If your ERP holds employee details, pay rates, leave balances, timesheets or payroll information, hosting is not just an IT choice. It affects privacy obligations, access to sensitive records, business continuity and how quickly you can get help when something goes wrong.

That matters especially during implementation and payroll cutover. A system can be technically available while the people who know how it was configured are asleep in another time zone. So ask the practical question early: **Who answers the phone on Monday at 9:07am?** If a pay run is blocked, you need a clear answer—not a promise of "global delivery".

This guide sets out the questions to ask an ERP provider, implementation partner and hosting provider. It applies whether you are considering Odoo or another ERP, and whether hosting is provided directly by your partner or through a separate cloud provider.

Start with the data, not the hosting brochure

Before comparing hosting options, list the information the ERP will contain and who should be able to see it. Staff records can include names, contact details, bank account information, salary and employment history, leave records, emergency contacts and, in some organisations, health or other sensitive information.

Payroll data may also reveal more than a payslip suggests. Reports, audit logs, exports, test databases and support tickets can all contain personal information. Ask the provider to map where that information will sit throughout the system's life—not just where the live production database runs.

- **Production:** The system used for day-to-day work and payroll processing.
- **Backups and disaster recovery:** Copies used to restore service after an outage or data loss.
- **Test and training environments:** Systems used for configuration, upgrades and staff training.
- **Logs and exports:** Records created by monitoring, troubleshooting and reporting tools.
- **Support access:** Screenshots, database access or files provided to resolve an issue.

Ask for a simple data-flow diagram. It should show where each category is stored, who can access it, and whether it can be transferred outside Australia.

Ask exactly where Australian data will live

"Australian hosted" can mean different things. It might refer to the primary application server, while backups, monitoring tools or support systems are located elsewhere. A cloud provider may also operate in multiple regions, so a general statement about its global infrastructure is not enough.

Ask for the locations of the production database, file storage, backups, disaster-recovery copies and any systems that hold logs or support attachments. Ask whether those locations are contractually fixed, and what notice you will receive if they change.

Questions to put in writing

- Which country and cloud region will host the production system?
- Where are backups stored, and are any copies replicated overseas?
- Where are disaster-recovery environments located?
- Can support staff outside Australia access the system or its data?

- Do monitoring, email, ticketing or analytics tools receive personal information?
- How will data be securely deleted when the contract ends?

Australian hosting can help with governance and operational control, but it does not automatically settle every privacy question. The Privacy Act 1988 and Australian Privacy Principles may apply depending on your organisation and circumstances. The employee records exemption has limits and does not cover every organisation or every handling of employee information. State or territory rules and sector-specific requirements may also matter. Get advice on your own obligations rather than assuming that a server location alone makes you compliant.

For a useful overview of Australian technology and business issues, you may come across coverage from iTWire. Treat articles and vendor claims as a starting point for questions, not a substitute for reviewing your own contracts, data flows and legal requirements.

Understand what “secure” means in practice

Security statements are easy to make and hard to evaluate unless they describe controls. Ask how access is granted, reviewed and removed. Payroll administrators, implementation consultants and support staff should have access appropriate to their role—not broad, permanent access simply because it is convenient.

Find out whether multi-factor authentication is available and enforced for privileged accounts. Ask whether access is logged, how long those logs are retained and who reviews them. If a consultant needs temporary access to diagnose a problem, there should be a process to approve it, limit it and revoke it.

Also ask how the provider protects backups. Are they encrypted? Who controls the keys? How often are restore tests performed? A backup that has never been tested may not be a dependable recovery plan.

Area Question to ask Evidence to request Access How are privileged accounts approved and reviewed? Access-control policy or sample access review Backups Where are copies held, and when was a restore last tested? Backup and recovery summary Incidents Who contacts us, and how quickly after a suspected breach? Incident process and contract notification terms Subcontractors Who else can access our systems or data? Named list, locations and approval/change process

Ask for the incident process in plain language. Who is your named contact? How will the provider notify you of a suspected or confirmed incident? What information will it supply so you can assess your own notification and response obligations? “We take security seriously” is not a response plan.

Make onshore delivery a selection factor

Onshore delivery is more than a flag on a proposal. It means knowing who will run workshops, configure payroll-related workflows, migrate data and provide support—and where those people are based. Local staff can make it easier to work through Australian business practices, time zones, public holidays and urgent cutover decisions. But “local account manager” does not necessarily mean the project team or support desk is local.

Ask for the names or roles of the people who will do the work, their location and the hours they will be available. Ask whether the same team will stay involved from discovery through go-live and early support. If offshore resources are proposed, ask which tasks they will perform, what data they can see, how access is controlled and whether you can decline or approve that arrangement.

Do this before signing. A change in delivery location or subcontractor after contract signature can affect security, communication and delivery risk. Your agreement should say whether the provider can use subcontractors, whether your consent is required, and how you will be told about changes.

