

## **MadeUpName, LLC**

### **Data Protection & Privacy Policy**

#### **Purpose**

MadeUpName, LLC is committed to protecting the privacy and security of personal and company data. This policy outlines how we collect, use, store, and protect personal information of employees, clients, and partners in compliance with applicable privacy laws.

#### **Scope**

This policy applies to all employees, contractors, and interns of MadeUpName, LLC who have access to personal or confidential information in the course of their work.

#### **1. Data We Collect**

We may collect personal information such as: - Employee data (e.g., name, address, contact information, Social Security number, payroll details). - Client or vendor contact information. - Usage data from company systems or websites.

#### **2. Purpose of Data Use**

Personal data is collected and used only for legitimate business purposes, including: - Managing employment relationships. - Delivering software development and client services. - Maintaining security and compliance. - Improving company operations and communication.

#### **3. Data Protection Principles**

All employees must adhere to the following principles: - **Lawfulness, fairness, and transparency:** Process data only for legitimate purposes and communicate clearly about how it's used. - **Data minimization:** Collect only what is necessary. - **Accuracy:** Keep data up-to-date. - **Storage limitation:** Retain data only as long as needed. - **Integrity and confidentiality:** Protect data against unauthorized access, loss, or misuse.

#### **4. Data Access and Sharing**

Access to personal data is restricted to employees who need it for legitimate business purposes. Data must not be shared externally without authorization or a proper agreement (e.g., NDA, Data Processing Agreement).

#### **5. Data Security**

All employees must: - Use strong passwords and multi-factor authentication where applicable. - Store digital data on secure company systems. - Report any data breach or loss immediately to IT and HR.

#### **6. Employee Responsibilities**

Employees are responsible for protecting personal and client information. Any misuse or negligent handling of data may lead to disciplinary action.

#### **7. Data Breach Procedure**

If a data breach occurs, the company will: 1. Notify IT and HR immediately. 2. Contain and assess the breach. 3. Notify affected parties and authorities if required by law. 4. Take corrective action to prevent recurrence.

## **8. Compliance**

This policy aligns with U.S. privacy regulations and, where applicable, GDPR principles for international clients.

## **9. Related Policies**

This policy should be read in conjunction with the Acceptable Use of Technology Policy and the Code of Conduct & Ethics Policy.

**Effective Date:** January 2025

**Next Review Date:** January 2026

**Policy Owner:** Human Resources Department