TPB practice note
TPB(PN) 4/2021
Use and disclosure of a client's TFN and TFN information in email communications

Tax Practitioners Board practice note

The Tax Practitioners Board (TPB) has released this practice note (PN) to provide practical guidance and assistance to registered tax practitioners in relation to using and disclosing a client's tax file number (TFN) and TFN information in email communications.

Disclaimer

This is a 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 1 September 2020. The closing date for the submissions was 30 September 2020.

The TPB considered the comments and submissions received and now publishes the following TPB(PN) based on the TASA as at 17 February 2021.

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2022, the TPB updated this TPB(PN) to remove references to tax (financial) advisers and replace references from the repealed Tax Agent Services Regulations 2009 to Tax Agent Services Regulations 2022.

Issued: 14 April 2021

Last updated: 1 April 2022

Contents

Use and disclosure of a client's TFN and TFN information in email communications

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 the TPB's position in relation to the use and disclosure of tax file numbers (TFNs) and TFN information by tax practitioners in email communications. For the purposes of this practice note, any reference to tax agent services includes BAS services and tax (financial) advice services, unless otherwise stipulated.
2. In this practice note, tax practitioners will find the following information:
    - protection of TFNs and TFN information (paragraphs 3 to 14)
    - obligations of tax practitioners when using or disclosing a client's TFN and TFN information in email communications (paragraphs 15 to 21)
    - suggested steps to consider when using or disclosing a client's TFN and TFN information in email communications (paragraphs 22 to 26)
    - consequences under the Code of Professional Conduct (the Code) (paragraphs 27 to 29)
    - further information (paragraph 30 to 31).

Protection of TFNs and TFN information

3. TFNs[1] and TFN information[2] are protected by the following non-exhaustive list of legislative frameworks:
    - obligations under the Privacy (Tax File Number) Rule 2015 (TFN Rule)
    - obligations under the *Privacy Act 1988* (Cth) (Privacy Act) and the Australian Privacy Principles (APPs), including –
        - the Notifiable Data Breaches scheme (NDB scheme)
        - APP 11 which requires entities to take reasonable steps to protect the personal information (which includes TFN information) that they hold
    - specific offence provisions under the *Taxation Administration Act 1953* (Cth) (TAA 1953).[3]

---

[1] 'Tax file number' is defined in section 202A of the *Income Tax Assessment Act 1936* (Cth).

[2] 'Tax file number information' is defined in subsection 6(1) of the *Privacy Act 1988* (Cth). It means information, whether compiled lawfully or unlawfully, and whether recorded in a material form or not, that records the tax file number of a person in a manner connecting it with the person's identity.

[3] For further information on other legislative frameworks relating to the handling of TFNs, see the Office of the Australian Information Commissioner's guidance on Tax file numbers and The Privacy (Tax File Number) Rule 2015 and the protection of tax file number information (as at 26 June 2019).

4. The TPB is not responsible for the administration of any specific legislation relating to the use and disclosure of TFNs. The Australian Information Commissioner and Commissioner of Taxation are primarily responsible for the administration of the laws relating to the use and disclosure of TFNs and TFN information.

5. The Australian Information Commissioner's responsibilities in relation to an individual's TFN information and personal information are set out under the Privacy Act.[4]

6. The TFN Rule issued under the Privacy Act regulates the collection, storage, use, disclosure, security and disposal of individuals' TFN information by TFN recipients (such as tax practitioners).[5] It requires that TFN information must only be used or disclosed (including for matching personal information about individuals) by TFN recipients for the following purposes:

    - for a purpose authorised by taxation law, personal assistance law or superannuation law; or
    - for the purpose of giving an individual any TFN information that the TFN recipient holds about that individual.[6]

7. The TFN Rule further requires that TFN recipients must take reasonable steps to protect TFN information from, amongst other things, unauthorised access, use, modification or disclosure.[7] TFN recipients are also required to take reasonable steps to:

    - ensure that access to records containing TFN information is restricted to individuals who need to handle that information for taxation law, personal assistance law or superannuation law purposes[8]
    - securely destroy or permanently de-identify TFN information where it is no longer required by law to be retained, or necessary for a purpose under taxation law, personal assistance law, or superannuation law (including the administration of such law)[9]
    - ensure that all staff are aware of the need to protect individuals' privacy when handling TFN information.[10]

8. The NDB scheme under the Privacy Act effectively mandates a reporting and notification process for eligible data breaches which are likely to result in serious harm to individuals whose personal information is involved. TFN recipients are also covered by the NDB scheme, in so far as any eligible data breach involves TFN information.[11]

---

[4] See subsection 5(2) of the TFN Rule.

