

How we handle your data

We build software that runs on accounts in your name. Here is what happens to your data while we build it and at handover. Your services agreement carries the binding terms.

Where it lives	In Australia, in accounts you own from day one
Who can see it	The people named on your project, each with their own login and multi factor sign in
What we build with	Code and made up test data. Never your real records
Backups	Run by your provider in Australia. We test a restore before go live
If something goes wrong	We tell you within 48 hours of becoming aware
At the end	Everything handed over, our access removed and confirmed in writing

Where it lives

Your product, its database, its files and its backups sit in accounts opened in your name, in Australian regions. We join those accounts as members and you can remove us at any time. We do not run a shared platform and we do not keep your data on our own systems.

Some services have no Australian region, most often the ones that deliver email and text messages. Where a project needs one, we name the provider and where it runs before the build starts, and you decide.

Who can see it

Only the people on your project, named in the statement of work. Each has their own login with multi factor sign in. We never share logins, between ourselves or with you. Anyone who works on your project signs confidentiality and intellectual property terms with us before they start, so their work passes to you with the rest once it is paid for.

What we build with

We build and test with code and made up data. Our tools, including AI coding assistants, never see your real customer records. If a fault can only be found in real data, we look at it inside your accounts, with your permission, and copy nothing out.

If your product has AI features, they run on your accounts, on your documents, and we name the provider and its region in the statement of work.

What we hold on our side

Emails and documents you send us sit in our Microsoft 365 tenant, never in personal accounts. Credentials for your accounts sit in an encrypted password manager, one folder per client, and move

into your own vault at handover. Our computers are encrypted, locked when idle and signed in with multi factor sign in.

Backups and restore

Your database is backed up by its provider in the same Australian region. Before each go live we restore a backup to prove it works and record the date in the handover pack. After go live you run the product, so backups are yours from then on.

If something goes wrong

If we become aware of a security incident affecting your data or your product, we tell you without delay and within 48 hours, help you respond, and help with any notice the Notifiable Data Breaches scheme requires.

At the end

At each go live you get the handover pack: the code, the account list, the credentials in your vault, the runbook and the changelog. When the agreement ends, the final pack follows within 10 working days. We remove our access on your instruction, confirm it in writing, and delete any copies of your information we still hold within 30 days. We keep only our own business records, such as invoices, for as long as the law requires.

The law

We handle personal information as if the Privacy Act 1988 and the Australian Privacy Principles apply to us in full. You give your customers the privacy notices and collect the consents your product needs. We help you write them.

Questions to support@lumanworth.com.