Privacy Policy

Enpro Labs - Zoho Marketplace Extensions

Last updated: 16 October 2026

1. About this Policy

This Privacy Policy explains how Enpro Labs (**ABN 57 230 933 932** , "**Enpro Labs**", "**we**", "**us**", "**our**") handles personal information in connection with the software extensions we publish for Zoho products, including extensions listed on the Zoho Marketplace (each an "**Extension**" and together the "**Extensions**").

This Policy applies to every Extension we publish. The Extensions covered by this Policy are listed in **Schedule 1**. Where a particular Extension handles information differently from the general position described in this Policy, that difference is recorded against that Extension in Schedule 1, and Schedule 1 prevails for that Extension.

2. What this Policy does not cover

This Policy covers only the Extensions and our own systems. It does not

cover:

A) **The Zoho platform.** Zoho CRM and other Zoho products are operated by Zoho Corporation Pty Ltd and its affiliates ("**Zoho**") under Zoho's own privacy policy. The data held in your Zoho organisation is held by Zoho on your behalf, not by us.

B) **Zoho Marketplace purchases.** Where an Extension is paid, any purchase, billing, payment-card, invoicing or tax information you provide is collected and handled by Zoho under Zoho's privacy policy, not by us. See clause 4.1(d).

C) **Third-party data sources.** Some Extensions retrieve data from third-party or government data sources on your instruction, such as the Australian Business Register ("**ABR**"), which is operated by the Australian Taxation Office. Those sources are operated by their respective operators under their own terms and privacy policies.

D) **Your own handling of data.** You remain responsible for your own compliance obligations in respect of the personal information you collect, hold, use and

disclose in your Zoho organisation, including information retrieved into your Zoho organisation using an Extension. See Clause 12.

3. Our approach to Australian privacy law

We handle personal information in accordance with the *Privacy Act 1988* (Cth) ("**Privacy Act**") and the thirteen Australian Privacy Principles ("**APPs**") in Schedule 1 to that Act. We are a small Australian business. Depending on our annual turnover and activities from time to time, we may fall within the "small business operator" exemption in section 6D of the Privacy Act, and so may not be an "APP entity" required by law to comply with the APPs. Where that is the case, we nevertheless adopt the APPs as our operating standard and apply this Policy as though the APPs bound us.

One of the circumstances in which that exemption does not apply is where a business discloses personal information about an individual for a benefit, service or advantage, or provides a benefit, service or advantage in order to collect personal information about an individual. We do neither of those things, and we will not.

This Policy is our APP 1 privacy policy. It is published at a publicly accessible address and is available free of charge on request.

4. The kinds of information we collect

4.1 Information we do not collect

The Extensions are designed on a principle of data minimisation. In particular, and except where Schedule 1 expressly states otherwise for a specific Extension, we do **not** collect, receive, transmit to ourselves, or store:

A) the content of any record in your Zoho organisation, including the names, addresses, telephone numbers, email addresses, notes, attachments or financial details of your leads, contacts, accounts, customers, employees or other individuals;
B) the content of any search term you enter into an Extension, or the content of any result returned to you by a third-party data source;
C) your Zoho login credentials, passwords, OAuth tokens or multi-factor authentication details; or
D) Payment-card, bank-account or billing information.

Where an Extension queries a third-party data source, the query and the response pass between your Zoho organisation and that data source. They do not pass to us, and we do not log their content.

4.2 Licensing and entitlement information

Where an Extension requires a licence or subscription check, we collect and

hold:

A) the unique identifier of your Zoho organisation;
B) a licence key or secret generated when the Extension is installed in that organisation;
C) the subscription or entitlement status associated with that organisation identifier, including the dates on which the Extension was installed, renewed, suspended or uninstalled; and
D) the name and edition of the Extension installed.

4.3 Diagnostic, error and support logs

Some Extensions record operational logs so that we can detect and diagnose faults and provide technical support. Clause 6 sets out the full list of purposes for which we use them. Where an Extension records such logs, those logs are limited to the minimum information necessary for those purposes, being:

A) The unique identifier of the Zoho organisation in which the Extension was operating, so that we can identify which customer's installation a request relates to;
B) the date and time of the event;
C) the name of the Extension and the Zoho module or operation being processed (for example, "Leads" or "Accounts");
D) The record identifier of the Zoho record being processed, where applicable. A Zoho record identifier is an opaque numeric reference generated by Zoho. It does not itself reveal the content of the record or the identity of any individual, and we do not store the content of the record to which it refers;
E) A description of the event or operation performed, its outcome, its duration, and any error code, error message or stack trace produced; and

F) Technical request metadata such as the internet protocol (IP) address from which a request originated, the browser user-agent string, and the version of the Extension in use.

We do not record the content of your records in these logs. The logs are designed so that field values, record content, search terms and the personal information of any individual whose details are held in your Zoho organisation are excluded. We do not seek to identify any individual from these logs, and we do not use them to build any profile of any individual.

We will never sell, rent, trade or license these logs, or any information contained in them, to any third party, and we will not use them for advertising, marketing, profiling, model training, resale or any other purpose unrelated to the operation, security, support and improvement of the Extensions.

