPS), VPNs, network segmentation
Endpoint Protection	Antivirus, EDR (Endpoint Detection & Response), secure configurations
Data Encryption	AES-256 encryption at rest, TLS 1.2+ for data in transit, encrypted backups
Logging & Monitoring	SIEM systems, audit trails, anomaly detection, log retention policies
Vulnerability Management	Regular VAPT (Vulnerability Assessment and Penetration Testing), patching, CVE tracking
Secure Development	Secure SDLC (Software Development Life Cycle), code reviews, OWASP Top 10 mitigation
Cloud Security	CSPM tools, IAM enforcement, encryption, region controls, logging (e.g., AWS CloudTrail, Azure Sentinel)

11.3 Administrative and Organizational Controls

- Confidentiality agreements for employees, contractors, and third-party vendors
- Background checks for staff handling sensitive personal data
- Onboarding and offboarding processes with access revocation protocols
- Clear desk and screen policies
- Data handling SOPs tailored to business functions

11.4 Breach Management and Incident Response

- All security incidents and suspected breaches are handled via a defined **Incident Response Plan (IRP)**
- Data breach notifications are issued to data subjects and regulators in accordance with GDPR (72-hour rule) and other applicable laws

- Breaches are documented, analyzed, and remediate via root cause analysis and preventive action

11.5 Third-Party Security Assurance

- All third-party processors are subject to **security due diligence**, including:
  - Contractual clauses on data protection
  - Sub processor disclosures and approval
  - Audit rights and breach notification timelines
- Security assessment questionnaires or SOC 2 / ISO 27001 reports are requested where applicable

11.6 Data Lifecycle Protections

Phase	Security Practice
Collection	HTTPS forms, CAPTCHA, consent capture
Storage	Encrypted databases, role-based access, restricted keys
Processing	Secure processing environments, log integrity, access reviews
Transfer	TLS encryption, IP allowlists, VPN tunnels, cross-border transfer checks
Disposal	Secure deletion tools, certified wiping, shredding physical media

11.7 Security Awareness and Training

- Mandatory security and privacy awareness training for all employees
- Phishing simulations, scenario-based learning, and refresher modules
- Specialized training for developers, security engineers, and data handlers

12. DATA SECURITY MEASURES

The organization ensures that the collection and use of personal data based on consent complies with the highest standards of **valid, informed, and revocable consent**. Consent is treated not as a one-time checkbox but as a dynamic expression of trust that individuals can exercise and withdraw at any point.

Our consent management practices are built around **transparency**, **user autonomy**, and **legal defensibility**, and are applied across all digital, physical, and operational interfaces where personal data is collected.

12.1 When Consent is Required

Consent is required in the following scenarios:

- Processing of sensitive personal data such as financial information, biometrics, health records, religious beliefs, or sexual orientation
- Direct marketing communications (email, SMS, phone calls, etc.)
- Behavioral profiling and analytics for personalization or performance monitoring
- Use of cookies or tracking technologies for non-essential (non-functional) purposes
- Cross-border transfers to jurisdictions without adequate data protection laws, where consent is the primary legal basis
- Third-party data sharing for purposes not clearly disclosed at the point of collection
- Optional program participation, including customer surveys, feedback campaigns, or referral schemes.

12.2 Consent Quality Standards

We adhere to the following requirements for all consent-based processing:

Requirement	Implementation Practice
Freely Given	Consent is not bundled with service access. No coercion or pre-checked boxes are used.
Specific & Purpose Bound	Each data processing purpose is listed separately, and consent is collected for each purpose individually.
Informed	Consent interfaces provide clear language (no jargon) on what data is collected and why.
Unambiguous	Requires clear affirmative action (e.g., checkbox, toggle switch, "I Agree" button).
Granular	Separate options are provided for types of communications (e.g., newsletters, promotions, calls).
Documented	The consent is logged with timestamp, IP address (or user ID), and purpose agreed to.
Easily Withdrawable	Mechanisms for consent withdrawal are as easy as giving consent.

12.3 Consent Collection Mechanisms

I. Digital Platforms

- Cookie banners with granular preferences
- Sign-up pages with purpose-specific consent fields
- Preference centers in user profiles for opt-in/opt-out
- Dynamic banners for new data collection points

II. HR and Employee Workflows

- Onboarding forms with consent to process employee information
- Consent to collect health data, emergency contacts, and background verification data
- Periodic re-affirmation for continued processing of sensitive employee data

III. Customer and Partner Portals

- Consent embedded in digital contract flows or onboarding forms
- CRM-integrated consent logs linked to communication preferences
- Third-party data sharing notices with opt-out controls

IV. Offline or Hybrid Channels

- Consent via paper forms with digital backup (scanned and logged)
- Call center scripts with verbal consent logging (if recorded)
- QR codes on physical documents to redirect users to digital consent interfaces

12.4 Consent Record-Keeping and Auditability

The organization maintains a **Consent Register** with the following minimum data points:

- Identity of the consenting party (name, ID, IP address, session ID)
- Consent date and time (timestamp)
- Specific purposes consented to
- Channel or method of consent collection
- Status of consent (active, withdrawn, expired)
- Version of privacy notice applicable at the time

These records are retained for the duration of processing for a minimum of 2 years for audit/legal traceability.

