

Privacy & Personal Data Protection Policy

Document name	Privacy & Personal Data Protection Policy
Version	1.0
Issue date	7 October 2026
Effective date	7 October 2026
Issued by	GLOW BOOKING TECH INC. (Glow)
SEC registration no.	2026090268132-07
TIN	815-552-907-00000
Registered address	Unit D, 3rd Floor, Prestoza-Borcelis Commercial Building, Tanza-Trece Road, Landmass Park Subd., Biga 4108, Tanza, Cavite, Philippines
Contact	support@glowphilippines.com · +63 46 889 6200 · glowphilippines.com

Welcome to Glow. GLOW BOOKING TECH INC. ("Glow", "we", or "us") applies technical, organizational, and physical measures appropriate to the nature of the data, the purposes of processing, and the level of risk, in order to protect Personal Data in accordance with applicable law. This Policy describes how Glow collects, uses, stores, discloses, transfers, and protects data when you use the Glow App and website.

This Policy forms part of Glow's Terms of Service and Operating Rules. Glow operates as an independent technology platform facilitating connections between Customers and independent Technicians and is not the provider of the underlying Technician Services. Message Data is also subject to the Non-Disclosure & Personal Data Protection Agreement, which Technicians and Customers must execute or affirmatively confirm through the mechanism published by Glow.

A. TYPES OF PERSONAL DATA COLLECTED

Glow processes data necessary to provide and support the Services, which may include the following.

Identity data

Full name, date of birth, sex, nationality, and government-issued identification details where reasonably necessary and lawful for verification purposes.

Where required, a criminal record clearance issued by the National Bureau of Investigation, collected solely to assess the suitability of a person who will attend a Customer's premises.

Contact data

Residential address or service address, telephone number, email address, and social-media or messaging identifiers where you provide them voluntarily or use them for a related Platform function.

Transaction and payment data

Payment status, transaction identifiers, and limited payment identifiers provided to Glow by a licensed payment service provider only to the extent reasonably necessary to support Advertising Credit Balance top-ups and related records. Glow does not store Customer payment card details and does not receive or hold the service payment made by a Customer to a Technician.

Electronic identity verification data

Where a Technician undergoes electronic identity verification, this may include an image of a government-issued identification document, a facial photograph, an image or video used to confirm that the person is physically present, the result of a facial comparison, and the result of document-authenticity checks. A facial image used to identify or verify an individual constitutes sensitive personal information within the meaning of the Data Privacy Act of 2012.

Glow collects, uses, and discloses such data on the basis of consent obtained separately from other consents, or on another lawful basis permitted by Section 13 of the Data Privacy Act of 2012. You may withdraw consent at any time. Withdrawal may mean that Glow can no longer verify your identity and can no longer display your Technician profile on the Platform.

Glow uses electronic identity verification data solely to verify and re-verify the identity of the account holder, including to detect the fraudulent use of an identity, and for no other purpose. Glow does not use biometric data for marketing, for profiling, for analytics, or for the training of any model, does not sell biometric data, and does not share biometric data for the commercial purposes of any third party.

Glow retains electronic identity verification data, including the images used for verification, the verification result, the reference identifier, and the timestamp, for as long as the account remains active, and thereafter for the period required by applicable law or reasonably necessary for the resolution of a dispute, the exercise or defense of a legal claim, the prevention of fraudulent re-registration, or compliance with a lawful request of a competent authority. Retention is subject to your right to request erasure or blocking under Section D, which Glow will act upon in the cases provided by law.

Location data

Your actual geographic location where reasonably necessary to enable a Technician to travel to and perform a Service at the agreed location.

Health information provided for service safety

Health information voluntarily provided by a User solely to facilitate the safe delivery of a requested Service, such as an allergy history or a pregnancy status. Glow does not provide medical examination, diagnosis, treatment, or advice, and does not process this information for any purpose other than the safe delivery of the requested Service.

Technical data

Internet protocol address, device type, operating system, cookies, and information about your use of the App.

Message Data and Platform interactions

Conversation and interaction history between Customers and Technicians, message content, attachments, sent, received, and read timestamps, conversation identifiers, account identifiers, processing status, system logs, flagged content, results of system or artificial-intelligence review, and related complaint-handling records.

Consent and electronic acceptance records

The time of consent or acceptance, the version of the Policy, Terms, or Operating Rules accepted, the scope of consent, the account concerned, device information, internet protocol address or session identifier, one-time password records, and equivalent electronic confirmation data.

