TD 2002/16 - Income tax: what are the obligations under the Income Tax Assessment Act 1936 where a business chooses to keep some of its records as encrypted information?

Taxation Determination

Income tax: what are the obligations under the *Income Tax Assessment Act 1936* where a business chooses to keep some of its records as encrypted information?

Preamble
The number, subject heading, date of effect and paragraphs 6 to 10 of this Taxation Determination are a 'public ruling' for the purposes of Part IVAAA of the Taxation Administration Act 1953 and are legally binding on the Commissioner. The remainder of the Determination is administratively binding on the Commissioner. Taxation Rulings TR 92/1 and TR 97/16 together explain how a Determination is legally or administratively binding.

Date of Effect
This Determination applies to years commencing both before and after its date of issue. However, this Determination does not apply to taxpayers to the extent that it conflicts with the terms of settlement of a dispute agreed to before the date of the Determination (see paragraphs 21 and 22 of Taxation Ruling TR 92/20).

1. When a person carrying on a business chooses to process and keep records in an electronic form, the records must be in a form which the ATO can access and understand in order to ascertain that person's taxation liability. This includes encrypted records.

2. Cryptography is the art and science of secret writing and communication. It has a long history extending from ancient times right up to present day.

The CSIRO has stated that:

> *'Classical cryptography is used to protect the contents of a message from being viewed by unauthorised parties. It is the art of transforming the contents of a message from its original form to one that cannot be decoded by unauthorised parties. This ensures that the message remains incomprehensible to unauthorised eyes, even if intercepted.*
>
> *The process of transforming the message from its original form to its incomprehensible form is known as **encryption** . The message to be encrypted is usually referred to as plaintext , and the encrypted message is known as **ciphertext** . The process of transforming the message from its incomprehensible form back to its original form is known as **decryption** . The function used to encrypt and decrypt the message is known as a **cryptographic algorithm**.'*[1]

[1] 1 Report of the Research Group into the Law Enforcement Implications of Electronic Commerce (RGEC), "The emerging Information Security Infrastructure", Research and Technical Advice (Vol 3), 1999, at page 91. A copy of this report is available, as at the date of publication of this Taxation Determination, at http://www.austrac.gov.au/text/publications/rgec/3/index htm.

3. Cryptography is today part of many business's data security arrangements and is being increasingly adopted to ensure trust in key elements of digital transactions, including integrity and confidentiality. Encryption is a component of cryptography and provides for confidentiality by "scrambling" a message so that it is virtually impossible for other people to read unless they have a "key"[2].

4. Encryption as explained by the CSIRO statement in relation to digital transactions is done by using a computer and software that applies a mathematical algorithm to a digital file associated with the original information (e.g., a text file). The algorithm generally uses large, unique numbers called "keys" in this process and transforms the plaintext into cyphertext. Without access to the correct key, data encrypted for confidentiality cannot be returned to plaintext without the expenditure of extraordinary computer power over periods of time.

5. Encryption is used by many businesses as one way to achieve security in an open network like the internet. Many commercial arrangements or transactions performed over the internet require a secure environment in which to take place. For example, encryption has enabled credit cards to be used as electronic payment systems on the internet by protecting the details of the card, cardholder and transaction during transmission.

6. Section 262A of the *Income Tax Assessment Act 1936* ('ITAA 1936') provides that a person carrying on business must keep records that record and explain all transactions and other acts that are relevant for the purposes of the ITAA 1936. Under subsection 262A(3), the person is required to keep records in the English language or in a form readily accessible and convertible into English and to keep records so as to enable the person's liability under the ITAA 1936 to be readily established. This would include all data not only encrypted data, including tables of figures and other non-text (e.g., numeric) data. The Explanatory Memorandum to the *Taxation Laws Amendment Bill* (No 5) 1989[3] that introduced subsection 262A(3) into the ITAA 1936 explained, at Clause 42:

> *'Subsection 262A(3) obliges a person who is required by the section to keep records, to keep those records:*
>
> - *by paragraph (a) - in the English language or, if not in written form (e.g., in an electronic medium such as magnetic tape or computer disc), in a form which is readily accessible and convertible into writing in English; and*
> - *by paragraph (b) - so as to enable the person's assessable income and allowable deductions, and any credits to which the person is entitled, to be readily ascertainable.'*

7. Where data encryption is used the record keeping requirements of section 262A will not be met unless:

- the encryption key, and all other means to decrypt the records, are maintained, or
- decrypted records are also kept.

8. Under section 263 the Commissioner or any duly authorised officer has the right of full and free access to all buildings, places, books, documents and other papers including electronically stored records required for the purposes of the ITAA 1936. The provision

---

[2] A detailed discussion of Internet security issues is contained in the RGEC Report Research and Technical Advice (Vol 3) 1999 (see footnote 1 above).

[3] The Bill was subsequently passed and became *Taxation Laws Amendment Act (No 5)* 1989.

enables an authorised officer to access and copy records held on an electronic storage medium.

9. Subsection 263(3) requires the occupier of a building or place to provide an authorised officer with all "reasonable facilities and assistance" for the effective exercise of powers under the section. In the context of electronically stored records, reasonable facilities and assistance extend to the provision of login codes, keys including encryption keys, passwords, etc, and access to hard copies of the records as well as allowing the authorised officer to read computer and software manuals. There are penalties under the tax law for failing to do so.

10. All records, including those kept for the purposes of the ITAA 1936, should be able to be examined by the ATO to determine their authenticity and their integrity. This may also include updating all of the encrypted data to allow for that data to remain accessible in the event of changes to either computer hardware or software and to ensure that the data stored on magnetic or other media does not become 'corrupted' over time.

11. Businesses should adopt prudential practices to reduce the likelihood of loss of decryption keys. These could include keeping a copy written down or on other storage media such as a floppy disk in a safe place or by the use of trusted third party arrangements.

Commissioner of Taxation
3 July 2002

Previous draft:
Not previously issued in draft form

Related Rulings/Determinations:
TR 92/1; TR 92/20; TR 97/16

Subject references:
- encryption
- record keeping
- audit
- electronic records
- internet

L*egislative references:*
- TAA 1953 Part IVAAA
- ITAA 1936 262A
- ITAA 1936 262A(3)
- ITAA 1936 263
- ITAA 1936 263(3)

ATO references:
NO: 2002/009086
ISSN: 1038-8982