

Just Life Group Limited

Privacy Policy

1. Purpose

Just Life Group Limited ("Just Life") complies with the New Zealand Privacy Act 1993 (the Act) when dealing with personal information. Personal information is defined as information about an identifiable individual (a natural person).

This policy sets out how we will collect, use, store, disclose and protect our customers' personal information.

2. Collection of Information

We collect information from:

- The individuals themselves when they provide the personal information, including through their signed agreement and through any contact with us (phone, email, text, chat); and
- Third parties where you have authorised this or the information is publicly available (for example, a credit check through Centrix).

3. Use of Information

We use information:

- 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 transactions 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.
- Any other purposes as authorised under the Privacy Act 1993.

4. Disclosing Information

We may disclose information to:

- Any business that supports our services and products, including any person that hosts or maintains any IT systems. Such a business may be located outside of New Zealand. This may mean personal information is held outside New Zealand;
- 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 Privacy Act or any other law (e.g. a law enforcement agency);
- Any person authorised by the customer of whom the personal information is being disclosed.

5. Storage and Security of Personal Information

We store personal information collected from our customer's and we will take all reasonable steps to keep the personal information safe from loss, unauthorised activity or any misuse.

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

The following steps are taken by Just Life 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;
- Backups are performed regularly and kept securely.

6. 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 Privacy Act 1993. A breach of a privacy principle can occur without causing harm to an individual.

If a suspected breach of privacy has occurred, Just Life will follow the Data breach notification guidelines, as provided by the Privacy Commissioner:

Step 1: Contain the breach and make a first assessment

Step 2: 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, 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.
- **Communicate with those who need to know.** Consider whether Marsh Insurance needs to be informed, as well as the auditors. If the breach is due to criminal activity, inform the Police.

Step 2: Evaluate the risks

The following is a best practice guide from the Government Chief Privacy Officer to assist in determining the scale and severity of privacy breaches and evaluate the risks associated with such a breach.

Criteria	Detail	Rating
Number of individuals affected	Single individual	10
	2 – 10 individuals	20
	11 – 50 individuals	40
	51 or more individuals	60
Sensitivity of the information (Select the highest level of sensitivity involved)	Minor sensitivity (e.g. name, employment position)	10
	More sensitivity (e.g. remuneration, contact details)	20
	Sensitive (e.g. financial, biometric)	50
	Highly sensitive (e.g. health, criminal records, information about people at risk, closed records, contact details for vulnerable people)	80
Potential or actual harm to the individual(s) (You can select several types of harm and/or actual harm. If an actual harm occurred, do not select the corresponding potential harm)	No potential or actual harm to the individual(s)	0
	Potential for financial loss to the individual(s)	20
	Potential for identity theft	25
	Actual unwanted intrusion into the individual's personal life	20
	Potential for loss of business, employment or other opportunities for the individual(s)	30
	Individual denied access to/correction of or statement of correction not included with their information without good reason	30
	Actual financial loss to the individual(s)	40
	Potential for physical harm to the individual(s)	50
	Actual identify theft	50
	Actual loss of business, employment, or other opportunities for the individual(s)	50
	Actual hurt, humiliation or reputational damage to the individual(s)	60
	Actual physical harm to the individual(s)	100
Potential or actual harm to the company (If several types of potential and/or actual harm are relevant, select 'more than one type of harm to the company'.	No potential or actual harm to the company	0
	Potential for loss of business opportunity for the company	10
	Potential for financial loss to the company	20
	Potential for reputational damage to the agency	20
	Potential for loss of trust in the company	20
	Loss of business opportunity for the company	20
	Financial loss to the company	40
	Reputational damage to the company	40
	Loss of trust in the company	40
	More than one type of harm to the company	50
Potential for media attention	No media interest occurring or likely to occur	0
	Some media interest occurring or likely to occur	20
	Widespread media interest occurring or likely to occur, and the agency, Privacy Commissioner, and others may be asked for comment	50
Privacy breach source	Inadvertent information handling error (e.g. email or letter sent to incorrect recipient, information provided to the wrong person over the phone)	10
	Information used by the company for a purpose not related to collection, and an exception does not apply	20
	Failure to provide access to personal information within statutory or extended timeframe, or failure to correct or attach a statement of correction to personal information	30
	Theft or loss of property containing personal information (e.g. USB stick, documents)	40

