Retail Service Provider Privacy Guidelines

Last Updated: 12th April 2022

Tuatahi First Fibre

Contents

Welcome

Introduction

Tuatahi First Fibre (TFF) values the privacy of our mutual end customers. Whilst the Privacy Act 2020 (the Privacy Act) and the Wholesale Services Agreement clearly set out the legal and contractual framework by which we handle personally identifiable information, we recognise the practical application is not always clearly defined and mutually understood.

This guideline is designed to provide clarity to Retail Service Providers (RSPs) in how TFF will handle the information we hold on your behalf (as an agent of an RSP).

Note: This guideline will not detail information that TFF is collecting for its own purposes. The terms by which TFF collects data for its own purposes are covered by the TFF Privacy Notice available from the TFF website (www.tuatahifibre.co.nz).

We always welcome feedback and enquiries from RSP's about how we are handling your data. Please direct any enquiries through your account manager, or directly to TFF's Privacy Officer (privacy@tuatahifibre.co.nz).

Personal Information

Data Minimisation

TFF, and any third parties we sub-contract to, will only collect the minimum personal information about resellers and end users to allow their business operations as an agent of the RSP. TFF is not responsible for defining what should be collected. This is the responsibility of the RSP.

TFF collects information using the following mechanisms on behalf of the RSP:

- Order form
- Transfer form
- Incident form
- Field technician notes
- Field booking information
- Incident information
- Emails from RSPs

Privacy Notices

RSP's are responsible for providing appropriate privacy notices to individuals prior to collection of their personal information by TFF.

The following items hold personal information that is also collected and held directly by TFF in its own capacity as an agency under the Privacy Act. TFF is responsible for providing privacy notices regarding this collection.

- End user consent form
- Neighbour consent form
- LAR Objection
- Competitions/promotions
- Preinstall certificate (in scope)
- Post install certificate
- Net promoter survey requests
- New connection requests received door to door
- Voice recordings of calls to TFF
- Transcripts of conversations through TFF chatbot
- Emails excluding those from RSPs
- CCTV footage.

Storage and Retention

TFF, and any third parties, may store personal information anywhere globally. Information held on behalf of the RSP's will be retained for the period shown below and then disposed of securely.

	Retention Period
Order Form	Until 30 days after a service is terminated (*)
Transfer Form	Until 30 days after a service is terminated (*)
Incident Form/Information	12 Months
Field Technician Notes	12 Months
Field Booking Information	12 Months
Emails from RSPs	Indefinitely

(*) At present these records are being retained indefinitely. Historic records which do not meet this requirement will be removed as part of a Telflow system enhancement in Q2 2022.

In the event that an RSP's Wholesale Services Agreement with TFF is terminated then all personal information held on behalf of the RSP will be either returned or destroyed in accordance with the Wholesale Services Agreement.

Security

TFF will take all reasonable steps to protect personal information from loss, unauthorised access, disclosure, or misuse. This includes all information held by third parties on behalf of TFF. Appendix 1 contains a high-level overview of the organisational and technical controls utilised. Further details are available to RSP's in the TFF Cybersecurity Whitepaper which is available upon request through their TFF account manager.

Third Parties

As part of delivering TFF services, TFF may sub-contract certain functions to third parties. TFF has in place contracts with these third parties that require:

- Notification of any privacy breach.
- Notification of any Privacy Act access or correction requests.
- Maintenance of appropriate security safeguards.
- Enforcement of retention periods and deletion activities.

Privacy Processes

Record of Privacy Officer Contact Details

It is essential that TFF maintains a Privacy Officer point of contact at each RSP in order to enable the processes below to be achieved within the statutory timeframes. We ask that each RSP ensures their account manager is kept up to date with a phone number and email address for their Privacy Officer.

Access or Correction of Personal Information

In the event that TFF (or one of its third parties) receives a law enforcement request or a Privacy Act request from a reseller or end user for personal information held as an agent of an RSP, TFF will transfer the request to the RSP's Privacy Officer, unless legally prohibited from doing so.

If the RSP requires assistance from TFF to respond to a request, assistance can be requested, by email, from the TFF Privacy Officer (privacy@tuatahifibre.co.nz). TFF may, at its sole discretion, charge for any assistance.

Personal Information Usage

TFF will not use personal information without first considering whether it is reasonably accurate, up-to-date, and complete.

Personal information held by TFF on behalf of a RSP will only be used for delivering services to the RSP and their resellers and end users.

TFF may market to, or conduct market research with, end users based on the information provided by the RSP in line with the terms of the WSA.

TFF and associated third parties will keep all information held on behalf of an RSP confidential.

Privacy Breaches

TFF has processes for reporting, managing, and escalating privacy breaches.

Any suspected privacy breach is reported to TFF's Privacy Officer, who will confirm whether there has been a privacy breach. In the event of a confirmed privacy breach involving information held on behalf of an RSP, the retail service provider's Privacy Officer will be notified promptly.

Questions or Complaints

Any questions or complaints about TFF's privacy practices should be directed to TFF's Privacy Officer at privacy@tuatahifibre.co.nz.

Appendix 1
Security Controls

Organisational Controls

- Breach processes
- Business continuity plans
- Configuration management
- Disaster recovery measures
- Incident Response plans
- Management information and reporting
- Management of elevated privileges
- Regular penetration testing
- Regular security controls reviews
- Risk assessments
- Security awareness and training
- Security Policies and Standards
- Segregation of duties.

Technical Controls

- Automation of user account lifecycle following least-privilege principles.
- Anti-Malware measures
- Backups and data replication
- Building security
- Encryption at rest
- Encryption in transit
- Logging, Monitoring and alerting
- Network segregation
- Platform hardening
- Replication of data
- Secure destruction of assets and data
- Shielding against DoS attacks
- Strong Access Control
- Use of datacentres with strong security compliance
- Vulnerability and patch management.

Contact

Jon Edney
TFF Privacy Officer
privacy@tuatahifibre.co.nz

11 Ken Browne Drive
Te Rapa, Hamilton, 3200
tuatahifibre.co.nz

Tuatahi
First Fibre