[5] See sections 5(1) and 10 of the TFN Rule. Also, 'TFN recipient' is defined in subsection 6(2) of the TFN Rule and has the same meaning as 'file number recipient' in the Privacy Act. A TFN recipient includes, amongst other things, an approved recipient, authorised recipient and the trustee of a superannuation fund.

[6] See section 10 of the TFN Rule.

[7] See paragraph 11(1)(a) of the TFN Rule.

[8] See paragraph 11(1)(b) of the TFN Rule.

[9] See subsection 11(2) of the TFN Rule.

[10] See section 12 of the TFN Rule.

[11] For further information on the application of the NDB scheme to tax practitioners, see the TPB's guidance on the *Notifiable Data Breaches scheme*.

9. As the TFN information of an individual is also personal information (as defined in the Privacy Act),[12] any tax practitioner who is subject to the APPs under the Privacy Act must also generally comply with the requirements under APP 11.1 to take reasonable steps to protect this information from:

    - misuse, interference and loss; and
    - unauthorised access, modification or disclosure.[13]

10. According to the Office of the Australian Information Commissioner (OAIC), an 'interference' includes an attack on a computer system that leads to exposure of personal information and an 'unauthorised access' includes any access by someone who is not permitted to do so. 'Unauthorised disclosure' occurs when an entity makes personal information accessible or visible to others outside the entity, and releases that information from its effective control – for example, sending an email containing TFN information to the wrong recipient would likely constitute an unauthorised disclosure.[14]

11. APP 11.2 provides that those subject to the APPs, who hold personal information of an individual, must also take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed for any purpose for which it may be used or disclosed under the APPs.[15]

12. The OAIC has also published guidance in *'The Privacy (Tax File Number) Rule 2015 and the protection of tax file number information'* and *'Guide to securing personal information'* on what action entities subject to the Privacy Act and TFN recipients (including tax practitioners) should consider taking to comply with the obligations under the APPs and the TFN Rule to protect personal information they hold. This guidance also covers recommended steps to safeguard TFN information from unauthorised loss, use or disclosure, whether this information is recorded in physical or electronic form (such as in an email).[16]

13. These steps include appropriate information and communication technology (ICT) and other security measures, and particularly suggested procedures to manage email communications of TFNs and improve the security of TFN information contained in emails, as email is, in itself, not considered to be a secure form of communication.[17] This is noting that, generally, due to technological systems and protocols, an email may be vulnerable to unauthorised access during transmission from sender to recipient, including when passing through networks and when stored on intermediate email servers.

14. In addition to the above, the TAA 1953 (which is administered by the Commissioner of Taxation) includes specific offence provisions in relation to the unauthorised recording, maintaining a record of, use or disclosure of a person's TFN, subject to certain exceptions.18 The TAA 1953 provisions protect the TFNs of all entities, including individuals and other entities such as corporations, partnerships, superannuation funds and trusts.

[12] See subsection 6(1) of the Privacy Act.

[13] See APP 11.1 in Part 4 of Schedule 1 to the Privacy Act.

[14] See the OAIC's APP guidelines, in particular, *Chapter 11: APP 11 – Security of personal information* (as at 22 July 2019).

[15] See APP 11.2 in Part 4 of Schedule 1 to the Privacy Act.

[16] These guides are available on the OAIC website.

[17] See Part B of the OAIC's *Guide to securing personal information*, as at 5 June 2018.

Obligations of tax practitioners when using or disclosing a client's TFN and TFN information

15. The TPB expects all tax practitioners to consider the relevant legislation and guidance, and in particular the TFN Rule, when including TFNs or TFN information of clients in email communications and whether such record or disclosure is appropriate and secure in the circumstances, noting that there is a risk of inadvertent disclosure to third parties when communicating over emails (for example, the risk of emails being intercepted by third parties).[19]

16. Steps taken by a tax practitioner to comply with the relevant legislation may also assist to ensure ongoing compliance with their obligation under subsection 30-10(6) of the Code in the *Tax Agent Services Act 2009* (TASA) to maintain client confidentiality. Code Item 6 requires that a tax practitioner must not disclose any information relating to a client's affairs to a third party[20] unless:

    - the tax practitioner has the client's permission; or
    - there is a legal duty to do so.[21]

17. To further minimise any risk of a breach of Code Item 6, in circumstances involving a disclosure of a client's TFN information by email without the client's permission, the TPB strongly recommends that tax practitioners seek prior specific written authority for any proposed disclosure, including the entity that will receive the information and the use of email to disclose the information. This may include under a signed letter of engagement or consent from the client. However, it is noted that obtaining the client's permission does not override the broader privacy and security obligations of tax practitioners under the TFN Rule and APP 11, that is, tax practitioners must still take reasonable steps to protect TFN information sent via email. The TPB also expects that tax practitioners ensure they have appropriate arrangements in place to prevent inadvertent disclosure of a client's TFN and TFN information to third parties.

