LogITm8

Privacy Policy

Day 4 Tech Pty Ltd | LogITm8

Version 1.0 — effective 1 October 2026

Contact: admin@logitm8.com

Effective date: 1 October 2026

1. About this policy

Day 4 Tech Pty Ltd operates LogITm8 and PressureLog.

This policy explains how we collect, use, disclose and retain personal information when people visit our website, use PressureLog, receive reports or communicate with us.

Personal information is information or an opinion about an identified person, or someone who can reasonably be identified.

PressureLog is provided to businesses. Those businesses determine which users participate, what job information they submit and who receives their reports. Their own privacy practices and obligations may also apply.

This policy describes our information-handling practices. It does not expand our rights to use Customer Data under an applicable subscription or pilot agreement, or limit rights that cannot lawfully be excluded.

2. Information we collect

Depending on how you interact with us, we may collect:

- Account and contact information: names, work email addresses, phone numbers, business details, roles and account permissions.
- Job and site information: customer details, locations, asset information, QR identifiers and information about the work being recorded.
- Test records: photographs, readings, results, notes, technician sign-offs, timestamps and generated reports.
- Technical information: device and browser information, login activity, security events, synchronisation information, usage and error records.
- Billing information: billing contacts, subscription details, invoices, transaction references and payment status.
- Communications: enquiries, support requests, privacy complaints and feedback.

Job information, photographs and reports may contain personal information about technicians, customer contacts or other people.

Only provide information reasonably needed for the relevant purpose. Avoid including unrelated people, documents or personal details in photographs and notes.

3. How we collect information

We collect information:

- Directly from you when you register, enter information, contact us or provide feedback.

- From the business that invites you to use PressureLog.
- From authorised users who enter job information, photographs, sign-offs or recipient details.
- Through operation of the website and service, including technical, synchronisation and security records.
- From relevant service providers, such as payment-status information from our payment provider.

If you provide information about another person, you must have an appropriate basis to do so and provide any required notice or obtain any required permission.

You can make a general enquiry without supplying unnecessary personal details. However, without information needed for an account, payment, report or support request, we may be unable to provide that function or resolve the request.

4. Why we use information

We use personal information as reasonably necessary to:

- Create and administer accounts and authorised-user access.
- Provide PressureLog's workflows and generate, store and deliver reports.
- Administer subscriptions, payments and billing.
- Respond to enquiries and provide support.
- Troubleshoot errors and investigate reported problems.
- Protect accounts, Customer Data and the service.
- Communicate account, service, billing and security information.
- Respond to privacy requests and complaints.
- Comply with applicable law and enforce our agreements.

Product improvement using customer usage statistics is limited to genuinely de-identified, aggregated statistics that do not identify a customer, person, site or job. We may also use feedback, subject to confidentiality obligations.

We do not treat permission to provide the service as permission to use identifiable job records for unrelated product development or marketing.

We do not sell Customer Data or use it to train a general-purpose AI model.

5. Who can receive information

We may disclose relevant information to:

- Authorised users within the customer's business, according to their access permissions.
- Report recipients nominated by the customer.
- Our personnel who need access to provide, support, administer or secure the service.
- Service providers performing hosting, data storage, account authentication, email delivery, payment processing, support or security functions.
- Professional advisers where reasonably necessary and subject to appropriate confidentiality obligations.
- Authorities or other recipients where disclosure is required by law.

We limit service-provider access to information relevant to their functions and the purposes permitted by the applicable customer agreement.

Payments are processed through Stripe. Stripe handles payment details entered through the designated payment checkout. We use relevant billing records and payment-status information to administer subscriptions.

Stripe's privacy policy explains its handling of personal information in connection with its payment services.

6. Report delivery and customer access

PressureLog sends reports as PDF attachments to recipients specified by the customer in its account.

The email provider processes the recipient information, email content and attachments needed to deliver those messages.

Customers must ensure that nominated recipients are correct and authorised to receive the information. Reports may contain personal information, photographs and confidential job details.

Once delivered or downloaded, a report may be stored in a recipient's email system or on their device. Deleting a report from PressureLog does not recall those copies.

If you believe a report has been sent to the wrong person, contact admin@logitm8.com promptly.

7. Overseas processing

Personal information may be stored, processed or accessed outside Australia, including in Singapore.

Overseas handling may involve service providers and personnel supporting the service. We take reasonable steps appropriate to the circumstances to address privacy and security when engaging service providers.

Overseas processing remains subject to the restrictions on our use of Customer Data in the applicable agreement and any legal obligations that apply.

This policy does not ask you to waive protections that may apply to overseas disclosure.

8. Cookies and information stored on devices

The website and PressureLog may use cookies and similar browser technologies to support sessions, application operation and security.

