# DATA PROTECTION POLICY

ECSSCORE

[DATE]

| | |
|---|---|
| **Company Name** | **ECS-Score Private Limited** |
| **Document Title** | Data Protection Policy |
| **Legal Compliance** | • Digital Personal Data Protection Act, 2023 (DPDP Act)<br>• Information Technology Act, 2000/2008 (IT Act)<br>• Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules – transitional relevance)<br>• ISO/IEC 27001:2022 (Information Security Management System Requirements) |
| **Version** | 1 |
| **Effective Date** | _____ |
| **Last Updated** | _____ |
| **Registered Office Address** | _____<br>_____ |
| **Website** | https://www.ecsscore.com |
| **Official Contact Email** | ecsscore@gmail.com |
| **Designated Grievance Officer (DPDP Requirement)** | Name: _____ Email: ecsscore@gmail.com |
| **Authorized Signatory** | **Name:** _____<br>**Designation:** _____<br>**Signature:** _____ |
| **Document Issued By** | ECS-Score Private Limited |

# ECS Aligned With ISO 27001:2022

| ISO 27001 Requirement | How ECS Score Policy Addresses It |
|---|---|
| Context & Scope (Clause 4) | Scope defined: employees, contractors, third parties, systems, and full data lifecycle. |
| Leadership & Commitment (Clause 5) | Management responsibilities, policy approval, resource allocation, and accountability are specified. |
| Risk Assessment & Treatment (Clause 6) | Security principles, access controls, encryption, monitoring, and retention policies address risk mitigation. |
| Information Security Objectives (Clause 6.2) | Confidentiality, integrity, availability, and compliance goals clearly stated. |
| Organizational Roles & Responsibilities (Clauses 5.3 & 7.2) | Roles for employees, management, Grievance Officer, and third parties assigned. |
| Awareness, Training & Competence (Clause 7.2) | Annual training, role-based awareness, cybersecurity modules included. |
| Operational Planning & Controls (Clause 8) | Data processing, consent management, sharing controls, retention, and secure disposal described. |
| Information Security Controls (Annex A) | Encryption, MFA, RBAC, secure development, cloud security, monitoring, incident management, and physical security included. |
| Performance Evaluation & Audits (Clause 9) | Logs, audit trails, reviews, and annual policy review included. |
| Continual Improvement (Clause 10) | Breach analysis, CAPA, and annual reviews included. |

# ECS Aligned With DPDP Act 2023

| DPDP Act Requirement | How ECS Score Policy Addresses It |
|---|---|
| Lawful Processing | Specifies consent, legitimate purpose, and legal obligations as processing bases. |
| Consent Principles (Sections 11–13) | Consent is free, informed, specific, unambiguous, revocable; withdrawal procedures included. |

| | |
|---|---|
| Data Principal Rights | Access, correction, deletion, withdrawal, grievance redressal, nomination rights listed. |
| Accountability | Roles (Grievance Officer, employees, third parties), audit trails, and internal reviews described. |
| Security of Personal Data | ISO-aligned controls ensure confidentiality, integrity, availability. |
| Cross-Border Transfers | Encrypted transfer and contractual safeguards included. |
| Data Breach Notification | Breach management plan includes timely notification to Data Principals and authorities. |
| Data Retention & Minimization | Purpose limitation, retention timelines, secure deletion aligned with DPDP principles. |
| Privacy by Design | Embedded in system, product, and process design considerations. |

## 1. Introduction

ECS-Score Private Limited the Company is committed to maintaining the highest possible standard of privacy, confidentiality, and data protection for all individuals whose personal data we process. As an employment credibility and verification platform, ECS Score handles sensitive personal information including employment records, identity documents, and professional references.
The objective of this policy is to provide a clear, transparent, and comprehensive explanation of how ECS Score collects, processes, stores, secures, shares, and disposes of personal data in compliance with the **Digital Personal Data Protection Act, 2023 (DPDP Act)**, **ISO/IEC 27001:2022**, and other applicable Indian IT laws.

