

● YOUR INFORMATION

Privacy Policy

We are a small Australian telco, so we only collect the information we genuinely need to connect you, bill you and support you — and we look after it properly. This policy explains what we collect, why we collect it, who we share it with, where it is kept, and how you can see it, correct it or complain.

● SCOPE

01 · About this policy

This policy applies to Pear Australia Pty Ltd (ABN 94 624 986 554), 25 Gordonian Grove, Baulkham Hills NSW 2153. In this policy, “we”, “us” and “our” mean Pear, and “you” and “your” mean the person whose personal information we hold.

We provide voice, data and internet services, and AI services for businesses and medical practices. This policy covers every way you deal with us — on the phone, by email, through our website, in person, through a dealer or partner, and through our AI services.

It covers the personal information we hold about:

- Customers — current, former and prospective — including the nominated contacts on a business account.
- People connected to an account: authorised representatives, secondary account holders, guarantors, and the holder of a card used to pay an account.
- People who use a service we provide to someone else — for example a patient who calls a medical practice that uses Aria.
- Suppliers, partners, contractors and their staff.
- Our employees and people who apply to work with us.

It sits alongside our Privacy Collection Statement, our Credit Reporting Policy, our Complaint Handling Policy and your Standard Form of Agreement. Where a service has its own collection statement, that statement gives you the detail for that service and this policy gives you the whole picture.

● LAW

02 · The privacy laws we follow

We are bound by the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs) set out in it. The APPs set the minimum standards for collecting, using, disclosing and handling personal information in any form, on paper or electronically. You can read them at oaic.gov.au.

As a telco, other laws apply to us as well:

- The Telecommunications Act 1997 (Cth), which places its own confidentiality obligations on carriage service providers and sets out the narrow circumstances in which we may disclose information about your service.
- The Telecommunications (Interception and Access) Act 1979 (Cth), which governs disclosure to law enforcement and national security agencies.
- The Do Not Call Register Act 2006 (Cth) and the Spam Act 2003 (Cth), which govern our marketing calls, emails and messages.
- The Health Records and Information Privacy Act 2002 (NSW) and equivalent state and territory health privacy laws, where we handle health information — for example through Aria for medical practices.

Two definitions matter throughout this policy:

- Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable — whether or not it is true, and whether or not it is written down. It includes sensitive information.
- Sensitive information means personal information about your racial or ethnic origin, political opinions or memberships, religious beliefs or affiliations, philosophical beliefs, professional or trade association or trade union memberships, sexual orientation or practices, or criminal record. It also includes health information, genetic information, and biometric information used for automated verification or identification and biometric templates.

We only collect sensitive information where you have consented, or where the law requires or allows us to collect it without consent.

● COLLECT

03 · What we collect

How much we collect depends on what you are asking us to do. Someone asking a general question gives us very little; someone opening a business account on credit gives us more. We aim to collect only what we actually need.

- Identity and contact details — name, date of birth, address, email address and phone numbers. For a business account, the name, position, work contact details and date of birth of the nominated contact.
- Proof of identity — driver licence, passport or other government identifier, so we can be sure we are dealing with the right person and that our records are accurate.
- Financial and credit information — bank account or card details, payment history, and where you apply for a service on credit, credit history and information about your financial position. Our Credit Reporting Policy explains how we handle credit information.
- Occupancy and status documents — where we need them, a tenancy agreement, a rates or utility notice, or a marriage, name-change or death certificate, usually when a service is being connected, transferred or closed.
- Service and usage information — the numbers and services on your account, call and data usage records, network and device information, and the information we must record to provide and bill the service.
- Public number customer details for the Integrated Public Number Database (IPND) — see section on our telecommunications obligations.
- Support and complaint records — your contact with us, call recordings and notes, faults, complaints and their outcomes.
- Website information — IP address, browser and device information, and pages visited.
- Employment information — for our own staff and job applicants, and for people whose employment details are relevant to a credit assessment.

