dspanz. digital service providers
australia new zealand

Data Minimisation & Retention

Best Practice Guidance for Australian Digital Service Providers

Version 1.0

Contents

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

Executive Summary

Digital Service Providers (DSPs) offer software solutions that taxpayers rely upon to manage their business and financial affairs. This includes meeting their tax, financial and employment reporting and record-keeping obligations. For this reason, DSPs typically follow Australian legislation and practice guidance that document record-keeping requirements for taxation, invoicing, employer obligation, business registry and superannuation records and retain data accordingly.

This document confirms that DSPs do not have specific legislative or regulatory obligations to retain customer data under Australian tax or employment law. DSPs retain customer data as a part of their services, as described in their contractual agreements with customers. Future changes to data retention and record-keeping legislation or regulations may better reflect how DSPs support taxpayers in meeting their obligations.

The central role software plays in business processes has led to government, tax practitioners and taxpayers relying on DSPs to access current and historical records. The digitalisation of business processes has only increased the reliance on software. At the same time, the risks and costs associated with managing cyber protections and data storage are rising, particularly with the shift to cloud storage models.

This document first outlines record-keeping requirements for taxpayers, tax practitioners and DSPs, mainly for tax, corporate compliance and employer obligation records. It then guides DSPs concerning data retention and data minimisation best practices that make sense in the current technical and cybersecurity environment. DSPANZ acknowledges the different requirements for different kinds of taxpayer data and the need for associated deletion processes. Finally, this document provides additional information that DSPs may consider when following this best practice guidance.

At the highest level, the best practice guidance for DSPs is as follows:

- Customers SHOULD be able to access and retrieve their data before deletion.
- DSPs SHOULD take reasonable steps to contact customers before deleting data.
- DSPs SHOULD have documented customer data retention and deletion policies or processes.
- DSPs SHOULD keep inactive, non-paying customer data for at least 12 months.
- DSPs MAY delete historical data 12 months after minimum retention periods.

Alongside publishing this guidance, DSPANZ will be working with other stakeholders to support the business community with any changes to DSP data minimisation and retention practices.

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

Introduction

The changing attitudes towards data following high-profile cyber attacks across 2022, the rising costs of data storage, and increasing digital transformation in the business software space have led to many DSPs rethinking their data minimisation and retention practices. As a result, DSPANZ formed the Data Retention and Minimisation Focus Group to work through this topic and produce this best practice guidance.

This guidance supports DSPs in adapting their data retention and minimisation processes to reflect current regulatory and operating practices.

Terms and definitions

Customer:
The individual or business paying for a software product or services of a Digital Service Provider (DSP). For this document, "customer" describes taxpayers in the context of their relationship with a DSP.

Customer Data:
The data or artefacts a customer enters into their software that ultimately form broader tax, employee obligation, invoicing, business registry or superannuation records.

Digital Service Provider:
Digital Service Providers, also known as DSPs, create, sell and use software solutions to securely capture, transmit and share information and are commonly used in the day to day management of a business and its employees. Common examples include tax and accounting or payroll software, point of sale systems, superannuation and contributions management systems, eInvoicing software and eCommerce platforms.

Inactive, Non-Paying Customer:
Customers who are inactive and non-paying that have ceased their commercial relationship with a DSP. The following could be considered as examples that signify the end of the commercial relationship:

- The payment method was declined and retried with failure
- Contract not renewed or extended
- Cancelled subscription
- Customer moves to another product

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

- Death, medical impairment or retirement of the primary customer
- Tax practitioner loses their registration
- Customer stops trading, goes into liquidation or is found to be fraudulent
- DSP exits the market.

Record (from the ISO 15489 definition):
Information created, received or maintained as evidence and as an asset by an organisation or person, in pursuit of legal obligations or in the transaction of business.

Taxpayer:
Individuals and businesses with compliance and record-keeping obligations in Australia. This document uses “taxpayer” more generally when describing their legislative or regulatory record-keeping obligations.

Who does this guidance apply to?

This industry best practice guidance primarily applies to Australian DSPs and third party providers within their network who offer solutions commonly used in the day to day management of a business - not limited to but including - taxation, accounting, reporting, payroll, superannuation, point of sale or eCommerce and eInvoicing solutions.

While this guidance has been written with DSPs in mind, other software providers and Sending Service Providers (SSPs) may also benefit from this document’s discussion on data minimisation and retention practices.

In all instances, DSPANZ encourages providers using this document to adhere to their respective obligations under the ATO’s Operational Security Framework and other requirements that may apply to them.

Record-keeping

All taxpayers must keep records under different legislation and regulations to support their claims, maintain compliance and demonstrate their financial position.

A non-exhaustive list of current record-keeping requirements for taxpayers, tax practitioners and DSPs can be found in Appendix 1. Other information and useful resources on record-keeping can be found in Appendix 2.

What is a record?

The ISO records management standard, ISO 15489, defines records as:

> Information created, received or maintained as evidence and as an asset by an organisation or person, in pursuit of legal obligations or in the transaction of business.