B. PURPOSES AND LEGAL BASES OF PROCESSING

Glow processes Personal Data for the purposes below. Processing may be based on the necessity of performing a contract to which you are a party, compliance with a legal obligation, the legitimate interests of Glow or a third party, consent, or another basis permitted by the Data Privacy Act of 2012 and its Implementing Rules and Regulations. Consent is not always required; processing may be based on contract performance, legal obligation, legitimate interest, or another lawful basis as applicable.

- Platform operations: supporting booking confirmation, connecting Customers with Technicians, recording transaction status, and providing technical connection or support in relation to a licensed third-party payment service provider.
- Customer support: responding to questions, complaints, requests, and feedback.
- Safety and legal compliance: detecting and preventing fraud, abuse, prostitution, paid dating, trafficking in persons, child trafficking, online sexual abuse or exploitation of children, child sexual abuse or exploitation material, other prohibited conduct, security threats, and violations of law or Platform rules; preserving evidence where required by law; and complying with lawful requests, orders, reporting duties, or other legal obligations.
- Identity verification: confirming that a Technician is the person they claim to be, that submitted documents are authentic, and that the person completing verification is physically present.
- Messaging-channel operation and review: operating the messaging channel between Customers and Technicians, supporting bookings, detecting attempts to move transactions off the Platform, identifying prohibited conduct and safety risks, handling complaints and disputes, and responding to lawful requests of competent authorities.
- Platform improvement: analyzing data only to the extent necessary to improve features, user experience, operational safety, capacity planning, and product analytics. Glow will not use Message Data to train general-purpose artificial-intelligence models unless Glow has an appropriate lawful basis and has given the notice or obtained the consent required by law.
- Marketing: sending promotions, offers, or marketing communications where you have given consent or where another lawful basis applies, subject to your right to opt out or object.

Where consent is the lawful basis for a material processing activity, Glow, its authorized personnel, and automated systems may access, read, store, filter, flag, and review Message Data only to the extent necessary, proportionate, and for the legitimate purposes stated in this Policy. Access to review results is limited by role, and material access or processing events are logged as appropriate.

C. DATA SHARING AND CROSS-BORDER TRANSFERS

Service providers and sub-processors

Technical service providers, artificial-intelligence service providers, cloud hosting providers, sub-processors, and providers of automation or operational-support tools engaged by Glow may access Personal Data only to the extent necessary to perform their functions for Glow. Such persons must process data on Glow's instructions, under an appropriate confidentiality and data-processing agreement, and in accordance with applicable data-protection law.

The categories of personal information processors engaged by Glow in the Philippines include electronic identity verification providers, electronic signature providers, licensed payment system providers, accounting and electronic invoicing providers, cloud hosting providers, and providers of automated or artificial-intelligence content review. Glow maintains a written data-processing agreement with each processor.

Disclosure to third parties

Glow does not sell your Personal Data. Glow discloses only the personal information reasonably necessary for the relevant purpose, which may include disclosure to:

- the Technician assigned to perform a requested Service, limited to the personal data reasonably necessary to perform that Service, which may include name, contact number, service location, and service-specific instructions you have provided;
- licensed payment service providers and technical service providers necessary for Platform operations, only to the minimum extent reasonably necessary for their specific function;
- authorized payment partners, insurers, or other service providers engaged by Glow, only to the extent necessary for the performance of their functions; and
- government agencies, regulators, courts, investigators, or law-enforcement authorities where disclosure is permitted or required by law, or pursuant to a lawful request or order.

Glow may disclose personal information only to the extent necessary and as permitted or required by applicable law, including the Data Privacy Act of 2012.

Cross-border transfer of Personal Data

To operate the Platform and provide the Services, Personal Data may be stored on cloud systems located outside the Republic of the Philippines and may be processed by personal information processors engaged by Glow that are located outside the Philippines.

In particular, Personal Data may be processed by a personal information processor engaged by Glow and located in the Socialist Republic of Viet Nam, for the purposes of platform development and system maintenance, hosting and system administration, technical and user support, content and safety review, fraud prevention, analytics, and operational reconciliation. That processor acts only on the documented instructions of Glow and does not determine the purposes or means of processing. Glow will identify the processor to a data subject, or to the National Privacy Commission, on lawful request.

