Subprocessor Monitoring Policy

1. Purpose

This policy outlines the framework and responsibilities for the regular monitoring of sub processors to ensure their compliance with Power Digital Marketing's data security and privacy standards, applicable to various security and privacy regulations and frameworks.

2. Scope

This policy applies to all sub processes engaged by Power Digital Marketing for processing data on behalf of our clients and our own internal operations.

3. Policy Statement

Power Digital Marketing commits to upholding the highest standards of data security and privacy. To this end, we require all engaged sub processors to comply with relevant data security policies and privacy regulations. This policy establishes the processes for ongoing monitoring and review to ensure subprocessor compliance.

4. Responsibilities

- **Data Security Team:** Tasked with executing regular audits, assessments, and monitoring of subprocessor compliance.
- **Compliance Officer:** Responsible for the policy's overall implementation and for coordinating with sub processors on compliance matters.
- **Subprocessors:** Required to adhere to Power Digital Marketing's data security and privacy standards and to cooperate fully with all audits, assessments, and reviews.

5. Procedures

Subprocessor Engagement:

- Conduct thorough due diligence prior to engaging any subprocessor to ensure their capability and commitment to meet our data security and privacy standards.

- Embed data security and privacy compliance clauses in all subprocessor agreements.

Continuous Audits and Assessments:

- Schedule and perform regular audits and security assessments of all sub processes to evaluate compliance with our standards.
- Identify and assess potential vulnerabilities or areas of non-compliance.

Incident Reporting and Management:

- Mandate immediate reporting by subprocessors of any security incidents or breaches.
- Establish clear protocols for incident response, including required actions, timelines, and communication procedures.

Performance and Compliance Review:

- Regularly review subprocessor performance against predefined compliance metrics and benchmarks.
- Evaluate adherence to data security and privacy requirements.

Corrective Actions and Improvement:

- Address non-compliance or potential areas for improvement identified during audits and reviews by working collaboratively with subprocessors.
- Monitor the implementation of corrective actions to resolve identified issues.

Documentation and Record-Keeping:

- Keep detailed records of all monitoring activities, including audit reports, assessment results, and corrective actions.
- Ensure documentation of all communications with subprocessors regarding compliance matters.

Policy Review and Updates:

- Annually review this policy or following significant changes to regulatory requirements or data processing operations.
- Update the policy as necessary to maintain alignment with current data security and privacy best practices.

Enforcement

Failure to comply with this policy by employees or subprocessors may result in disciplinary actions, including the termination of contracts. Subprocessor relationships will be reevaluated in cases of continued non-compliance with our data security and privacy standards.