Frontier Software

Privacy Statement

Author	**VM**
Version Number	**1-2**
Status	**Approved**
Last Updated	**15/10/2020**

Table of Contents

1 Document Management

1.1 Document Revision History

Version	Date	Author	Reason for change
0-1	01/09/2016	Victor Miloshis	Initial Document for Updated Policy
1-0	05/07/2017	Nick Southcombe	Minor corrections and approval.
1-1	22/02/2018	Victor Miloshis	Breach Notification Act, 2018 addition GDPR 2018 addition
1-2	14/10/2020	Victor Miloshis	- Added reference to Frontier Software ISMS - Removed National references in Reference section of this document, given their inclusion in the ISMS Policy document.

1.2 Glossary

Term/Abbreviations	Definition
NDB	Notifiable Data Breach
GDPR	General Data Protection Regulation (EU)

1.3 References

#	Document Name	File Location
1	Frontier Software ISMS Policies	

1.4 Distribution List

Name	Title	Reviewed/Approved
Board	Board	Approved
Nick Southcombe	CEO	Approved
Eugene La Fontaine	National Operations Manager – Managed Services	Approved
Melinda Lee	Quality Assurance Manager	Approved
Steve Pritchet	Finance Director	Review

2 Introduction

2.1 Background Information

Frontier Software is committed to keeping the data provided to it secure, accurate and up-to-date.

In doing so, Frontier Software addresses Privacy with recognition of statutes applied in the many countries it operates, continually assessing its position with global awareness to the changing privacy responsibilities expected of it.

Irrespective of arrangement, data and information which Frontier Software collects, stores or disseminates shall be controlled and under instruction of law and best practice.

Frontier Software is committed to keeping personal data secure and using established and compliant levels of procedure, technology and staff awareness to ensure the highest standard of security afforded to the data in its possession.

Frontier Software recognises the obligations of entities which have:

- legal control or ownership of the data / information;
- physical possession of the data / information.

2.2 Purpose

This document describes Frontier Software's approach and conduct related to its Privacy responsibilities.

2.3 Audience

- Customers
- Employees

3 Privacy

3.1 Awareness

In its treatment of personal information hosted by our Managed / Outsourced Services operation, Frontier Software looks to comply with the provisions of key privacy governances of other sovereignties, as outlined within our organisation's Information Security Management System.

Further reference and guideline, is located in our ISMS Policy document, an internal documented, available at to all, as it is a Public classified document.

Reference : Frontier_Software_ISMS_Policy.pdf

In all cases, Frontier Software seeks to ensure that personal information is afforded the best levels of privacy protection, managed in an open, transparent and law-abiding manner.

3.2 What personal information does Frontier Software collect?

Frontier Software acknowledges that data, if breached, is likely to result in serious harm to any individual to whom the information relates.

With this in mind, in order to fulfil its services commitment to your employer, Frontier Software may be required to collect:

- name,
- date of birth,
- address,
- tax file number,
- banking details,
- superannuation details,
- qualifications,
- performance appraisals,
- details of paid work.

Other detail may be required to be collected depending on changing circumstances.

No detail is divulged without the employer's written request and its authority.

To this, Frontier Software holds no other interest in holding this data beyond the prescribed maximum time, or any other time as requested the employer.

Whilst data categories shall vary due to specific demand, personal data shall be classified as **RESTRICTED** and used only for the purposes it has been designed and intended for.

3.3 Why we collect, use and disclose the information

Frontier Software is expected to collect this information in order to provide accurate services to its customers.

The primary purpose for collecting and storing the information is to maintain an individual's employment record in order to assist the associated needs and legal responsibilities of the Employer, Employee and the Service Provider.

Personal information may also be used in other related Human Resources processes for which Frontier Software has been engaged by Employers - and in an aggregated (non-identifying) form to report on its workforce profiles or to provide it to authorised Agencies.

An authorised Agency is one to which Frontier Software may be asked to contribute under lawful obligation or by direct and written request from an authorised Employer representative.

3.4 Accuracy, Security and Storage of Information

In its Managed Services / Outsourcing Payroll Services operation, Frontier Software will receive and process information that is provided by a Customer's authorised individual(s).

Frontier Software will be provided only that data which the Customer agrees to provide and is considered necessary and relevant to the contracted services required of it.

Frontier Software holds personal information in computer and paper based records and will take all reasonable steps to ensure that this information is protected from misuse, loss, unauthorised access, modification and disclosure.

Frontier Software will further protect its operational security through regular reviews of its network, application and operational conduct through the use of internal audits and external security assessments.

All audits shall be undertaken by suitably qualified personnel.

Unless specified otherwise, Frontier Software will not retain data and information beyond the legal minimum period. This period will be 7 years commencing from the first valid payroll run of a contract's life.

