



Telecommunications (Use of Integrated Public Number Database) Industry Standard 2005

The AUSTRALIAN COMMUNICATIONS AUTHORITY makes this industry standard under subsection 125 (3) of the *Telecommunications Act 1997*.

Dated 2005

Chair

Deputy Chair

[DRAFT ONLY - NOT FOR SIGNATURE]

Australian Communications Authority

Part 1 Preliminary

1 Name of industry standard

This industry standard is the *Telecommunications (Use of Integrated Public Number Database) Industry Standard 2005*.

2 Commencement

This industry standard commences on the day after registration under the *Legislative Instruments Act 2003*.

DRAFT ONLY

Part 2

Application of industry standard

3 Application of industry standard — transition period

For a person who is the IPND manager, a data provider or a data user referred to in this industry standard, and to whom the IPND code applies immediately before the commencement of this industry standard, the person is taken to comply with an obligation or condition imposed on the person by this industry standard if:

- (a) the obligation is required to be complied with within 3 months after the commencement; and
- (b) the person complies with the IPND code, as it existed immediately before the commencement.

4 Scope of industry standard

This industry standard applies to the *public number data* section of the telecommunications industry.

Note The *public number data* section of the telecommunications industry is determined under the *Telecommunications (Section of Telecommunications Industry) Determination 2005*.

5 Objects of industry standard

The objects of this industry standard are to ensure that:

- (a) customer data that is provided to the Integrated Public Number Database is treated lawfully; and
- (b) the use of the customer data is restricted and protected in accordance with national privacy principles; and
- (c) a customer to whom the data relates is informed, before or at the time the data is collected, of:
 - (i) the purposes for which it is being collected; and
 - (ii) the purposes for which it must be disclosed to a third party; and
- (d) a customer may choose whether his or her customer data is to be included in a public number directory.

6 Industry standard to prevail over agency arrangements

Subject to section 3, a data provider or a data user must comply with an obligation mentioned in Division 4.2 or 4.3, in spite of any inconsistent contract or agreement to which the person is a party.

Note Subsection 9 (2) provides that a restricted data user must comply with the obligations of a data user mentioned in Part 4.

7 Definitions

In this industry standard:

ACA means the Australian Communications Authority.

Act means the *Telecommunications Act 1997*.

approved purpose, for an open data user or restricted data user, has the meaning given by section 12.

carriage service provider has the meaning given by section 87 of the Act.

consent, in relation to a matter that requires a decision of a customer under this industry standard, means the agreement of the customer:

- (a) after receiving all advice or information required to be given in relation to the matter under this industry standard; and
- (b) that is a written statement:
 - (i) signed by the customer, or
 - (ii) recording the customer's oral agreement.

customer means a person supplied with a carriage service by a carriage service provider.

customer contact information means the part of a customer's customer data that comprises the customer's:

- (a) public number; and
- (b) directory name; and
- (c) directory address; and
- (d) for a non-residential customer — further information that does not exceed:
 - (i) 100 characters; or
 - (ii) if the IPND manager determines a greater number of characters — that number of characters.

customer data means the information mentioned in subclause 10 (4) of the *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*.

Note **customer data** includes **customer contact information**.

data provider means a carriage service provider who provides customer data to the IPND manager under Part 4 of Schedule 2 to the Act.

data user means a person approved under section 13 as:

- (a) an open data user; or
- (b) a restricted data user.

data washing services means services that use any customer contact information to:

- (a) compare or update a database; or
- (b) create a database or list.

directory assistance services, in spite of the meaning given by section 7 of the Act, means services that are:

- (a) provided to an end-user of a standard telephone service to help the end-user find the number of not more than one end-user of a standard telephone service; and
- (b) provided by an operator or by means of:
 - (i) an automated voice response system; or
 - (ii) another technology-based system;

but does not include services that are:

- (c) used to verify customer contact information; and
- (d) data washing services.

directory address means the address that the customer has consented to be used for the customer's listed number in a public number directory .

directory name means the name that the customer has consented to be used for the customer's listed number in a public number directory.

emergency call service has the meaning given by section 7 of the Act.

emergency service means the services mentioned in subparagraphs (b) (i), (ii), (iii), (iv) and (v) of the definition of **emergency call service** in section 7 of the Act.

enforcement agency has the meaning given by section 282 of the Act.

geographic number has the meaning given by the *Telecommunications Numbering Plan 1997*.

