

# Just Life Group Limited

## Privacy Policy for Customers

### 1. Purpose and application

Just Life Group Limited (**Just Life**) owns and operates a number of brands that share the goal of helping New Zealanders to live a healthy life in a healthy home, including but not limited to:

- Just Water
- About Health
- Herbal Ignite (Intenza)
- Natural Solutions
- Designer Tanks
- Hometech
- Solatube
- The Cylinder Guy
- Unovent

Together, Just Life and the brands listed above form the **Just Life Group**.

This policy applies to all the companies and brands in the Just Life Group, and sets out how we will collect, use, store, disclose and protect our customers' personal information. All references to "we", "us" and "our" in the policy refer to each member of the Just Life Group.

We comply with the New Zealand Privacy Act 2020 (the Act) when dealing with your personal information. Personal information is defined as information about an identifiable individual (a natural person).

### 2. Collection of Information

We collect personal information about you from:

- you, when you provide that personal information to us, including via the website and any related service, through any registration or subscription process, through any contact with us (e.g., telephone call or email), or when you buy or use our services and products.
- third parties where you have authorised this or the information is publicly available (for example, a credit check through Equifax or Centrix).

If possible, we will collect personal information from you directly. We use information:

- To verify your identity (we may ask you for your D.O.B. or your last payment amount);
- To provide services and products to our customers.

- To undertake credit checks.
- To invoice and collect money that is owed to us, including authorising and processing credit card and direct debit transactions.
- To respond to communications from our customers.
- To carry out market, product, and customer analysis.
- To protect and/or enforce our legal rights and interests, including defending any claim; and
- Any other purposes as authorised under the Act.

We may use your information to offer you products and services of any member of the Just Life Group that we believe meet your needs. You can notify us at any time if you do not wish to receive these offers by emailing us at [privacyofficer@justlife.co.nz](mailto:privacyofficer@justlife.co.nz) or writing to us at *Privacy Officer, Just Life Group, Private Bag 92-811, Penrose, Auckland, 1642*. We will act promptly on any such request.

### 3. Disclosing Information

We may disclose information to:

- Our employees, contractors, and other members of the Just Life Group.
- Any business that supports our services and products, including any person that hosts or maintains any IT systems.
- A credit check company for the purpose of credit checking a current or potential new customer.
- A debt collection agency where an account remains unpaid.
- A person who can require us to supply personal information (e.g., a regulatory authority).
- Any person authorised by the Act or any other law (e.g., a law enforcement agency).
- Liquidators, administrators, or other persons appointed to administer your financial affairs.
- Any person authorised by the customer of whom the personal information is being disclosed.

Some of the persons listed above may be located overseas. We will only transfer your personal information to a recipient that is obliged to protect your personal information with comparable safeguards to those contained in the Act and in compliance with the relevant privacy laws and regulations of the recipient country or otherwise we will obtain your express consent to transfer the personal information overseas.

We may disclose, sell, or transfer to third parties any non-personal, aggregated information that we collect from you and our other customers.

### 4. Storage and Security of Personal Information

We will take reasonable steps to keep your personal information safe from loss, unauthorised access and disclosure or any other misuse.

However, we cannot guarantee that all personal information cannot be accessed by an unauthorised person (forexample, a hacker) or that unauthorised disclosure will not occur.

The following steps are taken by us to help keep information secure:

- Policies and procedures are in place. Employees are aware of the policies and procedures and follow them. Where a policy or procedure has not been followed, feedback and corrective action is undertaken.

- Access to physical documents is appropriately restricted to the relevant employees.
- Access to personal information is limited to those employees with a demonstrable need. Digital footprints can be tracked if required.
- Information, including physical documents, are only disposed of securely.
- Software is kept regularly updated to ensure that known vulnerabilities are addressed promptly; and
- Backups are performed regularly and kept securely.

## 5. Accessing and Correcting your Personal Information

Subject to certain grounds for refusal set out in the Act, you have the right to access your readily retrievable personal information that we hold and to request a correction to your personal information. Before you exercise this right, we will need evidence to confirm that you are the individual to whom the personal information relates.

You can request access to your information by emailing us at [privacyofficer@justlife.co.nz](mailto:privacyofficer@justlife.co.nz)) or writing to us at [The Privacy Officer, Private Bag 92811, Penrose, Auckland 1642.]. This service is free unless the information you request requires significant research or preparation time. Before we act upon requests of this nature, we will tell you how much this service will cost.

This policy does not limit or exclude any of your rights under the Act. If you wish to seek further information on the Act, see [www.privacy.org.nz](http://www.privacy.org.nz).

## 6. Internet Use

While we take reasonable steps to maintain secure internet connections, if you provide us with personal information over the internet, the provision of that information is at your own risk.

If you post your personal information on any websites, social media sites, or chat rooms, you acknowledge and agree that the information you post is publicly available.

