Privacy Policy

Waves For Water Philippines

1. Our Commitment

Waves for Water Organization, Inc. doing business as **Waves For Water Philippines** ("Waves For Water," "W4W", the "Organization," "we," "us," or "our") is committed to protecting and safeguarding the legal rights of our donors, beneficiaries, communities, volunteers, employees, partners, and website users with respect to their personal information. This Privacy Policy explains how we collect, use, store, share, protect, and dispose of personal information, and the rights available to data subjects.

We process personal information in accordance with the Data Privacy Act of 2012 (Republic Act No. 10173, the "DPA"), its Implementing Rules and Regulations ("IRR"), and the issuances of the National Privacy Commission ("NPC"), guided by the principles of transparency, legitimate purpose, and proportionality.

2. Scope

This Policy applies to all personal information processed by the Organization in the course of its programs and operations, whether collected in physical or electronic form, and covers the following data subjects:

- Donors and prospective donors, including individuals donating through payment platforms;
- Beneficiaries and members of communities we serve, including participants in WASH and disaster response programs;
- Volunteers, employees, job applicants, trustees, and officers;
- Partners, suppliers, contractors, and representatives of partner organizations and government agencies; and
- Visitors to our website, social media pages, and events.

It covers all data subjects whose personal information we collect, whether through physical forms, digital channels, or partner organizations and individuals.

3. Definitions

- **Personal information** — any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained, or which, when put together with other information, would directly and certainly identify an individual.
- **Sensitive personal information** — personal information about, among others, an individual's race, ethnic origin, health, education, genetic information, religious, philosophical or political affiliations, government-issued identifiers (such as TIN, SSS, or PhilHealth numbers), and other information classified as sensitive under the DPA.
- **Processing** — any operation performed upon personal information, including collection, recording, organization, storage, updating, retrieval, use, consolidation, disclosure, or destruction.
- **Consent** — any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic, or recorded means, and may be given on behalf of a data subject by a lawfully authorized agent.
- **Filing system** — any structured set of information relating to natural or juridical persons which is organized, whether by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible.

4. Personal Information We Collect

We collect only the personal information necessary for our declared, specified, and legitimate purposes, which may include:

- **Donors:** name, contact details (email address, mobile number, address), donation amount and history, payment reference numbers, TIN (where a Certificate of Donation is requested), and communication preferences. We do not collect or store complete card numbers, CVVs, or e-wallet credentials; these are processed directly by our authorized payment providers.
- **Beneficiaries and communities:** name, age, address or community location, household information, and, where necessary for program delivery and monitoring, health- or sanitation-related information, photographs, and video recordings.

- **Volunteers and employees:** identification and contact details, government-issued identifiers, emergency contacts, and employment- or engagement-related records.
- **Website and online interactions:** device and usage information such as IP address, browser type, and cookies or similar technologies used for website functionality and analytics.

5. How We Collect Personal Information

- Directly from the data subject, through donation forms, registration forms, surveys, program intake documents, correspondence, and events, and digital platforms;
- From payment platforms and processors (such as Xendit) that transmit donor and transaction details necessary to record, verify, and acknowledge donations;
- From partner organizations, local government units, and community leaders, in connection with program implementation; and
- Automatically, through our website and online channels.
- From publicly available sources where lawful and relevant

6. Purposes of Processing

We process personal information for the following purposes:

- Processing, recording, acknowledging, and receipting donations, and issuing certificates of donation where applicable;
- Planning, implementing, monitoring, and evaluating our clean water, WASH, and disaster response programs;
- Communicating with donors, volunteers, beneficiaries, and partners, including sending updates, reports, and, with consent, fundraising communications;
- Recruiting, engaging, managing, and supporting employees and volunteers;
- Complying with legal and regulatory obligations, including those under tax, anti-money laundering, labor, and corporate laws, and cooperating with lawful requests from government authorities;
- Maintaining the security of our premises, systems, and records; and
- Establishing, exercising, or defending legal claims.

