# **Compliance & Privacy Policy**

**Nexora Technologies** *Last updated: July 2025*

## **1. Purpose**

This document outlines how **Nexora Technologies** ensures compliance with relevant laws, regulations, and best practices related to data privacy, security, and ethical use of information. It is mandatory reading for all employees, contractors, and third-party vendors.

## **2. Data Privacy Policy**

### **2.1 Personal Data We Collect**

* **Customers:** Names, emails, usage logs, billing info.
* **Employees:** HR records, contact info, device access metadata.
* **Website visitors:** IP addresses, session cookies, usage patterns.

### **2.2 How We Use Personal Data**

* Provide and improve our services
* Manage customer support
* Ensure security and system integrity
* Internal analytics (aggregated and anonymized)

### **2.3 Your Rights (GDPR/CCPA)**

Depending on your location, you may:

* Request access to your data
* Request correction or deletion
* Object to processing
* Request data portability

Submit requests at: **privacy@nexora.tech**

## **3. Regulatory Compliance**

| **Regulation** | **Description** | **Nexora's Status** |
| --- | --- | --- |
| **GDPR** | EU privacy law for user data | Compliant |
| **CCPA/CPRA** | California privacy laws | Compliant |
| **SOC 2 Type I** | Security and privacy controls (attestation) | In Progress (Q4 2025) |
| **ISO/IEC 27001** | Information Security Management Standard | Roadmap for 2026 |
| **HIPAA** | Health data protection (for healthcare customers) | Not applicable yet |

## **4. Data Handling Practices**

### **4.1 Data Encryption**

* All data encrypted **at rest** (AES-256) and **in transit** (TLS 1.2+)
* Passwords stored using salted bcrypt hashes

### **4.2 Data Retention**

* Customer data: 5 years or until termination
* Logs: 12 months (unless longer retention is legally required)
* Email & communication records: 3 years

### **4.3 Data Minimization**

* Collect only what is needed
* Anonymize data where feasible
* Regular reviews of stored PII

## **5. Third-Party & Vendor Compliance**

All third-party services must:

* Sign a **Data Processing Agreement (DPA)**
* Provide documentation for **security controls**
* Be reviewed annually for compliance

Vendors we use:

* **AWS** (Hosting)
* **PostHog** (Product analytics – self-hosted)
* **OpenAI/Groq** (LLM APIs – with region controls)

## **6. Breach Response Plan**

If a data breach occurs:

1. **Internal alert** to Security & Legal within 1 hour
2. **Root cause analysis** and containment within 24 hours
3. **Customer notification** (if needed) within 72 hours
4. **Full audit report** published internally