5.1 Introduction

Unisoftwares is committed to protecting personal data and respecting privacy rights under applicable laws including:

- Pakistan: Personal Data Protection Bill (pending/applicable regulations)
- USA: CCPA (California), state-specific laws
- International clients: GDPR (EU), PIPEDA (Canada)

5.2 Data Protection Principles

5.2.1 Lawfulness, Fairness & Transparency

- Collect data only with legal basis (consent, contract, legitimate interest)
- Inform data subjects about data collection and use
- Privacy notices available on website and contracts

5.2.2 Purpose Limitation

- Collect data only for specified, explicit purposes
- Don't use data for incompatible purposes without new consent

5.2.3 Data Minimization

- Collect only data necessary for the purpose
- Example: Don't collect date of birth if only age verification needed

5.2.4 Accuracy

- Keep personal data accurate and up to date
- Provide mechanisms for data subjects to correct information

5.2.5 Storage Limitation

- Retain data only as long as necessary
- Delete or anonymize data after retention period

5.2.6 Integrity & Confidentiality

- Protect data with appropriate security measures
- Encrypt sensitive data at rest and in transit

5.2.7 Accountability

- Demonstrate compliance with data protection principles
- Maintain records of processing activities

5.3 Types of Data We Process

5.3.1 Employee Data

- Personal details (name, address, contact, CNIC/SSN)
- Employment records (contract, performance reviews, salary)
- Health information (medical certificates for leave)
- Financial data (bank account, tax information)

5.3.2 Client Data

- Business contact information
- Contract and billing information
- Website analytics data (for client sites we manage)
- Communication records (emails, meeting notes)

5.3.3 Website Visitor Data

- IP addresses, browser type, device information
- Cookies and tracking technologies
- Form submissions (contact forms, newsletter signups)

5.4 Legal Basis for Processing

5.4.1 Consent

- Explicit consent for marketing communications
- Consent is freely given, specific, informed, unambiguous
- Right to withdraw consent at any time

5.4.2 Contract Performance

- Processing necessary to fulfill employment or client contracts

- Example: Payroll processing for employees

5.4.3 Legal Obligation

- Compliance with tax laws, labor laws
- Example: Retaining employment records per legal requirements

5.4.4 Legitimate Interest

- Business operations, fraud prevention, security
- Balanced against individual's rights and freedoms

5.5 Data Subject Rights

5.5.1 Right to Access

- Request copy of personal data we hold
- Response within 30 days
- Free of charge (unless excessive requests)

5.5.2 Right to Rectification

- Correct inaccurate or incomplete data
- Update via HR portal or email request

5.5.3 Right to Erasure ("Right to be Forgotten")

- Request deletion of personal data
- Exceptions: Legal obligations, contract performance

5.5.4 Right to Restrict Processing

- Limit how we process data in certain circumstances
- Example: During dispute about data accuracy

5.5.5 Right to Data Portability

- Receive data in structured, machine-readable format
- Transfer data to another controller

5.5.6 Right to Object

- Object to processing based on legitimate interest

- Absolute right to object to direct marketing

5.5.7 Rights Related to Automated Decision-Making

- Right not to be subject to solely automated decisions
- Human review available for significant decisions

5.6 How to Exercise Your Rights

Contact: privacy@unisoftwares.pk
Subject Line: Data Subject Request - [Your Name]

Provide:

- Full name
- Employee ID or relationship to company
- Specific right you're exercising
- Details to help us locate your data

Response Time: Within 30 days (may extend 60 days for complex requests)

5.7 Data Retention Schedule

Data Type	Retention Period	Legal Basis
Employee records (active)	Duration of employment	Contract
Employee records (former)	7 years after separation	Legal obligation
Payroll records	7 years	Tax/labor law
Client contracts	7 years after completion	Legal obligation
Marketing consents	Until withdrawn + 1 year	Consent records
Website analytics	26 months	Legitimate interest
CCTV footage (office)	30 days	Security/legitimate interest
Email communications	3 years (operational), 7 years (legal)	Business operations

---

5.8 Data Sharing & Transfers

5.8.1 Internal Sharing

- Data shared on need-to-know basis within company
- Access controls and permissions managed by IT

5.8.2 Third-Party Processors

We share data with:

- **Payroll providers**: Salary processing
- **Cloud storage**: Google Workspace, AWS
- **Email service**: Office 365, SendGrid
- **CRM**: HubSpot, Salesforce
- **Analytics**: Google Analytics

Data Processing Agreements (DPA) in place with all processors.

5.8.3 International Transfers

- **Pakistan to USA**: Standard contractual clauses
- **To EU clients**: GDPR-compliant mechanisms
- Adequate safeguards for all international transfers

5.8.4 No Data Selling

- We never sell personal data to third parties
- No sharing with advertisers without consent

5.9 Data Security Measures

5.9.1 Technical Safeguards

- Encryption at rest (AES-256)
- Encryption in transit (TLS 1.3)
- Regular security patches and updates
- Firewall and intrusion detection systems
- Multi-factor authentication

- Access logging and monitoring

5.9.2 Organizational Measures

- Employee training on data protection
- Background checks for staff with data access
- Confidentiality agreements (NDAs)
- Data protection impact assessments (DPIAs)
- Regular security audits

5.9.3 Physical Security

- Biometric access control to data centers
- CCTV monitoring
- Visitor logs and escort policy
- Secure disposal of physical documents (shredding)

5.10 Data Breach Response

5.10.1 Detection & Assessment

- Monitor systems for unusual activity
- Investigate suspected breaches immediately
- Assess severity and scope

5.10.2 Notification

- **Supervisory Authority**: Within 72 hours (GDPR)
- **Affected Individuals**: Without undue delay if high risk
- **Details**: Nature of breach, likely consequences, mitigation measures

5.10.3 Remediation

- Contain breach, fix vulnerability
- Implement additional security measures
- Document incident and lessons learned

5.11 Cookies & Tracking

5.11.1 Website Cookies

Strictly Necessary: Essential for website functionality (no consent needed) **Performance**: Analytics to improve site (Google Analytics) **Functional**: Remember preferences, language **Targeting**: Marketing and advertising (requires consent)

5.11.2 Cookie Management

- Cookie banner on first visit
- Granular consent options
- Opt-out links provided
- Cookie policy page: unisoftwares.pk/cookie-policy

5.12 Children's Privacy

- We do not knowingly collect data from children under 16
- If discovered, data will be deleted immediately
- Parent/guardian consent required if applicable

5.13 Privacy by Design

- Privacy considerations in all new projects
- Data Protection Impact Assessments (DPIA) for high-risk processing
- Privacy settings default to most protective
- Regular privacy audits

5.14 Contact & Complaints

Data Protection Officer (DPO): dpo@unisoftwares.pk

Complaints:

- First contact: privacy@unisoftwares.pk
- If unsatisfied: File complaint with local data protection authority
  - Pakistan: Pending data protection authority

- USA: State attorney general
- EU: Local supervisory authority

FAQs (Data Privacy)

Q1: How can I request my personal data?
A: Email privacy@unisoftwares.pk with your name and employee ID. We'll respond within 30 days. (Source: Data_Privacy_GDPR_Policy.pdf, Section 5.6)

Q2: How long do you keep employee records?
A: Active employees: duration of employment. Former employees: 7 years after separation. (Source: Data_Privacy_GDPR_Policy.pdf, Section 5.7)

Q3: Do you sell personal data?
A: No, we never sell personal data to third parties. (Source: Data_Privacy_GDPR_Policy.pdf, Section 5.8.4)