DATA RETENTION

Guidelines for Service Providers

The Attorney-General's Department has prepared this guide to assist industry participants to understand the obligations arising from the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*. This guide is not a substitute for legal or professional advice. Users should obtain appropriate advice tailored to their circumstances.

This is a live document and subject to periodic review. To ensure that you have the latest version, please contact the Attorney-General's Department at cac@ag.gov.au or (02) 6141 2884.

Issued by the Communications Access Co-ordinator
Version 1.1 – July 2015

TABLE OF CONTENTS

Part 1: General information

1. Purpose of the guide

The Attorney-General's Department has developed this guide to assist providers to understand their data retention obligations. This guide also contains information to assist providers to submit a Data Retention Implementation Plan or to apply for an exemption from and/or a variation of their obligations.

A template form, Data Retention Implementation Plan and/or Exemption and/or Variation Application, is available from the Communications Access Co-ordinator (CAC).

This guide is intended to be read with Version 1.1 of the Frequently Asked Questions for Industry (FAQs) on the data retention obligations, which provides further information about the data retention regime as well as answers to common queries affected service providers may have about their obligations.

2. Commencement

The obligation to have fully compliant data retention capability for all relevant services begins on 13 October 2015.

However, providers can choose to apply for up to a further 18 months to achieve compliance by lodging an Implementation Plan, setting out each relevant service.

3. Regulated 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.

The CAC may declare that services otherwise excluded are subject to the data retention obligations. For example, the CAC may make a decision where an otherwise excluded service is of significant investigative value to law enforcement or security agencies. The CAC has not made such a determination.

4. Communications

The term "communication" is defined in section 5 of the *Telecommunications (Interception and Access) Act 1979*, and focuses on conversations and messages between persons, being that which has traditionally been considered the content of a communication.

5. Retention period

Service providers must retain the required data for at least two years, starting when the information or document is created. A provider may keep telecommunications data for longer periods for its own business purposes.

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

Service providers are not required to have two years of retained data at the date of commencement. However, during the implementation period, service providers may not reduce the period for which they keep, or cause information to be kept.

6. Information to be kept

The legislation sets out the types of data that a service provider must retain to comply with the obligation. 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. Please refer to the industry FAQs, Version 1.1 for guidance.

7. Data retention does not apply to web browsing histories or the contents of communications

Service providers are not required to retain:

a) information that is the contents 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 2013*, or
d) information about the location of a telecommunications device that is not information used by the service provider in relation to that service.

8. Data retention does not apply to a person's "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 Telecommunications Act 1997. The immediate circle exclusion will typically exclude corporate networks that are not available to the public.

For service providers comprised of an individual or a partnership, the immediate circle consists of all employees and management. For body corporate service providers, the immediate circle consists of management, the officers, other body corporates related to the company and the officers of other related bodies corporate.

9. Data retention does not apply to "same area" services

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 Telecommunications 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. The same area exclusion will typically operate to exclude local area networks and wireless access points that only serve one building.

10. Data retention does not apply to 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 operate to exclude services that deliver television or radio programs. The exclusion does not apply to on-demand services.

11. Penalties for non-compliance

Industry participants may face pecuniary penalties and infringement notices if they do not comply with their data retention obligations. The obligation to retain and secure the data set, commencing from 13 October 2015, is a civil penalty provision. Compliance with the obligations is a condition of all carrier licences and part of the service provider rules.

Where a service provider has an agreed Implementation Plan, compliance with that Plan becomes a civil penalty provision in place of the general obligation. Identified non-compliance may be referred to the Australian Communications and Media Authority (ACMA).

ACMA can issue infringement notices where a service provider contravenes a civil penalty provision of the Telecommunications Act. Penalties under the infringement notice regime are currently set at $10,200 per contravention. Under the Telecommunications Act, if the Federal Court is satisfied that a person has contravened a condition of its carrier licence or the service provider rules, the Court may order the person to pay to the Commonwealth up to $10 million for each contravention.

12. Access by law enforcement

Access to telecommunications data by law enforcement and national security agencies is substantively unchanged by the data retention obligations.