Note In the Plan, 'geographic number' is the term for what is generally known as a 'landline'.

integrated public number database (IPND) means the database of customer data established and maintained under subclause 10 (1) of the *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*.

IPND code means the industry code *ACIF C555:2002 Integrated Public Number Database (IPND) Data Provider, Data User and IPND Manager* published by the Australian Communications Industry Forum in August 2000, and updated to the second edition in April 2002.

IPND manager means the licensee mentioned in subclause 10 (1) of the *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*.

listed number means a database record in the IPND that contains customer contact information that is available:

- (a) in a public number directory; and
- (b) for directory assistance services.

location dependent carriage services means carriage services that:

- (a) are provided on the basis of the geographic location of the caller; and
- (b) route telephone calls to a particular location.

mobile telephone service has the meaning given by the *Telecommunications Numbering Plan 1997*.

mobile telephone service number means a number assigned to a mobile telephone service; or

national privacy principles means the principles mentioned in Schedule 3 to the *Privacy Act 1988*.

open data user has the meaning given by section 13.

operator assistance services means services involving the connection of a telephone call by an operator.

operator services has the meaning given by Part 2 of Schedule 2 to the Act.

public number means a number mentioned in the numbering plan made under section 455 of the Act.

public number directory (PND) means a database of listed numbers in electronic or documentary form that serves to direct the reader to the public number of a customer, and that:

- (a) contains only customer contact information; and
- (b) does not have a reverse search function; and
- (c) if the listed number is a suppressed address listing — does not disclose the directory address; and
- (d) does not contain any customer data that relates to an unlisted number.

restricted data user has the meaning given by section 13.

reverse search function means the ability to query a database, in order to determine the name, address or telephone number of a customer, using:

- (a) a telephone number, or part of a telephone number; or
- (b) an address, or part of an address.

suppressed address listing means a listed number of a customer, for whom:

- (a) the directory address is omitted from the customer contact information; and
- (b) the suburb and postcode are included.

unlisted number means a database record in the IPND that contains customer contact information that is not available:

- (a) in a public number directory; or
- (b) for directory assistance services.

Part 3 The Integrated Public Number Database (IPND)

Division 3.1 Management of the IPND

8 IPND manager to assist the ACA

The IPND manager must assist the ACA in administering and monitoring this industry standard.

Note Telstra Corporation is required to establish and maintain the IPND under section 10 of the *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*.

9 Access to customer data in the IPND

- (1) The customer data contained in the IPND, or collected for that purpose, may be used or dealt with only if:
 - (a) the person using or dealing with the data is:
 - (i) the IPND manager; or
 - (ii) a data provider; or
 - (iii) a person approved under section 13 as an open data user or a restricted data user; and
 - (b) if the person is a restricted data user — only if the data is customer contact information; and
 - (c) the customer data is used or dealt with for an approved purpose in relation to the person; and
 - (d) the person uses or deals with the data in accordance with conditions or requirements mentioned in Part 4 in relation to the person.
- (2) A person who is an open data user or a restricted data user must comply with the obligations of a data user mentioned in Part 4.

Division 3.2 Approved purposes for use of customer data

10 Use of customer data — IPND Manager

- (1) Subject to section 9, the IPND Manager may use customer data:
 - (a) for a purpose related to the administration and maintenance of the IPND, including monitoring compliance with the obligations mentioned in Part 4; and
 - (b) any other purpose specified by the ACA by written notice to the IPND Manager under subclause 10 (1) (g) of the *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*.

11 Use of customer data — data provider

Subject to section 9, a data provider may use customer data for the following purposes:

- (a) the collection and use of customer data in the course of carrying on a business as a carriage service provider;
- (b) the forwarding of customer data to the IPND manager.

