



LEGAL DOCUMENT

Aero Ranger Privacy Policy

Pixelcase Group Pty. Ltd. ABN 74 608 040 357, trading as Aero Ranger · Effective 26 August 2026

DOWNLOADABLE COPY

Generated from <https://www.aeroranger.com/privacy-policy/>. The website is the current source if this copy is retained after the document changes. Content version 972c6a60dc4808a0.

Contents

- | | |
|---|---|
| 1. Who we are | 11. Access, correction and deletion |
| 2. Our two roles | 12. Complaints |
| 3. Information we collect | 13. Cookies and website analytics |
| 4. Vehicle and number-plate information | 14. Marketing |
| 5. How we use information | 15. New Zealand |
| 6. Automated processing | 16. Users outside Australia and New Zealand |
| 7. Who we disclose information to | 17. Data breaches |
| 8. Overseas disclosure | 18. Changes to this policy |
| 9. Storage and security | 19. Contact us |
| 10. Retention | |

1. Who we are

We are Pixelcase Group Pty. Ltd. ABN 74 608 040 357, trading as Aero Ranger ("Aero Ranger", "we", "us", "our"), of 431 Charles Street, North Perth WA 6006, Australia.

Aero Ranger provides automatic number-plate recognition (ANPR) and compliance-management technology to councils, government agencies and commercial organisations. This comprises cloud platforms (including core.aeroranger.com and dashboard.aeroranger.com), mobile applications, and vehicle-mounted and fixed hardware supplied as a service (our Services).

We handle personal information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles, and, for our New Zealand operations, the Privacy Act 2020 (NZ) (see section 15).

2. Our two roles

We handle personal information in two distinct capacities, and your rights differ depending on which applies:

Role	Information	Who decides how it is used
Service provider to our customers. Councils and other organisations use our Services to capture and manage vehicle, parking, permit and compliance records for their own regulatory and business functions.	Vehicle and number-plate records, images, location and related operational records captured or managed through a customer's deployment ("Customer Records").	The customer organisation. It determines the purposes of capture, is the appropriate first point of contact for requests about those records (section 11), and is responsible for the lawfulness of its collection. We handle Customer Records for that customer under our agreement with it and this policy, and also use them for the product-improvement purposes described in section 5.
In our own right.	Account and contact details, billing records, support communications, product usage and device telemetry, website visitor data, marketing lists.	Aero Ranger.

3. Information we collect

From customers and their users

- name, work email address, phone number, role and organisation;
- login credentials and access logs;
- billing and payment details (invoicing contact and records);
- support requests and communications with us;

- product usage information and device telemetry from our apps, platforms and hardware (device identifiers, operating system and version, IP address, app events, diagnostic logs, and location of Aero Ranger hardware units).

Through customer deployments

- vehicle images and video frames;
- number-plate reads and OCR results, including confidence values;
- GPS position, direction and time of capture;
- related records the customer creates: infringements, permits, cases, notes and evidence.

From website visitors

- pages visited, referring pages, approximate location, and device/browser information, via cookies and similar technologies (section 13);
- anything you submit through our forms – demo bookings, contact requests, newsletter sign-ups, account-deletion requests.

4. Vehicle and number-plate information

Our Services photograph vehicles in public places and read their number plates. A number plate linked to a time and place can be personal information about the vehicle's registered operator, and we treat it accordingly.

- Capture is carried out by or for our customers – councils and other organisations – for their parking, permit, local-law and compliance functions. The customer determines where and why capture occurs and is responsible for its lawful basis, including any signage or notification obligations that apply to it.
- We host and process those records on the customer's behalf, apply the security measures described in section 9, and use them as described in section 5.
- If your vehicle has been recorded and you wish to access, correct or query a record – for example in connection with an infringement – contact the organisation that operates the deployment (typically the council named on any notice you received). We assist customers to respond to such requests. Section 11 explains how to reach us if you are unsure who the customer is.

5. How we use information

We use personal information to:

1. provide, operate, secure and support the Services;
2. administer accounts, billing and debt collection;
3. verify identity and manage access;

4. improve and develop our products, including training, evaluating and improving the machine-learning models that perform plate detection and recognition, and producing analytics and statistical reports. Wherever practicable we use de-identified or aggregated information for these purposes, and the outputs of this work (such as trained models and aggregate statistics) do not identify individuals;
5. communicate with users about service, security and account matters;
6. market our products and services (with opt-out – section 14); and
7. meet our legal obligations and enforce our agreements.

6. Automated processing

The Services use computer vision and machine learning to detect vehicles and read number plates automatically, and can automatically match reads against lists configured by the customer (for example permit holders or vehicles of interest) and generate alerts or measurements (such as time-limit overstays).

The personal information used in this automated processing comprises vehicle images and video frames, number-plate reads, and the associated location and time of capture. These automated outputs inform decisions made by our customers; they do not make final decisions about individuals by themselves. Enforcement and similar decisions (such as whether to issue an infringement) are made by the customer organisation and its authorised officers under their own procedures, which ordinarily include human review of the evidence. Recognition results carry confidence indicators and can be corrected by authorised users.