7. Legal Bases for Processing

We process personal information only where a lawful basis exists under Sections 12 and 13 of the DPA, including:

- **Consent** of the data subject, obtained prior to collection or as soon as practicable and reasonable, and evidenced by written, electronic, or recorded means;
- **Contract** — where processing is necessary and related to the fulfillment of a contract with the data subject, or in order to take steps at the request of the data subject prior to entering into a contract;
- **Legal obligation** — where processing is necessary for compliance with a legal obligation to which the Organization is subject;
- **Vital interests** — where processing is necessary to protect the life and health of the data subject or another person, such as in humanitarian and disaster response operations;
- **Legitimate interests** — where processing is necessary to pursue the legitimate interests of the Organization or a third party, except where overridden by the fundamental rights and freedoms of the data subject.

Sensitive personal information is processed only in the cases permitted under Section 13 of the DPA, such as with the specific consent of the data subject or where required by law.

8. Consent

- The Organization shall always obtain the consent of the data subject where consent is the applicable basis of processing. Consent refers to any freely given, specific, informed indication of will whereby the data subject agrees to the collection and processing of his or her personal information.
- Consent shall be evidenced by written, electronic, or recorded means.
- Data subjects may withdraw consent at any time, without affecting the lawfulness of processing carried out prior to withdrawal, by contacting our Data Protection Officer.

9. Sharing and Disclosure of Personal Information

We do not sell, rent, or trade personal information. We share personal information only as follows:

- **Payment providers.** Donor and transaction information is shared with Xendit and other authorized payment providers solely to process, verify, confirm, and, where applicable, refund donations. These providers process such information under their own privacy policies and applicable BSP regulations.
- **Service providers.** We may engage personal information processors (e.g., IT, cloud storage, accounting, and audit providers) under contracts requiring confidentiality and security measures consistent with the DPA.
- **Partners and funders.** Aggregated or, where necessary and with appropriate safeguards or consent, identifiable program data may be shared with partner organizations and funders for program coordination, monitoring, and reporting. Data sharing with other personal information controllers shall, where required, be covered by a data sharing agreement consistent with NPC issuances.
- **Government authorities.** We may disclose personal information where required by law, regulation, court order, or lawful government request, including to the BIR, SEC, NPC, and law enforcement agencies.
- **Cross-Border Transfers**.Where personal information is transferred outside the Philippines (for example, to cloud services or our international affiliate), the Organization remains accountable and shall ensure a comparable level of protection through contractual or other reasonable means, consistent with Section 21 of the DPA.

10. Protection of Beneficiaries, Children, and Vulnerable Groups

- We apply heightened safeguards to the personal information of beneficiaries, particularly children and members of vulnerable communities. Where the data subject is a minor, consent shall be obtained from a parent or legal guardian, and the minor shall be informed in an age-appropriate manner.
- Photographs, videos, and stories of beneficiaries are collected and published only with informed consent, in a manner that preserves the dignity of the individuals and communities concerned, and consistent with applicable child protection laws and safeguarding standards.
- No personal information is used for profiling, discrimination, or beneficiary targeting inconsistent with humanitarian principles.

11. Security Measures

The Organization implements reasonable and appropriate organizational, physical, and technical measures to protect personal information against accidental or unlawful destruction, alteration, and disclosure, and against any other unlawful processing, including:

- **Organizational:** appointment of a Data Protection Officer; privacy and security policies; privacy training for employees and volunteers; access limited to authorized personnel on a need-to-know basis; and confidentiality undertakings.
- **Physical:** secure storage of physical records in locked cabinets and controlled premises, and secure disposal of records through shredding or equivalent means.
- **Technical:** safeguards to protect our computer network against accidental, unlawful, or unauthorized usage, or interference with or hindering its functioning or availability, including access controls, passwords, encryption where appropriate, malware protection, and regular data backups.
- The Organization conducts regular monitoring for security breaches and maintains a process for taking preventive, corrective, and mitigating action against security incidents that may lead to a personal data breach.