This policy sets forth not only the legal compliance obligations but also ECS Score's internal framework for ensuring responsible data governance, risk management, and implementation of appropriate technical and organizational security measures.

## 2. Policy Purpose

The purpose of this Data Protection Policy is to:

1. Establish a robust governance structure for managing personal data
2. Define lawful bases for processing and the rights of Data Principals
3. Ensure integrity, confidentiality, and availability of personal data through secure processes
4. Provide employees, partners, and external stakeholders with clarity on their responsibilities
5. Prevent unauthorized access, misuse, alteration, loss, or destruction of personal data
6. Align ECS Score's data protection practices with international standards like ISO 27001

This policy serves as a foundational document for ECS Score's privacy and information security framework.

## 3. Applicability & Scope

This policy applies to:

- All personal data processed digitally by ECS Score
- All employees, contractors, advisors, fellows, and interns
- All third-party processors, service providers, and verification partners
- All ECS Score products, APIs, systems, cloud services, and applications
- All data principals including users, employers, partners, and internal staff

The policy covers the **entire data lifecycle**, including collection, recording, storage, alteration, retrieval, transmission, sharing, archival, and erasure.

## 4. Definitions & Key Terminology

### 4.1 Personal Data

Any data that can identify an individual, either directly or indirectly. This includes names, contact details, documents, accounts, and employment history.

### 4.2 Sensitive Personal Data

As per SPDI Rules (transitionally applicable): identity proofs, financial information, biometric identifiers, employment documents, and other sensitive attributes.

### 4.3 Data Principal

The individual whose personal data is being processed (e.g., ECS Score users).

### 4.4 Data Fiduciary

ECS Score, which determines the purpose and means of processing personal data.

### 4.5 Data Processor

Any third party that processes personal data on behalf of ECS Score.

### 4.6 Consent

Clear, specific, informed agreement provided freely by the Data Principal for the intended processing purposes.

### 4.7 Processing

Any action performed on data—collection, storage, retrieval, transmission, sharing, modification, or deletion.

### 4.8 Data Breach

Unauthorized or accidental access, disclosure, alteration, loss, or destruction of personal data.

### 4.9 Privacy by Design

Embedding data protection principles in system architecture from the earliest stages of product development.

These definitions ensure uniform understanding across the organization.

## 5. Categories of Data Processed by ECS Score

ECS Score processes the following types of data:

### 5.1 Identity Information

Full name, phone number, email address, government-issued IDs, biometric details (if provided).

### 5.2 Employment Information

Past and current employer details, job titles, tenure, experience letters, appraisal documents, and verification inputs.

### 5.3 Professional Credibility Inputs

Peer endorsements, references, performance assessments, and trust indicators.

### 5.4 System & Activity Data

IP addresses, device metadata, login patterns, audit logs, and user activity metrics.

### 5.5 Communication Data

Emails, customer support messages, queries, requests, and consent logs.

This diverse data collection supports ECS Score's core function of generating credibility scores and verification outputs.

### 6. Lawful Bases for Processing

Under the DPDP Act, ECS Score processes data only under lawful bases, including:

#### 6.1 Consent

Explicit, informed, unambiguous user consent is the primary basis for processing.

#### 6.2 Legitimate Use

Processing necessary to deliver services requested by the user (verification, scoring, document validation).

#### 6.3 Compliance with Law

Disclosure to government authorities, courts, or agencies as required under applicable law.

#### 6.4 Employment-related Processing

Data processing required to verify employment records or provide Trust Seal services.

No processing occurs without a clearly documented legal basis.

## 7. Data Principal Rights

ECS Score ensures that every Data Principal can exercise the following rights:

- **Right to Access** – obtain details of personal data being processed
- **Right to Correction** – fix inaccurate or incomplete data
- **Right to Deletion** – request removal unless retention is legally necessary
- **Right to Withdraw Consent** – stop processing at any time
- **Right to Grievance Redressal** – escalate concerns to the Grievance Officer
- **Right to Nominate** – assign a nominee in case of death or incapacity (DPDP requirement)

Requests may be emailed to **ecsscore@gmail.com**

### 8. Data Protection Principles

ECS Score applies the following principles:

### 8.1 Lawfulness, Fairness, Transparency

Users are informed about what data is collected and why.

