WEBACUMEN SOFTWARE DEVELOPMENT AND HOSTING

POPIA Operator Agreement (Data Processing Agreement)

This is the written operator contract that section 21 of POPIA requires between a client (the responsible party) and WebAcumen (the operator) for personal information the client stores on our hosting, email and VPS services. It is published at webacumen.co.za/legal/dpa, linked from the Terms of Service and every hosting and VPS quote, and is accepted with the quote. A signed copy is provided when a client asks for one.

1. Parties and purpose

This agreement is between WebAcumen Software Development and Hosting ("**WebAcumen**" or the "**Operator**"), and the client named in the quote, order or signature block (the "**Client**" or the "**Responsible Party**").

1.1 The Client uses WebAcumen's hosting, email, VPS and related services, and stores or processes personal information on them.

1.2 For that personal information the Client is the responsible party and WebAcumen is the operator, as defined in section 1 of the Protection of Personal Information Act 4 of 2013 ("**POPIA**").

1.3 This agreement is the written contract required by section 21 of POPIA. It forms part of WebAcumen's Terms of Service. If the two conflict on the processing of personal information, this agreement applies.

1.4 WebAcumen's own handling of the Client's contact, billing and account details is covered by our POPIA / Privacy Notice, where WebAcumen is the responsible party. It is not covered here.

2. Definitions

Terms defined in POPIA have the same meaning here. In addition:

- **Client Personal Information**: personal information that the Client, its users or its website visitors store on, send through or process with the Services.
- **Services**: the hosting, email, VPS, backup, domain and related services WebAcumen provides to the Client under its quote or order.
- **Security Compromise**: reasonable grounds to believe that Client Personal Information has been accessed or acquired by an unauthorised person (section 22 of POPIA).

- **Sub-processor**: a third party WebAcumen engages to provide infrastructure or other parts of the Services that may give it access to Client Personal Information.

3. Scope of processing

3.1 WebAcumen processes Client Personal Information only to provide the Services: storing it, serving it, sending and receiving email, making backups, restoring them on request, and keeping the infrastructure secure and available. Schedule 1 describes the processing.

3.2 The Client decides what personal information it collects, why, and for how long. The Client is responsible for having a lawful basis for it and for meeting its own POPIA duties towards data subjects.

3.3 **Self-managed services.** On a self-managed VPS or server, the Client controls the operating system, applications, users, logs and their security. WebAcumen's obligations then cover the infrastructure layer: hardware, hypervisor, network, power, physical security and the backups WebAcumen provides. They do not cover the Client's own configuration.

4. WebAcumen's obligations

WebAcumen will:

1. process Client Personal Information only on the Client's documented instructions, which include this agreement and the Client's use and configuration of the Services, unless the law requires otherwise. In that case WebAcumen tells the Client first, unless the law forbids it;
2. treat Client Personal Information as confidential, and not disclose it unless the Client authorises it or the law requires it (section 20 of POPIA);
3. never sell Client Personal Information, never use it for its own marketing, and never use it for any purpose other than providing the Services;
4. allow access only to staff and contractors who need it to provide the Services and who are bound by confidentiality;
5. not log in to a self-managed server or access Client content unless the Client asks it to, for example in a support request, or an emergency requires it to protect the Services. Any such access is recorded.

5. Security measures

5.1 WebAcumen maintains appropriate, reasonable technical and organisational measures to protect the integrity and confidentiality of Client Personal Information, as section 19 of POPIA requires. Schedule 2 lists the current measures.

5.2 WebAcumen reviews these measures regularly and updates them as risks and safeguards change. It will not reduce the overall level of protection during the term.

5.3 No system is completely secure. The Client is responsible for the security of everything under its own control, including passwords, user accounts, website code, plugins and, on self-managed services, the operating system.

6. Security compromises

6.1 If WebAcumen has reasonable grounds to believe that Client Personal Information has been accessed or acquired by an unauthorised person, it will notify the Client immediately, as section 21(2) of POPIA requires, and in any event within 24 hours of becoming aware of it.

6.2 The notice will include what WebAcumen knows at the time: what happened, when, the systems and kinds of information affected, the steps taken, and a contact person. WebAcumen will update the Client as it learns more.

6.3 WebAcumen will take reasonable steps to contain the compromise and limit its effects. It will give the Client the information it reasonably needs to notify the Information Regulator and data subjects under section 22. The Client, as responsible party, decides on and makes those notifications.

7. Sub-processors

7.1 The Client authorises WebAcumen to use Sub-processors for data-centre, infrastructure, backup and email-delivery services.

