TPB Practice Note
TPB(PN) 1/2017

Cloud computing and the Code of Professional Conduct

Tax Practitioners Board practice note

The Tax Practitioners Board (TPB) has released this practice note to provide practical guidance and assistance to registered tax practitioners in understanding their obligations under the Code of Professional Conduct in relation to the use of cloud computing.

Disclaimer

This is a Tax Practitioners Board (TPB) practice note (TPB(PN)). It is intended to be for information only. While it seeks to provide practical assistance and explanation, it does not exhaust, prescribe or limit the scope of the TPB's powers in the *Tax Agent Services Act 2009* (TASA) or the Tax Agent Services Regulations 2022(TASR).

In addition, please note that the principles and examples in this TPB(PN) do not constitute legal advice and do not create additional rights or legal obligations beyond those that are contained in the TASA or which may exist at law.

Document history

The TPB originally released this document as a draft practice note in the form of an exposure draft on 13 October 2016, based on the TASA as at 5 March 2016. The closing date for the submissions was 28 November 2016.

The TPB considered the comments and submissions received and now publishes the following TPB(PN).

On 1 April 2022, the TPB updated this TPB(PN) to remove references to tax (financial) advisers and replace references from the repealed Tax Agent Services Regulations 2009 to Tax Agent Services Regulations 2022.

Issue date: 25 January 2017

Last updated: 1 April 2022

Cloud computing and the Code of Professional Conduct

Introduction

1. This practice note has been prepared by the Tax Practitioners Board (TPB) to provide practical guidance and assistance to registered tax agents and BAS agents (collectively referred to as tax practitioners) to understand their obligations under the Code of Professional Conduct (Code), as contained in section 30-10 of the *Tax Agent Services Act 2009* (TASA), in relation to the use of cloud computing.

2. In this practice note, you will find the following information:
    - what is cloud computing? (paragraphs 3 to 6)
    - factors to consider when entering into cloud arrangements (paragraphs 7 to 16)
    - consequences of having inadequate cloud arrangements (paragraph 17 and 18)
    - where to find further information (paragraph 19).

What is cloud computing?

3. Cloud computing, at a broad level, is the provision of information technology resources as a service through a network (including storing, managing and processing data), typically over the internet, instead of using a local server or a personal computer.

4. Services can range from data storage to the use of software programs, with data being stored and processed by a cloud service provider. It can include applications, databases, email and file services, and entrusts remote services with a user's data, software and computation. In particular, cloud computing services are usually grouped into the following categories:
    - Software as a service – the provision of software over a network rather than the software being loaded directly onto a locally available computer.
    - Platform as a service – the provision of computing platforms that create the environment for other software to run (for example, operating systems) over a network rather than being loaded directly onto a locally available computer.
    - Infrastructure as a service – the provision of access to computer infrastructure (for example, data storage or processing capability) over a network that is used to complement local platform resources. Outsourced cloud storage services may involve sharing, creating or storing information on remote servers accessed through the internet. The data can be stored either onshore or offshore depending upon what contractual agreement the client reaches with the provider.
    - Combination of the above.

5. These services are generally operated from facilities located in premises remote from the places where the data was created. All information stored in a cloud service is physically located somewhere in one or more data centres. Information refers to the acquiring or deriving of knowledge (directly or indirectly) and includes capturing information known about a client.

6. Tax practitioners may use cloud computing for a range of purposes, such as information storage, lodgement of returns, digital signatures, client information portals and practice management software.

Factors to consider when entering into cloud arrangements

General considerations

7. When entering into cloud arrangements, various factors will need to be considered, depending on the nature of the particular cloud arrangement and also the circumstances of the tax practitioner. However, as a starting point, tax practitioners may wish to consider the following general factors:

    - what are the details of any limitation of liability arrangements (for example, clauses contained in the terms and conditions of the cloud provider agreement(s) or terms of use)?
    - whether the provider is allowed to unilaterally change relevant terms of the agreement (that is, without input from the tax practitioner), including in relation to how or where data is stored or managed?
    - how is the information being transferred between systems and data integrity being maintained?
    - how is the information being stored?
    - whether information is being held offshore (that is, information that is stored or processed in equipment not located in Australia) and, if so, the consequences (including relevant additional legislative and regulatory requirements that the information may be subject to)?
    - what processes does the cloud provider have in place in relation to the backup and archiving of information (such as multiple backup servers)?
    - what security controls are the tax practitioner and provider responsible for (such as issues around passwords, encryption and backups)?
    - what protections are in place to prevent service access being disrupted?
    - what processes are in place for managing and resolving disputes in relation to access to client information?
    - what processes are in place when the arrangement ends (including, for example, the return of or access to data held in the cloud)?

Code obligations

8. When entering into cloud arrangements, tax practitioners should also be mindful of their obligations under the Code. The Code, as contained in section 30-10 of the TASA, regulates the personal and professional conduct of tax practitioners, and contains obligations in relation to honesty and integrity, independence, confidentiality, competency, and other obligations, such as responding to requests from the TPB.

9. In particular, it is important to be mindful of Code Item 6 which provides that a tax practitioner must not disclose any information relating to a client's affairs to a third party without the client's permission, unless there is a legal duty to do so.

10. A third party is any entity other than the client and the tax practitioner. This includes entities that maintain offsite data storage systems (including 'cloud storage'), recognising that there is a distinction between data storage that a third party cannot effectively access (for instance, through the use of encryption) and disclosure to a third party.

