DATA PROTECTION

Data Processing Agreement

Wayne Conrad Advisory · Version 1.0 · 18 October 2026

Short answer: this agreement applies whenever I process personal data for you during a sprint. It is signed before any client data is shared, and it forms part of the written agreement for your project. It covers instructions, security, sub-processors, breach notice, deletion, audits and international transfers.

1. Parties and roles

1.1 This agreement is between the business named in the signature block ("you", the "Client") and Wayne Conrad Advisory, a division of Poseidon Network Systems CC, South Africa ("I", the "Provider").

1.2 You decide why and how personal data is processed. That makes you the controller (UK GDPR and EU GDPR), the responsible party (POPIA), the business (CCPA) or the organisation that holds the information (Australian Privacy Act). I process personal data on your behalf, as a processor, operator or service provider.

1.3 "Data Protection Laws" means, to the extent they apply: the UK GDPR and Data Protection Act 2018, the EU GDPR, the Protection of Personal Information Act 2013 (POPIA), the California Consumer Privacy Act as amended by the CPRA (CCPA), and the Australian Privacy Act 1988 including the Australian Privacy Principles (APPs). "Personal Data" means the personal information I process for you under the written agreement.

1.4 This agreement forms part of the written agreement and the Terms of Service. If they conflict on data protection, this agreement applies. If the transfer clauses in section 12 conflict with anything else, they apply.

2. What I process and why

2.1 I process Personal Data only to deliver the sprint set out in the written scope: mapping the workflow, building and testing it, handing it over, and fixing defects during the support or tuning window. Schedule 1 describes the subject matter, nature, purpose, data types and people affected.

2.2 The processing lasts from the first time I access your Personal Data until the support or tuning window ends, plus the time needed to delete or return it under section 10.

3. Instructions

3.1 I process Personal Data only on your documented instructions. This agreement and the written scope are your instructions. You can give more in writing, including by email. That includes instructions about transfers, unless the law requires me to act differently. If it does, I tell you before I act, unless the law forbids that.

3.2 If I think an instruction breaks Data Protection Laws, I tell you and may pause that part of the work until we agree.

3.3 I do not decide the purposes or means of processing. I do not use Personal Data for my own purposes, including marketing or training AI models.

4. Confidentiality

4.1 I keep Personal Data confidential. Anyone I authorise to access it is bound by a duty of confidence, and access is limited to what the sprint needs.

5. Security

5.1 I put in place appropriate technical and organisational measures to protect Personal Data, as UK GDPR and EU GDPR Article 32 and POPIA section 19 require. Schedule 2 sets out the minimum.

5.2 I access your systems only through credentials you grant, scoped to the workflow, which you can revoke at any time. I use business or API accounts only, and send tools only the fields a workflow needs.

6. Sub-processors

6.1 You authorise me to use the sub-processors listed in Schedule 3 and the tools named in the written scope for your project. Tools in your own accounts, contracted by you directly (for example your CRM), are your processors, not mine.

6.2 I give you at least 14 days' written notice before I add or replace a sub-processor. You may object in writing on reasonable data protection grounds within that time. If we cannot resolve the objection, you may end the affected work under the termination clause in the written agreement.

6.3 I bind each sub-processor to data protection obligations equivalent to these, and I remain responsible to you for their performance as the law requires.

7. Requests from individuals

7.1 If someone contacts me about their Personal Data, or complains, I pass it to you within 5 working days and do not respond except to say I have done so. I give you reasonable help to answer requests for access, correction, deletion or other rights, and to cooperate with consumer requests under the CCPA.

8. Personal data breach

8.1 I tell you without undue delay, and in any case within 48 hours, after I become aware of a personal data breach affecting your Personal Data. Where POPIA applies, I tell you immediately if I have reasonable grounds to believe an unauthorised person has accessed or acquired it.

8.2 My notice says what happened, which data and roughly how many people are affected, the likely consequences, and what I have done and will do. I help you assess the breach, contain it and meet your own notification duties. You decide whether to notify regulators or individuals.

9. Help with your obligations

9.1 I give you reasonable help with data protection impact assessments, prior consultation with a regulator, and security and breach duties, and the information you need to show that I comply with this agreement. Help that is part of the sprint is free. Other help is quoted in writing before I start.

10. End of the project

10.1 When the support or tuning window ends, or earlier if you ask in writing, I remove my access. At your choice I return or delete the Personal Data and project copies, and I confirm in writing if you ask.

10.2 The exception is backups and records I am legally required to keep. I keep those protected and use them for no other purpose.

11. Audits and information

11.1 I give you the information needed to show that I comply with this agreement. You, or an auditor you appoint, may audit me with at least 14 days' written notice, during business hours, not more than once in 12 months unless there has been a breach or a regulator requires it. We start with documents and a call. You bear the cost of the audit unless it finds material non-compliance. Auditors keep what they learn confidential.