4.4 Support and business correspondence

If you contact us for support, or to make an enquiry, request or complaint, we collect the information you choose to give us. That ordinarily includes your name, your email address, the name of your organisation, and the details of your enquiry, including any screenshots, log extracts or configuration details you send us.

We ask that you do not send us the personal information of your own customers, contacts or staff when seeking support. If information of that kind is reasonably necessary to diagnose a problem, we will tell you, ask you to provide only what is necessary, use it only to resolve the matter, and delete it when the matter is resolved.

4.5 Unsolicited personal information

If we receive personal information that we have not solicited, and that we could not lawfully have collected under APP 3, we will destroy or de-identify that information as soon as practicable, if it is lawful and reasonable to do so, in accordance with APP 4.

4.6 Is this information "personal information"?

Most of the information described in clauses 4.2 and 4.3 identifies an organisation and a system event rather than an individual. We consider that it is unlikely to be "personal information" within the meaning of section 6 of the Privacy Act, because it does not relate to an identified individual or to an individual who is reasonably identifiable.

We acknowledge, however, that information such as an IP address or an organisation identifier may in some circumstances be capable of being linked to an individual, particularly where an organisation is operated by a sole trader. We therefore treat all of the information described in clause 4 as though it were personal information, and we handle it in accordance with this Policy, regardless of how it is ultimately characterised.

5. How we collect information

We collect information:

A) automatically from the Extension operating in your Zoho organisation, through the installation, licensing and logging mechanisms described in clause 4;
B) from Zoho, where Zoho notifies us that an Extension has been installed in, or uninstalled from, an organisation, or that a subscription has commenced, renewed, lapsed or been cancelled; and
C) directly from you, when you contact us.

Our collection is limited to information that is reasonably necessary for the functions and activities described in clause 6, as required by APP 3.

6. Why we collect, hold, use and disclose information

We use the information described in clause 4 only for the following

purposes:

A) to make an Extension available to your organisation and to operate it as intended;
B) to verify that your organisation holds a current licence or subscription for an Extension, and to suspend or discontinue access where it does not;
C) to detect, investigate, diagnose and resolve faults, errors, outages and security incidents affecting an Extension;
D) to respond to your support requests, enquiries and complaints;
E) to maintain, secure, test and improve the Extensions, including by understanding which operations fail and why;
F) to maintain records we are required to keep, and to establish, exercise or defend a legal claim; and
G) to comply with our obligations under any applicable law.

We will not use or disclose the information for any other purpose unless you would reasonably expect it, you consent to it, or we are required or authorised by law to do so, consistent with APP 6.

7. Anonymity and pseudonymity

The Extensions do not require any individual user to create an account with us, to identify themselves to us, or to provide any personal information to us in order to use an Extension. Licensing and logging operate at the level of the Zoho organisation rather than the individual user. You may contact us anonymously or under a pseudonym, although we may be unable to respond substantively to a request if we cannot verify your identity or your authority to make it. This reflects APP 2.

8. Disclosure of information

We do not sell, rent or trade personal information, and we will not do so. We disclose the information described in clause 4 only:

A) to our service providers, for the purpose of hosting, storing, transmitting, monitoring and securing it on our behalf. Our principal infrastructure provider is Microsoft (Microsoft Azure). We choose providers that publish contractual data-protection commitments covering the information they hold for us, and we do not authorise any provider to use that information for its own purposes;
B) to any personnel or contractors we engage, where they need it to perform the purposes in clause 6, and on terms requiring them to keep it confidential;
C) to you, or to a person you authorise;
D) to a purchaser or proposed purchaser of our business or assets, where the information is transferred as part of that business and the recipient agrees to handle it in accordance with this Policy; and
E) where required or authorised by or under law, including in response to a subpoena, a court or tribunal order, or a lawful request from a regulatory, taxation or law enforcement authority.

9. Overseas disclosure

We host our systems on Microsoft Azure. We seek to use Australian Azure regions for the storage of the information described in clause 4. Some information, particularly diagnostic and error logs and platform telemetry, may nevertheless be stored or processed on

infrastructure located outside Australia, including in the United States, or may be accessible to our service providers' support personnel located outside Australia.

Where we disclose information to an overseas recipient, we take such steps as are reasonable in the circumstances to ensure that the recipient does not breach the APPs in relation to that information, as required by APP 8. Those steps include selecting reputable providers that offer contractual data-protection commitments, and limiting the information disclosed to what is necessary.

10. Security, retention and destruction

We take such steps as are reasonable in the circumstances to protect the information we hold from misuse, interference and loss, and from unauthorised access, modification and disclosure, as required by APP 11, and to ensure that it is accurate, up to date, complete and relevant, as required by APP 10. Those steps include:

A) transmitting information over encrypted connections using Transport Layer Security;
B) keeping credentials and keys out of the Extensions' browser-side code and out of our public code repositories;
C) limiting access to the information to those people who need it to perform the purposes in clause 6; and
D) using managed cloud services that are maintained and security-patched by the provider, rather than servers we administer ourselves.