It is also worthwhile considering the ATO's definition of a record in the context of tax and super-related transactions:

> A record explains the tax and super-related transactions conducted by a business. The record needs to contain enough information for [the ATO] to determine the essential features or purpose of the transactions, so [the ATO] can understand the relevance of the transactions to your business's income and expenses.[1]

Records can be kept electronically or in paper form. The ATO recommends that businesses use electronic record-keeping where possible as they progressively move towards electronic reporting for tax and super obligations[2]. While there is a general preference for electronic record-keeping, some legislation or regulations may require paper copies of records. Examples of records can include the following:

Tax	Corporate Compliance	Employment
• Income tax return • Gross sales and income • Expenses • Invoices and receipts	• Financial statements • Registration details • Minutes of members or directors' meetings • Resolutions	• Payslips • Timesheets • Rosters • Superannuation contributions

[1] What is a record - Overview of record-keeping for business

[2] Business.gov.au - How to keep records

Disclaimer:

This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

Record-keeping requirements

This section considers the current record-keeping requirements for taxpayers, tax practitioners and DSPs. A non-exhaustive list of record-keeping requirements can be found in Appendix 1 and at www.dspanz.org.

For this document, it is important to note the following two observations across record-keeping requirements:

1. Taxpayers, or the business owners, are ultimately responsible for record-keeping and understanding their obligations, noting that these can change over time; and

2. There is minimal information about electronic record-keeping requirements or how software assists taxpayers with their record-keeping.

Each piece of relevant legislation or regulation outlines what records taxpayers must keep, how they must store records, how long they must retain records and the penalties for failing to keep records or making false or misleading records.

While record-keeping requirements may vary across different legislation and regulations, at a high level, taxpayers should:

- Keep all records relating to starting, running, changing, selling, or closing a business relevant to tax, super, and corporate affairs.
- Keep records for 5 to 7 years from the date a record is created, updated or when transactions relating to a record are completed or indefinitely in some instances.
- Only change records if correcting an error or making an amendment.
- Store records in a way that protects them from being altered or damaged.
- Be able to produce records (in the prescribed format) when required.
- Keep records in English or easily convert them into English.
- Not keep false or misleading records.

Record-keeping for taxpayers

Taxpayers must comply with a broad range of record-keeping requirements. This section explores tax return, corporate compliance and employer obligation record-keeping requirements.

Tax return record-keeping:
At a minimum, tax records must include the following information:

- Date, amount and character (for example, sale, purchase, wages, rental) and the relevant GST information for the transaction;
- Purpose of the transaction; and
- Relationships between parties to the transaction, if relevant.

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

There are circumstances where the retention starting date may differ or the record must be kept longer than 5 years, including:

- FBT: must be kept for 5 years from the date an FBT return is lodged.
- Amended tax returns or documents: must be kept for 5 years from the date the ATO gives the notice of assessment. Records relating to the original return and subsequent amendments must be kept long enough to cover the required retention and review periods.
- Depreciating assets: must be kept for as long as the taxpayer has the asset and then another 5 years after the asset is sold or disposed of.
- Capital gains tax (CGT) assets: must be kept for as long as the taxpayer has the asset and then another 5 years after the asset is sold or disposed of.
- Petroleum resource rent tax: must be kept for 7 years or more.

Taxpayers must keep records long enough to cover the ATO's review period (or amendment period). Examples include:

- Income tax returns: 2 years for individuals and small businesses and 4 years for other taxpayers from the day after the ATO gives the notice of assessment.
- Business activity statements (BAS): 4 years from the day after the notice of assessment is given.
- Fringe benefits tax (FBT) return: 3 years from the date of lodgment.

In many cases, the 5 year retention period will also cover the review period. However, where the Commissioner of Taxation has formed an opinion that a taxpayer's behaviour amounts to fraud or evasion, there is no time limit for amending an assessment[3].

Corporate compliance record-keeping:
The Australian Securities and Investments Commission (ASIC) requires most financial and corporate records to be kept for 7 years after the transactions covered by the records are complete. Other records may need to be kept for the lifetime of an entity, for example:

- Constitution of the company, including all amendments
- Certification of company incorporation
- Certification of business name registration, trademarks, domain names, patent registrations and copyright information
- Minutes of meetings, including general, director and committee meetings.

Employer obligation record-keeping:
Taxpayers who are also employers have record-keeping obligations under the Fair Work Work Act and Regulations. Employers generally must keep employee-related records for

[3] ATO Decision-Making Process - Fraud or Evasion and the Normal Period of Review

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

7 years, but there are circumstances where records must be kept longer, for example, to calculate long service leave entitlements.

At a high level, employers must keep records of the following: general employment, pay, hours of work, leave, superannuation contributions, individual flexibility arrangements, annualised wage arrangements, guarantee of annual earnings, termination and transfer of business. More detailed information about employee records can be found here.

Each state and territory also has specific requirements for retaining employment records, including payroll tax and long service leave obligations. Most states and territories require these records to be kept for the duration of employment. However, retention periods vary after the end of employment.

Record-keeping for tax practitioners

Tax practitioners have business and employment record-keeping obligations as taxpayers and employers themselves. Tax practitioners have no additional client record-keeping requirements under the *Tax Agent Services Act 2009*. However, it is recommended that registered agents keep copies of signed “authority to lodge” documents for insurance and compliance purposes.

The Tax Practitioners Board (TPB) requires tax practitioners to keep records of client proof of identity checks for at least 5 years after the engagement with a client ends. Tax practitioners should only keep a record of conducting these checks and should not store originals or copies of client identity documents.