7. Who we disclose information to

We disclose personal information only as needed to operate the business and the Services:

- the customer organisation whose deployment captured or holds the relevant records, and its authorised users;
- our personnel and contractors bound by confidentiality obligations;
- our service providers and subprocessors – hosting, communications, support, analytics and payment providers. Our current subprocessors are listed in the Aero Ranger Trust Centre;
- our related bodies corporate;
- our professional advisers, insurers and auditors;
- law-enforcement, regulatory and government bodies where required or authorised by law; and
- a purchaser or prospective purchaser of our business or assets, under confidentiality obligations.

We do not sell personal information.

8. Overseas disclosure

Some of our service providers and related entities store or access information from outside Australia. Where we disclose personal information to overseas recipients, we take reasonable steps to ensure it is handled consistently with the Australian Privacy Principles and this policy. The service providers we use, and where they operate, are listed in the Aero Ranger Trust Centre.

9. Storage and security

- The CORE platform's production and staging data is hosted in AWS's Sydney region, with backups held in the Melbourne region.
- Our information security management system is certified to ISO/IEC 27001:2022.
- Information is encrypted in transit and at rest, access is role-based and logged, and customer organisations' data is logically separated.
- Our published security posture, certifications and controls are available in the Aero Ranger Trust Centre.

No transmission or storage system is completely secure; we cannot guarantee absolute security, but we maintain and test our controls continually.

10. Retention

- Customer Records are retained in accordance with our agreement with the customer and the customer's configuration. Records may be retained after a customer relationship ends where our agreement permits; identified personal information within retained records is de-identified or deleted when it is no longer required for the purposes described in section 5 and, in any event, as the Privacy Act requires.
- Account and billing information is retained for the life of the account and thereafter as required for legal, accounting and dispute-resolution purposes.
- De-identified and aggregated data (which no longer identifies any individual) is not personal information and may be retained and used by us, including for the product-development purposes in section 5.

When personal information is no longer required, we take reasonable steps to delete or de-identify it.

11. Access, correction and deletion

- Your account with us: you may request access to or correction of your personal information, or deletion of your account, at privacy@aeroranger.com or via aeroranger.com/account-deletion. We respond within a reasonable period (ordinarily 30 days, and within any shorter period the law requires – for New Zealand see section 15) and do not charge you for making a request.
- Records held in a customer's deployment: direct your request to that organisation, which controls the records; we assist it to respond, and where the law requires us to deal with a request made to us – including by transferring it to the responsible organisation or responding ourselves – we will do so. If you are unsure which organisation that is, contact us and we will help you identify it where we reasonably can.

- If we refuse a request, we will tell you why in writing and how to complain.

12. Complaints

If you believe we have mishandled your personal information, contact us at privacy@aeroranger.com. We will acknowledge your complaint promptly, investigate, and respond within 30 days. If you are not satisfied with our response, you may complain to the Office of the Australian Information Commissioner (oaic.gov.au, 1300 363 992) or, for New Zealand matters, the Office of the Privacy Commissioner (privacy.org.nz).

13. Cookies and website analytics

Our website and applications use cookies and similar technologies for sign-in and session management, preferences, security, and to understand how our website is used. You can control or disable cookies in your browser settings; some features (such as staying signed in) will not work without them.

14. Marketing

We may send you information about our products and services. Every marketing message includes an unsubscribe mechanism, and you can opt out at any time at support@aeroranger.com. We comply with the Spam Act 2003 (Cth) and the Unsolicited Electronic Messages Act 2007 (NZ). Opting out of marketing does not stop service and account communications.

15. New Zealand

For personal information we collect in connection with our New Zealand operations, we comply with the Privacy Act 2020 (NZ) and its Information Privacy Principles. Where personal information is collected other than directly from the individual concerned – as with vehicle and number-plate capture – awareness of the collection is provided through this policy and through the notices and signage of the customer organisation operating the deployment, as IPP 3A contemplates. New Zealand individuals have rights of access to and correction of their personal information (sections 11 and 12 above apply, and requests are handled within 20 working days as that Act requires). We disclose New Zealand personal information to a recipient outside New Zealand (other than a person holding it on our behalf) only where IPP 12 permits, including where we believe on reasonable grounds that the recipient is subject to privacy safeguards comparable to the Privacy Act 2020 (NZ). Notifiable privacy breaches affecting New Zealand individuals are handled under that Act (section 17).

16. Users outside Australia and New Zealand

Our Services are designed for, and offered to, organisations in Australia and New Zealand. If you access our website from elsewhere, we handle your personal information under this policy and Australian law. Where the law of another jurisdiction nevertheless grants you additional rights in relation to your personal information, you may exercise them by contacting privacy@aeroranger.com.

17. Data breaches

We maintain a data-breach response plan. Where a breach involving personal information is likely to result in serious harm, we will notify affected individuals and the Office of the Australian Information Commissioner in accordance with the Notifiable Data Breaches scheme (Part IIIIC, Privacy Act 1988 (Cth)), and the New Zealand Privacy Commissioner where the Privacy Act 2020 (NZ) requires. Where the affected records are Customer Records, we work with the customer organisation concerned so it can meet its own obligations.

18. Changes to this policy

We may update this policy from time to time. The current version, its effective date and a summary of material changes are always available at aeroranger.com/privacy-policy. For material changes we will give notice through the Services or by email before the change takes effect.

19. Contact us

Privacy Officer Pixelcase Group Pty. Ltd. trading as Aero Ranger 431 Charles Street, North Perth WA 6006, Australia privacy@aeroranger.com · support@aeroranger.com