The legislation continues to enable a limited group of enforcement and security agencies to authorise the disclosure of telecommunications data in certain circumstances. Providers are required by the Telecommunications Act to give such help as is reasonably necessary in responding to those requests. Service providers must provide help to agencies requesting access to retained data on the basis that the service provider neither profits from nor bears the cost of giving that help.

Where access to 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 receiving requests must comply with the record-keeping requirements in Part 13, Division 5 of the Telecommunications Act.

13. Data Retention Implementation Plans

Part 2 of this document contains detailed information on how to complete an Implementation Plan. A template is available from the CAC.

14. Applying for exemptions and/or variations

Service providers may consider lodging an application with the CAC for exemptions from and/or variations of their data retention obligations. The CAC can exempt a service provider from all or part of its data retention obligations and/or vary a service provider's data retention obligations in relation to a particular service.

Part 3 of this document contains detailed information about applying for exemptions and/or variations. A template is available from the CAC.

Part 2: Data Retention Implementation Plans

1. Data Retention Implementation Plan Summary

The obligation for a service provider to have fully compliant data retention capability on all relevant services offered by that provider begins on 13 October 2015. However, providers can choose to apply for up to a further 18 months to progressively achieve compliance by seeking approval of a Data Retention Implementation Plan. If a plan is approved, providers can use this additional time to plan, build and test data retention systems.

A service provider may apply to the CAC for approval of an Implementation Plan for one or more of the services that it operates. Service providers wishing to submit an Implementation Plan should do so by mid August 2015 to enable consideration and approval of the plan before the obligations commence. Providers that are not fully compliant with the data retention obligations and do not have an approved plan or exemption/variation in place on 13 October 2015 are in breach of their obligations. If a provider has an Implementation Plan in force, the service provider must comply with it.

A service provider and the CAC can agree to amend an Implementation Plan once in force. Please refer to **Section 6,** Amending Data Retention Implementation Plans**,** for further details.

The Implementation Plan should clearly set out if a service provider cannot achieve full compliance within 18 months. In those instances, the provider must also apply for an exemption and/or variation of their obligations in respect of the period after 12 April 2017. A template form, Data Retention Implementation Plan and/or Exemption and/or Variation Application, is available from the CAC. For further detail on exemptions refer to Part 3 of this document.

The signatory to the Implementation Plan and/or Exemption/Variation Application should be an appropriately senior representative capable of representing the views of the company.

2. Contents of a Data Retention Implementation Plan

When completing an Implementation Plan, service providers must ensure that provided information is accurate and complete. Knowingly producing a document in compliance with a law of the Commonwealth that is false or misleading is an offence under subsection 137.2(1) of the Criminal Code.

The Data Retention Implementation Plan and/or Exemption and/or Variation Application template is designed to guide a service provider to provide the following relevant information:

a) For each service, an explanation of *the current practices for keeping the information and documents required, if the plan were not in force.*

To meet this requirement, providers should detail the “status quo” arrangements for data retention, including the types of information already retained and for how long. Providers should also explain how retained data is secured, including the extent to which encryption is used.

b) For each service, details of the interim arrangements that the service provider proposes to implement, while the plan is in force, for keeping required information and documents.

To meet this requirement, providers should detail milestones that demonstrate they are progressively working towards full compliance. These milestones should be appropriate for the size and complexity of the provider.

For example, providers could aim to be compliant with more straight-forward obligations early within the implementation period, progressively addressing more technically challenging issues over a longer period.

c) For each service, the date by which the service provider will comply with the obligation to keep the required information and documents.

For each service, providers must nominate a date, not later than 13 April 2017, by which that service will be fully compliant with the data retention obligations. Compliance dates may vary across services.

d) Any regulated services operated by the service provider that the plan does not cover.

Providers must list any services they provide that are not covered by the Implementation Plan. This includes any services for which the provider is already compliant or for which the provider is seeking an exemption.

a) The contact details of the officers or employees of the service provider in relation to the plan.