Glow remains responsible for Personal Data transferred outside the Philippines in accordance with the principle of accountability under the Data Privacy Act of 2012. Glow implements the following safeguards in relation to each cross-border transfer:

- a written data-processing agreement with the overseas processor, containing obligations no less protective than those imposed on Glow under this Policy and applicable law, including obligations of confidentiality, security, sub-processor control, assistance with data-subject requests, breach notification, and deletion or return of data on termination;
- a requirement that the overseas recipient provide a level of protection comparable to that required under the Data Privacy Act of 2012 and other applicable laws;
- technical and organizational security measures appropriate to the risk, including access control, encryption in transit and at rest where appropriate, role-based permissions, and access logging;
- restriction of the transfer to the Personal Data reasonably necessary for the stated purposes; and
- a prohibition on the overseas processor using the Personal Data for its own purposes, including the training of any model, or for any purpose in another territory, without Glow's prior written instruction.

Glow will maintain records of its cross-border transfers and will make information about those transfers available to the National Privacy Commission on lawful request. You may obtain further information about the safeguards applied to a transfer by contacting Glow using the details in Section H.

Business transfer and change of platform operator

In the event of a corporate reorganization, merger, transfer of business in whole or in part, transfer of assets, assignment of contractual rights and obligations, or a change in the operator of the Glow Platform in the Philippines, Glow may transfer or make available your Personal Data to the transferee or to the new platform operator to the extent necessary for you to continue receiving the Services.

Such a transfer is based on the necessity of performing a contract to which you are a party, and on the legitimate interest of maintaining continuity of service and completing outstanding work, in accordance with the Data Privacy Act of 2012. For sensitive personal information, including biometric data, Glow will obtain your consent before the transfer unless an exception under applicable law applies.

The new operator must be bound by data-protection measures no less protective than those set out in this Policy and will process your data only for the original purposes. Glow will notify you of the change through the App, by email, or by another reasonable channel before, or within a reasonable period after, the transfer takes effect, and will identify the new operator and the channels for exercising your rights. Your rights under Section D continue to apply against the new operator. You may object to the transfer of your Personal Data, or request its deletion or destruction, as provided by law, by contacting Glow using the details in Section H.

D. RIGHTS AND RESPONSIBILITIES OF DATA SUBJECTS

Subject to the conditions, exceptions, and limitations provided by law, a data subject may exercise the following rights:

- Right to be informed: to receive information about the collection, use, disclosure, and processing of their Personal Data.
- Right to object: to object to processing in the cases recognized by law, including processing for direct marketing or processing based on legitimate interests.
- Right to access: to request access to, and a copy of, Personal Data relating to them, together with the related information required by law.
- Right to rectification: to request correction of Personal Data that is inaccurate, incomplete, or out of date.
- Right to erasure or blocking: to request the deletion, destruction, blocking, or removal of Personal Data in the cases provided by law.
- Right to withdraw consent: where processing is based on consent, to withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing carried out before withdrawal and does not affect processing that may lawfully continue on another basis.
- Right to data portability: where applicable law provides, to obtain Personal Data in an electronic or structured format commonly used and to transmit or transfer that data.
- Right to damages: to be indemnified for damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of Personal Data, as provided by law.
- Right to lodge a complaint: to file a complaint with the National Privacy Commission or to pursue other legal remedies available under applicable law.

You are responsible for taking reasonable care to protect your own Personal Data and for providing Glow with accurate and current information.

E. EXERCISING DATA-SUBJECT RIGHTS AND WITHDRAWING CONSENT

Where Glow relies on consent for accessing, reading, reviewing by artificial-intelligence tools, or otherwise processing Message Data, consent will be requested through an affirmative action such as a separate checkbox, a popup, a one-time password, an in-app confirmation, or another traceable electronic method. Glow will not treat a pre-ticked box, silence, or a failure to respond as consent, and will present a consent request separately from other matters, in a form that is readily accessible, in clear and plain language, and not misleading. Where an activity involves several purposes requiring consent, the purposes will be presented so that the data subject can clearly indicate the scope of consent.

When recording consent electronically, Glow may retain evidence of consent, including the time, the document version, the scope, the account concerned, device information, internet protocol address or session identifier, and the confirmation method, to the extent necessary for legal compliance and accountability.

You may exercise the rights described above by sending a written request to support@glowphilippines.com.

Glow will acknowledge requests promptly and will process them within the period required or reasonably permitted under applicable law, taking into account the nature and complexity of the request. Where applicable law permits an extension, or where additional identity verification is reasonably necessary, Glow will inform you of the reason and the expected time for completion.

F. DATA SECURITY AND RETENTION

Message Data between Customers and Technicians is subject to a default operational retention period of thirty (30) days from the end of the conversation or completion of the related transaction. Message Data may be retained longer to the extent reasonably necessary for evidence, legal compliance, dispute resolution, refund handling, fraud prevention, security investigations, protection of lawful rights and interests, or another legitimate business purpose, or where required by law or a competent authority.