12.5 Consent Withdrawal Process

Data subjects may withdraw consent via:

- A link in communications (e.g., unsubscribe in emails)
- Their user account privacy settings or profile dashboard
- Directly contacting the DPO or privacy team
- Privacy rights request portals or mobile app settings Once consent is withdrawn:

- All processing for the specific purpose is immediately halted
- No retaliation, denial of service, or degradation of experience is imposed
- Systems and data handlers are alerted via backend workflows or task assignments

12.6 Expiry and Renewal of Consent

- Where consent is required for long-term processing (e.g., talent pipelines, marketing), periodic **consent renewal prompts** are issued
- For sensitive data, re-consent is collected every 12–24 months or after a major policy change
- Expired consent is treated as revoked and data is removed unless alternative legal grounds apply

12.7 Special Consent Considerations

12.7.1 Children and Minors

- Consent is collected **only from parents or legal guardians** for users below the digital consent age.
- Age verification mechanisms are applied during signup or collection workflows
- Additional protections and review layers are enforced in platforms targeting minors

12.7.2 Biometrics and Sensitive Personal Data

- Explicit consent is mandatory before collecting biometrics, medical records, or identity documentation
- Such data is encrypted at rest and access-controlled
- Consent records are tagged for sensitivity and reviewed more frequently

12.7.3 Data Transfers Based on Consent

- Consent-based cross-border transfers are used only when no adequacy or standard contractual clauses are available
- The risks of international transfer are communicated clearly, and consent is logged

13. ENFORCEMENT

The organization uses cookies and similar tracking technologies on its websites, applications, and platforms to enhance user experience, analyze usage patterns, and deliver personalized content, in full compliance with applicable privacy regulations.

This section describes what cookies we use, why we use them, and how users can control or reject them.

13.1 What Are Cookies?

Cookies are small text files stored on your browser or device when you visit a website. They help us remember your preferences, enable functionality, and analyze user behavior.

In addition to traditional cookies, we may use:

- Web beacons / pixel tags
- Local storage and session storage
- SDKs (Software Development Kits) in mobile applications

13.2 Types of Cookies We Use

Category	Purpose	Examples
Strictly Necessary	Essential for website functionality, login sessions, load balancing, etc.	Session ID, CSRF token, load balancer routing
Performance / Analytics	Track website usage to improve functionality and user experience	Google Analytics
Functionality	Remember user preferences, region, or language	Language selector, dark/light mode
Marketing / Targeting	Track user behavior to personalize ads and content	Facebook Pixel, Google Ads Remarketing
Social media	Enable content sharing and embedded media playback	LinkedIn, Twitter, YouTube embeds

13.3 Legal Basis for Cookie Use

- Strictly necessary cookies do not require consent
- All other cookies (analytics, marketing, social media) require explicit opt-in consent
- Our website uses a cookie banner and preference center to manage consent in compliance with GDPR and privacy Directive

13.4 Cookie Consent and Management

Upon visiting our website, users are presented with a **cookie banner** that:

- Lists cookie categories with brief descriptions
- Allows granular control (Accept All / Reject All / Customize)
- Links to this Cookie Usage section
- Stores the user's choice with timestamp and IP

Users may update their cookie preferences at any time by:

- Clicking “Cookie Settings” in the website footer
- Accessing the privacy control panel via their account (if logged in)

13.5 Retention and Expiry

Cookies are stored for different durations based on their function:

Cookie Type	Typical Lifespan
Session Cookies	Deleted when browser is closed
Persistent Cookies	6 months to 2 years
Analytics/Marketing	Based on tool (e.g., Google Analytics: 2 years)

13.6 Third-Party Cookies

We may allow trusted third-party services to place cookies on your browser for:

- Web analytics
- Embedded videos or social feeds
- Advertising and retargeting campaigns

Each third party maintains its own cookie and privacy policy, and their data collection practices are subject to their terms.

13.7 How to Disable Cookies

Most web browsers allow users to:

- View, delete, or block specific cookies
- Set default cookie settings for all sites
- Receive alerts before cookies are stored

Note: Disabling certain cookies may limit the functionality of the website.

13.8 Do Not Track (DNT) Signals

Our systems honor “Do Not Track” browser signals where technically feasible and legally required, although full implementation may depend on third-party services.

14. POLICY REVIEW AND UPDATES

The organization recognizes that data protection is a continuously evolving area, driven by regulatory changes, technological advancement, and business transformation. To ensure that

this Privacy Policy remains accurate, effective, and compliant with applicable laws, it is subject to periodic review and timely updates.

14.1 Review Frequency

- The Privacy Policy is **formally reviewed at least once every 24 months** by the **Data Protection Officer (DPO)** in collaboration with the Legal, Information Security, and Compliance teams.
- Interim reviews may be triggered by:
  - Significant regulatory changes (e.g., updates to GDPR, DPDP)
  - Changes in data processing activities or system architecture
  - Introduction of new products, services, or platforms that involve personal data
  - Findings from internal audits or data breach investigations