We do not collect your personal information from marketing lists, data brokers or data aggregation services, and we do not buy databases of prospective customers.

● HEALTH

04 · Health information and our AI services

Some of our services — including Aria, our AI team member for medical practices — operate inside a practice's phone system and, where the practice enables it, connect to its practice management software. In that arrangement the practice is responsible for the patient record; we handle the information on the practice's behalf and under a written agreement with it.

Where a practice uses those services, we may handle:

- Caller details and the reason for the call, so the call can be answered, triaged or routed.
- Appointment and booking details, where appointment functions are enabled.
- Limited clinical information the practice chooses to make available, only where the practice has enabled it and only to the extent needed to deliver the service.

- Voice recordings and transcripts of calls, held securely and kept only as long as we need them to deliver the service or as the law requires.

We do not use personal information, sensitive information or health information to train AI models unless you have expressly consented. We may use de-identified information — with every identifier removed, so it cannot be traced back to a person — to check quality and improve our services. If you would rather we did not use your information even in de-identified form, email hello@peartelco.com.au and we will honour that; it will not affect the service you receive.

If you would prefer a call not to be recorded, say so during the call or contact our Privacy Officer. Some features may not work without a recording, and we will tell you if that is the case.

● WHY

05 · Why we collect it

We collect personal information so that we can:

- Confirm who you are and decide whether we can supply the service you have asked for.
- Connect, provision, change, move and disconnect services.
- Bill you, take payment, and manage credit and collections.
- Support you — answer questions, fix faults and handle complaints.
- Keep you informed about your service, including outages, changes and notices we are required to send.
- Tell existing customers about our other products and services, subject to the marketing section below.
- Improve our services, train our staff and check the quality of our work.
- Meet our legal obligations, including our obligations under telecommunications, tax and record-keeping law.

If you do not give us the information we need, we may not be able to supply or keep supplying the service, and in some cases the law simply does not allow us to proceed. We will always tell you if that is the situation rather than leave you guessing.

● HOW

06 · How we collect it

Most of the time we collect information directly from you. We may also collect it:

- From someone acting for you — an authorised representative, an advocate, a family member, or the business that holds the account.

- From our dealers, partners and suppliers, and from a previous provider when you transfer a service to us.
- From a credit reporting body, a bank or a referee, where you have applied for a service on credit and consented to those checks.
- From our own network and systems, which record how a service is used.
- From publicly available sources such as the Australian Business Register or a public website.

Where we need to collect information about you from a third party, we will ask for your consent first, unless the law authorises the collection without it. If we collect information about you from someone else without your knowledge, we take reasonable steps to make sure you are told.

You can deal with us anonymously or under a pseudonym for general enquiries — asking what a plan costs, or reporting a fault on a public payphone, for example. Once the enquiry concerns a specific account or service, we have to identify you before we can help, both for your protection and because the law requires it.

Sometimes we receive personal information we did not ask for. If we could not lawfully have collected it, we destroy it or de-identify it, provided it is lawful to do so.

● USE

07 · How we use and disclose it

We use personal information for the purpose we collected it for, and for related purposes you would reasonably expect — for example, using account details collected at sign-up to verify your identity, connect the service, bill it, and fix it when it breaks. For sensitive information we stay within the directly related purpose.

We disclose personal information to others where we need to, including:

- Carriers, wholesale suppliers and network operators whose networks carry your service, so that it can be provisioned, maintained and repaired.
- The operator of the Integrated Public Number Database (IPND), as the law requires.
- Credit reporting bodies, debt collection agents and, where necessary, our lawyers, in line with our Credit Reporting Policy.
- Payment processors and banks, to take and reconcile payments.
- IT, cloud hosting, communications and support providers who help us run our systems.
- Our professional advisers — accountants, lawyers, auditors and insurers.
- The Telecommunications Industry Ombudsman (TIO), where a complaint has been referred to it.