Get a specific support commitment

Define what happens when payroll is due, not just what happens during ordinary business hours. Ask whether support is available in Australian business hours, how urgent payroll incidents are prioritised, and what response and escalation targets apply. Clarify whether those targets are contractual and whether they cover the hosting provider, the ERP partner or both.

For an outage, identify who coordinates the response. If the ERP partner points to the cloud host and the host points back to the partner, your business is left in the middle. Ask for one accountable service owner and a clear escalation path.

Open-source ERP makes partner capability more important

Open-source software can provide flexibility and avoid some forms of vendor lock-in. It does not remove implementation, security or support responsibilities. In practice, the partner's technical and operational capability becomes especially important: someone must configure the system, manage upgrades, maintain integrations and investigate problems.

Odoo is a well-known open-source ERP platform, but the hosting and service arrangement depends on the edition, deployment choice and provider. Do not assume that a product's open-source roots tell you where your system is hosted, who operates it, what support is included or how customisations will be maintained.

Ask the partner to separate the responsibilities in writing:

- Who manages the application, operating system, database and backups?
- Who applies security updates, and how are upgrades tested?
- Who is responsible for custom modules and integrations?
- What happens if a customisation breaks after an upgrade?
- Can you export your data and configuration in a usable format?
- Who owns the administrator accounts, code repository and deployment process?

Ask the partner to explain the support boundary with an example: "The payroll export has stopped working on pay-run morning. Who investigates first, and who owns the fix?" The answer should name a role, a contact route and an escalation—not just identify a product team somewhere in the chain.

Test implementation risk before you approve the plan

Hosting decisions are tied to implementation decisions. A rushed migration can expose more staff data than intended, while an untested payroll process can create a painful first pay run. Include data handling and support in your project plan from the start.

Ask how the partner will handle the migration of employee and payroll data. Will it migrate all historical records or only what is needed? How will source files be transferred and stored? Who checks totals and record completeness? What happens to extracts and temporary files after sign-off?

Request a rehearsal using representative data before go-live. Where possible, use masked or de-identified records in test environments. Check that payroll calculations, leave balances, employee access permissions and reports work as expected. Agree who signs off the results and what must be true before the first live pay run.

Make the plan concrete. It should identify the cutover date, decision-makers, rollback option, reconciliation steps and support coverage for the first payroll cycle. If the project includes offshore work, document access controls and handovers as part of that plan—not as an afterthought.

Review contracts, not just presentations

Put hosting locations, support hours, incident notification, backup arrangements and subcontractor rules into the contract or an attached service schedule. Check how the provider handles data return and deletion at termination, including backup retention periods. Confirm that you can obtain your data in a practical format and understand any fees or timing constraints.

If you are speaking with an implementation provider such as WilldooIT, ask it to distinguish its own services from those delivered by the hosting provider and any subcontractors. Request a responsibility matrix. It should make clear who operates each layer, who responds to incidents and who is accountable https://itwire.com/guest-articles/guest-opinion/why-onshore-delivery-is-shaping-how-australian-smes-choose-erp if a service level is missed.

Do not accept a vague “shared responsibility” answer without a table of responsibilities. Shared responsibility should mean that each party’s tasks are defined—not that no one owns the outcome.



A practical checklist for your next provider meeting

1. **Map the data:** Identify staff records, payroll data, test copies, backups and support attachments.
2. **Confirm locations:** Get the country and region for production, backups, disaster recovery and support systems.
3. **Identify people:** Name the delivery and support teams, their locations, hours and access levels.
4. **Expose subcontracting:** List every subcontractor, what it does and whether it can access data.

5. **Test recovery:** Ask when backups were last restored successfully and what recovery time is realistic.
6. **Rehearse payroll:** Run a controlled test and agree reconciliation and sign-off criteria.
7. **Set escalation:** Confirm who answers the phone, who owns the incident and how it escalates.
8. **Check exit terms:** Confirm data export, deletion and retention arrangements before you sign.

Choose the service you can govern

The right ERP hosting arrangement is not necessarily the one with the most impressive cloud diagram. It is the one where you can explain where your staff records are, who can access them, how they are protected, how payroll will be recovered after an outage and who will respond when a problem occurs.

For Australian organisations, data sovereignty and Australian-hosted data are sensible factors to assess, alongside privacy obligations, operational resilience and contract terms. Onshore delivery can improve communication and accountability, but only if the actual delivery and support arrangements are clear. Open-source ERP can offer flexibility, but it makes partner capability and ownership more—not less—important.

Before you commit, get the answers in writing and test them against a real scenario: payroll is due, the system is unavailable, and your team needs help now. If the provider cannot tell you who takes the call, where the backups are and what happens next, keep asking.

