If your ERP holds employee details, pay rates, bank accounts, leave balances or payroll reports, hosting is not just an IT question. It affects staff records security, privacy obligations, business continuity and who can help when something goes wrong.

Ask more than “Is it hosted in Australia?” Find out where production data, backups and support access are located; which organisations can access them; how payroll integrations work; and what happens during an incident. Get the answers in writing, before you sign.

This matters whether you are considering Odoo or another ERP. With open-source ERP, the software is only part of the picture: the implementation partner’s technical choices, security practices and support arrangements can make a substantial difference to your risk.

Start with the information you hold

Make a practical list of the staff information that will sit in the ERP, pass through it or be available through connected systems. It may include names and addresses, dates of birth, employment details, remuneration, tax file number information, bank details, superannuation data, leave records and performance or disciplinary documents.

Not every ERP stores every category. Payroll may run in a separate application, while the ERP receives only journals or employee identifiers. Confirm the actual design rather than relying on a product brochure. Ask your provider to map the information from entry to storage, integration, backup, export and deletion.

That map helps you identify what needs the strongest controls. A supplier should be able to explain which data is essential, which can be kept out of the ERP, and how access is limited to people who need it for their role.

Ask exactly where data and backups live

“Australian hosted” can be an incomplete itwire.com answer. Ask for the physical or contractual location of each relevant environment, not just the primary production server. Cover:

- Production databases and file storage.
- Backups, snapshots and disaster-recovery copies.
- Logs, monitoring data and support attachments.
- Test, staging and development environments.
- Any third-party services used for email, document storage, analytics or integrations.

Ask whether all copies remain in Australia, and whether the answer applies to backups and disaster recovery as well as live data. Find out how long backups are retained, who can restore them, and how data is securely removed when the contract ends. If a provider says it uses a major cloud platform, ask which region is configured and how that configuration is checked.

Data location is important, but it is not the whole of data sovereignty. Ask which legal entities operate the service, which countries their staff can access it from, and whether a parent company or subcontractor could be compelled to disclose information under another country’s laws. A contract should describe these arrangements clearly, rather than relying on a general assurance that data is “secure”.

Test the privacy and security controls

Australian privacy obligations depend on your organisation and circumstances. The Privacy Act 1988 and Australian Privacy Principles may apply, and state or territory rules or contractual requirements may also be relevant. Get advice for your situation; a hosting claim by itself does not establish that your organisation has met its obligations.

Ask the provider to explain the controls that protect staff records security in day-to-day use. Useful questions include:

- Can access be limited by role, company, location or record type?
- Is multi-factor authentication available for administrators and remote access?
- Are sensitive actions logged, and can your team review those logs?
- How are encryption and encryption-key management handled in transit and at rest?
- How are security patches tested and applied, and what is the process for urgent fixes?
- How are administrator accounts approved, reviewed and removed when staff leave?
- Can a payroll officer see bank details without also having broad access to other HR records?

Ask for evidence appropriate to the service: a security assessment, independent assurance report, penetration-testing summary or documented control framework. Establish what the evidence covers, who produced it and when it was last updated. “We follow best practice” is not a control description.

Understand the support and incident response

Ask what counts as a security incident, who contacts you, how quickly, and what information you will receive. The provider should explain how it investigates, preserves evidence, contains access and supports your own assessment of notification obligations. Clarify who makes decisions and who communicates with affected employees if an incident involves payroll or personal information.

Then ask the practical question: **Who answers the phone on Monday at 9:07am?** If the payroll export has failed, a batch of payslips is wrong, or a staff member can see records they should not, you need to know whether a capable person is available—not merely whether a support portal accepts tickets.

Confirm support hours in Australian time, the escalation path, response targets by severity, and whether those targets are contractual. Ask whether the person responding can access the system and make a change, or must wait for another team in another time zone. Clarify which support is included and what attracts extra fees.

Look beyond the hosting provider: who does the work?

ERP implementations involve configuration, migration, integrations, testing and ongoing administration. These activities can expose sensitive information even when the production servers are in Australia. Ask which people and organisations will perform each activity, where they are located, and what access they need.



