

Data Processing Agreement (DPA)

Parties

Processor: Otuso, 1166 Bonin Crescent, Milton ON L9T 0B1 — info@otuso.ca

Controller: [Client legal name and address]

Purpose and scope

This DPA governs Processor's processing of Controller personal data in connection with marketing services and related deliverables under the parties' main services agreement.

Roles

Controller: determines purposes and means of processing.

Processor: processes personal data only on Controller's documented instructions unless required by law.

Categories of personal data and data subjects

- Categories: contact details (name, email, phone), identifiers (client IDs), communications (emails, messages), project materials containing personal data, billing/contact info, technical/usage data (IP, cookies), marketing preferences.
- Data subjects: Controller's customers/prospects, employees, contractors, website visitors and other individuals whose data Controller supplies.

Duration

Processing period = term of the main services agreement and any retention period thereafter as required by Controller or by law.

Processor obligations

- Process only on Controller's documented instructions.
- Implement and maintain appropriate technical and organizational measures (examples below).
- Ensure personnel with access are bound by confidentiality.
- Promptly notify Controller of any request from data subjects that relates to the Controller's instructions, unless legally prohibited.
- Assist Controller in responding to data subject requests and regulatory inquiries.
- Maintain records of processing activities relevant to services.

Security measures

- Access controls and role-based permissions.
- Encryption in transit (TLS) and at rest where feasible.
- Regular vulnerability management and patching.
- Logging, monitoring and retention of secure audit logs.
- Secure development practices and periodic security testing.

Data Processing Agreement (DPA)

- Backup and disaster recovery procedures.
- Personnel security, training, and least-privilege access.

Sub-processors

Processor may engage sub-processors (e.g., hosting, analytics, email platforms).

Processor will:

- Maintain a current list of sub-processors and provide it to Controller on request.
- Notify Controller of new sub-processors and allow Controller [10] business days to reasonably object; if objection is reasonable and unresolved, Controller may suspend services or terminate for cause.
- Require sub-processors to comply with equivalent contractual obligations.
- Remain liable for breaches by sub-processors to the same extent as for Processor's own acts.

International transfers

Personal data may be transferred or processed outside Canada. Processor will implement safeguards (contractual clauses, encryption, access controls). Controller consents to transfers as necessary to provide the services.

Data subject rights and assistance

Processor will assist Controller to respond to access, rectification, deletion, portability, objection and restriction requests within Controller's prescribed timelines, to the extent possible and as required by law.

Breach notification and cooperation

- Processor will notify Controller without undue delay after becoming aware of a confirmed personal data breach affecting Controller's data.
- Notification will include: nature of breach, categories and approximate number of affected data subjects and records, likely consequences, measures taken and planned remedial actions, and contact details for further information.
- Processor will provide reasonable cooperation and assistance in mitigation, investigation, and regulatory notifications.

Return and deletion

On termination or upon Controller's written request, Processor will, at Controller's choice, return all personal data and copies or securely delete it within a reasonable timeframe unless retention is required by law. Processor will certify deletion on request.

Audit and inspection

Controller may audit Processor's compliance (subject to confidentiality) with reasonable notice and during business hours, or accept third-party audit reports/certifications (e.g.,

Data Processing Agreement (DPA)

SOC 2). Audits must be conducted no more than once per 12 months unless required by law or after a confirmed breach.

Liability

Liability subject to limits in the main agreement. Nothing in this DPA excludes liability for gross negligence, willful misconduct, or liabilities that cannot be limited by applicable law.

Miscellaneous

- Governing law: Ontario, Canada.
- Severability: invalid provisions do not affect others.
- Entire agreement: this DPA and main agreement control processing terms.

Signatures

Controller: _____
Name / Title / Date

Processor (Otuso): _____
Name / Title / Date