Tax practitioners who also provide a DSP service must meet the client verification requirements outlined by the ATO and TPB. More information about these requirements can be found here:

- ATO - Agent client verification methods
- TPB(PN) 5/2022 Proof of identity requirements for client verification

Record-keeping for DSPs

Under the ATO’s DSP Operational Security Framework, DSPs must implement audit logging and keep these logs for at least 12 months. Audit logs should include access and event-based logs, including changes to privileges, permissions and authorisations as specified in the Operational Security Framework requirements. DSPs who provide desktop or server-based software may not be able to comply with this requirement fully and may find alternative ways to support it.

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

DSPs who are eInvoicing Service Providers are required by the Peppol Service Provider Service Level Agreement[4] to log all executed transactions and archive the logged data for at least 3 months.

While DSPs have no legal requirements to retain customer records, many will follow taxpayer or tax practitioner guidance to assist customers with meeting their record-keeping obligations.

[4] Peppol Service Level Agreement

Disclaimer:

This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

The relationship between the DSP and taxpayer

How DSPs assist customers with meeting their record-keeping obligations will depend on their service offering and hosting environment.

In both examples outlined below, DSPs act as data custodians for their customers, who ultimately own the data and records they generate when using their software or service, regardless of where the data is located.

Customer data and the software as a service (SaaS) model

DSPs who offer SaaS solutions will grant their customers a licence to use the software so long as they continue to pay their subscription. DSPs will provide information on how their subscriptions work, cancellation, data security and other important information when a customer signs up and in their terms of service.

DSPs will host and back up a customer's data while the customer is paying. It is important to note that providing this service to customers does not transfer the data ownership to DSPs. Instead, it creates a shared responsibility between the customer and DSP for protecting, managing and retaining the data while in the DSP's custody. Many DSPs will reflect these respective roles in their terms of service and will particularly note that customers should not solely rely on the software for archiving or backing up their data.

When customers stop paying for their subscriptions, their ability to access their data and the software varies across DSPs. For example, some DSPs retain the customer's data for up to 7 years, while others allow customers to retrieve it for up to 90 days. After a DSP's stated customer data retention period, they will endeavour to delete this data or anonymise any retained data.

Customer data and desktop or hosted products

Where DSPs provide desktop software, customers are in control of their data. DSPs will have a limited ability to influence the customer's data retention and minimisation practices unless they implement license activation processes that prevent access to expired or unlicensed data or software. Ultimately, customers are responsible for backing up and deleting data that is no longer required.

In a hosted environment, the DSP will host the customer's data. When the customer ends the commercial relationship, the DSP may automatically provide customers with a copy of their data and delete the hosted environment.

DSP industry best practice

The below best practice guidance aims to assist DSPs with understanding how long they should retain customer data and how they can delete customer data that is no longer required. This guidance is based on the understanding that record-keeping is ultimately the taxpayer's responsibility. Taxpayers are responsible for ensuring they understand their record-keeping obligations, retaining records for their required periods and substantiating them when asked.

DSPANZ considers the following as data retention and minimisation best practice for DSPs:

- Customers SHOULD be able to access and retrieve their data before deletion.
- DSPs SHOULD take reasonable steps to contact customers before deleting data.
- DSPs SHOULD have documented customer data retention and deletion policies or processes.
- DSPs SHOULD keep inactive, non-paying customer data for at least 12 months.
- DSPs MAY delete historical data 12 months after minimum retention periods.

DSPs must comply with the ATO's Operational Security Framework and other security or privacy obligations outside of this best practice guidance.

MUST: DSPs must comply with requirements through legislation, legislative requirements, regulations or binding rulings.

SHOULD: Considered as best practice for DSPs.

MAY: Optional for DSPs but can be considered to improve user experience or for operational benefits.

How DSPs implement or reflect this best practice guidance may depend on their product architecture and the business interactions they facilitate. DSP's terms of service or contracts should ideally follow this best practice guidance. More information on considerations for implementation can be found below.

Customers SHOULD be able to access and retrieve their data before deletion

DSPs should allow customers to access and retrieve their data before it is deleted to ensure they can continue to comply with their record-keeping obligations. DSPs can choose how they provide data to their customers, but at a minimum, data should be human-readable without specialist software. Options to make customer data available include providing read-only access to the software or the ability to download PDF or CSV copies of their data. See examples of records and their suggested formats below.

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

Type of record	Suggested formats
Lodged Business Activity Statement	● PDF that was signed by the taxpayer ● Transactions in CSV ● Copies of receipts and invoices in PDF
Lodged income tax return	● PDF that was signed by the taxpayer
Payroll	● Payrun data displayed in PDF ● Timesheets and pay slips in PDF ● Tax File Number Declarations and super choice forms in PDF
eInvoice	● PDF representation of the sent invoice (from the seller) ● PDF representation of the paid invoice (from the buyer)
Business register change notification	● PDF that was signed by the business

DSPs should advise customers how long they can access their data before it is deleted, which may include providing customers with the number of days they have to access their data. The timeframe that customers have to access their data may not align with the timeframe that DSPs should delete data within.

Before deleting any data, DSPs may wish to provide information to their customers on their record-keeping obligations and the handling of sensitive or personally identifiable information. More information on these other considerations can be found here.

Please note: this guidance considers data portability between software products developed by different DSPs to be out of scope.

DSPs SHOULD take reasonable steps to contact customers before deleting data

DSPs should take reasonable steps to contact a customer before deleting their data. While the nature of this contact may differ between DSPs, at a high level, it should include the following information:

- What data will be deleted
- When the data will be deleted
- How to access the data before it is deleted.