[18] See section 8WB of the TAA 1953.

[19] Note: The ATO expects that tax practitioners use the ATO's portal mail when electronically communicating TFNs and/or TFN information to the ATO, as the ATO is unlikely to accept email as a secure channel for communicating TFNs and/or TFN information.

[20] For the purposes of Code Item 6 and the TASA, a third party means any entity other than the client and the tax practitioner.

[21] For further information in relation to client permission and what is a legal duty, see *TPB(I) 21/2014 Code of Professional Conduct – Confidentiality of client information for registered tax and BAS agents*.

18. In relation to all TFNs generally (including of individuals and other entities) and whether a disclosure by a practitioner of a TFN in an unsecured email would amount to an offence under the TAA 1953; this would be determined by the surrounding circumstances and would include consideration of the steps taken by the tax practitioner. As a matter of best practice and to minimise the risk of any unauthorised access or disclosure of a client's TFN (whether an individual or other entity client), the TPB strongly recommends that tax practitioners have regard to the requirements under the TFN Rule, in addition to the TAA 1953, when recording and disclosing all client TFNs in email communications.

19. Whether a communication of a client's TFN in an email breaches the relevant legislation will depend on the facts and circumstances of the disclosure, including whether the tax practitioner had taken reasonable steps to have ICT controls in place to protect the security of the TFN. According to the OAIC's guidance, what steps are reasonable in a given case ultimately depends on the circumstances of the tax practitioner, which include:

    - the nature of the tax practitioner entity
    - the amount and sensitivity of the personal information held by the tax practitioner (for example, if a tax practitioner holds TFN information relating to a significant number of clients, they should adopt more rigorous and reliable security measures to safeguard electronically secured and communicated information)
    - the possible adverse consequences for an individual in the case of a breach (in relation to any resulting loss or misuse of TFN information, these consequences include the risk of identity theft)
    - the practical implications (such as time and cost) involved in implementing the security measure
    - whether the security measure itself is privacy invasive.[22]

20. As such, the inclusion of a client's TFN in an email by a tax practitioner does not, on its own and without further information, necessarily give rise to a breach of a law regulating the use and disclosure of TFNs. However, if such communication occurs in circumstances where the tax practitioner has not taken reasonable steps and strategies to safeguard this information (which can include ICT measures to increase the security of information stored on emails and recorded in email communications), the tax practitioner may breach obligations under the Privacy Act and TFN Rule.

21. The TPB recommends that tax practitioners review their practices, procedures and systems in relation to the use and disclosure of TFNs and TFN information in email communications to ensure they comply with their obligations under the relevant legislation.

[22] See Part A of the OAIC's *Guide to securing personal information*, as at 5 June 2018.

Suggested steps to consider when using and disclosing a client's TFN and TFN information in email communications

22. Consistent with guidance published on the OAIC website, the TPB considers the following non-exhaustive list are reasonable steps for tax practitioners to adopt to protect the security of electronically held TFNs and TFN information of clients, and to ensure compliance with the relevant legislation, particularly the Privacy Act and TFN Rule:

    - implementing security measures to restrict access to records containing this information to only those staff who need to handle this information under taxation, personal assistance or superannuation law
    - having governance, culture and training frameworks in place to foster staff awareness of privacy and security (for example, maintaining authority and accountability for decisions relating to personal information security, and providing staff training on physical and ICT security and information handling)
    - taking ICT security measures to protect practice hardware and software from loss or unauthorised access, use or disclosure – for example:
        - regular software and application tests
        - maintaining current versions of software and applications and effective security software across all network components
        - maintaining network intrusion prevention and detection systems
        - procedures to manage email communications of TFN information
    - encryption of systems, devices and communications that record TFN information
    - having policies, procedures and resources in place to determine whether TFN information held by the tax practitioner needs to be destroyed or de-identified.