Specific statutory retention periods may apply to traffic data, system logs, subscriber information, or certain other categories of data. Glow will retain such data for the periods and on the conditions required by applicable Philippine law, including the Cybercrime Prevention Act of 2012 (Republic Act No. 10175), and by lawful orders or requests of

competent authorities. Such statutory retention does not automatically require all general message content to be retained for the same period.

Where a complaint, dispute, incident, refund request, security matter, or legal requirement arises, Glow may suspend deletion and retain the relevant Message Data for so long as reasonably necessary to verify and handle the matter, to protect the lawful rights and interests of Glow, a Customer, a Technician, or a third party, or to comply with law or a lawful request or order.

Where Message Data is reviewed by systems, artificial-intelligence tools, or authorized personnel, Glow applies access control, event logging, and appropriate security measures.

Security measures: Glow applies technical and organizational measures appropriate to the level of risk, which may include encryption in transit and at rest where appropriate, firewalls, role-based access control, access logging, internal controls, periodic review, and specific measures for location data, health information, Message Data, and other sensitive personal information.

Personal data breach: where a personal data breach occurs, Glow will assess the incident and will notify the National Privacy Commission and affected data subjects within the period and in the manner required by the Data Privacy Act of 2012, its Implementing Rules and Regulations, and applicable National Privacy Commission issuances.

Retention: Glow will retain Personal Data only for so long as reasonably necessary to fulfill the purposes of processing, or until the expiry of the retention period required by applicable law, whichever is later. Certain records, including tax, accounting, and legal records, must be retained even where a data subject requests deletion.

Deletion upon request: Glow will take reasonable steps to delete or otherwise lawfully dispose of Personal Data as soon as practicable following a valid request, subject to applicable legal obligations, ongoing investigations, and backup-cycle limitations. Data held in backup media may be deleted through the ordinary overwrite or backup cycle, provided that Glow does not actively restore or use that data for a new purpose.

On expiry of the applicable retention period, Glow may delete Personal Data or convert it into data that is genuinely de-identified or aggregated so that an individual can no longer reasonably be identified. Glow may retain and use such de-identified or aggregated data for statistics, service analysis, safety analysis, product development, and operational planning, for so long as the data cannot reasonably be linked back to an identifiable individual.

G. CHILDREN AND MINORS

The Services are not intended for persons under eighteen (18) years of age. Glow does not knowingly collect Personal Data from minors for the purpose of using the Services. If Glow becomes aware that it has collected data from a person who is not eligible to use the Services, Glow will take reasonable steps to delete, destroy, or otherwise lawfully handle that data promptly, subject to applicable legal obligations.

H. PERSONAL INFORMATION CONTROLLER AND DATA PROTECTION OFFICER

GLOW BOOKING TECH INC.

Registered office: Unit D, 3rd Floor, Prestoza-Borcelis Commercial Building, Tanza-Trece Road, Landmass Park Subd., Biga 4108, Tanza, Cavite, Philippines

Telephone: +63 46 889 6200

Data Protection Officer: support@glowphilippines.com

User support and data-subject requests: support@glowphilippines.com

Security and data-breach contact: support@glowphilippines.com

Glow has designated a Data Protection Officer in accordance with the Data Privacy Act of 2012 and applicable National Privacy Commission issuances, and is in the process of registering its data processing systems with the National Privacy Commission.

For requests concerning Personal Data, please use the channels above. Glow may request information reasonably necessary to verify the identity or authority of a requester before acting on a request.

I. CUSTOMERS REQUIRING PARTICULAR CARE

For Customers who are pregnant, elderly, or who voluntarily provide health information relevant to service safety, Glow will process and disclose to the assigned Technician only the information reasonably necessary for the requested Service and only within the scope the Customer has permitted and the law allows. A Technician may decline a booking where there is a reasonable basis to believe that the Technician is not qualified or able to perform the Service safely. Glow does not assess or certify the professional competence of a Technician for such cases.

J. CHANGES TO THIS POLICY

Glow may amend this Policy to reflect changes in applicable law or in the operating model. Each new version will be published with an effective date. Material amendments affecting the scope of processing, cross-border transfers, retention periods, or the rights of data subjects will be communicated through reasonable prior notice and, where required by applicable law or the nature of the change, Users will be asked to provide a renewed affirmative confirmation before continuing to use the affected feature. Amendments will not apply retroactively unless permitted by law.