11. It is only necessary that the information relates to the affairs of a client. Therefore, the information does not have to belong to the client, or have been directly provided by the client to the tax practitioner.

12. Relevant factors to consider in ensuring compliance with Code item 6, among other things, include the following:

    - Tax practitioners must obtain permission from each client prior to divulging client information to a third party (including cloud service providers). When obtaining this permission, it is recommended that the tax practitioner clearly inform the client about the proposed disclosure (including noting to whom and where the disclosure will be made, and where data will be stored). A general authority consenting to disclosure to third parties may also be acceptable.
    - Client permission may be by way of a signed letter of engagement (refer to *TPB(PN) 3/2019 Letters of engagement*), signed consent, or other communication such as a relevant 'fact find' and consent.
    - There should be appropriate controls to maintain confidentiality and integrity (such as encryption) to avoid any information leakage, including as a result of:
        - inadvertent disclosure
        - any change in IT assets (such as portable storage devices, software configurations and data fixes)
        - data corruption and accidental deletion.

13. There are a number of controls that could be employed to assist in maintaining and protecting the confidentiality, integrity and availability of data, such as:
    - an appropriate confidentiality agreement between the tax practitioner and their cloud service provider
    - other appropriate protocols, such as:
        - use of a secured website and encrypted network traffic
        - security credentials
        - access controls ensuring unauthorised persons do not have access to data standardised reporting
        - audit trails
        - appropriate segregation of duties
        - approval and review of data changes.

14. For further information, including in relation to 'permission' and 'legal duty', refer to *TPB(I) 21/2014 Code of Professional Conduct – Confidentiality of client information.*

Privacy Act

15. In addition to their obligations under the Code in the TASA, tax practitioners should also be aware that the *Privacy Act 1988* (Cth) sets out a number of Australian Privacy Principles (APPs) which govern the use of, storage and disclosure of personal information.

16. Tax practitioners should seek their own advice about whether the provisions of the Privacy Act apply to them. Information about obligations under the Privacy Act is provided by the Privacy Commissioner and is accessible from the Office of Australian Information Commissioner's website at oaic.gov.au.

Consequences of having inadequate cloud arrangements

17. If a tax practitioner breaches the Code, including in the context of cloud arrangements, the TPB may impose one or more administrative sanctions, including issuing a written caution or order or suspending or termination of a tax practitioner's registration.

18. In addition to the above consequences of any breach of the Code, or any other relevant statutory consequences (such as, from the Privacy Act), a tax practitioner should also consider relevant commercial consequences such as legal action for damages.

Further information

19. Outlined below is a listing of reference material that may provide further guidance in relation to what is cloud computing, general considerations and issues to consider in contemplating a cloud computing arrangement:

	Information product	Purpose of document
Tax Practitioners Board	*TPB(I) 21/2014 Code of Professional conduct – Confidentiality of client information*	Further information regarding Code item 6 in the *Tax Agent Services Act 2009* – confidentiality.
	TPB(PN) 3/2019 Letters of engagement	Further information regarding engagement letters.
	TPB(I) 19/2014: Code of Professional Conduct - Managing conflicts of interest for registered tax and BAS agents	Further information regarding Code item 5 in the *Tax Agent Services Act 2009* – having adequate arrangements for managing conflicts of interest for tax practitioners.
Accounting Professional & Ethical Standards Board Limited	Guidance Note GN 30: Outsourced Services	Provides information in regard to managing risks associated with providing or utilising outsourced services.
Australian Prudential Regulation Authority	Information Paper: Outsourcing involving cloud computing services	Includes guidance on general considerations - including governance arrangements, risk considerations and assurance mechanisms - when assessing the use of Cloud services.
	Prudential Practice Guide: CPG 234 – Information security	Includes guidance in relation to managing security risk.
	Prudential Practice Guide: CPG 235 - Managing data risk	Includes guidance in relation to managing security risk.

	Information product	Purpose of document
Australian Taxation Office	*ATO portal access* and *Standard Business Reporting*, refer to www.ato.gov.au and www.sbr.gov.au	For further information in relation to *ATO portal access* and *Standard Business Reporting.*
Department of Communications	Consumer factsheet: Cloud computing and privacy	Includes information in relation to privacy.
	Consumer factsheet: Questions to ask about a cloud service	Includes information in relation to a list of potential questions to ask a potential cloud service provider in relation to privacy and security.
Department of Defence (Cyber Security Centre)	Cloud Computing Security Considerations	Includes information in relation to security considerations.
Department of Finance	Better Practice Guide: Negotiating the cloud – legal issues in cloud computing agreements	Includes information in relation to a checklist of some legal issues to consider and address in contemplating a cloud computing arrangement.
	Better Practice Guide: Privacy and Cloud computing for Australian government agencies	Includes information in relation to privacy and cloud computing, including a guiding summary of checkpoints.
Department of the Prime Minister and Cabinet	Australia's Cyber Security Strategy	Notes themes of action for Australia's cyber security.
Digital Transformation Agency	Secure Cloud Strategy	Includes information about the Government cloud computing policy.
Office of Australian Information Commissioner	Guide to securing personal information	Provides guidance on protecting personal information and in relation to destroying or de-identifying personal information once information is no longer needed.

	Information product	Purpose of document
	Australian Privacy Principle Guidelines	Outlines requirements of the Australian Privacy Principles (APPs), how the OAIC will interpret the APPs, and matters the OAIC may take into account when exercising functions and powers under the *Privacy Act 1988* (Cth).