Our website does not use website analytics, advertising cookies or other non-essential tracking technologies.

PressureLog may store information on a device to support offline operation and synchronisation. This can include information awaiting upload to the service.

Browser controls may allow you to restrict or clear cookies and stored information. Doing so may affect access or operation and may delete information that has not yet synchronised.

Check that information has synchronised and the completed report has been saved before clearing browser data or removing the application.

9. Security

We use reasonable measures to protect personal information against unauthorised access, disclosure, alteration and loss.

Access by our personnel is limited to relevant business purposes, including support, troubleshooting, administration and security.

No internet service or storage system is completely secure. Customers and users should protect their credentials, manage access appropriately and use reasonable safeguards on devices containing reports or offline information.

If we become aware of a security incident affecting Customer Data, we will notify the affected customer without undue delay, provide relevant information as it becomes available and reasonably cooperate with legally required notifications.

Where notification to individuals or a regulator is legally required, we will take the steps required of us.

Report suspected security or privacy issues to admin@logitm8.com. Do not include passwords or unnecessary sensitive information in your message.

10. Retention and deletion

We retain information for the purposes described in this policy and to meet applicable legal obligations.

For paid subscriptions, the Subscription Terms provide a 90-day period after the subscription ends to view and export existing completed reports. If a qualifying export failure is reported before the deadline, the extension described in those Terms applies.

After that period, we delete Customer Data from active production systems unless retention is legally required.

A separate pilot or trial agreement may specify a different export and deletion period.

Residual copies may remain in protected backups until their ordinary expiry. Relevant billing, security, legal and support records may be retained for their legitimate purposes and applicable retention requirements. This does not permit indefinite retention or unrelated use of job records.

Retained copies remain subject to applicable restrictions on access and use. If a backup is restored for disaster recovery, we take reasonable steps to reapply deletions so that deleted Customer Data is not returned to ordinary use.

Customers and recipients manage copies on their devices, in downloaded files and in their email systems.

11. Sensitive information

Do not upload health information, sensitive personal information, personal government identifiers or payment-card details into job records, photographs, notes or reports.

Sensitive personal information includes information such as racial or ethnic origin, religious beliefs, sexual orientation, criminal records and certain biometric information.

This restriction does not prohibit ordinary business identifiers, such as ABNs, or payment details entered through the designated payment checkout.

If prohibited information is uploaded accidentally, contact us promptly. We will assess appropriate restriction, removal or preservation steps. We do not guarantee that every upload is inspected or prohibited information automatically detected.

12. Marketing and publicity

We may send marketing communications where you have agreed to receive them or another lawful basis permits us to do so. You can opt out using an available unsubscribe facility or by contacting admin@logitm8.com.

Opting out of marketing does not stop necessary account, billing, service or security communications.

Day 4 Tech Pty Ltd will not use a customer’s business name, logo, genuine testimonial or case study for marketing unless the customer has separately agreed to that use. Any permission applies only to the

materials and purposes reasonably covered by it and does not authorise publication of confidential job records or personal information without an appropriate basis.

A customer may withdraw marketing permission as described in its agreement. Individuals may contact us separately about personal information used in publicity.

13. Access, correction and deletion requests

You may contact admin@logitm8.com to:

- Request access to personal information we hold about you.
- Ask us to correct inaccurate or incomplete information.
- Request deletion of personal information.
- Ask questions about how information is handled.

We may need to verify your identity and clarify the information involved. Please do not send identity documents unless we request an appropriate verification method.

Where information forms part of a business customer's job records, we may need to consult that customer. We will assess the request having regard to your rights, other people's privacy, record integrity and applicable retention obligations.

A request does not automatically require deletion of an entire job report or another person's information. Where appropriate, correction may involve an amendment or supplementary record rather than silently overwriting a historical record.

We will respond within a reasonable period and meet any applicable legal deadline. If we cannot fulfil a request, we will explain the reason where lawful and outline available next steps.

14. Privacy complaints

If you have a privacy concern, email admin@logitm8.com with a description of the issue and the outcome you are seeking.

We will review the complaint, seek further information where necessary and explain our response. We will keep you informed if resolving it requires additional time.

If you remain dissatisfied, you may seek independent advice or approach an appropriate regulator. Where the matter falls within its jurisdiction, you may contact the Office of the Australian Information Commissioner at www.oaic.gov.au.

15. Changes to this policy

We may update this policy to reflect changes in our practices or applicable requirements. The current version will show its effective date.

For material changes, we will provide an appropriate notice, such as an account notice, email or prominent website notice.

An update to this policy does not itself broaden our contractual permission to use Customer Data. Where agreement or consent is required, we will obtain it before undertaking the relevant changed processing.