	Information collected by unlawful, unfair or unreasonably intrusive means	50
	Unauthorised access of systems or information (e.g. staff member accessing information not for work purposes and contrary to company policies/procedures)	50
	Systematic system or business process issue (e.g. insufficient security controls, asking for and receiving information not necessary for purpose, not responding to requests, withholding information without good reason, retaining information through an information-matching programme)	60
	Cyber security incident (e.g. hacking)	60
	Information recovered/destroyed and not accessed by an unauthorised individual	1
Status of the privacy breach	Individual provided access to their information, or information corrected/statement of correction included	10
	Information not recovered but encrypted and unlikely to be accessible	20
	Information recovered/destroyed/no physical copy disclosed, and accessed by an unauthorised individual(s)	50
	Information not recovered and accessible	60

The total score from the above is then used to determine the impact of the breach.

Privacy breach impact ratings:

Rating range	Level	Situation Summary	Actions to be Undertaken
0 – 170	1	<ul style="list-style-type: none"> Small number of people affected, with little or no potential or actual harm to the individual(s). Little or no indication of systematic problems within the company. 	<ul style="list-style-type: none"> Company will consider tracking privacy breaches and taking corrective action if there are a number from a similar source.
171 – 220	2	<ul style="list-style-type: none"> Small number of people affected, with minor potential or actual harm to the individual(s). Little or no indication of systematic problems within the company. 	<ul style="list-style-type: none"> Company will track privacy breaches and taking corrective action if there are a number from a similar source.
221 – 270	3	<ul style="list-style-type: none"> Either the information is not sensitive/highly sensitive and the potential or actual harm to the individual(s) is more than minor, or the information is sensitive/highly sensitive and the potential or actual harm to the individual(s) is minor. 	<ul style="list-style-type: none"> Company will track privacy breaches and take corrective action.
271 – 320	4	<ul style="list-style-type: none"> Breach of sensitive or highly sensitive information, with serious potential or actual harm to the individual(s). The incident may imply a systematic failure that could undermine company systems. 	<ul style="list-style-type: none"> Company will track privacy breaches and take corrective action. Affected customers will be notified in accordance with Step 3.

321 and above	5	<ul style="list-style-type: none"> Breach of sensitive or highly sensitive information, with serious potential or actual harm to the individual(s). It is likely that more than one type of harm has occurred, and that harm is likely to be ongoing. 	<ul style="list-style-type: none"> Company will track privacy breaches and take corrective action. Immediate cessation of external access until security verified by external party with appropriate expertise relative to the reason for the privacy breach All potentially affected customers will be notified in accordance with Step 3.
---------------	---	---	--

Step Three: Notify affected people if necessary

Notifying individuals:

- If a privacy breach creates a risk of harm to an individual, those affected should usually be notified.
- If from the above matrix it has been identified as an actual or potential risk or loss to an individual, then it is most likely it is a situation where the individuals should be notified.
- It is always best to notify affected individuals directly – by phone, letter, email or in person. Indirect notification should only occur where direct notification could cause further harm, is prohibitively costly or the contact information is not known.

Breach notifications should generally contain the following information:

- 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 the company is doing to control or reduce the harm;
- What it is doing to help people and what steps they can take to protect themselves;
- Contact information for enquiries or complaints;
- Whether the company has notified the Office of the Privacy Commissioner;
- Contact information for the Privacy Commissioner.

Consider whether any of these third parties need to be notified:

- Police;
- Insurers;
- Credit card companies, financial institutions or credit reporting agencies;
- Third party contractors;
- The Board;
- Union or other employee representatives.

Step Four: Prevent a repeat

Following a breach, the company shall investigate the cause of the breach and make changes to their prevention plan and how it is being applied. The amount of effort should reflect the significance of the breach and whether it happened as a result 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.

7. Policy Approval Date

This policy was approved at the Just Life Group Limited Board Meeting held on the 6th December 2018.

A handwritten signature in blue ink, appearing to read "Tony Falkenstein", is positioned above a horizontal line.

Tony Falkenstein

CEO

Just Life Group Limited

<i>Policy Owner: Audit and Risk Committee</i>	<i>Approved Date: 6th Dec 2018</i>	<i>Next Review Date: June 2020</i>
---	------------------------------------	------------------------------------