The Implementation Plan should nominate names, addresses, phone-numbers and e-mail addresses for officers that can engage with law enforcement and national security agencies about retained data relevant to each service outlined in the Implementation Plan.

b) Connectivity: The range of connections between customers, and between customers of this service, and those in other networks. Suggested categories are:

- any to any – such as PSTN, ISDN, Internet, packet data networks
- fixed multipoint – such as intranets and closed networks which may be switched or semi-permanent but which always involve the same terminals, and
- point to point – such as dark fibres, private lines, EFTPOS services.

c) *Number of customers:*

Providers must estimate the number of customers subscribed to the service.

d) *Target market:*

Providers must detail the market segment to which the service is targeted. Example answers include:

- universal – service is expected to be used by all types of customer, such as mobile phone services and Internet access services
- domestic –service is most likely to appeal to residential customers
- SME businesses – service is most likely to be used by small to medium businesses and/or may be directed at particular business segments, such as ISDN Basic Access and hosted Intranet services
- wholesale/retail service provider
- business partners
- strategic alliances
- niche – service is directed at particular demographic segments, such as international call back services, and
- large government/corporate – service is intended for large government and large corporations, such as Centrex and ISDN PRA.

e) *Geographic distribution*:

Providers must describe the area over which the service is available to customers. Example answers include:

- universal – services widely available with Australia-wide coverage
- capital cities – services mainly offered in the capital cities and their suburbs
- regional – services intended for a regional market, such as an ISP offering services to a regional city or country town, and
- international services.

3. Implementation Plans for interrelated businesses and those offering multiple services

Providers that offer more than one service should separately list each relevant service in their Implementation Plan.

Where providers have interrelated corporate structures, Implementation Plans should explain these structures and ensure that Implementation Plans are consistent.

Implementation Plans should clearly detail any related service providers, particularly wholesale/retail relationships.

4. Lodgement date for Data Retention Implementation Plans

Implementation Plans must be submitted to the CAC and agreed prior to 13 October 2015. If a provider does not have an Implementation Plan in force for services, then those services will need to be compliant with the data retention obligations from 13 October 2015.

Providers should submit Implementation Plans sufficiently in advance of the deadline so that an agreement can be reached, noting that the CAC may request amendment of the plan. The legislation provides that, if the CAC takes longer than 60 days to respond to an Implementation Plan application, the Implementation Plan is taken to be agreed until such time as the CAC communicates the decision to the service provider. Service providers should submit Implementation Plans to the CAC in electronic form.

5. Decision-making and notice requirements for Data Retention Implementation Plans

As soon as practicable after receiving an application to approve an Implementation Plan, the CAC must give a copy of the Implementation Plan to enforcement agencies and security authorities and invite those parties to provide comments.

Before making a decision to approve an application for an Implementation Plan, the CAC must take into account:

a) the desirability of achieving substantial compliance with the obligation to keep the specified information and documents for the two-year period as soon as practicable

b) the extent to which the plan would reduce the regulatory burden imposed on the service provider by the data retention obligations

c) whether the service provider is contravening its obligation to keep the specified information and documents for the two-year period, at the time the CAC receives the application

d) the interests of law enforcement and national security

e) the objects of the Telecommunications Act, and

f) any other matter that the CAC considers relevant.

The CAC will endeavour to communicate the decision to the service provider in writing within 60 days. If the CAC does not communicate a decision within 60 days, the CAC is taken to have made the decision the service provider applied for until a decision is provided.

The CAC may ask a service provider to amend its Implementation Plan, in which case that service provider will be given 30 days to respond.

6. Amending Data Retention Implementation Plans

Once in force, an Implementation Plan may only be amended with the agreement of both the provider and the CAC.

Service providers may apply to the CAC for approval of an amendment. Alternatively, the CAC may request the service provider make an amendment. If the CAC makes this request, the service

provider must accept the request, amend the Plan and give the amended Plan to the CAC, or refuse the request with reasons.

Where a service provider refuses a request for an amendment, the CAC must refer the request and the service provider's response to the ACMA. The ACMA will then make a determination as to whether an amendment is required. If an amendment is required, the service provider will receive a copy of the determination.

