

PRIVACY NOTICE **FOR CLIENTS**

When you engage the services of **Lacson & Lacson Insurance Brokers, Inc.** (“we”, “us”, LLIBI), you entrust us with your personal information. This Privacy Notice explains what data we collect, why we collect it, and how we handle it. Please review this notice carefully to understand our practices and your rights as the data subject.

Our Commitment LLIBI is committed to safeguarding your privacy and upholding your rights regarding your personal data. This notice details our methods for collecting, using, disclosing, and managing your personal information, ensuring transparency and accountability in accordance with the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations, and relevant National Privacy Commission (NPC) issuances.

What we collect This notice applies to all clients of LLIBI from whom we collect personal and sensitive personal information, as necessary, for arranging and managing insurance policies, claims assistance, fraud prevention, and compliance with regulatory requirements.

Depending on the type of insurance policy and applicable regulations, we may collect and process the following personal data:

- **Personal identification details** (name of insured, beneficiaries, dependents, authorized representatives (if applicable); birthdate, age, gender, civil status, nationality, occupation, employer, address, email address, telephone/mobile number)
- **Sensitive personal information** (medical records including diagnosis/chief complaints, confinement and claims details, prescribed medications, laboratory results, medical certificates, annual physical examination results; biometric data)
- **Government-issued identification documents** (passport, driver’s license, Social Security/Tax Identification numbers, and other government-issued numbers as required for Know-Your-Customer (KYC) and Anti-Money Laundering (AML) compliance)
- **Policy and underwriting information** (policy numbers, coverage details, endorsements, claims history, and other risk-related data)
- **Company profile and corporate information** (for corporate clients: corporate documents, authorized signatories, and other KYC/AML requirements)
- **Financial information** (premium payments, bank account details, billing records, receipts, and details of other necessary transactions)
- **Claims information** (incident reports, medical evaluations, and other necessary claims documentation)
- **Communication and interaction records** (correspondence with us, insurers, reinsurers, healthcare providers, adjusters, and other service providers; call recordings where applicable; and data captured by LLIBI surveillance systems when you visit our offices)
- **Regulatory and compliance information** (information required under issuances of the Insurance Commission, Anti-Money Laundering

Council, and other applicable regulatory bodies, including customer due diligence and source-of-funds information)

- **Other information** necessary for the performance of our brokerage services, legal compliance, fraud detection and prevention, dispute resolution, and the protection of lawful interests.

When you provide us the data of another person, you represent that you are authorized and have obtained the requisite consent. When you designate a minor as a beneficiary or dependent under your insurance program, we will collect the necessary information from you, whether you are the parent, legal guardian, or acting on behalf of your organization.

When local regulations permit or so require and to the extent allowed by applicable laws, we may also source the above and other categories of personal information from third parties such as in compliance with our AML and sanctions screening duties.

As your insurance broker, we rely on the information you provide. You are expected to give us complete, accurate, and up-to-date information and to promptly inform us of any material changes.

Why We Collect Them

We process your personal and sensitive information to:

- respond to your inquiries, enhance our services, and address concerns;
- maintain effective communication;
- confirm your membership and verify your identity and coverage;
- arrange suitable insurance coverage with insurers and providers which may include preparing and securing insurance quotations;
- arrange suitable insurance placement, renewal, invoicing, and surveys;
- properly administer the contracted services, benefits, and obligations;
- facilitate claims processing and settlement including healthcare claims which involve obtaining, examining, and processing of medical records;
- share relevant service information, updates, and announcements to the members;
- implement AML and Terrorism Financing measures;
- comply with legal obligations or law enforcement requirements;
- mitigate risks to life or health; or
- conduct other activities subject to your prior consent.

Your information, whether shared with us electronically or manually, is managed securely and confidentially, following our strict information security policies to prevent fraud and protect your rights as the data subject.

Your Rights and How to Exercise Them

Under the DPA, you are entitled to certain rights regarding the collection, processing, and storage of your personal data.

- The right to be fully informed, to access your personal and/or sensitive personal information, and to request for a copy of the personal and/or sensitive personal information we have on file. This includes your right to data portability which would allow you to obtain and electronically copy your personal data in a secure format, where technically feasible.

- The right to object to the processing of your personal information and the right to withdraw consent. By withdrawing your consent, however, please note that we may be unable to continue providing certain services to you.
- The right to request for your personal and/or sensitive personal information to be rectified or updated, to ensure that your personal and/or sensitive personal information on file is reliable, accurate, complete, and as current as possible. We will be happy to assist you with this, subject to receipt of a written request or a request made through our recorded lines.
- The right to request for your personal and/or sensitive personal information to be erased or deleted from our files.
- The right to lodge a complaint or report any misuse of your personal and/or sensitive personal information.