7.2 WebAcumen binds every Sub-processor by written contract to data-protection obligations no less protective than those in this agreement. WebAcumen remains responsible to the Client for its Sub-processors' performance.

7.3 WebAcumen keeps a current list of its Sub-processors. Because it is commercially confidential, the list is given to the Client on written request under a confidentiality undertaking.

7.4 WebAcumen will give the Client at least 30 days' notice before adding or replacing a Sub-processor that processes Client Personal Information. If the Client has a reasonable data-protection objection, the parties will discuss it in good faith. If they cannot resolve it, the Client may end the affected Service without a cancellation fee.

8. Data location and transfers abroad

8.1 WebAcumen hosts all Client Personal Information, including backups, in South Africa, on the Teraco Isando campus in Johannesburg. Our managed hosting servers run in the Teraco JB3 data centre, and

their backups are stored in the Teraco JB1 East data centre, a separate building. All backups, including VPS backups, are stored off-site from the server they protect.

8.2 WebAcumen will not move Client Personal Information outside South Africa without the Client's prior written consent. Any transfer it makes will meet section 72 of POPIA.

8.3 Where the Client itself sends information abroad, for example through plugins, third-party APIs or email to foreign recipients, that transfer is the Client's responsibility.

9. Assistance

9.1 If a data subject contacts WebAcumen directly about Client Personal Information, WebAcumen will pass the request to the Client and will not respond itself unless the Client asks it to.

9.2 WebAcumen will give the Client reasonable help to answer data subjects' access, correction and deletion requests, and enquiries from the Information Regulator, as far as the Client cannot do this through its own access to the Services.

9.3 Help that goes beyond what the Services already allow is billed at WebAcumen's standard support rate, unless the request arises from WebAcumen's own breach of this agreement.

10. Return and destruction at the end of the Services

10.1 Before a Service ends, the Client is responsible for exporting its data. On request, WebAcumen provides one full account backup free of charge. Moving the data to another provider is a separate paid service.

10.2 When a Service ends, WebAcumen deletes Client Personal Information as follows:

Data	When it is destroyed
VPS disks	Immediately on termination
Hosting accounts and mailboxes (web, WordPress, email)	Held for up to 180 days after termination so the account can be restored if the Client returns, then destroyed
VPS backups and snapshots	30 days after termination; not recoverable after that

10.3 On written request, WebAcumen confirms in writing that the data has been destroyed.

10.4 WebAcumen may keep information only where the law requires it to. In that case clauses 4 and 5 continue to apply to it.

11. General

11.1 **Information and audits.** On written request, WebAcumen gives the Client the information reasonably needed to show compliance with this agreement. A documentary review is the default. An on-site audit needs reasonable notice, takes place no more than once a year, is at the Client's cost, and is subject to confidentiality and Sub-processor site rules.

11.2 **Liability.** Each party's liability under this agreement is governed by the limitation of liability in the Terms of Service.

11.3 **Term.** This agreement applies for as long as WebAcumen processes Client Personal Information. Clauses 5, 10 and 11 continue after the Services end.

11.4 **Changes.** WebAcumen may update this agreement to reflect changes in law or in the Services. It gives the Client 30 days' notice of material changes, and changes never reduce the Client's protection.

11.5 **Governing law.** The law of the Republic of South Africa governs this agreement.

11.6 **Acceptance.** Accepting a WebAcumen quote, or using the Services after this agreement has been published, is acceptance of this agreement. No signature is needed. Where a Client asks for a signed copy, WebAcumen will sign one on request.

	WebAcumen	Client
Name		
Title		
Signature		
Date		

Schedule 1: Description of processing

Item	Description
Services	Web and WordPress hosting, email hosting, VPS, backups, domains and DNS
Nature of processing	Storage, hosting, transmission, backup, restore on request, security monitoring

Item	Description
Data subjects	The Client's staff, clients, website visitors, email correspondents, and others the Client chooses
Categories of information	Decided by the Client. Typically names, contact details, account and order details, and email content
Special personal information	Only if the Client chooses to store it. The Client is responsible for its lawful basis
Duration	The term of the Services, plus the deletion periods in clause 10

Schedule 2: Security measures

- Encryption in transit (SSL/TLS) on websites, control panels and email, and encryption at rest on storage and backups
- Hashed passwords; role-based access for staff, limited to those who need it
- Isolated hosting accounts; each VPS is a separate virtual machine
- Firewalls, malware scanning and brute-force protection on shared servers
- Automated off-site backups kept for 30 days
- 24/7 infrastructure monitoring
- Data centres with controlled physical access, redundant power and cooling
- Confidentiality obligations on staff and contractors