Disclaimer:

This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

DSPs should communicate this to their customers as soon as their commercial relationship ceases or when the data is flagged for deletion. DSPs may consider further communications as required. Note that there may be circumstances where the customer's contact details are no longer valid.

DSPs should certify the permanent and full deletion of all data, whether at the customer's request or at the agreed time, to mitigate any perceived or real risk for the DSP. DSPs should retain a register of certifications and customer acknowledgment for a minimum of 10 years.

DSPs SHOULD have documented customer data retention and deletion policies or processes

DSPs should make information about how they retain and delete customer data readily available to their customers, for example, in their terms of service or contracts. This information should include:

- How long they retain data;
- How they delete data; and
- How customers can access or export their data before deletion.

DSPs should consider reflecting the following points on data retention and deletion in their policies, terms of service or contracts:

- Indicate all roles and responsibilities of both the customer and DSP, including decision making capability, actions and approvals. This should include responsibility for monitoring legislative changes that would impact the retention of the data held by the DSP and the application of any changes to historical data.
- Mechanisms for the customer to audit (or have an audit performed) on the reliability and integrity of the data to ensure their data remains viable and readable for the entire retention time.
- How the DSP manages data during a merger or acquisition?
- Conditions under which the DSP would agree with a customer request to retain data longer than the legislated retention period and how often the DSP would seek disposal authorisation from the customer.
- How data will be disposed of to ensure the permanent erasure of data held by the DSP and the assurance provided to the customer (in the form of a disposal certificate or similar mechanism) certifying that the data is no longer recoverable.
- The treatment of backups (data copies), which should be retained for shorter periods but also need to be managed and disposed of appropriately.
- Specify the formats in which data is provided after the end of the commercial relationship to ensure that accessibility is maintained even without the appropriate software.

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

DSPs SHOULD keep inactive, non-paying customer data for at least 12 months

If a customer has ended their commercial relationship with a DSP, the DSP should keep the customer data for at least 12 months before it is deleted.

This 12 month retention period follows the ATO's DSP Operational Security Framework where access logs must be retained for 12 months. DSPs should retain customer data for as long as they retain user access log information.

DSPs may be required to delete data sooner than the stated 12 month time period as required under different privacy or security obligations.

Following the above guidance, DSPs should ensure they take reasonable steps to contact customers and confirm the end of the commercial relationship before deleting their data.

Customer data is primarily the data or artefacts that ultimately form tax, employee obligation, invoicing, superannuation or business registry records. DSPs may or may not delete other customer data, such as contact information, depending on their approach to data deletion. Where DSPs retain data for analytical purposes, this data should be anonymised, and in line with the *Privacy Act,* any personal information should be de-identified.

This best practice guidance broadly applies to production data, with the deletion of backups considered out of scope for this document. More details on the retention and deletion of backups can be found below.

DSPs MAY delete historical data 12 months after minimum retention periods

DSPs will retain data for paying customers to support them in meeting their record-keeping requirements in line with their terms and conditions.

If DSPs would like to implement processes for minimising historical customer data, they may look to delete data 12 months after it reaches its minimum retention period. However, DSPs should consider that record retention periods may vary and that customers may have templates or records they do not want to be deleted.

It is important to recognise that while minimum retention periods exist, taxpayers may choose to retain data longer to meet cultural, community, historical or other business needs. More extended retention periods can be often be permitted through an agreement between customers and DSPs.

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

Data deletion may impact aggregated data sets and will likely be a catalyst for longer retention. For DSPs to retain as little data as possible, the responsibility for maintaining aggregated datasets may lie solely with the data owner (the customers) rather than the DSPs. However, the customer needs to fully understand the implications of this scenario and the impacts on reporting from existing systems.

Before deleting any customer data, DSPs should take reasonable steps to contact their customers.

A note on employment and corporate compliance records:
While taxpayers must keep most employment and corporate compliance records for 7 years, there are circumstances where records should be retained for an employee's tenure or the lifetime of an entity.

For example, state and territory employment record-keeping requirements often require employers to retain former employee's records for up to 7 years after termination.