**Who Collects
Your Data and
How to Contact
Them**

We collect data via physical forms, emails, phone calls, or company representatives authorized by you. Collection is conducted exclusively by authorized personnel such as Client Care Executives, Corporate Account Executives, Account Officers, or Business Development Officers, and always with your consent or based on legal grounds. Collection is limited strictly to necessary data for purposes stipulated herein.

**With Whom Will
We Share the
Data**

We share your data for legitimate purposes, in compliance with our contractual and regulatory obligations, or on a need-to-know basis. We will transfer only the data necessary to fulfill the purpose/s and ensure to transfer the data in a secure manner.

We may share the information with our legal counsel, auditors, and service providers who we engage with for support services or in the fulfilment of our obligations. We may also share them with insurers and their underwriters, healthcare providers and medical professionals, adjusters, and other relevant third parties for them to assess whether they may insure you, at what price, and at what terms they would be willing to do so. If such partners are already providing you insurance coverage and the information submitted is in respect of a claim, the information will be used to facilitate settlement of your claim.

Where possible, we may share anonymized or statistical data with other parties to limit the processing of your personal data.

In cases not required by law, such arrangements are covered by the appropriate data sharing agreements and non-disclosure/confidentiality agreements to ensure the same level of protection is observed by the third party.

Where a valid request from a competent authority is received, we may also submit your information to such agencies or regulators for the fulfilment of their functions.

**How We Protect
your Information**

We employ a combination of reasonable physical, technical, and organizational safeguards to protect your personal data from unauthorized access, misuse, loss, alteration, or destruction. These measures include, but are not limited to:

- *Physical Security:* Our offices maintain controlled access points, with CCTVs in place, to safeguard confidential client, policy, and claims information.
- *Technical Security:* Our servers and digital systems are regularly scanned for vulnerabilities, maintained through backups, and updated to address security threats. Electronic data is stored securely in encrypted servers, with cloud backups managed in compliance with industry best practices. Access to electronic data is restricted to authorized personnel only.
- *Organizational Security:* Employees with access to personal data are knowledgeable in data security protocols and privacy practices.

Furthermore, we strictly prohibit the selling, trading, or renting of your personal data. Your data will only be shared or processed when necessary for legitimate business purposes, as outlined in this Privacy Notice, and will not be disclosed to third parties without your consent unless required by law.

Storage and Retention

All personal data, whether in electronic or physical form, is stored securely at our main office, with back-ups maintained in secure cloud-based systems. Certain electronic records are stored directly in cloud infrastructure. Data stored in the cloud may be hosted outside of the Philippines. In such cases, we ensure that appropriate safeguards, contractual protections, and security measures are in place to protect your personal data in accordance with applicable data privacy laws and regulatory requirements. Personal data is retained only for as long as necessary to fulfill the purposes for which it was collected, or as required by legal or regulatory obligations. All AMLC-related documentations are retained during the business relationship plus five (5) years thereafter; tax-related records are kept for ten (10) years.

Physical documents are stored securely at our offices during the applicable retention period. Once that period expires, records are promptly destroyed in a secure manner. Where necessary, records may be temporarily stored in secure off-site archival facilities solely for destruction (ex. physical shredding) scheduling and legal or compliance purposes. Electronic records are permanently deleted from our systems in accordance with our data retention schedule once the applicable retention period has lapsed.

After deletion or destruction, we may retain information in anonymized form for business analytics and operational improvement purposes. Anonymized data does not identify you and cannot reasonably be used to re-identify you.

Integrity and Retention of Personal Information

We strive to maintain accurate, complete, and current personal information. For data access or correction requests, please contact our representatives or Data Protection Officer. Requests may require supporting documentation. Following the required retention period or upon request, your information is permanently deleted from our electronic systems and securely disposed of physically, if with hardcopies.

**Changes and
Updates to This
Privacy Policy**

Our Privacy Policy may change from time to time to comply with applicable laws and regulations and to reflect changes to our information practices. We will post updates in our website, and if the changes are significant, we will provide a more prominent notice (such as an e-mail notification of privacy policy changes). We will also keep prior versions of this Privacy Policy in an archive for your review.

Contact Us

For any inquiries, feedback, requests, or complaints regarding our Privacy Policy, you may contact our Data Protection Officer through the following:

E-mail: privacy@llibi.com

Address: 15/F Burgundy Corporate Tower, 252 Sen. Gil Puyat Ave.,
Makati City, Metro Manila, Philippines.

We commit to respond to you within 10 days of receiving your complaint, inquiry, or feedback.

Updated February 24, 2026