SMART 5 Consulting Limited

Personal Data Processing Policy

t: +44(0) 20 3686 6135
m: +44(0) 780 944 9726 [Syed]
w: https://www.smart5.co.uk
e: syed@smart5.co.uk,
info@smart5.co.uk

SMART 5 Consulting Limited. Registered in England and Wales. Company Registration No. 12281263, Registered Office: 23, Quarles Park Road, Romford, RM6 4DE.

Effective Date: 12-06-2024

Version: 1.0

1. Introduction

This Personal Data Processing Policy outlines the technical and organizational measures that Smart 5 Consulting Limited (hereafter referred to as "the Company") has in place to ensure compliance with Data Protection Legislation, including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy specifically addresses the data protection measures relevant to the services offered in our tender responses.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who process personal data on behalf of Smart 5 Consulting Limited.

3. Technical Measures

3.1 Data Encryption
- Encryption at Rest: All personal data stored within our systems is encrypted using AES-256 encryption.
- Encryption in Transit: TLS protocols are used to encrypt personal data transmitted over networks.

3.2 Access Control
- Authentication: Multi-factor authentication (MFA) is implemented for all user access to systems processing personal data.
- Authorization: Role-based access controls (RBAC) are enforced to ensure only authorized personnel access specific data.
- Audit Logs: Comprehensive logging and monitoring of access and modifications to personal data.

3.3 Data Minimization and Pseudonymization
- Data Minimization: Collection and processing of only the minimal amount of personal data necessary for specified purposes.
- Pseudonymization: Techniques used to protect personal data by replacing identifiable information with pseudonyms.

3.4 Secure Development Practices
- Code Reviews and Testing: Rigorous code reviews and security testing, including penetration testing and static code analysis.
- Secure Coding Standards: Adherence to OWASP best practices to mitigate security risks.

4. Organizational Measures

4.1 Data Protection Policies
- Data Protection Policy: Regularly reviewed and updated to reflect changes in legislation and best practices.
- Employee Training: Annual and onboarding training on data protection principles, security practices, and GDPR responsibilities.

4.2 Incident Management
- Incident Response Plan: Defined procedures for identifying, reporting, and responding to data breaches.
- Breach Notification: Commitment to notifying the relevant supervisory authority within 72 hours and affected data subjects without undue delay.

4.3 Data Subject Rights
- Rights Management: Processes to handle data subject requests for access, rectification, erasure, restriction, data portability, and objection.
- Transparency: Clear and transparent information about data processing activities provided through privacy notices and consent forms.

4.4 Data Processing Agreements
- Third-Party Contracts: Data processing agreements (DPAs) with all third-party service providers processing personal data on our behalf.
- Vendor Due Diligence: Due diligence process to assess data protection capabilities and compliance of third-party vendors.

5. Compliance with Data Protection Principles

5.1 Lawfulness, Fairness, and Transparency
- Lawful Basis for Processing: Ensuring all personal data processing activities have a lawful basis.
- Transparency: Detailed privacy notices provided to data subjects.

5.2 Purpose Limitation
- Specific Purposes: Personal data collected for specified, explicit, and legitimate purposes only.
- Documentation: Documenting processing activities, purposes, and legal bases.

5.3 Data Accuracy
- Data Accuracy: Ensuring personal data is accurate, complete, and up-to-date.
- Rectification: Procedures to promptly rectify or delete inaccurate or incomplete data.

5.4 Storage Limitation
- Retention Policy: Retaining personal data only as long as necessary for the purposes collected or as required by law.
- Secure Disposal: Secure deletion or anonymization of personal data when no longer needed.

6. Data Protection Impact Assessments (DPIAs)

- Risk Assessment: Conducting DPIAs for high-risk processing activities.
- Mitigation Measures: Implementing appropriate measures to mitigate identified risks.

7. Data Protection Officer (DPO)

- DPO Appointment: A Data Protection Officer is appointed to oversee data protection compliance.
- DPO Contact Information: Provided in privacy notices and accessible to data subjects and stakeholders.

8. Conclusion

Smart 5 Consulting Limited is committed to maintaining the highest standards of data protection and privacy. We have implemented comprehensive technical and organizational measures to comply with Data Protection Legislation and protect personal data. Our proactive approach ensures that we meet contractual requirements and maintain the trust of our clients and stakeholders.

For further information or clarification on our data protection measures, please contact:

Data Protection Officer
Smart 5 Consulting Limited
23 Quarles Park Road, Chadwell Heath, Romford, RM6 4DE, UK
Email: syed@smart5.co.uk
Phone: 07809449726