**Data Security Policy**

**Effective Date:** [Insert Date]
**Last Updated:** [Insert Date]
**Applies to:** All operations and systems under KabirCreation.com

**1. Purpose**

The purpose of this Data Security Policy is to ensure the confidentiality, integrity, and availability of all data—especially **personal and payment-related data**—collected, processed, and stored by **KabirCreation.com**. This policy outlines our approach to mitigating risks associated with unauthorized access, data breaches, and misuse of customer information.

**2. Scope**

This policy applies to:

* All employees, contractors, third-party service providers, and stakeholders with access to KabirCreation.com systems
* All systems, applications, networks, databases, and endpoints under the organization’s control
* All personal data collected from customers, suppliers, and employees in the course of business operations

**3. Legal and Regulatory Framework**

This policy is designed in compliance with:

* **General Data Protection Regulation (EU) 2016/679 (GDPR)**
* **German Federal Data Protection Act (BDSG)**
* **PCI-DSS** standards (for payment data)
* Any applicable national and international data protection laws relevant to operations

**4. Data Classification**

Data is categorized into three main types:

| **Category** | **Example** | **Protection Level** |
| --- | --- | --- |
| Public | Product descriptions, blog content | Low |
| Internal | Operational notes, supplier data | Medium |
| Confidential | Customer personal data, payment data | High |

Special attention is given to **"Personal Data"** and **"Sensitive Personal Data"** as defined under Article 4 of GDPR.

**5. Security Measures**

**5.1 Access Control**

* Role-based access control (RBAC) with **least privilege** principle
* User access is reviewed quarterly and upon employee departure or role change
* MFA (Multi-Factor Authentication) is enforced for all admin-level accounts
* Strong password policies (minimum 12 characters, complexity requirements)

**5.2 Data Encryption**

* **TLS 1.2+** encryption for data in transit (via HTTPS)
* **AES-256 encryption** for data at rest (databases, backups)
* Encrypted email communication for sensitive internal and external exchanges

**5.3 Secure Development Practices**

* Web application follows **OWASP Top 10** security guidelines
* Code is peer-reviewed and tested in isolated environments
* Secrets and credentials are never hardcoded in source code

**5.4 Network Security**

* Firewalls and Intrusion Detection Systems (IDS) in place
* Network segmentation separates front-end systems from internal data processing units
* Regular port scans and security assessments conducted

**5.5 Hosting and Infrastructure**

* Hosted on **GDPR-compliant** servers (e.g., AWS Frankfurt or other EU-based providers)
* Daily automatic backups stored in secure, geo-redundant locations
* Patching and OS updates are applied on a weekly schedule or immediately in case of vulnerabilities

**6. Data Breach Response Plan**

In case of a data breach:

1. Immediate incident detection and containment
2. Notification to DPO and executive team within **12 hours**
3. Report to affected users and relevant authority (**BfDI**) within **72 hours** as per GDPR
4. Root cause analysis and corrective measures applied
5. Documentation of incident and resolution process

A dedicated **Incident Response Team (IRT)** is assigned and trained annually.

**7. Third-Party & Vendor Security**

All third-party vendors are assessed for:

* GDPR compliance
* Data processing agreements (DPAs) in place
* Security certifications (ISO 27001, SOC 2, etc.)
* Regular vendor risk assessments

Examples include:

* **Stripe/PayPal** for secure payments
* **Mailchimp** for email communication
* **Logistics partners** with encrypted data transfers

**8. Data Minimization and Retention**

* Only necessary data is collected (data minimization principle)
* Retention schedule defined in the Privacy Policy (Section 7)
* Secure deletion of data upon expiration or user request (using wipe/overwrite techniques)

**9. Employee Security Awareness**

* Mandatory onboarding and annual **security training** for all staff
* Specialized training for devs and customer service on secure handling of personal data
* Confidentiality agreements signed by all employees and contractors

**10. Monitoring and Auditing**

* Continuous monitoring of user activity and system logs
* Monthly internal security audits
* External audits conducted annually by certified providers
* Logs are stored securely and maintained for a minimum of 12 months

**11. Physical Security (if applicable)**

For on-premise or backup data centers:

* Restricted access to authorized personnel
* CCTV surveillance and access logs maintained
* Fire suppression, redundant power supplies, and biometric entry (where applicable)

**12. Policy Review and Updates**

* This policy is reviewed **annually** or after major changes in operations or legal requirements
* All updates are documented and versioned
* Users and staff are notified of significant policy changes

**13. Contact Information**

For questions or concerns related to this Data Security Policy, contact:

**Kabir Creation – Data Protection Officer**
Email: [privacy@kabircreation.com]
Phone: [Insert Number]
Address: [Insert Company Address, Germany]

**14. Version Control**

| **Version** | **Date** | **Change Summary** |
| --- | --- | --- |
| 1.0 | [Insert Date] | Initial release |