Co-Host - Maggie Leese (DSPANZ): Hello and welcome to this data minimisation and retention webinar. This session is designed to guide how DSPs can align their data collection and retention processes with industry best practice that make sense in the current technical and cyber security environment.

I'm Maggie Leese the Policy Lead at DSPANZ, and I'm joined by Matthew Prouse, Director at DSPANZ.

Co-Host - Matthew Prouse (DSPANZ): Thanks Maggie. In this session, we'll walk you through the key points from our Data Minimisation and Retention Best Practice Guidance Paper for Australian DSPs.

We're going to cover a brief background on the best guidance paper and how it came together. The role DSPs play in data retention and record-keeping in Australia. We'll provide some insights into best practice data minimisation and retention for software developers working in both Australia and New Zealand. And, we'll identify some of the key challenges and what we can do to overcome them.

We'll start with a quick overview before we get into the details.

Slide change

Co-Host - Matthew Prouse (DSPANZ): Maggie, why did DSPANZ start thinking about data minimisation and retention?

Co-Host - Maggie Leese (DSPANZ): After a few high-profile cyber attacks across 2022, we started to see changing attitudes towards data privacy and collection in Australia. There are a lot of people impacted and a lot of people, you know, questioning how much data the services they interact with collect.

At this time, we also started to see the potential outcomes of the Privacy Act Review.

DSPs in this time were navigating the rising data storage costs and the increasing amount of data they are expected to collect and retain due to digital transformation in the business software space.

These events are why DSPANZ began working with the ATO and DSPs in 2023. To help the business software industry navigate the best way forward while supporting their customers. After consultation, we officially published the best practice guidance in 2024.

Co-Host - Matthew Prouse (DSPANZ): And Maggie, can you give us a quick overview of the best practice guidance?

Slide change

Co-Host - Maggie Leese (DSPANZ): Yes, I sure can.

We have a summary of the recommendations for DSPs up on the screens now.

As a quick overview, essentially the guidance ensures that DSPs enable customers to access and retrieve their data before it's deleted and that they are well informed about this process and how DSPs retain and delete customer data.

We also provide the best practice timeframe for deleting historical data if DSPs want to consider this.

Co-Host - Matthew Prouse (DSPANZ): Maggie, accepting that DSPs don't sign up to the National Archieves, who does the guidance apply to?

Slide change

Co-Host - Maggie Leese (DSPANZ): The best practice guidance is for DSPs that provide tax, accounting, reporting, payroll, superannuation, point of sale, eCommerce and eInvoicing software services or solutions. It's a big list but businesses commonly rely on these platforms to support their record-keeping practices. However, any software provider can actually benefit from this guidance.

Slide change

Co-Host - Maggie Leese (DSPANZ): The best practice guidance highlights that legislated record-keeping requirements do not generally apply to DSPs. The ATO's Operational Security Framework requires DSPs to retain their audit logs for 12 months, but that's about it.

However, DSPs follow record-keeping obligations to support their customers. Can you tell me more about the role DSPs play and what it means for best practice data retention?

Slide change

Co-Host - Matthew Prouse (DSPANZ): Sure thing Maggie.

So first of all, I acknowledge we live in a connected digital economy where most businesses, employers and taxpayers rely on electronic systems to store their records that they use for other things, capture and record business processes. In fact, there's an increased reliance on software to enable a business to run those day to day operations and meet a range of legislative or regulatory obligations. The software they use captures, processes and stores a wide range of business processes and financial records to support customers.

However, DSPs don't exist in legislation. The record-keeping requirements that exist in Australian law apply to taxpayers or employers. They do not apply to the software that they use.

Through a number of big government projects such as Single Touch Payroll, we've effectively mandated the use of payroll software, but the record-keeping obligation in the law still speak to paper based records.

In fact, if we leverage the terminology from the Europen Union GDPR, DSPs act as data custodians for customers. Their customers, the customers of DSPs, ultimately own the data and records they generate when they use their software or service regardless of where the data is hosted or located. DSPs act as data custodians for as long as the customer is paying for the service or product supplied by the DSP in line with the obligations on the DSP. And the DSP might retain that data for certain periods after they stop paying but that's governed by the terms of use of the software and not any official record-keeping requirements in legislation.

When DSPs retain data on behalf of their customers, it's recommended that they follow best practice security standards and requirements to protect their customer data.

Slide change

Co-Host - Maggie Leese (DSPANZ): Let's move on to data minimisation now.

Slide change

Co-Host - Maggie Leese (DSPANZ): While the principle is simple - collect only the data you need to fulfil a specific business purpose - in the context of this best practice guidance, we're considering how DSPs can delete the historic data they currently hold while continuing to support their current customers and ensuring they have access to the data and records they need.

Co-Host - Matthew Prouse (DSPANZ): While we're talking about data minimisation Maggie, can you explain why it's important for DSPs?

Co-Host - Maggie Leese (DSPANZ): Data minimisation is integral to good data lifecycle management and security practices. Collecting only what is necessary for your software or service to run smoothly reduces the amount of data that you must retain and protect at the end of the day.

Co-Host - Matthew Prouse (DSPANZ): And what practical techniques can DSPs implement to reduce the amount of data they collect?

Slide change

Co-Host - Maggie Leese (DSPANZ): This can be hard one considering different DSPs will collect different data for the software and services they provide. But we recommend three key considerations for reducing the amount of data DSPs collect, categorising them into define, audit and inform.