Circumstances that may give rise to a request to amend an Implementation Plan may include the following:

- a service provider starts offering a new service to its customers that is not detailed in the agreed Implementation Plan
- extenuating circumstances that prevent a service provider from meeting previously agreed-to implementation milestones
- variations to contractual arrangements with 3rd parties occur that affect implementation timeframes, or
- substantial changes in the law enforcement and security environment.

The circumstances described above are not prescriptive and are provided as examples only.

There is no prescribed form for amending Implementation Plans. These will occur on a case-by-case basis. As noted above, amendments to Implementation Plans may only occur with the agreement of both a service provider and the CAC. Service Providers wishing to amend their Implementation Plan may commence discussions by contacting the CAC by phone, email or mail.

Part 3: Exemptions and/or variations

1. Summary of exemptions and/or variations applications

The CAC may exempt a service provider from all or part of its data retention obligations and/or vary a service provider's obligations in relation to a particular service.

Exemption applications will generally be considered on a case-by-case basis. However, exemptions may be granted in relation to a class of service. For example the CAC may specify that any service provider that provides a particular kind of service is not required to retain any data in relation to that service.

Exemptions and variations must remain confidential. Public knowledge of an exemption application adversely affects law enforcement and national security interests. These are interests that the CAC is required to take into account when granting or revoking exemptions and variations. Failure to maintain 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. Providers can also share this information with wholesalers where there is a commercial agreement to retain data on their behalf.

2. Applying for exemptions from and/or variations of your obligations

The applicant should set out relevant administrative details, including the name and address of the service provider and details of a suitable contact person within the organisation. The template provides further advice as to what information service providers should include in their application.

3. Factors the Communications Access Co-ordinator must or may take into account in deciding upon exemption and/or variation applications

In considering exemption and variation applications, the CAC must take into account the interests of law enforcement and national security and the objects of the Telecommunications Act.

The principal objects of the Telecommunications 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 is also required to consider:

- the service provider's history of compliance with its data retention obligations
- the service provider's costs, or anticipated costs, of complying, and
- any alternative data retention 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 CAC may also take into account any other relevant matters. Some of the matters that the CAC may consider 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.

4. 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 ACMA.

The CAC considers the agencies' comments before making a decision about whether to grant the exemption and/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.

5. Review of exemption and/or variation decisions

A service provider may apply in writing to the ACMA for a review of a decision by the CAC in relation to an exemption from or variation to its data retention obligations. The ACMA may then either confirm the original decision, or substitute a new decision.

Before substitution of the decision, the ACMA must give a copy of the application to the CAC, and relevant enforcement agencies and security authorities. The ACMA may substitute the decision for another decision that the CAC may have made in relation to the exemption or variation.

Factors that the ACMA may consider are detailed in **point 3: Factors the CAC must or may take into account in deciding upon an exemption.**

Part 4: Contact details

Please direct applications and any other queries to the CAC.

Phone: (02) 6141 2884
Email: cac@ag.gov.au

Annexure A: Kinds of information to be kept

Topic	Description of information	Explanation
1. The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	The following: (a) any information that is one or both of the following: i) any name or address information; ii) any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; (b) any information relating to any contract, agreement or arrangement relating to the relevant account, service or device; (c) any information that is one or both of the following: (i) billing or payment information; (ii) contact information; relating to the relevant service, being information used by the service provider in relation to the relevant service; (d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device; (e) the status of the relevant service or any related account, service or device	This category includes customer identifying details, such as name and address. It also includes contact details, such as phone number and email address. This information allows agencies to confirm a subscriber's identity or link a service or account to a subscriber. This category also includes details about services attached to account, such as the unique identifying number attached to a mobile phone, or the IP address (or addresses) allocated to an internet access account or service. This category further includes billing and payment information. Information about the status of a service can include when an account has been enabled or suspended, a relevant service has been enabled or suspended or is currently roaming, or a telecommunications device has been stolen. The phrases 'any information' and 'any identifiers' should be read to mean the information that the provider obtains or generates that meets the description which follows that phrase. If the provider has no information that meets the description, including because that kind of information does not pertain to the service in question, no information needs to be retained. For instance, if a provider offers a free service and therefore has no billing information, no billing information needs to be retained by that provider with respect to that service the provider will need to retain subscriber and transactional data with respect to that service, but no billing information needs to be retained. Service providers are not required to collect and retain passwords, PINs, secret questions or token codes, which are used for authentication purposes.
2. The source of a communication	Identifiers of a related account, service or device from which a communication has been sent or attempted to be sent by means of the relevant service.	Identifiers for the source of a communication may include, but are not limited to: • the phone number, IMSI, IMEI from which a call or SMS was made • identifying details (such as username, address, number) of the account, service or device from which a text, voice, or multi-media communication was made (examples include email, Voice over IP (VoIP), instant message or video communication) • the IP address and port number allocated to