23. The TPB further suggests that tax practitioners should consider the following non-exhaustive list of ICT security measures and procedures to protect the security of TFNs and TFN information in email communications:

    - using more secured methods than email to communicate this information – for example, a secure website, online mailbox or secure messaging (where appropriate and available)
    - validating the email address with a recipient before sending any unencrypted email to them, to minimise the risk of unauthorised disclosure to a person who is not the intended recipient
    - only sending this information by email as an encrypted or password protected attachment
    - using software which redacts TFNs and TFN information within documents
    - maintaining records of emails sent and received.

24. The TPB also recommends that tax practitioners have the following non-exhaustive list of ICT controls in place to protect the security and confidentiality of client records (which may include TFNs) and minimise the risk of a cyber attack:

    - installing and maintaining anti-virus software on workplace computers
    - deploying firewalls on workplace computers and/or workplace networks
    - ensuring that computer operating systems and programs always have the latest security patches
    - protecting client records or files, using encryption where possible
    - regularly changing passwords
    - using, wherever possible, a second form of authentication to protect online accounts (for example, email).

25. Given that the above lists are not intended to be prescriptive or exhaustive, tax practitioners should exercise their professional judgment when considering what steps should be taken in their particular circumstances and may wish to seek independent professional advice from an ICT security provider about what controls are appropriate for their business and risk circumstances.[23]

26. The TPB also encourages tax practitioners to contact the Australian Taxation Office (ATO) and/or the OAIC, or refer to the information published on their websites for any further guidance on obligations under the Privacy Act and TAA 1953 regarding the use and disclosure of TFNs and TFN information in email communications.

Consequences for non-compliance under the TASA

27. If a tax practitioner fails to take reasonable steps to protect the TFNs and / or TFN information of clients, there may be implications in relation to the TASA, in particular, Code Item 6 (client confidentiality).

28. If a tax practitioner breaches the Code, the TPB may impose one or more administrative sanctions, as follows:

    - issuing a written caution
    - imposing an order requiring the tax practitioner to take one or more actions
    - suspension of registration
    - termination of registration.

29. Ultimately, determining whether a tax practitioner has contravened the TASA (including the Code) will be a question of fact. This means that each situation will need to be considered on a case-by-case basis having regard to the particular facts and circumstances of that case.

[23] For further information, the Australian Cyber Security Centre provides advice and information on a range of cyber security topics for agents of government services.

Further information

30. Further guidance about obligations under the Privacy Act (including the NDB Scheme and APPs) and the TFN Rule are provided by the OAIC and accessible from its website at www.oaic.gov.au.

31. Outlined below is a listing of reference material that may provide further guidance in relation to issues to consider when using and disclosing a client's TFN and TFN information in email communications:

Agency	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 TASA – confidentiality of client information.
	Notifiable Data Breaches scheme	Provides guidance on the application of the Notifiable Data Breaches scheme to tax practitioners.
	TPB(PN) 01/2017: Cloud computing and the Code of Professional Conduct	Provides practical guidance and assistance to tax practitioners in understanding their obligations under the Code of Professional Conduct in relation to the use of cloud computing.
	TPB(PN) 3/2019: Letters of engagement	Provides practical guidance and assistance to tax practitioners in relation to the use of letters of engagement.
Australian Taxation Office	Data breach guidance for tax professionals	Provides information and guidance on data breaches for tax professionals.
	Online security	Provides general information and guidance on online security.
	Top cyber security tips for individuals	Provides general guidance on the top identity security tips to keep information safe for individuals.
	Top cyber security tips for businesses	Provides general guidance on the top identity security tips to keep information safe for businesses.
	Digital record keeping for businesses	Provides general guidance on how to choose suitable record-keeping software.

Office of the Australian Information Commissioner	The Privacy (Tax File Number) Rule 2015 and the protection of tax file number information	Provides a number of steps an agency or organisation should consider to protect the privacy of TFN information and ensure compliance with the binding TFN Rule issued under section 17 of the *Privacy Act 1988* (Cth).
	Tax file numbers	Provides an overview of the legislation and guidance materials relating to the handling of TFNs.
	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.
	Notifiable Data Breaches	Provides information on the Notifiable Data Breaches scheme.
	Australian Privacy Principles Guidelines	Outlines the mandatory requirements of the 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).
	Rights and responsibilities	Provides guidance on the rights of individuals under the *Privacy Act 1988* (Cth), what organisations and agencies it covers and does not cover.
Australian Cyber Security Centre	Cyber Security for Agents of Government Services	Provides advice and information on a range of cyber security topics, such as, multi-factor authentication, passwords, PINs and passphrases, protecting businesses online, and preparing for and responding to cyber security incidents.
Australian Prudential Regulation Authority	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.