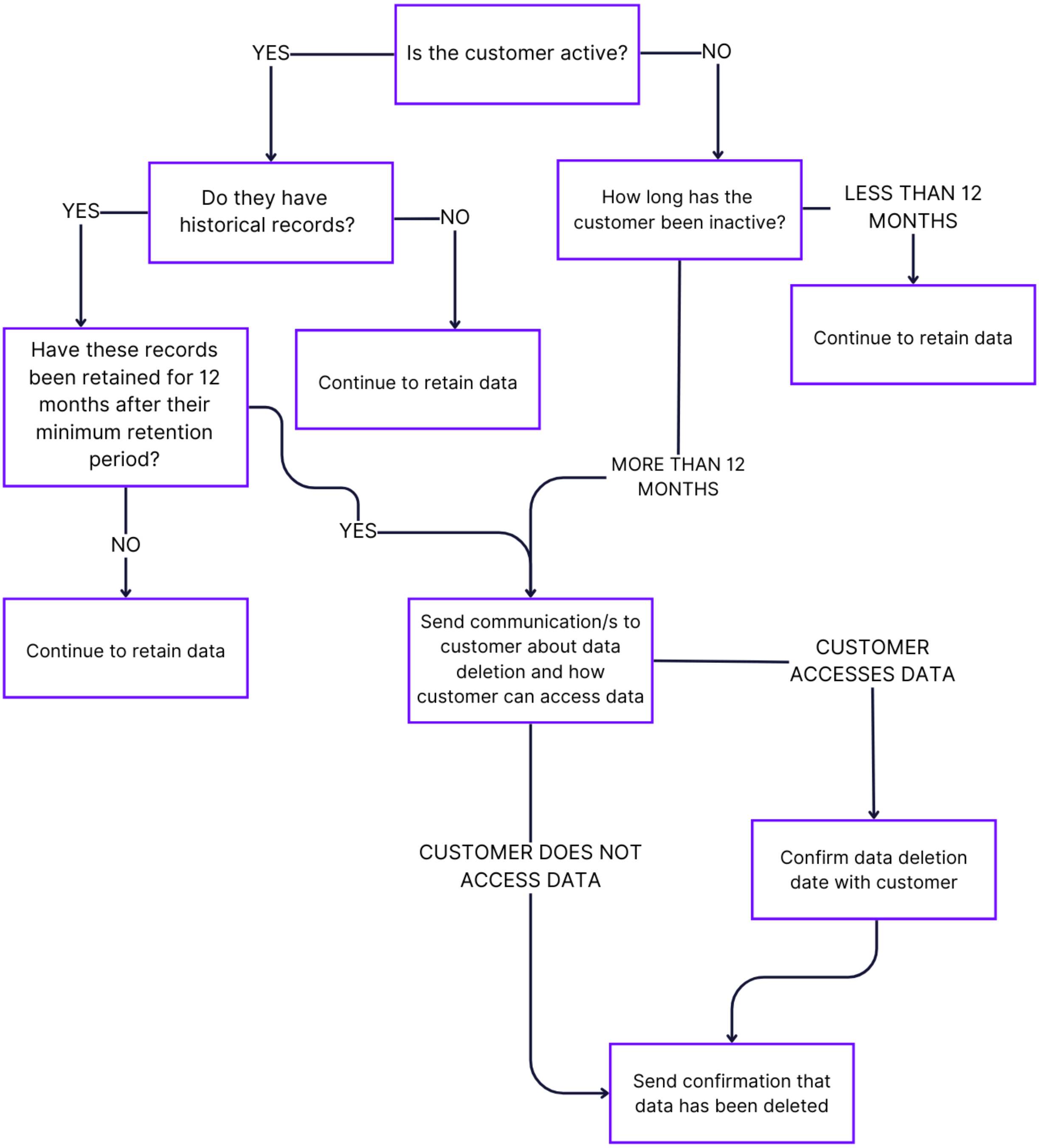
For these reasons, it is not recommended to delete historical payroll or corporate compliance records automatically.

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

Automating data deletion

DSPs looking to automate data deletion and follow the above best practice may utilise the following decision tree to assist with their approach. Please note that no timeframes have been prescribed in the decision tree as this approach may differ from DSP to DSP.

More information on other data retention and minimisation considerations can be found in the next section.


Is the customer active?
YES
NO
Do they have historical records?
How long has the customer been inactive?
LESS THAN 12 MONTHS
YES
NO
Have these records been retained for 12 months after their minimum retention period?
Continue to retain data
Continue to retain data
MORE THAN 12 MONTHS
YES
NO
Continue to retain data
Send communication/s to customer about data deletion and how customer can access data
CUSTOMER ACCESSES DATA
CUSTOMER DOES NOT ACCESS DATA
Confirm data deletion date with customer
Send confirmation that data has been deleted

Disclaimer:

This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

Other considerations for data retention and minimisation

Outside of the best practice guidance included in this document, DSPs should also consider the following in their approach to data minimisation and retention:

- Take a customer-centric approach
- Software hosting environment
- Trial software
- Unsupported and end of life software
- Challenges with deleting data
- Add-on ecosystems
- Security of personal information
- Inactivity and deletion
- Retention of backups.

This guidance does not provide recommendations for how to delete or minimise data. Instead, it offers relevant information and resources for DSPs to take the approach that best suits their environment.

Further resources and materials for DSPs and other stakeholders will be available on the DSPANZ website.

Take a customer-centric approach

DSPs should take a customer-centric approach to data deletion, which includes considering the impacts of deleting data on customers and talking to internal customer retention and marketing teams about preferred approaches and how this will be communicated to customers.

DSPs should also educate customers before enacting any changes to their data minimisation and retention practices. The time and level of education required will differ between DSPs. DSPANZ will also engage in conversations with industry peers to support the broader community with any changes to DSP data minimisation and retention practices.

Examples of customer-centric considerations include:

- Reminding customers of their record-keeping obligations under current legislation and what records they need to keep.
- Giving customers the ability to flag records or artefacts that should not be deleted.
- Providing data in a human-readable format or the ability to convert their data into a human-readable format, i.e. the ability to convert data into PDFs or CSVs.

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

Software hosting environment

A DSP's hosting environment will considerably impact its data minimisation and retention approach.

For desktop environments, the customer controls their data and will continue to control their data when they stop being a customer. DSPs will be limited to influence the customer's data retention and minimisation practices unless they implement license activation processes that prevent access to expired or unlicensed data or software.