- Emergency service organisations, law enforcement and government agencies, where the law requires or authorises it.
- A buyer or potential buyer of our business, under confidentiality, if we ever sell or transfer part of it.

We do not sell your personal information.

We do not sell, rent or trade personal information, and we do not hand it to other organisations so that they can market to you. Where we share information with a supplier, it is because that supplier does something we need done to deliver your service — and they are contractually required to protect it and to use it only for that purpose.

We may also disclose personal information without your consent where privacy law permits it, including:

- To lessen or prevent a serious threat to life, health or safety.
- For law enforcement, crime prevention or the investigation of unlawful activity.
- To help locate a missing person.
- For use in legal proceedings or dispute resolution.

Other than in the situations described above, we will not disclose your personal information without your consent.

● **TELCO**

08 · Telecommunications obligations, the IPND and law enforcement

Some of our privacy obligations exist only because we are a telco. They are not optional and we cannot contract out of them, so it is worth knowing what they mean for you.

- IPND. The law requires us to give your name, address, service number and other public number customer details to the operator of the Integrated Public Number Database. IPND data is used to produce directories and to help emergency service organisations locate a caller. If your number is unlisted or suppressed, it is flagged that way in the IPND and its use and disclosure is tightly controlled.
- Emergency calls. Information needed to handle a call to 000 may be provided to emergency service organisations.
- Law enforcement. Under the Telecommunications Act 1997 and the Telecommunications (Interception and Access) Act 1979 we may be required to disclose information to law enforcement and national security agencies. Where the law allows us to tell you, we will; often it does not.
- Complaints. We may disclose information about your account to the TIO where you have taken a complaint there.

You are entitled to ask us what we have provided about you to the IPND, and to have it corrected. There is no charge for either — see the section on access and correction.

● MARKETING

09 · Marketing, and how to opt out

Our marketing is modest and it is about our own services. We contact our existing customers about Pear products and services that may be useful to them, and we contact people who have asked us about a service. That is the extent of it.

So that there is no doubt:

- We do not buy marketing lists, databases or data aggregation services.
- We do not market other organisations' products to you, and we do not provide your details to other organisations for their marketing.
- We do not do door-to-door canvassing.
- We never use sensitive information — including health information — for marketing.

We may contact you by email, SMS, phone or post. Every marketing email and message carries an unsubscribe, and you can opt out at any time by emailing hello@peartelco.com.au or calling 1300 007 327. We will action it promptly and we will not ask you to justify it. Our marketing complies with the Spam Act 2003 (Cth) and the Do Not Call Register Act 2006 (Cth).

Opting out of marketing does not stop the messages we have to send you about your own service — bills, outage notices, price change notices and similar. Those keep coming while you are a customer.

● STORAGE

10 · Where your information is stored

Customer data is stored in Australia, on secure, encrypted servers, unless we have agreed something different with you in writing.

Your personal information does not leave Australia, and it is not accessed or processed from outside Australia. Our systems are operated and supported from within Australia, and access to customer information is limited to Pear Australia and people working under our direct authority. We do not use offshore support, offshore processing or offshore call centres. If this position ever changes, we will update this policy and notify customers before the change takes effect, and we will comply with APP 8 (cross-border disclosure of personal information) before any information leaves Australia.

If you have any questions about where your information is kept, email hello@peartelco.com.au and we will tell you.

● SECURITY

11 · How we protect it

We are a small team, which means access to customer information is tightly held and easy to keep track of. We back that up with proper controls.

- Encryption. Information in transit is protected with current industry-standard protocols (HTTPS and TLS). Information at rest is encrypted.
- Access control. Access is role-based, granted only where a person's job requires it, and protected by individual logins and multi-factor authentication. Access to payment and credit information is more restricted again.
- Logging. Access to and changes made in our systems are logged, and we review those logs.
- Identity checks. We verify your identity before discussing an account, and we use that moment to confirm our records about you are correct.
- Staff training. Everyone at Pear is trained on privacy and information security when they start, and is bound by confidentiality obligations.
- Suppliers. Our agreements with suppliers require them to protect personal information, to use it only for the purpose we engaged them for, and to meet standards equivalent to our own.
- Disposal. Paper records are securely destroyed and electronic records are securely deleted or de-identified when we no longer need them.

