

Privacy Policy

LAST UPDATED · 11 OCTOBER 2026

Operated by Nexotec Pty Ltd · ABN 12 674 499 024 · Queensland, Australia
hello@myglo.app · myglo.app

1. About this Policy

1.1 Nexotec Pty Ltd, trading as MyGlo (MyGlo, we, us, our), operates a marketplace connecting Clients with independent beauty and wellness Providers.

1.2 This Policy explains how we collect, hold, use and disclose personal information through our websites, applications, booking and payment features, communications and related operations.

1.3 Personal information is information or an opinion about an identified or reasonably identifiable individual. Sensitive information includes health information and certain other information protected by privacy law.

1.4 We handle personal information in accordance with this Policy and applicable Australian privacy law, including the Privacy Act 1988 (Cth) and Australian Privacy Principles where they apply to us.

1.5 This Policy explains our practices. It does not, by itself, constitute consent to every collection, use or disclosure described. Where privacy law requires a separate consent, we seek that consent separately.

2. Information we collect

2.1 Account information. Depending on your use of MyGlo, we collect your name, contact details, account identifiers, login and authentication information, age confirmation and profile preferences.

2.2 Provider information. We collect business names, ABNs, business contact details, service addresses, exact service-location coordinates, personnel contact details, service descriptions, prices, availability and relevant qualification, licence, insurance and verification information.

2.3 Bookings and transactions. We collect Booking details, selected Services, dates, prices, payment status, transaction identifiers, fees, refunds, cancellations, payout information and dispute records.

2.4 Payments and verification. Stripe collects information needed to process payments and verify connected accounts. We receive or access payment and account information relevant to our integration, such as payment status, transaction references, limited payment-method details, connected-account identifiers, verification status and payout records. MyGlo does not store full Client card numbers or Provider bank-account details.

2.5 Booking notes and support communications. We collect free-text booking notes, including client_notes and access_notes, as well as enquiries, support communications, complaints and related records. Users may choose to include information in these fields that is sensitive; clause 4 explains how we handle it.

2.6 Content and activity. We collect profiles, photographs, videos, reviews, ratings, comments, follows and other interactions you submit or make through the Platform.

2.7 Technical and diagnostic information. We collect information relevant to operating and securing the Platform, including device and browser information, IP addresses, operating system, access times, usage events, crash/error information and technical logs. Some infrastructure and error-monitoring suppliers may process IP addresses even where MyGlo does not use IP addresses to determine your location.

2.8 Location. Providers' business or service addresses and exact coordinates are stored so they can be shown and ranked geographically. Where the nearby-discovery feature is enabled, the app may request a Client's device location with permission to show nearby Providers. If permission is declined, the Client may choose an area manually. MyGlo intends to save only a coarse area against the Client account for this purpose and does not use background location tracking.

2.9 The information involved depends on the features you use. We seek to limit collection to information reasonably necessary for our functions and activities.

3. How we collect information

3.1 We generally collect information from you when you create an account, set up a Provider profile, make or manage a Booking, pay, enter Booking notes, upload content or contact us.

3.2 We also collect information automatically through Platform operation and technologies described in clauses 10 and 11.

3.3 Relevant information may come from Providers, Clients, Stripe and other service suppliers, or from a person making a complaint or report. Where lawful and reasonably necessary, verification information may come from public business or professional registers.

3.4 Where appropriate, we provide an additional collection notice explaining a particular collection, its purpose, recipients and the consequences of not providing information.

3.5 You may make a general enquiry anonymously or under a pseudonym where practicable. Identifying information is ordinarily necessary to manage accounts, Bookings, payments, verification and disputes.

3.6 If you do not provide necessary information, we may be unable to provide the relevant feature or process the relevant transaction.

3.7 If we receive unsolicited personal information, we assess whether we could lawfully have collected it. Where required, we destroy or de-identify it if lawful and reasonable to do so.

4. Health and other sensitive information

4.1 A user may include health or other sensitive information in a Booking note or support request, including information about allergies, sensitivities, skin conditions, injuries, pregnancy, medications or medical conditions.

4.2 General free-text Booking notes are not intended to be medical records. Please provide sensitive information only where it is reasonably necessary for the relevant Booking or support issue.

4.3 If you voluntarily include health information in a Booking note intended for a Provider, MyGlo may collect, hold and disclose that information to the booked Provider for the purpose of arranging or safely providing the Booking. We do not use health information for advertising or direct marketing.

4.4 If MyGlo introduces dedicated fields that expressly request health or other sensitive information, we will provide an appropriate collection notice and seek express consent before collection unless a legal exception applies. General acceptance of our Terms or this Policy does not replace consent where separate consent is required.

4.5 We use or disclose sensitive information for the purpose for which it was provided, a directly related purpose where legally permitted and reasonably expected, or another purpose permitted or required by law.

4.6 A Provider may independently collect information directly from you outside MyGlo, including during a consultation or through its own forms. That independent handling is governed by the Provider's own practices and applicable law. Ask the Provider for its privacy information.