12. Confidentiality

Employees, volunteers, and other personnel of the Organization who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality where such information is not intended for public disclosure. This obligation continues even after leaving the service, transfer to another position, or termination of employment or contractual relations.

13. Personal Data Breach Management

- The Organization maintains a security incident management policy and a data breach response team responsible for containing, assessing, and remediating security incidents and personal data breaches.
- Where a personal data breach requiring notification occurs — involving sensitive personal information or information that may enable identity fraud, where there is reason to believe the information has been acquired by an unauthorized person and the breach is likely to give rise to a real risk of serious harm — the Organization shall

notify the NPC and the affected data subjects within seventy-two (72) hours from knowledge of, or reasonable belief in, the breach, in accordance with the DPA and NPC issuances.

- The Organization documents all security incidents and personal data breaches, including their facts, effects, and the remedial actions taken.

14. Retention and Disposal

Personal information is retained only for as long as necessary for the fulfillment of the purposes for which it was collected, for the establishment, exercise, or defense of legal claims, or as required by applicable laws and regulations (such as tax and accounting rules requiring retention of records for prescribed periods). Thereafter, personal information is securely destroyed or disposed of, or anonymized, in a manner that prevents further processing or unauthorized access.

15. Rights of Data Subjects

Subject to the conditions and limitations under the DPA, every data subject has the right to:

- **Be informed** whether personal information pertaining to him or her is being or has been processed, and of the details of such processing;
- **Object** to the processing of his or her personal information, including for direct marketing purposes;
- **Access** his or her personal information held by the Organization, upon reasonable request;
- **Rectification** — to dispute inaccuracies or errors and have them corrected;
- **Erasure or blocking** — to suspend, withdraw, or order the blocking, removal, or destruction of personal information that is incomplete, outdated, false, unlawfully obtained, or no longer necessary;
- **Data portability** — to obtain a copy of personal information processed electronically in a structured and commonly used format;
- **Damages** — to be indemnified for damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of personal information; and
- **File a complaint** with the National Privacy Commission.

To exercise these rights, data subjects may contact our Data Protection Officer using the details below. We will respond to requests within a reasonable period and in accordance with the timelines under the DPA and NPC issuances. These rights may also be exercised by the data subject's lawful heirs or assigns in the circumstances allowed by law.

16. Website, Cookies, and Online Channels

Our website and online donation pages may use cookies and similar technologies to enable core functionality, remember preferences, and generate aggregate analytics. Users may manage cookies through their browser settings; disabling certain cookies may affect website functionality. Our channels may contain links to third-party sites (including payment pages operated by Xendit), whose privacy practices are governed by their own policies.

17. Compliance

The Organization shall comply with all applicable laws and regulations of the Philippine government relating to data protection, including the DPA, its IRR, and NPC circulars and advisories, and shall register its data processing systems with the NPC where required.

18. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in law, regulation, or our practices. The latest version, with its effective date, will be posted on our website and made available at our office. Significant changes will be communicated through appropriate channels.

19. Contact Information / Data Protection Officer (DPO)

For questions, concerns, or requests relating to your personal information, including the exercise of your rights under the Data Privacy Act, you may contact our Data Protection Officer through the following channels:

Data Protection Officer
Waves For Water Philippines
3/F One Salcedo Center, 170 Salcedo Street,

Legaspi Village, Makati City, Philippines

Email: dpo@wavesforwater.org

The Data Protection Officer is responsible for overseeing compliance with the Data Privacy Act, responding to data subject requests, managing privacy-related inquiries, and coordinating with the National Privacy Commission when required.

Requests or concerns submitted to the DPO will be acknowledged within a reasonable period and processed in accordance with NPC rules and the Organization's internal privacy procedures.