For cloud environments, DSPs host and retain the customer's data while they are paying and may continue to host their data for a set period after they stop paying. DSPs will be responsible for implementing data retention and minimisation practices and informing their customers about how they handle their data.

Trial software

DSPs can determine how they manage customer data retention and deletion from trial software.

Trial software is not intended for business record-keeping purposes (whilst it is a trial version) and should not connect to ATO or superannuation systems via Application Programming Interfaces (APIs). DSPs may delete all data immediately or at the end of the trial period.

Unsupported and end of life software

DSPs may have a limited ability to assist customers with accessing and retrieving their data from unsupported software products.

When sunsetting software products, DSPs can follow the best practice guidance for inactive and non-paying customers. Following the guidance, DSPs should communicate with customers before any data is deleted and allow them to access and retrieve it in a human-readable format.

Challenges with deleting data

Depending on a DSP's product or data architecture, removing all instances of data or records from their system may be complex. Where it is difficult to delete data, DSPs could look to anonymise any personally identifiable information.

Disclaimer:

This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

For some DSPs, deleting data may require teams of people to investigate where the data is, how to delete it successfully and understand whether there will be implications from deleting it.

There may also be circumstances where a customer requests to delete their data or certain records, which may impact future processes within the software, for example, end-of-month or end-of-year finalisations. In such circumstances, DSPs may consider their obligation to assist customers with meeting their reporting requirements before deleting data.

Further, suppose customers seek data deletion before minimum retention periods. In that case, DSPs may wish to consider additional actions to manage reputation and other risks from early data deletion or data loss, such as providing data disposal certificates. DSPs may also consider options to transfer data back to customers for them to action the deletion to avoid risk entirely.

This guidance primarily deals with the deletion of production data and considers the deletion of backups as out of scope.

Add-on ecosystems

For DSPs who support add-on marketplaces or allow applications to connect and share data via APIs, there can be challenges with different approaches to customer data retention and the amount of data transmitted through to the DSP.

DSPs may only receive aggregated data from third-party applications. In these circumstances, DSPs will not have complete copies of the broader tax or business record datasets. DSPs should advise customers they cannot be solely relied upon to access each piece of data that makes up a customer's broader record set.

Point of Sale (POS) example:
POS software often shares daily summaries with a taxpayer's accounting software. The POS software will retain the raw transaction data until the customer cancels their subscription. Across different POS systems in Australia, the customer's data will often be deleted within 90 days and, in some cases, immediately upon cancellation.

If a taxpayer has changed their POS software and not obtained copies of their data from the old system, it may cause future challenges as they cannot access this data.

Security of personal information

DSPs covered by the *Privacy Act* must take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure. The

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

Australian Privacy Principle (APP) 11 contains detailed information on the security of personal information.

There may be other security and privacy requirements for specific records or datasets that DSPs may need to consider. For example, the *Privacy Act (Tax File Number) Rule 2015* protects individuals' Tax File Number (TFN) information as they are intended to be a unique identifier issued for life. Employers, financial and superannuation entities and tax practitioners who receive or store TFNs must safeguard this information and securely destroy or de-identify TFN information when it is no longer required.

Customers of DSPs, the taxpayers, may also have obligations to protect personal information under the *Privacy Act*, among other requirements.

Inactivity and deletion

While periods of inactivity can be considered a factor determining the end of the DSP-customer relationship, DSPs may want to consider reasons for inactivity and whether customers or user profiles should remain inactive or be actioned for deletion.

Some customers may only engage with their software once a year in line with the annual tax cycle and may have extended periods of inactivity. Similarly, some user profiles may be inactive as they engage with the software on an ad-hoc basis. In most cases, these customers or user profiles should either be designated for deletion, disabled or have passwords reset to minimise the cybersecurity risk of unauthorised access by third parties in line with the ATO's Operational Security Framework.

Where customers have ended their commercial relationship or a user profile is actioned to be deleted, DSPs should remove all records of the customer or user from the system where practicable.

Retention of backups

The ATO's Operational Security Framework requires DSPs to keep audit logs for at least 12 months. Outside of this requirement and other industry requirements that may apply, DSPs can choose an approach to backing up data that best suits their environments.

DSPs may consider security controls to better protect backup data, such as encryption at rest, which is often an existing feature in many cloud hosting providers that DSPs can turn on.

More general backup information can be found in the Australian Information Security Manual.

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

The future of data minimisation & retention for DSPs

DSPs will play an increasingly important role in assisting taxpayers with meeting their record-keeping obligations as Australia moves closer to making tax and business processes ‘just happen’.

Whilst this document is a starting point for DSP best practice around data minimisation and retention, it aims to move the business software industry towards a point where DSPs only retain the information needed to support current customer decisions and outcomes.

This document provides best practice guidance as there are no current, explicit requirements for DSPs to retain customer data for record-keeping purposes.

Australian legislation has yet to keep up with technological advancements in tax return and payroll reporting processes. However, there may be opportunities for changes around data retention and record-keeping to reflect better how DSPs support taxpayers in meeting their obligations.

DSPANZ looks forward to continuing the conversation on data minimisation and retention with the government and our industry peers.

Disclaimer:

This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

Appendix 1 - Record-keeping requirements

The information below is accurate at the time of publication on 13 March 2024.