If you follow a link on our website to another site, the owner of that site will have its own privacy policy relating to your personal information. We suggest you review that site's privacy policy before you provide personal information.

We use cookies (an alphanumeric identifier that we transfer to your computer's hard drive so that we can recognise your browser) to monitor your use of the website. You have the option to disable cookies by changing the settings on your browser, although this may mean that you cannot use all the features of the website.

## 7. Data Retention

We retain personal information only for as long as we need it to continue to provide you with our services, maintain the security of our websites or as required by law.

## 8. Privacy Breaches

A privacy breach occurs when an organisation or agency does not comply with one or more of the Information Privacy Principles set out in section 6 of the Act. A breach of a privacy

principle can occur without causing serious harm to an individual.

If a suspected breach of privacy has occurred, we will follow the 'Notify Us' guidelines and assessment-based tool, as provided by the Privacy Commissioner:

- Step 1: **Contain** the breach and make a first assessment.
- Step 2: **Assess** the impact of the privacy breach - evaluate the risks.
- Step 3: **Notify** affected people (If necessary)
- Step 4: **Prevent** a repeat.

### **Step 1: Contain the breach and make a first assessment.**

- **Contain the breach.** Depending on the type of breach, stop the unauthorised practice, try and get back the records/lost information, consider disabling the system that was breached, cancel or change the computer access codes and try to fix any weaknesses in the physical or electronic security.
- Our **Privacy Officer** will be appointed to **lead the initial investigation**.
- **Determine whether a team needs to be put together.** It may be people in and outside the business, depending on the expertise required.

### **Step 2: Assess**

- Just Life will assess the seriousness of a privacy breach by using the [NotifyUs](#) tool; a resource tool from the Privacy Commissioner.

### **Step 3: Notify affected people as identified by NotifyUs tool**

- If the assessment from NotifyUs identifies the breach as Notifiable, then we will notify the Privacy Commissioner.
- And those individuals affected (depending on the circumstances we may need to notify the Police and our insurers).
- We will endeavour to notify affected individuals directly – by phone, letter, email or in person. Indirect notification will only occur where direct notification could cause further harm, is prohibitively costly or the contact information is not known.

If individuals could suffer harm because of our organisation's privacy breach, we will inform them (unless an exception applies). We will be prompt and open about the breach for individuals to have the opportunity to protect themselves (for example, they may need to change their passwords or monitor their bank accounts for malicious activity).

When we are informing individuals about a breach of privacy, the type of information we will let them know is the following:

- Information about the incident, including when it happened.
- A description of the personal information that has been disclosed and what has not been disclosed.
- What we are doing to control or reduce the harm.

- What we are doing to help people and what steps they can take to protect themselves.
- Contact information for enquiries or complaints.
- Whether we have notified the Office of the Privacy Commissioner.
- Contact information for the Privacy Commissioner.

#### **Step 4: Prevent a repeat.**

Following a breach, we will investigate the cause of the breach and make changes to our prevention plan and how it is being applied. The amount of effort will reflect the significance of the breach and whether it happened because of a systematic problem or an isolated event. It could include:

- A security audit of both physical and technical security.
- A review of policies and procedures.
- A review of employee training procedures.
- A review of any service delivery partners caught up in the breach.

#### **WHAT TO DO IF YOU THINK WE HAVE MADE AN ERROR**

We are committed to protecting your privacy and our policies, processes and systems have been developed with this in mind. However, if you think we have made an error, please email us at [privacyofficer@justlife.co.nz](mailto:privacyofficer@justlife.co.nz) or write to us at *Privacy Officer, Private Bag 92-811, Penrose, Auckland 1642*, to let us know. Where we have made an error, we will endeavour to correct the error as soon as reasonably practicable.

#### **QUESTIONS AND COMPLAINTS**

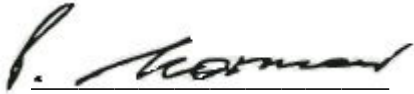
If you have a question or complaint about the way we have dealt with your personal information, please contact us by email or in writing at the addresses above. We will endeavour to respond promptly to your question or complaint. If we cannot adequately address your privacy concerns, you have the right to complain to the Office of the Privacy Commissioner. For more information on privacy see the Privacy Commissioner's website: <https://www.privacy.org.nz/>

#### **CHANGES TO POLICY**

We may change this policy at any time by publishing the amended policy on our website. We will endeavour to inform you of any changes to the policy by email or on the website.

## 9. Policy Approval Date

This policy was approved by the board of Just Life Group Limited on the 21<sup>st</sup> April 2023. This policy will be reviewed periodically to ensure its relevance and effectiveness.



Phil Norman  
Chair  
Just Life Group Limited

Policy Owner: Board	Approved Date: 21 April 2023	Next Review Date: April 2024
---------------------	------------------------------	------------------------------