dspanz. digital service providers australia new zealand

Secure Storage and Management of Tax File Numbers and Personal Information

Best Practice Guidance for Australian Business Software Providers

Version 1.0

Executive Summary

The *Secure Storage and Management of Tax File Numbers and Personal Information: Best Practice Guidance for Australian Business Software Providers* investigates best practice controls for managing and securing Tax File Numbers (TFNs) and personal information in software.

This guidance is intended for document management, financial planning, workforce management and practice management software providers in the broader tax, accounting, employer obligation, superannuation, invoicing and business registry ecosystem that operate outside the scope of government security requirements that typically apply to Digital Service Providers (DSPs).

The document provides actionable best practice controls for securely capturing and storing TFNs and personal data, including:

- Data Collection
- Input Validation
- User Authentication
- Secure User Interfaces
- Redaction and Masking
- Role-Based Access Controls
- Logging and Monitoring
- Secure Data Transmission
- Secure API Configurations
- Encryption at Rest
- Data Minimisation: Retention and Disposal
- Secure Backups
- Database Security
- Tokenisation
- Secure Browser Storage
- Security of Cloud Data Centres
- Regular Audits
- Security Training
- Incident Response Planning
- Compliance.

DSPANZ will update this guidance as legislative or best practice security requirements change.

Contents

Introduction

Many Digital Service Providers (DSPs) will capture and store personal data as part of the software products and services they offer to customers. While DSPs comply with a wide range of security requirements to protect their customer's data, there is a lack of clear, actionable guidance for how DSPs should securely collect and store personal data, particularly Tax File Numbers (TFNs), in software solutions.

DSPs interacting with certain government agencies may be required to comply with specific security standards. For example, DSPs directly connecting to the Australian Taxation Office's (ATO) digital services must meet the Operational Security Framework (OSF) and DSPs regulated by the Australian Prudential Regulation Authority must meet Prudential Practice Guide CPS 234.

There is a broader ecosystem of software providers that operate across the tax, accounting, employer obligation, superannuation, invoicing and business registry experiences that are out of the scope of government security requirements that may capture and store TFNs and personal data. Examples of these software products and services can include:

- Corporate compliance and company secretarial software
- Document management software
- Financial planning software
- Workforce management software (e.g. human resources, time and attendance)
- Investment management software
- Practice management software
- Self Managed Super Fund (SMSF) management software.

DSPANZ has produced this guidance to support the broader DSP ecosystem in implementing best practice controls for handling and protecting TFN and personal data in software products and services.

Definitions

Digital Service Provider:
Digital Service Providers, or DSPs, create, sell, and use software solutions to securely capture, transmit, and share information. These solutions are commonly used in the day to day management of a business and its employees.

This guidance particularly considers document management, financial planning, HR and workforce management and practice management software solutions.

Personal Information:
Personal information includes a broad range of information or opinions that could identify an individual. Personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances.

Personal information may include:

- An individual's name, signature, address, phone number or date of birth
- Credit information
- Employee record information
- Internet protocol (IP) addresses
- Location information from a mobile device
- Photographs
- Sensitive information (see below)
- Voice print and facial recognition biometrics.[1]

Sensitive Personal Information:
Sensitive Personal Information is personal information that includes information or an opinion about the following relating to an individual:

- Criminal record
- Health or genetic information
- Political opinions or associations
- Racial or ethnic origin
- Sexual orientation or practices
- Some aspects of biometric information
- Trade union membership or associations.