Relevant legislation and regulations

Legislation or Regulation	Records	Required Retention Period	Record Format
Corporations Act 2001	**Financial Records** Section 286 A company, registered scheme, registrable superannuation entity or disclosing entity must keep written financial records that: ● Correctly record and explain its transactions and financial position and performance ● Would make true and fair financial statements able to be prepared and audited. Extends to transactions undertaken as a trustee.	7 years after the transactions covered by the records are completed.	Section 287 Records may be kept in any language, but an English translation of financial records not kept in English must be made available when requested. Section 288 If financial records are kept in electronic form, they must be convertible into hard copy. A hard copy must be made available to a person who is entitled to inspect the records. Section 289 The company can decide where to keep their records.
	Registers Section 168	A register kept under Chapter 2C.1 is proof of the	Section 172 Registers that relate to a

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

	A company or registered scheme must set up and maintain: ● A register of members ● If the company or scheme grants options over unissued shares or interest - a register of option holders and copies of options documents ● If the company issues debentures - a register of debenture holders.	matters shown in the register under the Chapter.	company (or a registered scheme) must be kept at: ● The company's registered office ● The company's principal place of business in this jurisdiction ● A place in this jurisdiction (whether of the company or of someone else) where the work involved in maintaining the register is done ● Another place in this jurisdiction approved by ASIC. Companies or schemes must notify ASIC of the address where a register is kept within 7 days after the register is: ● Established at an office that: ○ Is not the registered office of the company or responsible entity ○ Is not the principal place of business of the company or
	Register of members Section 169 The register of members must contain the following information about each member: ● Member's name and address ● Date on which the entry of the member's name in the register is made.		
	Register of option holders and copies of option documents Section 170 The register of option holders must contain information about each holder of options over unissued shares in the company or unissued interests in the scheme. The register must be updated whenever		

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

	options are exercised or expire.		responsible entity in this jurisdiction - Moved from one place to another.
	Register of debenture holders Section 171 The register of debenture holders must contain the following information about each holder of a debenture: - The debenture holder's name and address - The amount of debentures held.		
Fair Work Act 2009 Section 535	An employer must make and keep employee records of the kind prescribed in the regulations (covered below) in relation to each of its employees. An employer must not make or keep records that the employer knows are false or misleading.	7 years.	Records must be in a form prescribed by the regulations (covered below) and include any information prescribed by the regulations.
Fair Work Regulations 2009 Sections 3.31 - 3.44	Employers must keep records for each employee about: - Basic employment details ○ Employer's name ○ Employee's name ○ Full-time or part-time employment ○ Permanent, temporary or casual employment ○ Date employment began ○ ABN of the employer - Pay	7 years.	Records must be legible, in English and in a form readily accessible to an inspector.

	- Overtime - Averaging of hours - Leave - Superannuation contributions - Individual flexibility arrangements - Guarantee of annual earnings - Termination of employment - Transfer of business.		
Fringe Benefits Tax Assessment Act 1986 Section 132	You must keep records that: - Show how you calculated the taxable value of benefits - Support any fringe benefits tax (FBT) exemptions or concessions you used.	5 years after the completion of the transactions or acts to which they relate (e.g. 5 years from the date of the FBT return).	Records must be kept in English or can be easily converted to English.
Income Tax Assessment Act 1936 Section 262A	A person carrying on a business must keep records that record and explain all transactions and other acts engaged in by the person that are relevant for any purpose of this Act. Records include: - Any documents relevant for the purpose of ascertaining income and expenditure - Documents containing particulars of any election, choice, estimate, determination or calculation and, in the case of an estimate, determination or calculation,	5 years after records were prepared or obtained, or 5 years after the completion of the transactions or acts to which those records relate, whichever is later. 5 years after an amendment.	Records must be kept in English or can be easily converted to English.

	particulars showing the basis on which and method by which the estimate, determination or calculation was made.		
Superannuation Guarantee (Administration) Act 1992 Section 79	Employers must keep records that record and explain all transactions and other acts engaged in by the employer or required to be engaged in by the employer, under the Act. Records must include documents relevant to ascertaining the individual superannuation guarantee shortfalls of the employer for a quarter.	5 years after the records were prepared or obtained, or the completion of the transactions or acts to which those records relate, whichever is later.	Records must be kept in English or can be easily converted to English.
Taxation Administration Act 1953 Subdivision B TR 2018/2	You are required to keep records that explain all electronic business transactions that are relevant for any income tax purpose. The minimum information that must be recorded: ● Date ● Amount ● Character of transaction. A person commits an offence if: ● The person required under, or pursuant to, a taxation law to keep any accounts, accounting records or other records; and ● The person keeps the accounts or records; and	5 years after the records are prepared or obtained, or the transactions are completed, whichever occurs later.	Records must not be altered or manipulated and must be stored in a way that restricts information from being altered or manipulated. They must be in English or a form the ATO can access and easily convert to English. Records must be capable of being provided to the ATO when required.

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

	● The accounts or records do not correctly record and explain the matters, transactions, acts or operations to which they relate. There are further offences for recklessly incorrectly keeping records and incorrectly keeping records with the intention of deceiving or misleading.		