We are a small business, and the steps we take are proportionate to our size and to the limited and low-sensitivity nature of the information we hold, as described in clause 4. We do not hold the content of your records, your credentials or your payment details, and the measures described above should be read in that light. No method of transmission or storage is completely secure, and we cannot guarantee absolute security.

We retain information only for as long as we need it for the purposes in clause 6, or for as long as we are required to retain it by law. In particular:

E) licensing and entitlement records are deleted, or retained only in de-identified form for financial record-keeping, within a reasonable period after an Extension is uninstalled from an organisation or a subscription ends;

F) diagnostic, error and support logs are retained for no longer than twelve (12) months from the date of the event, after which they are deleted or aggregated into de-identified statistics that cannot be linked to any organisation or individual; and
G) support correspondence is retained for as long as reasonably necessary to deal with the matter and to maintain a record of the support we have provided.

11. Data breaches

If we suspect or become aware of unauthorised access to, unauthorised disclosure of, or loss of information we hold, we will act promptly to contain the incident and to assess whether it is likely to result in serious harm.

Where an eligible data breach occurs and we are required to do so, we will notify affected individuals and the Office of the Australian Information Commissioner ("**OAIC**") in accordance with the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act. Where a breach affects information associated with your organisation, we will notify you without undue delay and give you the information you reasonably require to meet your own notification obligations, whether or not we are ourselves required to notify.

12. Your obligations as the operator of your Zoho organisation

The Extensions are tools that operate inside your own Zoho organisation, on your instruction. You decide what information you enter into your Zoho organisation, what records you process using an Extension, and what data you retrieve into your records from third-party data sources.

You are responsible for:

A) your own compliance with the Privacy Act and any other privacy, data protection or secrecy law that applies to you;
B) ensuring that you are entitled to collect, hold, use and disclose the information you process using an Extension, and that you have given any notice and obtained any consent required to do so;

C) the content of your own privacy policy and collection notices, including any disclosure required about data you obtain from third-party data sources; and
D) complying with the terms of use of any third-party data source an Extension connects to

Where an Extension retrieves data about a sole trader, partnership or other entity operated by an individual, that data may constitute personal information about that individual in your hands, even where it is drawn from a public register.

13. Government related identifiers

Some Extensions handle government related identifiers, such as an Australian Business Number or Australian Company Number, by retrieving them on your instruction and writing them to fields in your own records. We do not adopt any government related identifier as our own identifier of any individual, and we do not use or disclose any government related identifier except as permitted by APP 9.

14. Direct marketing

We do not use the information described in clauses 4.2 and 4.3 for direct marketing. If we send you a service communication about an Extension you have installed, such as a notice of a security issue, an outage, a material change to an Extension, or a change to this Policy, that is not direct marketing. Where we send you a marketing communication, we will do so only where permitted under APP 7 and the *Spam Act 2003* (Cth), we will identify ourselves, and we will provide a simple means of opting out, which we will action promptly and at no cost to you.

15. Access and correction

You may request access to the personal information we hold about you, and you may request that we correct it, under APP 12 and APP 13. Requests should be sent to the contact details in clause 18. We will respond to a request within a reasonable period, and ordinarily within thirty (30) days. We do not charge for making a request, and we do not charge for correcting information.

We may charge a reasonable, non-excessive fee for giving access, and if we do we will tell you before we incur it. We may require you to verify your identity, and your authority to act for an organisation, before we give effect to a request. If we refuse a request, in whole or in part, we will give you written reasons and tell you how to complain about the refusal, except to the extent it would be unreasonable to do so. If we correct information we have

previously disclosed, and you ask us to notify the recipient, we will take reasonable steps to do so.

16. Complaints

If you believe we have interfered with your privacy, or breached the Privacy Act, the APPs or this Policy, please contact us using the details in clause 18. Please describe the conduct you are concerned about and what you would like us to do. We will acknowledge your complaint promptly, investigate it, and give you a written response within thirty (30) days. If we need longer, we will tell you why and when you can expect a response.

If you are not satisfied with our response, you may complain to the OAIC:

- Online: https://www.oaic.gov.au/privacy/privacy-complaints
- Telephone: 1300 363 992
- Post: OAIC, GPO Box 5288, Sydney NSW 2001

17. Changes to this Policy

We may update this Policy from time to time. The current version is always published at the address in clause 18 with a revised "Last updated" date. Where a change is material, we will take reasonable steps to notify you before it takes effect, including by in-product notice or by email to the address associated with your installation.

18. How to contact us

Privacy enquiries, access and correction requests, and complaints may be

directed to:

EnPro Labs

ABN 57 230 933 932

Email: support@enprolabs.com.au

Schedule 1 - Extensions covered by this Policy

The particulars for each Extension are set out below. Clause 1 explains how this Schedule operates.

Extension	**Zoho Marketplace Link**
ABN Lookup for Zoho CRM	

Future Extensions

Each further Extension we publish will be added to this Schedule before or at the time it is published, with the same particulars. Unless this Schedule records otherwise for a given Extension, that Extension collects no information beyond that described in clauses 4.2, 4.3 and 4.4.