No system is perfect. If you think your account or your information has been compromised, tell us straight away on 1300 007 327 — we would much rather hear about it early.

● RETENTION

12 · How long we keep it

We keep personal information only for as long as we need it for the purpose we collected it, or for as long as the law requires us to keep it — whichever is longer. After that, it is securely destroyed or de-identified.

- Account, billing and tax records are kept for the period required by tax and record-keeping law after your account closes.
- Credit information is kept and disposed of in line with the Privacy Act and our Credit Reporting Policy.

- Complaint records are kept for at least two years, as the complaint handling rules require.
- Call recordings and transcripts are kept only as long as we need them to deliver the service, resolve a dispute, or meet a legal obligation.
- Identity documents are kept only as long as we need them to satisfy our identity verification obligations.

If you close your account and want to know what we still hold and why, ask us and we will tell you.

● BREACH

13 · If something goes wrong — data breaches

We are covered by the Notifiable Data Breaches scheme in the Privacy Act 1988 (Cth). If personal information we hold is lost, or accessed or disclosed without authorisation, we act on it — and if it is serious, you will hear about it from us.

- **Contain.** As soon as we suspect a breach, we act to contain it and stop any further access or loss.
- **Assess.** We assess a suspected breach within 30 days — usually far sooner — to work out what happened, whose information is involved, and how serious it is.
- **Notify.** Where a breach is likely to result in serious harm, we notify the affected individuals and the Office of the Australian Information Commissioner (OAIC) as quickly as we can. Our notice will explain what happened, what information was involved, what we are doing about it, and the steps you should take.
- **Fix.** We remediate the cause and change what needs changing so it does not happen again, and we record what we learned.

If we ever notify you of a breach

Change the password on any affected account and on any other account where you used the same password; turn on multi-factor authentication where you can; be alert to calls, emails or texts that use the leaked details to sound convincing — including anyone claiming to be from Pear and asking for a password or a code; and contact your bank if payment details were involved. We will never ring you and ask for your password or a one-time code. If you are not sure whether a message is really from us, hang up and call 1300 007 327.

You can report a suspected breach to us at any time at hello@peartelco.com.au. You can also raise it directly with the OAIC at oaic.gov.au or on 1300 363 992.

● AUTOMATED

14 · Automated decisions

The Privacy and Other Legislation Amendment Act 2024 requires us to be upfront about computer programs that make, or substantially help make, decisions about people where the decision could significantly affect their rights or interests. Those requirements apply from December 2026, and we are telling you now.

Pear does not use your personal information in a computer program to make, or to substantially help make, a decision that has a legal or similarly significant effect on you. Decisions that matter — whether we can supply you a service, whether we accept a credit application, whether we suspend or disconnect a service, how we deal with a complaint or a hardship request — are made by a person at Pear.

Where you apply for a service on credit, we may obtain a credit report and score from a credit reporting body, and that score may be produced automatically by that body. We use it as one input. A person at Pear makes the decision, and if we decline your application we will tell you why and how to have it reviewed. Our Credit Reporting Policy sets out your rights in that process.

Our AI services, including Aria, use automated processing to understand a call, triage it, route it and handle bookings. They do not make clinical decisions, they do not decide whether anyone receives care or treatment, and they do not decide anything about your Pear account. Clinical judgement stays with the practice and its staff.

If this ever changes, we will update this policy to say plainly what kinds of decisions are automated and what information is used, before we start.