Other relevant requirements

Requirement	Records	Required Retention Period
ATO Digital Service Provider Operational Security Framework	Audit logging functionality must be implemented in software products to enable traceability of user access and actions.	Audit logs must be kept for a minimum of 12 months.
Capital Gains Tax (CGT)	You must keep records of every transaction, event or circumstance that may be relevant to working out whether you have made a capital gain or loss from a CGT event.	5 years after you sell or otherwise dispose of an asset unless you keep an asset register. A further two years for individuals or small businesses, or four years for other taxpayers from the year of the offset if you have offset a capital loss against a capital gain in a later year.
Depreciating assets	You generally need to keep records of depreciating assets.	For as long as you have the asset

		and then another 5 years after you sell or otherwise dispose of the asset.
Goods and Services Tax (GST)	You need to keep records that show the income and expenses used to calculate and support the amounts you report and claim for GST credits. This includes all sales, tax invoices and other GST-related transactions, fees, expenses, wages and any other business costs.	5 years from when you prepared or obtained the records or completed the transactions or acts those records relate to, whichever is later.
Long Service Leave	Employers must keep employee records relating to long service leave throughout an employee's employment.	Retention periods for each state or territory are provided below.
	ACT *Long Service Leave Act 1976*	Records must be kept for 7 years after the day employment ends. If employment ends on the employee's death, records must be kept for 7 years after the day all amounts owing to the legal personal representative are paid.
	NSW *Long Service Leave Act 1955*	Records must be kept for at least 6 years after the day employment ends.
	NT *Long Service Leave Act 1981*	Records must be kept for 3 years after the day employment ends. If employment ends on the employee's death, records must be

Disclaimer:

This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

		kept for 6 years after the day all money owing to the legal personal representative are paid.
	QLD *Industrial Relations Act 2016*	Employers must keep records for 6 years after the day the work to which the record relates is performed.
	SA *Long Service Leave Act 1987*	Records must be kept throughout the period of the worker's service and for at least 3 years after the termination of that service.
	TAS *Long Service Leave Act 1967* *Industrial Relations Act 1984* *WorkSafe Tasmania*	Records must be kept for 12 months after the termination of employment.
	VIC *Long Service Leave Act 2018*	Employers must keep long service leave records relating to an employee for at least 7 years after the employee ceases employment.
	WA *Long Service Leave Act 1958*	Records must be retained during the employment of the employee and for not less than 7 years thereafter.
Peppol Service Provider Service Level Agreement (SLA)	The Peppol Service Provider shall log all transactions executed (e.g. sent or received Peppol Business Documents) and archive the logged data for a period of time no less than stated.	5 years for message exchange services in pre-award procurement. 3 months for message exchange

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

		services in post-award procurement.
Payroll tax	Employers are required to keep records of the payroll tax they pay in different states and territories: ● ACT ● NSW ● NT ● QLD ● SA ● TAS ● VIC ● WA	Retention periods are typically defined by state and territory tax administration legislation which is typically 5 years.
Tax practitioner proof of identity requirements	The TPB requires that registered tax practitioners keep a record of the proof of identity (POI) checks that they undertake in relation to each client and/or individual representative of a client.	A minimum of 5 years after the engagement with the client has ceased.

Disclaimer:

This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

Appendix 2 - Further information and resources

Organisation or Agency	Resource
ACNC	ACNC record-keeping obligations
APRA	CPG-235 Managing Data Risk
ASIC	ASIC requirements for storing signed documents lodged online
ASIC	What books and records should my company keep?
ATO	Employment and payroll records
ATO	Record keeping rules for business
ATO	TR 2018/2 Income tax: record keeping and access - electronic records
ATO	TR 96/7 Income tax: record keeping - section 262A - general principles
AUSTRAC	AML/CTF record-keeping
Business.gov.au	Record keeping
FWO	Record-keeping & pay slips
OAIC	Security of personal information - APP 11
OAIC	The Privacy (Tax File Number) Rule 2015 and the protection of tax file number information
TPB	TPB (EP) 01/2022 Code of Professional Conduct

Appendix 3 - About the Data Minimisation & Retention Focus Group

Following an initial conversation about data retention in the Australian Taxation Office's DSP Strategic Working Group, DSPANZ formed the *Data Minimisation and Retention Focus Group* to work through this topic in greater detail.

The Data Minimisation and Retention Focus Group (the focus group) met 5 times between April and October 2023 to inform this industry best practice document. The focus group covered:

Disclaimer:

This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.

- Current record-keeping requirements for DSPs and taxpayers;
- What data and metadata should be retained by DSPs;
- Appropriate minimum and maximum data retention periods;
- Technical requirements and limitations; and
- The differing expectations around data retention.

The focus group included representatives from tax, accounting, payroll, superannuation, eInvoicing and business registry software providers, as well as representatives from the ATO and other industry bodies. More information about the focus group can be found on the DSPANZ website.

Appendix 4 - Acronyms

API	Application Programming Interface
APP	Australian Privacy Principles
ASIC	Australian Securities and Investment Commission
ATO	Australian Taxation Office
BAS	Business Activity Statements
CGT	Capital Gains Tax
DSP	Digital Service Provider
DSPANZ	Digital Service Providers Australia New Zealand
FWO	Fair Work Ombudsman
FBT	Fringe Benefits Tax
GST	Goods and Services Tax
POS	Point of Sale
SaaS	Software as a Service
SSP	Sending Service Provider
TFN	Tax File Number
TPB	Tax Practitioners Board

Disclaimer:
This document intends to provide best practice guidance for Digital Service Providers on data retention and minimisation alongside commentary on current record-keeping requirements. It should not be treated as a complete record-keeping or data management guide. DSPANZ intends to continuously update this document to reflect industry and regulatory changes.