Sensitive personal information generally involves more privacy protections than other personal information.[2]

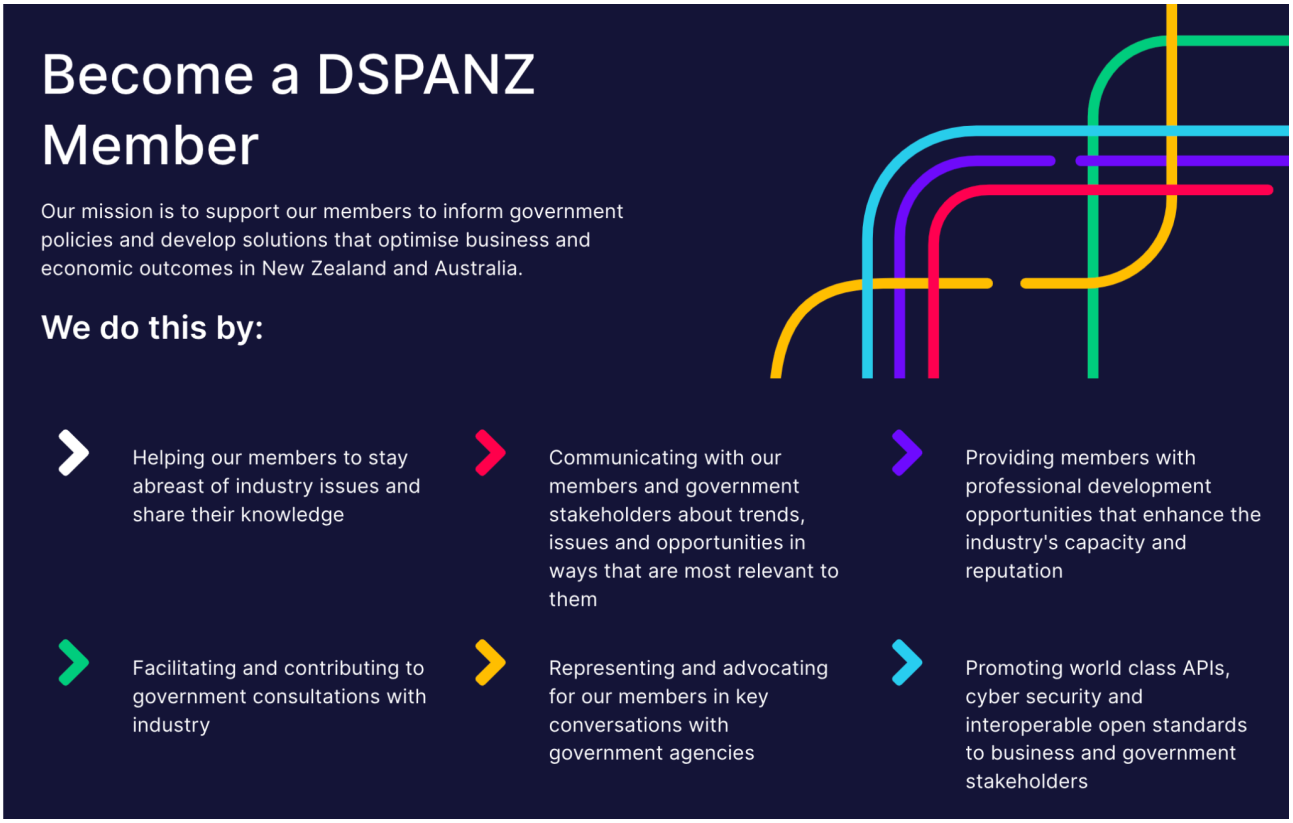
[1] OAIC - What is personal information?
[2] OAIC - What is sensitive information?

Tax File Number:
A tax file number (TFN) is a personal reference number in the tax and superannuation system generated by the Australian Taxation Office (ATO) that is:

- A unique number (usually 9 digits)
- An important part of an individual's identity
- Issued to an individual for life.[3] [4]

Tax File Number (TFN) Information:
When a TFN is linked with information identifying an individual, such as their name and date of birth, this is known as TFN information.[5]

User:
The users of a DSP's software products or services. Types of users may include taxpayers, tax agents, employers and employees.



[3] ATO - What is a tax file number?
[4] OAIC - Your tax file number
[5] OAIC - Your tax file number