12. International transfers

12.1 I am based in South Africa. The sub-processors listed in Schedule 3 process data in the United States. Tools you name in the written scope may process data elsewhere, and I state where in that scope. Personal Data is transferred only under a valid transfer mechanism where the law requires one.

12.2 **EU and EEA.** Where the EU GDPR applies and a transfer to me needs a safeguard, the Standard Contractual Clauses in Commission Implementing Decision (EU) 2021/914, Module Two (controller to processor), are incorporated by reference. You are the data exporter and I am the data importer. Clause 7 (docking) applies. Clause 9(a) uses Option 2 (general authorisation) with the 14-day notice in section 6.2. The optional wording in Clause 11 is not used. Clause 17 uses Option 1 and Clause 18(b) names the courts of the EU Member State where you are established, or Ireland if you have none. Annex I is completed from Schedule 1 and the signature block, Annex II from Schedule 2 and Annex III from Schedule 3.

12.3 **United Kingdom.** Where the UK GDPR applies and a transfer to me needs a safeguard, the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner, in the version in force on the date of signature, is incorporated by reference. Table 1 is completed from the signature block, Table 2 from section 12.2, Table 3 from Schedules 1 to 3. In Table 4, the exporter may end the Addendum.

12.4 **South Africa.** I transfer Personal Data outside South Africa only as you instruct, in line with POPIA section 72, and only to sub-processors bound to protections substantially similar to these.

12.5 **Australia.** Where you disclose Personal Data to me or to my overseas sub-processors under the Privacy Act, I handle it in line with the APPs other than APP 1. Schedule 1 sets out the types of information and the purpose. Section 6 covers subcontractors, section 7 covers complaints and section 8 covers breach notice.

13. United States state privacy laws

13.1 Where the CCPA applies, I am your service provider. I process Personal Data only for the business purposes in Schedule 1. I do not sell or share it. I do not retain, use or disclose it for any other purpose, or outside my direct business relationship with you. I do not combine it with personal information from other sources, except as the CCPA allows.

13.2 I comply with the CCPA and give the same level of privacy protection it requires of you. I tell you within 5 business days if I can no longer meet these obligations. You may take reasonable steps, including under section 11, to confirm that I use the data consistently with your CCPA duties, and on notice I will stop and remedy any unauthorised use. I bind my sub-processors to the same terms and tell you about them under section 6. I certify that I understand these restrictions and will comply with them.

14. Liability

14.1 The limit of liability in section 7 of the Terms of Service applies to this agreement. Nothing in this agreement limits liability that cannot lawfully be limited, or the rights of the people whose data is processed.

15. Term, changes and law

15.1 This agreement starts when you sign it and ends when I have deleted or returned the Personal Data under section 10. Sections 4, 8, 10, 14 and this section survive.

15.2 Changes must be in writing and signed by both of us. If the law changes, we agree any needed amendments in good faith. I may publish a newer version of this template, but the version you signed applies to your project.

15.3 The governing law and how disputes are handled are those in the written agreement, except that the SCCs and the UK Addendum are governed as stated in section 12.

Schedule 1: The processing

Subject matter	Delivering the AI workflow sprint described in the written scope.
Duration	From first access until the support or tuning window ends, then deletion or return under section 10.
Nature and purpose	Mapping, building, testing, handing over and supporting a workflow inside your own accounts. Business purposes for the CCPA: providing those services to you.
Types of Personal Data	As stated in the written scope. Typically: names, business email addresses, phone numbers and job titles; enquiry and message content; project, invoice and payment-status records. No special category, children's or financial account data unless the written scope says so.
People affected	Your staff, clients, prospects and suppliers.
Frequency	Continuous during the build and support window, as the workflow runs.
Provider contact for data protection	privacy@wayneconrad.com, +27 21 300 8278

Schedule 2: Security measures

- Access to your systems only through credentials you grant, scoped to the workflow and revocable by you at any time.
- Multi-factor authentication on the accounts I use to reach your systems, where the service offers it.
- Business or API accounts only for AI and automation tools. These do not train on your content by default.
- Only the fields a workflow needs are sent to a tool.
- Credentials kept in a password manager, never in documents or messages.

- Work devices with disk encryption, screen locks and current security updates. No personal data on removable media.
- Encrypted connections for all data in transit.
- Access removed and project copies deleted when the support or tuning window ends, or earlier if you ask.

Schedule 3: Sub-processors

The sub-processors I use for this website, its diagnostic and its Ask a Question page (Netlify, Anthropic, Resend, HubSpot, and Google Analytics and Tag Manager) are listed on the Trust page. All five process data in the United States. For your project, the tools that may handle your data are named in the written scope before any data is shared. Section 6.2 applies to any change.

Signature

Client (legal name)	_____
Registered address	_____
Signatory and title	_____
Signature and date	_____
Provider	Wayne Conrad Advisory, a division of Poseidon Network Systems CC, South Africa
Registration number and address	_____
Signatory	Wayne Conrad
Signature and date	_____