



Telecommunications (Interception and Access) Act 1979

Guideline – Data Retention

Overview

This Guideline has been prepared to assist service providers to understand their data retention obligations arising from Chapter 5 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

This guide also contains information to assist providers to apply for an exemption from, or a variation of, their obligations. A template form, Data Retention Exemption and/or Variation Application, is available from the Communications Access Coordinator (CAC).

Carriers and carriage service providers (CSPs), including Internet Service Providers (ISPs) (referred to as Service Providers throughout the rest of this document), have legislative obligations under the *Telecommunications Act 1997* (the Telco Act) and the TIA Act to provide assistance to law enforcement and national security agencies.

Assistance can take many forms, but most commonly involves providing information regarding consumers of telecommunications services and their communications for the purposes of:

- enforcing the criminal law and laws imposing pecuniary penalties
- assisting the enforcement of the criminal laws in force in a foreign country and of international law
- protecting the public revenue, and
- safeguarding national security.

Service providers must meet their obligations under both Acts. Penalties may be imposed for non-compliance, so it is important that carriers and CSPs are aware of their obligations. Breach of a carrier licence condition or a carriage service provider rule may lead to legal proceedings.

It is the responsibility of service providers to be aware of any changes to legislation and regulatory arrangements. Service providers are encouraged to seek independent legal advice about their obligations.

Obligation to retain Information and Documents

The TIA Act requires ‘**service providers**’ who operate a ‘**relevant service**’ to keep or cause to keep specified information or documents containing information of that kind relating to any communications carried by means of the relevant service.

Relevant Services

The data retention obligations apply to a service that is:

- A. for carrying communications or enables communications to be carried, by guided or unguided electromagnetic energy
- B. operated by a carrier, carriage service provider, or internet service provider
- C. operated by a person that owns or operates, in Australia, infrastructure that enables the provision of any relevant service, and
- D. not otherwise excluded.

For example, a voicemail service or an authentication system that enables communications to be carried are “relevant services”. An example of a service that is **not a relevant service** is a domain name system (DNS)

service. DNS is required for the operation of communication but it does not enable communications within the legislative scheme.

In some instances, the CAC may declare that services otherwise excluded as “relevant services” are subject to the data retention obligations. For example, the CAC may determine an otherwise excluded service is of significant investigative value to law enforcement or security agencies. To date, the CAC has not made a determination.

Retention period

In accordance with section 187C of the TIA Act, service providers must retain the required data for at least two years, starting when the information or document is created. A provider may keep the data for longer periods for its own business purposes.

Service providers must also keep subscriber information throughout the life of the account and for a further two years after closure of the relevant account.

Note this advice relates to requirements of the TIA Act. Service providers may also have data retention obligations under other legislation.

Information required to be retained

The TIA Act sets out the types of data that a service provider must retain to comply with the obligation at section 187AA. This data, including some explanation and examples, is set out in Annexure A.

Service providers will need to consider the data for each of the services they offer. Depending on the type of service offered, service providers may not be required to retain all of the categories.

The data to be retained is set out in six categories:

1. the subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service
2. the source of a communication
3. the destination of a communication
4. the date, time and duration of a communication, or of its connection to a relevant service
5. the type of a communication or of a relevant service used in connection with a communication, and
6. the location of equipment, or a line, used in connection with a communication.

The data to be retained must be encrypted and protected from unauthorised interference or unauthorised access.¹ A table with further information and examples is provided below.

Information not subject to retention requirement

Service providers are not required to retain:

- A. information that is the content or substance of a communication
- B. in the case of internet access services, information that states an address to which a communication was sent on the internet (that is, internet browsing history)
- C. information that the service provider is required to delete because of the *Telecommunications (Service Provider — Identity Checks for Prepaid Mobile Carriage Services) Determination 2017*, or
- D. information about the location of a telecommunications device that is not information used by the service provider in relation to that service.

¹ Section 187BA

Immediate Circle

The obligation to retain data does not apply to a service provider if the service is provided only to a person's "immediate circle", within the meaning given by section 23 of the Telco Act. The immediate circle exclusion will typically exclude corporate networks that are not available to the public. For example, where a university offers internet services to only current staff and students (excluding alumni), that service may fall within the "immediate circle" exclusion.