4.7 You may contact us to withdraw consent for future consent-based handling. Withdrawal may affect a relevant feature or Booking and does not necessarily require deletion of records we must lawfully retain.

5. Why we use information

5.1 We use personal information as reasonably necessary to:

- create and administer accounts;
- display Provider profiles, services and User Content;
- enable discovery, follows and other Platform interactions;
- arrange and manage Bookings, cancellations and reminders;
- process card payments, MyGlo fees, refunds, transfer adjustments and Provider payouts;
- record cash Bookings and related Booking status where that feature is used;
- communicate about accounts and transactions;
- provide support and handle complaints and payment disputes;
- verify accounts and detect or respond to fraud or misuse;
- maintain security and moderate content;
- analyse technical performance and improve Platform functionality;
- personalise nearby discovery using relevant location or coarse-area information and recency;
- administer and enforce our Terms proportionately;
- meet legal, regulatory, tax and accounting obligations; and
- send marketing as explained in clause 12.

5.2 We do not treat publication of information online as unrestricted permission to use it for any purpose. Sensitive information remains subject to clause 4.

6. Public information and information shared for Bookings

6.1 Provider profiles, portfolios, listed service locations and content submitted for publication may be visible to other users and the public. Public material may be copied or indexed by third parties.

6.2 Reviews, comments and other public interactions may identify the associated account. Consider what personal information you include.

6.3 We share relevant Client and Booking details, including necessary Booking notes, with the selected Provider, and relevant Provider details with the Client, to arrange and deliver Services and address related issues.

6.4 A Provider's access to Client information does not authorise unrestricted marketing. Providers must obtain any consent needed for their own communications.

6.5 Removing content from MyGlo does not necessarily remove copies held independently by others. We remain responsible for handling information within our control.

7. Stripe and payment information

7.1 Where card payments are enabled, MyGlo uses Stripe Connect. Providers complete Stripe-hosted onboarding and Stripe independently collects identity, business, bank and payment information required for its services.

7.2 Card charges are created on Nexotec's Stripe platform account and Provider shares are transferred through Stripe to connected accounts. We exchange relevant account, transaction, verification, refund, dispute and payout information with Stripe to operate these features.

7.3 Stripe applies its own fraud, risk and compliance screening to payments and connected accounts. Stripe's independent handling is subject to its own privacy policy and agreements.

7.4 For cash Bookings, MyGlo does not process the cash payment itself, although the Platform may retain the Booking record and status.

8. Service suppliers and other disclosures

8.1 We disclose relevant personal information to service suppliers where reasonably necessary to operate MyGlo. Current or planned production suppliers include:

- Supabase for database, authentication, file storage, realtime functions and server functions;
- Stripe for payment processing, connected-account onboarding, fraud screening, refunds, disputes and payouts;
- Resend for transactional email;
- Sentry for crash and error monitoring;
- Shorebird for over-the-air application updates;
- Google Maps Platform and device geocoding services from Apple or Google for location and address functionality where enabled;
- Netlify for hosting the myglo.app website; and
- other hosting, content-delivery, security or technical suppliers needed to operate particular website or app features.

8.2 We may also disclose relevant information to professional advisers, insurers and auditors; regulators, courts, law enforcement and government agencies where required or permitted by law; and parties involved in a proposed or completed business sale, investment or restructure, subject to appropriate safeguards.

8.3 Where legally required, disclosures may include Provider and transaction information supplied to the Australian Taxation Office.

8.4 We limit disclosures to information appropriate for the purpose and use reasonable contractual and operational safeguards. We do not sell personal information.

9. Overseas handling

9.1 Our primary application database and file storage are hosted in Sydney, Australia through Supabase. Some other suppliers process or access information outside Australia.

9.2 Based on our current supplier configuration, overseas recipients or processing locations are likely to include the United States, Japan, Germany and other countries in the European Union or European Economic Area. Some global suppliers may also process information in other countries in which they or their subprocessors operate.

9.3 Overseas processing may include transactional email, payment services, website hosting, error monitoring, application-update infrastructure, mapping or device-platform services.

9.4 Where applicable, before disclosing personal information overseas we take reasonable steps required by Australian privacy law to ensure appropriate handling by the recipient. Overseas handling may expose information to laws different from Australian laws.

9.5 You may contact us for further information about relevant overseas handling.

10. Automated Platform features

10.1 The Platform uses automated processes for some routine functions. These currently or at launch may include expiring unanswered booking requests, sending booking reminders, ordering nearby discovery content using distance and recency, and automatically refunding an eligible card Booking when a Client cancels within the Provider's disclosed free-cancellation window.

10.2 The personal information used for these processes may include Booking status and timing, Provider cancellation settings, transaction status, Provider service location, a Client's permitted device location or saved coarse area, and relevant Platform activity.

10.3 Where an automated outcome affects a Booking or payment and you believe it is incorrect, you may contact hello@myglo.app to request review. MyGlo does not currently use its own automated system to suspend accounts, verify Providers or make final content-moderation decisions.

