Data Policy for Software in Consulting Engagements

Effective Date: 1 January 2020

Purpose
This Data Policy establishes guidelines for the collection, storage, processing, and protection of data handled by MobiCycle ("the Company") in connection with its consulting and software development services. The policy ensures transparency, compliance with data protection laws, and a commitment to safeguarding client and end-user data.

1. Scope

This policy applies to all employees, contractors, and third parties involved in handling, processing, or managing data collected, stored, or generated during client engagements. It covers all types of data, including personal, client-provided, and generated data.

2. Data Collection and Use

2.1 Client-Provided Data
The Company collects data provided directly by clients necessary to fulfill consulting or software development services. This includes business data, project requirements, and any additional information provided to ensure successful delivery.

2.2 Generated Data
During consulting and software development, the Company may generate data related to system performance, user engagement, or analytics to enhance project outcomes. This data is used solely for the purpose of delivering services and improving client outcomes.

2.3 Personal Data
If the project involves personal data of the client's end users, the Company will process this data in accordance with data privacy laws and any client-specified requirements. The Company does not use personal data for any purposes other than those outlined in the client agreement.

3. Data Storage and Security

3.1 Data Storage Locations
The Company stores data securely in [tbd storage locations, e.g., secure servers, cloud storage providers] located in [tbd regions, e.g., United States, EU-compliant regions]. Data storage complies with relevant laws and industry standards.

3.2 Data Protection Measures
The Company employs industry-standard security measures to protect all stored data, including but not limited to:

- Encryption of data at rest and in transit.
- Multi-factor authentication for access to data systems.
- Regular security audits and vulnerability assessments.
- Role-based access controls to limit data access to authorized personnel only**.**

3.3 Data Retention
The Company retains data only as long as necessary to fulfill the project's requirements or comply with legal obligations. Upon project completion, data will be archived, anonymized, or securely deleted in accordance with client agreements or applicable laws.

4. Data Sharing and Confidentiality

4.1 Data Sharing
The Company does not share client-provided or generated data with third parties except:

- With client permission.
- As required by law or regulatory requirements.
- With trusted third-party vendors for specific project needs, under strict confidentiality agreements and only to the extent necessary.

4.2 Confidentiality Obligations
All employees, contractors, and third-party vendors with access to client data are bound by confidentiality agreements. They are required to handle data in accordance with this policy, ensuring that data confidentiality, integrity, and privacy are maintained.

5. Compliance with Data Privacy Laws

5.1 General Compliance
The Company adheres to relevant data privacy laws, including but not limited to the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), as applicable. Compliance with these regulations ensures that data subjects' rights are respected and upheld.

5.2 Client-Specific Compliance Requests
The Company will accommodate client-specific compliance requirements, including Data Protection Impact Assessments (DPIAs) and Data Processing Agreements (DPAs), when requested.

6. Data Access and Control

6.1 Client Access to Data
Clients may request access to data collected or generated during a project. The Company will provide such access upon request, ensuring that data is made available in a secure and structured format.

6.2 Data Subject Rights
If personal data is processed, data subjects have rights under applicable privacy laws, including rights to access, correction, and deletion of their data. The Company will assist clients in responding to data subject requests as required.

7. Breach Notification

7.1 Incident Response Plan
In the event of a data breach, the Company will follow an incident response plan to identify, contain, and mitigate the breach. The plan includes steps for rapid investigation and remediation.

7.2 Notification to Clients and Authorities
If a data breach occurs that affects client data, the Company will promptly notify the client in accordance with applicable laws and contractual agreements. If required by law, the Company will also notify relevant authorities and affected individuals.

8. Policy Updates

The Company reserves the right to amend this Data Policy as needed to reflect changes in laws, technology, or business practices. Clients will be notified of any material changes that may impact their data rights under this policy.

Contact Information
For questions regarding this policy, please contact:

MobiCycle
1603 Capitol Ave
Cheyenne, Wyoming 82001
legal@mobicycle.group