### 8.2 Purpose Limitation

Data is used only for explicit, legitimate purposes.

### 8.3 Data Minimization

Only necessary data is collected.

### 8.4 Accuracy

Data is verified and maintained accurately.

### 8.5 Storage Limitation

Data is retained only for required durations.

### 8.6 Integrity and Confidentiality

Robust security controls protect data at all stages.

### 8.7 Accountability

ECS Score maintains records, logs, policies, and audit trails demonstrating compliance.

## 9. Information Security & ISO 27001 Controls

ECS Score implements comprehensive technical and organizational measures consistent with ISO/IEC 27001:2022 requirements.

### 9.1 Access Control

- MFA for privileged accounts
- RBAC (Role-Based Access Control)
- Periodic access reviews
- Password complexity enforcement

### 9.2 Encryption Controls

- AES-256 encryption at rest
- TLS 1.2+/HTTPS for all data in transit
- Secure key management via KMS

### 9.3 Application & System Security

- Secure coding practices
- OWASP Top 10 compliance
- Regular vulnerability assessments
- Patch and configuration management

### 9.4 Network Security

- Firewalls and intrusion detection
- Zero-trust architecture elements
- Segregated production environments

### 9.5 Cloud Security

- ISO-certified cloud providers
- Continuous monitoring
- Daily encrypted backups

### 9.6 Logging & Monitoring

- System and access logs
- Real-time monitoring for anomalies
- Forensics and root-cause analysis

### 9.7 Physical Security

- Controlled office access
- CCTV monitoring
- Secure server and device storage

## 10. Data Sharing & Third-Party Processing

ECS Score shares data **only when necessary** and under strict contracts.

Third parties include:

- Employment verification partners
- Cloud hosting providers
- Email/SMS/notification providers

- Analytics and support tools

All processors must:

- Sign Data Processing Agreements
- Implement equivalent or stronger security controls
- Comply with audit requirements

No third-party processing occurs without proper safeguards.

## 11. Cross-Border Data Transfers

If data is transferred outside India:

- Transfer will only occur to countries not restricted by the Government of India
- Transfer will be encrypted
- Contractual and security measures will apply

ECS Score maintains logs of all outbound transfers.

## 12. Data Retention & Secure Disposal

Retention of personal data is based on:

- Verification requirements
- Legal/regulatory timelines
- Fraud prevention needs

After retention ends, data is securely destroyed using:

- Cryptographic wiping
- Secure deletion
- Contractual deletion by processors

## 13. Data Breach Response & Notification

ECS Score maintains a structured **Incident Response Plan**.

In the event of a breach:

1. **Immediate containment**
2. **Root-cause analysis**
3. **Notification to affected users**
4. **Regulatory reporting (if mandated)**
5. **Corrective and preventive actions (CAPA)**

All breaches are documented and reviewed.

## 14. Roles & Responsibilities

### 14.1 Management

- Ensures compliance
- Allocates resources
- Approves policies

### 14.2 Employees

- Follow this policy
- Protect confidential data
- Report suspicious activity

### 14.3 Grievance Officer

- Handles complaints
- Coordinates with authorities
- Ensures timely responses

### 14.4 Third-Party Processors

- Maintain required safeguards
- Support audits and investigations

### 15. Training & Compliance Awareness

All employees undergo:

- Data protection & privacy training
- Cybersecurity awareness programs
- Role-specific modules for handling sensitive data

Training occurs **annually** or when major changes arise.

## 16. Policy Review & Approval

This policy is reviewed each year or upon:

- Changes in regulatory requirements
- New services or technological changes
- Major incidents or breaches

Updates require approval from the **Authorized Signatory**.

ECS-Score Private Limited reiterates its commitment to safeguarding personal data with the highest level of care, transparency, and security. We work continuously to protect the trust of our users, clients, employees, and partners through strong governance, robust security practices, and responsible data management.

For any questions or concerns regarding this policy, please contact:
✉ **ecsscore@gmail.com**