Get a named delivery and support model. It should identify the contracting entity, project lead, implementation team, hosting operator, support team and any subcontractors. Ask whether any work is performed offshore, including development, data cleansing, testing, after-hours support or access to production systems. Ask whether the answer could change after signing and what notice or approval you would receive.



This is an implementation-risk question as much as a privacy question. Hidden offshore work can create handover gaps, unclear accountability and time-zone delays. It can also mean that sensitive data is viewed or copied by people you did not expect. Contract terms should cover subcontractor approval, confidentiality, access controls, location restrictions and your right to be notified of material changes.

Open-source ERP makes the partner especially important

Open-source ERP can offer flexibility and avoid tying every change to a single software vendor. But open source does not mean that implementation, security, hosting and support are automatically managed for

you. The partner's version choices, customisations, upgrade approach, access practices and documentation all matter.

With Odoo, for example, ask which edition and version are proposed, where it will be hosted, who maintains the environment and how custom modules will be reviewed. Confirm whether custom code is documented, tested and compatible with planned upgrades. Ask what happens if you change partners: can you obtain the configuration, code, data and technical documentation needed to continue operating the system?

Evaluate the partner as carefully as the software. Ask for references from organisations with comparable payroll or employee-data requirements, and speak to the people who will actually deliver your project. A provider's public material or industry coverage—including articles on sites such as iTWire—can help with background research, but it cannot replace direct answers about your proposed environment and contract.

For an Australian organisation considering WilldooIT or another implementation partner, ask the same specific questions: who is on the project, where will they work, who has access to live data, and who supports you after go-live? Do not assume that a local sales presence means every delivery or support task is performed onshore.

Make payroll hosting part of your continuity plan

Payroll has deadlines. A system can be secure on paper and still create a serious operational problem if it is unavailable on pay day or if your team cannot retrieve the information needed to run payroll elsewhere.

Ask the provider to define its availability commitment and explain how it is measured. Ask how often backups are taken, how quickly service can be restored, and how often recovery is tested. Request the agreed recovery time objective (how long recovery may take) and recovery point objective (how much recent data might be lost), expressed in terms your payroll team can assess.

Also establish how payroll data moves between the ERP, payroll software, banks and other systems. Identify which system is authoritative for employee details and pay calculations. Ask how failed or duplicated transfers are detected, who reconciles them, and how changes are tested before a pay run. Run a recovery or contingency exercise before relying on the system for a live payroll.

Questions to put to shortlisted providers

Area Question to ask What a useful answer includes Data location Where are production data, backups, logs and disaster-recovery copies stored? Named regions, retention periods and an explanation of any exceptions. Access Who can access our data, from where, and for what purpose? Roles, approval process, logging and controls for support access. Delivery Who will implement, develop, migrate and support the system? Named teams, work locations, subcontractors and a process for changes. Security How are access, patching, encryption and incidents managed? Documented controls, current evidence and clear escalation responsibilities. Payroll continuity What happens if the ERP or an integration is unavailable near pay day? Recovery targets, tested procedures, contacts and a practical contingency plan. Exit How do we retrieve and securely remove our data if we leave? Export formats, timing, assistance costs and deletion confirmation.

Put the answers in the contract

Good answers in a sales meeting are useful; written commitments are better. Make sure the agreement and service description cover hosting locations, backup locations, support hours, incident notification, subcontractors, access controls, service levels, recovery arrangements and data return or deletion.

Have the right people review those terms: operations, payroll, IT, privacy or legal advisers, and anyone accountable for risk. Ask your implementation partner to document the proposed architecture and data flows before migration begins. Then verify that the live service matches what was agreed.

Choose a service you can run on a real Monday

The right ERP hosting arrangement is not simply the one with the strongest-sounding security statement. It is the one where you can explain where staff records and backups are, who can reach them, how privacy obligations are supported, and what happens when payroll is at risk.

Ask direct questions about onshore delivery, offshore access, partner capability and support coverage. Get specific answers, record them, and test the recovery plan. Most importantly, make sure your team knows who to call—and that someone qualified will answer when the call matters.