So first up, clearly define data collection requirements based on business needs and compliance obligations.

Number two, conduct regular audits of your data collection methods to ensure they continue to align with operational needs.

And number three, ensure customers are informed about your data minimisation and retention practices and are kept up to date whenever they change.

DSPANZ also has a best practice document on securely collecting and storing sensitive data, such as TFNs, that may be useful for further reading in this space.

Slide change

Co-Host - Maggie Leese (DSPANZ): Now that we've considered data minimisation, let's look at data retention for DSPs.

How long should different types of business data be retained, and what determines these timelines, Matthew?

Slide change

Co-Host - Matthew Prouse (DSPANZ): So, in the guidance, we categorise the record-keeping obligations and requirements for DSPs into three broad categories. To support customers with respect to income tax returns, in respect to corporate compliance and their obligations as employers.

This slide provides a few examples of the kinds of records that fall into these categories and how long they must typically be retained.

If you visit our website, you will find a list of the most common record-keeping requirements that DSPs should follow to support their customers. The list is also available as an the appendix to the best practice guidance document.

Co-Host - Maggie Leese (DSPANZ): Thanks for that.

Now, the guidance recommends keeping inactive customer data for at least 12 months. Why is that timeframe significant?

Slide change

Co-Host - Matthew Prouse (DSPANZ): So first of all, let's just define inactive customer data. We're talking about customers that no longer have a commercial arrangement with the DSP. They've stoped paying, they've cancelled their service.

As DSPANZ developed the best practice guidance material, we found that DSPs were taking vastly different approaches to retaining and deleting former customer data. In some cases, customer information was removed within minutes of a customer cancelling their subscription or ceasing using a particular service. In others, data was being retained for 7 years or indefinitely. We wanted to land somewhere in the guidance material that reduced how long DSPs are expected to retain data, at their cost, while ensuring that customers have enough time to retrieve what they need to meet their record-keeping obligations.

DSPs who need to meet the ATO's Operational Security Framework are required to retain audit logs for at least 12 months. This is the one record-keeping obligation that genuinely applies to most DSPs operating in Australia. We aligned keeping former customer data for as long as 12 months with the audit logging requirement in the Operational Security Framework. This means if an incident does occur and it impacts an inactive or former customer, the data and the audit logs are available to help with the investigation. Essentially, the DSP can review the logs that were generated and the customer data that was impacted as part of their incident management process.

Slide change

Co-Host - Matthew Prouse (DSPANZ): We know that transforming or changing data minimisation, retention and deletion practices can present some challenges for some DSPs.

Maggie, what are the key challenges that are covered in the document and how can DSPs overcome them?

Co-Host - Maggie Leese (DSPANZ): For some DSPs, following this guidance will involve significant changes to their data management practices, which ultimately impact their customers.

DSPs will need to communicate with their customers about their roles and responsibilities, ensuring they're informed about how they can access their data when they need to, particularly if they stop being a customer.

We also know there will be challenges with deleting all instances of data or records from a system. It can be very challenges to go down the rabbit hole and find where everything has ended up. Where this is the case, DSPs could look to anonymise any personally identifiable information that can be found across data sets.

And one last challenge for DSPs who allow third party apps to connect and share data, such as a point of sale system connecting to an accounting software platform, is that DSPs may not have complete copies of the broader tax or business records from that point of sale system. Here, DSPs should advise their customers that they cannot be solely relied upon to access that full data set from their point of sale system.

Do you have any challenges or tips to round us out, Matthew?

Co-Host - Matthew Prouse (DSPANZ): I think the last one is DSPs need to be very mindful of their terms of use and make sure that they say what they do and do what they say with respect to their terms of use. If your Ts and Cs say that the customer is obliged to keep backups and retain records themselves and aren't relying on the software for legal purposes, you need to give them a mechanism to allow them to back up and extract their data for that purpose. Similarlym if your Ts and Cs say that you don't retain any data for more than 30 days after they stop paying your, or 12 months as we recommend, you need to make sure that you don't have any data after 12 months to follow best practice guidance.

So being aware of what your terms and conditions are and how you communicate them to customers, being transparent about them and being transparent about the data retention process and the data minimisation processes in your terms and conditions are going to be really critical as you navigate the kind of of change management for you and your paying and your non-paying customers.

Co-Host - Maggie Leese (DSPANZ): That's a great call out. Thanks.

Co-Host - Matthew Prouse (DSPANZ): Maggie, we've covered quite a lot around data minimisation and retention for DSPs today. Here are the key takeaways.

Slide change

Co-Host - Matthew Prouse (DSPANZ): DSPs play a critical role in helping businesses meet their record-keeping obligations and act as data custodians while retaining their paying customers' data.

Data minimisation practices not only help to minimise how much data DSPs collect but are also part of good cyber security practices.

DSPs should take a customer-centric approach to transforming their data retention practices and policies and should be mindful of changes to the Privacy Act.

What are some of the recommend next steps for our audience, Maggie?

Slide change

Co-Host - Maggie Leese (DSPANZ): We encourage DSPs to download the complete best practice guidance from the DSPANZ website and conduct a review of your data handling practices and policies to implement this best practice guidance.

If you do feel the need to reach out, you might have some questions about the guidance or about DSPANZ, contact us at hello@dspanz.org.

Thank you all for joining in and please don't hesitate to reach out to DSPANZ. Thank you.

Co-Host - Matthew Prouse (DSPANZ): Thank you.