Upon contract cessation, data written on common tape media as a part of the overall service backup process shall remain on that media until such time that its maximum retention period is reached. Beyond this time, the tape media is destroyed in line with its information security practice.

Until that time, information will be retained and may be restored in order to meet relevant information retrieval laws along with the access entitlement of the individual.

3.5 Quality of Personal Information

At all times, information accuracy and quality will be the responsibility of the Customer and its employees.

3.6 Disclosure of Information

Frontier Software will only disclose data or information as required by law, or by its Customer.

At all times, written authority will be required should information be required to be provided to organisations that are beyond the scope of the Contract.

Frontier Software will further protect information disclosure through regular reviews of its network, application and operational conduct through the use of internal audits, along with external security assessment audits by qualified parties.

Frontier Software will provide information only to the Customer's authorised representative(s) requesting that detail.

3.7 Access to Personal Information

Implied through Contract permission, skilled and hence privileged Frontier Software staff have direct access to your personal information only on an as required basis.

Beyond Lawful requirement, access to information by an individual seeking their data will be normally facilitated through their Employer.

Personal information will not be immediately offered, if it is suspected that providing such detail may have undesirable impact on the privacy of others.

A matter such as this is expected to be considered by individuals and their employer beforehand.

Access to and correction of personal information is handled in accordance with relevant sovereign the Freedom of Information Acts.

Applications for access under the relevant Freedom of Information Acts should be addressed to the :

a. For Frontier Software staff
   - Human Resources Manager.

b. For Managed Services / Outsourcing Payroll Services operations
   - National Outsourcing Services Manager.

Employees of organisations whose data Frontier Software hosts must direct all requests through their relevant employer channels.

Frontier Software will not divulge information of a Customer's employees without Customer or employee approval.

3.8 Job Applications

Information provided by job applicants is used solely for the purpose of the recruitment function.

The information is disclosed only to staff and/or relevant panel members involved in the selection process, and will remain **Restricted**.

As a general rule, Frontier Software keeps an electronic copy of all job applications and these are disposed, usually, within a year after the recruitment process is completed.

3.9 Direct Marketing

Frontier Software does not involve itself with the direct marketing of its Customers' employee information.

3.10 Cross Border Data Transfer

Where Frontier Software is legally protected to do so, cross-border data transfers shall only occur by Customer request.

Such requests must be written and be approved by the Customer's authorised representative.

Requests may be reflected in:

- the Contract,
- a Contract Variation,
- ad-hoc documented request.

In doing so, data will only be transferred in approved encrypted or hashed protection manner.

Frontier Software reserves its right to assess its risk when dealing with matters of Data Sovereignty.

3.11 Adoption, Use or Disclosure of Government Related Identifiers

Adoption, use or disclosure of government related identifiers will be determined by the Customer.

3.12 Anonymity and Pseudonymity

Identity obfuscation is provided through the ability of employees to be identified by a numeric representation.

3.13 Dealing with Unsolicited Personal Information

Unless directed otherwise by its Customer, Frontier Software will not deal with unsolicited personal information requests.

If an approach is considered threatening, Frontier Software will report the instance to its Customer and/or appropriate Authorities.

3.14 Collection of Solicited Personal Information

Frontier Software excludes itself from this practice.

Data and information Frontier Software collects as a part of its contracted services to the Customer is used solely for that purpose.

3.15 Privacy Management

Complaints regarding Privacy matters may be addressed to:

1. For Frontier Software employees :
    - Human Resources Manager or Senior Management, escalating to Executive Management where deemed necessary.

2. For Managed Services / Outsourcing Payroll Services Customers:
    - National Outsourcing Manager or Senior Management, escalating to Executive Management where deemed necessary.

3.16 Questions

Questions regarding your privacy and rights in relation information we collect and store are requested to be sent to

Frontier Software at privacy@frontiersoftware.com.au

3.17 Use of Frontier Software IT Facilities

In its use of IT facilities, identities may be momentarily ascertained by the inherent network management security and management system, the solution's application logs, or, a server's operating system logs.

This solutions application log records changes to data. Its recording is configurable by the Customer.

Frontier Software may be asked to assist in any forensic requirement and will do so, turning to its logged detail. Logs are used in the course of managing the solution services

From time to time, access to the Server Operating System logs may be required under general maintenance requirement, or for fault rectification or performance management purpose.

Facilities without exclusion may also be used in the course of authorised investigations into security matters, or authorised disciplinary investigations.

Staff are not permitted access to the logs except to the extent necessary to perform their duties. Information may be disclosed to third parties if we are required or authorised to do so by law.

Email sent or received by staff in the course of Frontier Software duty may be subject to law.