● ACCESS

15 · Seeing and correcting your information

You have the right to ask for the personal information we hold about you, and to ask us to correct it if it is wrong, out of date, incomplete or misleading. Email hello@peartelco.com.au, call 1300 007 327 or write to us at 25 Gordonia Grove, Baulkham Hills NSW 2153.

- We respond within 30 days. If a request is unusually large or complex, we will tell you before that deadline and agree a timeframe with you.
- Access is generally free. In the rare case where a request is so complex that it involves significant work, we may ask you to cover our reasonable costs — but we will tell you what it will cost before we do any of it, and you can withdraw or narrow the request.
- Correction is always free. We never charge to fix information we hold about you.

- We may need to verify your identity first, and we may ask you for evidence supporting a correction — the correct spelling of a name, for example.
- If we correct information we have already disclosed to someone else, we will tell them about the correction if you ask us to.
- You can ask us for the details we have provided about you to the IPND, and to correct them. There is no charge, and corrections are made in line with IPND requirements.
- Where it is feasible, you can ask us to provide your information in a commonly used, machine-readable format so you can take it to another provider.

There are limited situations where the law lets us refuse access or correction, including where giving it would:

- Prejudice law enforcement or crime prevention.
- Pose a serious threat to the life, health or safety of any person.
- Have an unreasonable impact on another person's privacy.
- Prejudice negotiations or legal proceedings between us.
- Reveal commercially sensitive decision-making information.
- Be unlawful, or be information we are required by law to withhold.

If we refuse, we will tell you in writing why, and how to complain about that decision. If we decline to correct something, you can ask us to attach a statement to the record noting that you disagree, and we will do that.

● ONLINE

16 · Our website, cookies and social media

This policy also applies to information you email us, submit through our website, or send us through a social media page.

When you visit our website we record the IP address of your device and basic browsing information. We use it in aggregate — to understand which pages are useful and how people find us — not to identify individual visitors. Our website may use cookies and similar technologies for the same purpose. You can block or delete cookies in your browser; parts of the site may then not work as well.

Our website links to other websites. We are not responsible for how those sites handle your information — read their privacy policies before giving them anything. The same goes for social media platforms: anything you post publicly on a social platform is governed by that platform's terms, not ours.

● COMPLAINTS

17 · If you have a privacy complaint

If you think we have mishandled your personal information, tell us and we will look into it. It costs nothing to complain and it will not affect your service.

Contact our Privacy Officer:

- Email — hello@peartelco.com.au.
- Phone — 1300 007 327.
- Post — The Privacy Officer, Pear Australia Pty Ltd, 25 Gordonia Grove, Baulkham Hills NSW 2153.

We will acknowledge your complaint promptly, investigate it, and tell you the outcome in writing within 30 days. If it turns out that someone other than Pear has caused the problem, we will take it up with them as well. If we got it wrong, we will say so, fix it, and tell you what we have changed.

If you are not satisfied with our answer, or you have not heard from us within 30 days, you can take your complaint to the Office of the Australian Information Commissioner. Complaints to the OAIC must be in writing. Visit oaic.gov.au or call 1300 363 992.

For complaints that are not about privacy — a bill, a fault, a service problem — see our Complaint Handling Policy. Those complaints can be escalated to the Telecommunications Industry Ombudsman on 1800 062 058 or at tio.com.au.

● CHANGES

18 · Changes to this policy

We review this policy at least once a year, and whenever our practices or the law change. The current version is always available on our website, and we will tell you about significant changes by email or a prominent notice on the site.

If you would like this policy in another format — large print, or a plain-language summary — ask our Privacy Officer and we will provide it. If English is not your first language, you can reach us through TIS National on 131 450, and if you are deaf or have a hearing or speech impairment you can reach us through the National Relay Service.

● TALK TO US

Your information. Ask us anything about it.

Email hello@peartelco.com.au or call 1300 007 327 and ask what we hold, why we hold it, or to have it corrected. There is no charge, and no need to explain why you want to know.