Topic	Description of information	Explanation
		the subscriber or device connected to the internet at the time of the communication, or • any other service or device identifier known to the provider that uniquely identifies the source of the communication. In all instances, the identifiers retained to identify the source of the communication are the ones relevant to, or used in, the operation of the particular service in question.
3. The destination of a communication	Identifiers of the account, telecommunications device or relevant service to which the communication: a) has been sent; or b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.	Subsection 187A(4)(b) puts beyond doubt that service providers are not required to keep information about subscribers' web browsing history. The destination of a communication is the recipient. Identifiers for the destination of a communication may include, but are not limited to: • the phone number that received a call or SMS • identifying details (such as username, address or number) of the account, service or device which receives a text, voice or multi-media communication (examples include email, VoIP, instant message or video communication) • the IP address allocated to a subscriber or device connected to the internet at the time of receipt of the communication, or • any other service or device identifier known to the provider that uniquely identifies the destination of the communication. For internet access services, the Act explicitly excludes anything that is web-browsing history or could amount to web-browsing history, such as a URL or IP address to which a subscriber has browsed. In all instances, the identifiers retained to identify the destination of the communications are the ones relevant to, or used in, the operation of the particular service in question. If the ultimate destination of a communication is not feasibly available to the provider of the service, the provider must retain only the last destination knowable to the provider.
4. The date, time and duration of a communication, or of its connection to a relevant service	The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): a) the start of the communication b) the end of the communication c) the connection to the relevant service, and	For phone calls this is simply the time a call started and ended. For internet sessions this is when a device or account connects to a data network and ends when it disconnected – those events may be a few hours to several days, weeks, or longer apart, depending on the design and operation of the service in question.

Topic	Description of information	Explanation
	d) the disconnection from the relevant service.	
5. The type of a communication and relevant service used in connection with a communication	The following: a) the type of communication; Examples: Voice, SMS, email, chat, forum, social media. b) the type of the relevant service; Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE. c) the features of the relevant service that were, or would have been, used by or enable for the communication. Examples: call waiting, call forwarding, data volume usage.	The type of communication means the form of the communication (for example voice call vs. internet usage). The type of the relevant service (5(b)) provides more technical detail about the service. For example, for a mobile messaging service, whether it is an SMS or MMS. Data volume usage, applicable to internet access services, refers to the amount of data uploaded and downloaded by the subscriber. This information can be measured for each session, or in a way applicable to the operation and billing of the service in question, such as per day or per month. Note: This item will only apply to the service provider operating the relevant service: see Subsection 187A(4)(c).
6. The location of equipment or a line used in connection with a communication	The following in relation to the equipment or line used to send or receive the communication: a) the location of the equipment or line at the start of the communication; b) the location of the equipment or line at the end of the communication. Examples: Cell towers, Wi-Fi hotspots.	Location records are limited to the location of a device at the start and end of a communication, such as a phone call or Short Message Service (SMS) message. For services provided to a fixed location, such as an ADSL service, this requirement can be met with the retention of the subscriber's address. Subsection 187A(4)(e) of the Act provides that location records are limited to information that is used by a service provider in relation to the relevant service. This would include information such as which cell tower, Wi-Fi hotspot or base station a device was connected to at the start and end of communication. Service providers are not required to keep continuous, real-time or precise location records, such as the continuous GPS location of a device. These limitations seek to ensure that the locations records to be kept by service providers do not allow continuous monitoring or tracking of devices.