10.4 Stripe separately uses automated fraud and risk systems in connection with card payments and connected accounts. Questions about Stripe's independent decision-making may also be subject to Stripe's own privacy information and review processes.

11. Cookies, SDKs, diagnostics and tracking

11.1 Our websites and applications may use essential cookies, local storage, software development kits and similar technologies to maintain sessions, support security, deliver updates and operate features.

11.2 At the date of this Policy, MyGlo does not use advertising trackers or behavioural advertising analytics in the app, and we are not aware of advertising or analytics scripts on myglo.app. Netlify and other infrastructure suppliers may process IP addresses and technical request information in server logs, and Sentry processes crash and diagnostic information.

11.3 If we introduce analytics, advertising tracking or another materially different tracking technology, we will update this Policy and provide any notice or choice required by law before using it.

11.4 Browser and device settings may allow you to restrict cookies, identifiers or permissions. Restricting essential technologies may affect Platform functionality.

12. Marketing communications

12.1 We send electronic marketing where we have express consent or another legally sufficient basis under applicable marketing law.

12.2 Marketing messages identify the sender and provide a functional unsubscribe method. You may also contact hello@myglo.app to opt out.

12.3 We action unsubscribe requests within the legally required period, including within five working days for messages covered by the Spam Act 2003 (Cth).

12.4 Opting out does not prevent necessary, non-promotional Booking, security, payment or account messages. We do not use sensitive information for direct marketing.

13. Security, backups and retention

13.1 We take reasonable technical and organisational steps to protect personal information against misuse, interference, loss, unauthorised access, modification and disclosure. Safeguards are selected having regard to the nature and sensitivity of the information and the risks of the relevant systems.

13.2 No method of storage or transmission is completely secure. We investigate suspected data incidents and notify affected individuals and regulators where required by law.

13.3 We retain information only for as long as reasonably necessary for a permitted purpose, including providing the Platform, maintaining transaction records, resolving disputes and meeting legal, tax and accounting obligations.

13.4 When an account is deleted, profile information, photographs and posts are removed or anonymised so they no longer appear through the account. Booking and payment records may be retained in de-identified or otherwise lawfully retained form where reasonably necessary for tax, accounting, fraud-prevention or dispute purposes.

13.5 For the production Supabase configuration planned for launch, daily database backups are retained for 7 days. Information deleted from live systems may therefore remain in backup copies until the relevant backup expires. Backups are not retained as a means of avoiding deletion obligations.

13.6 If our backup, legal-retention or production configuration changes materially, we will update this Policy as appropriate.

14. Access, correction and deletion

14.1 You may request access to personal information we hold about you, correction of inaccurate information, or deletion of your account or information through available in-app controls or by contacting hello@myglo.app.

14.2 We may take reasonable steps to verify your identity without requesting unnecessary information.

14.3 We respond within a reasonable period and aim to respond within 30 days. If more time is needed, we explain why.

14.4 There is no charge to make an access request or to request correction. If a reasonable access charge is permitted and proposed, we tell you before proceeding.

14.5 We may refuse or limit a request only where permitted by law. Where required, we explain the reasons in writing and available complaint options.

14.6 If we disagree with a requested correction, you may ask us to associate a statement of your position with the record. Where required, we also take reasonable steps to notify relevant recipients of a correction.

14.7 Australian privacy law does not provide an unrestricted right to erase every record. We assess deletion requests against our retention obligations and explain any information that must remain.

14.8 Deleting information held by MyGlo does not necessarily delete independent records held by a Provider, Stripe or another third party. You may need to contact them separately.

15. Children and information about other people

15.1 MyGlo accounts and Booking functionality are intended for adults aged 18 or over.

15.2 Users must not provide information or images about another person without appropriate authority and any required consent.

15.3 If we discover that an underage person has created an account, or that a child's information has been collected improperly, we assess the circumstances and take appropriate steps, which may include account restriction and deletion where lawful.

15.4 Contact us if you believe a child's information has been handled improperly through MyGlo.

16. Privacy complaints

16.1 Send a privacy complaint to hello@myglo.app, addressed to the Privacy Contact, describing the issue and the outcome you seek.

16.2 We will acknowledge the complaint, investigate and aim to provide a substantive response within 30 days. If we need longer, we will explain the delay and expected response time.

16.3 If you are dissatisfied or do not receive a response within a reasonable time, you may contact the Office of the Australian Information Commissioner at oaic.gov.au. Its ability to investigate depends on its jurisdiction and applicable law.

17. Changes and contact

17.1 We may update this Policy to reflect changes in our practices, suppliers, technology or legal obligations. We will make the current version available and take reasonable steps to notify users of material changes.

17.2 An update does not retrospectively authorise handling that previously required consent. Where a new use requires consent, we will seek it separately.

17.3 Privacy enquiries, requests and complaints may be sent to: Privacy Contact, Nexotec Pty Ltd, trading as MyGlo, ABN 12 674 499 024, Queensland, Australia. Email: hello@myglo.app.