For service providers who are an individual or a partnership, the immediate circle includes all employees and management. For body corporate service providers, the immediate circle includes officers of the body corporate, any other body corporate related to the company and the officers of those related bodies corporate.

Same Area

The obligation to retain data does not apply to a service provider whose service is provided only to places that are in the "same area" as defined in section 36 of the Telco Act.

Generally, places are in the same area if they are in the same property. Places may also be in the same area if they consist of properties that are next to each other and the principal users of the properties are the same. For example, the same area exception will apply to local area networks and wireless access points serving one building, or one organisation spanning adjacent properties.

Broadcasting

The data retention obligations do not apply to a broadcasting service within the meaning of the *Broadcasting Services Act 1992*. The exclusion of broadcasting services will typically exclude services that deliver television or radio programs. The exclusion does not apply to on-demand services such as ABC iView or Netflix.

Applying for Exemptions or Variation of Obligations

A CAC may exempt a service provider from its data retention obligations in full or in relation to a particular service, or vary a service provider's obligations in full or relation to a particular service. A provider may apply to the CAC for an exemption.

Exemption applications will be considered on a case-by-case basis and are treated as confidential by the CAC. Failure to maintain reasonable confidentiality regarding the existence of an approved exemption may result in the exemption being revoked. Providers can share particulars of exemptions with third party contractors or vendors as necessary to develop compliant systems, and with wholesalers where there is a commercial agreement to retain data on their behalf.

Factors considered by the CAC in deciding upon exemption or variation application

In considering exemption and variation applications, the CAC must take into account:

- A. the interests of law enforcement and national security
- B. the objects of the Telco Act.
- C. the service provider's history of compliance with its data retention obligations
- D. the service provider's costs, or anticipated costs, of complying, and
- E. any alternative data retention or information security arrangements that the service provider has identified (for example, if the service provider is requesting to be exempted from some items of the data set but proposes to fully comply with other items).

The principal objects of the Telco Act are to provide a regulatory framework that promotes:

- the long-term interests of end-users of carriage services or of services provided by means of carriage services
- the efficiency and international competitiveness of the Australian telecommunications industry, and

- the availability of accessible and affordable carriage services that enhance the welfare of Australians.

The CAC may also take into account any other relevant matters. These include:

- the number of subscribers and market share of the service provider
- the degree to which an exemption would effectively mitigate costs and minimise impacts on the service provider's cash flow, and
- the adequacy of current arrangements or partial capability that can be implemented.

Approval process

Once received, the CAC distributes exemption and variation applications to law enforcement agencies and security authorities for consideration. The CAC may also provide applications to the Australian Communications and Media Authority (ACMA). The CAC considers the agencies' comments before making a decision about whether to grant the exemption or variation.

The CAC has 60 days to make a decision on the application. In the event that a decision is not made and communicated to the service provider within 60 days, the exemption or variation is taken to have been granted on the terms set out in the application. This agreement remains in effect until the CAC makes a decision and communicates it to the service provider.

After considering the application, the CAC will respond in writing to the person nominated as the contact person in the application. The CAC may review exemptions, which may involve contacting relevant service providers.

Access by law enforcement and national security agencies

Where access to retained data is required, an authorised officer of an enforcement agency or an eligible person in a security agency will approach the service provider and request the data that is subject to an authorisation. If the provider is uncertain about the credentials of the authorised officer or eligible person, the provider can contact the requesting agency or the CAC to confirm whether the person has the authority to make the request.

Providers must help agencies requesting access to retained data on the basis that the provider neither profits from nor bears the cost of giving that help.

Providers receiving requests must comply with the record-keeping requirements in Part 13, Division 5 of the Telco Act.

Penalties for non-compliance

Compliance with the data retention obligations is a condition for all carriers and CSPs. Industry participants may face pecuniary penalties and infringement notices if they do not comply with their data retention obligations. Identified non-compliance may be referred to the ACMA and serious penalties may apply.

Additional Information

This guide is not a substitute for legal or professional advice. Users should obtain appropriate advice tailored to their circumstances.

Further information on other obligations including interception for carriers and nominated CSPs is available on the website of the Department of Home Affairs.

Contact details

Office of the Communications Access Coordinator

Email: cac@homeaffairs.gov.au

Website: www.homeaffairs.gov.au

Australian Communications and Media Authority

Telephone: (03) 9963 6800

Email: icp@acma.gov.au

Website: www.acma.gov.au