12 Use of customer data by data users — approved purposes

(1) Subject to section 9, for an approval by the IPND Manager under subsection 13 (5), the IPND Manager may approve 1 or more of the following purposes as a purpose for which an open data user may use customer data:

- (a) providing operator services or operator assistance services;
- (b) providing location dependent carriage services;
- (c) the operation of an emergency call service or assisting an emergency service under Part 8 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999*;
- (d) assisting enforcement agencies or safeguarding national security under Part 14 of the Act;
- (e) verifying the accuracy of information provided by the data provider and held in the IPND, against information held by the data provider;
- (f) assisting the ACA to verify the accuracy and completeness of information held in the IPND.

(2) Subject to section 9, for an approval by the IPND Manager under subsection 13 (5), the IPND Manager may approve 1 or both of the following purposes as a purpose for which a restricted data user may use customer contact information:

- (a) providing directory assistance services;
- (b) publishing and maintaining a public number directory.

Division 3.3 Approval for use of customer data

13 IPND manager may approve open data user or restricted data user

- (1) A person may apply to the IPND manager to be approved as:
 - (a) an open data user; or
 - (b) a restricted data user.
- (2) An application under subsection (1) must be in writing, and must state the purpose or purposes for which the person intends to use customer data.
- (3) At the time of the application the applicant must have in place internal dispute resolution procedures that comply with *Australian Standard AS 4269-1995 Complaints Handling* published on 5 February 1995.

-
- (4) The IPND manager must, within 30 days, make a decision approving or not approving the application.
 - (5) The IPND manager may approve the applicant as:
 - (a) if the person applied under subsection (1) to be approved as an open data user — an open data user who may use customer data; or
 - (b) if the person applied under subsection (1) to be approved as a restricted data user — a restricted data user who may use customer contact information.
 - (6) If the application is approved, the IPND manager must nominate 1 or more purposes for which the approval is given, having regard to the purpose or purposes stated in the person's application under subsection (2), as follows:
 - (a) if the data user is an open data user — a purpose mentioned in subsection 12 (1);
 - (b) if the data user is a restricted data user — a purpose mentioned in subsection 12 (2).
 - (7) If the application is not approved the IPND manager must, within 14 days after making the decision, provide the applicant with a statement of reasons for the decision.

14 Data user must commence within 3 months

- (1) A data user must, within 3 months after receiving access to customer data (*approval period*), commence using the data for the purposes for which the approval was given.
- (2) Within 5 days after the end of the approval period, the data user must:
 - (a) notify the ACA that the customer data has been used during the approval period for all the purposes mentioned in the approval; and
 - (b) submit a statement to the ACA containing a detailed description of the uses being made of the customer data; and
 - (c) if the data user has approval to access customer data for the purpose of producing a public number directory — provide a copy of the public number directory to the ACA.
- (3) If the data user has not used the customer data for a purpose mentioned in the approval, the data user must notify the ACA within 5 days after the end of the approval period.
- (4) The ACA may notify the IPND Manager if the ACA becomes aware that a data user:
 - (a) has used customer data for a purpose that is not an approved purpose in relation to the data user; or
 - (b) has failed, within the period mentioned in section 14, to use customer data for the purpose that was approved in relation to the data user.

15 IPND manager may withdraw approval

- (1) The IPND manager may withdraw the approval of a data user if the IPND manager becomes aware that the data user:
 - (a) has used customer data for a purpose that is not an approved purpose in relation to the data user; or
 - (b) has failed, within the period mentioned in section 14, to use customer data for the purpose that was approved in relation to the data user.
- (2) If the IPND manager withdraws an approval of a data user, the IPND manager must:
 - (a) within 1 day — advise the data user of the decision; and
 - (b) within 14 days — provide the data user with a statement of reasons for the decision.

16 IPND manager must advise ACA

The IPND manager must, within 14 days after making a decision approving or not approving an application or withdrawing an approval, provide the ACA with copies of the following documents:

- (a) the application;
- (b) a statement of the decision of the IPND manager;
- (c) if the application was not approved, or an approval was withdrawn — the statement of reasons provided to the applicant.

Part 4 Obligations and conditions**Division 4.1 Obligations of the IPND manager****17 Database records in IPND — default listing of numbers**

In recording customer data in the IPND, the IPND manager must adopt a system that requires, as a default, the customer's number to be:

- (a) if the number is a geographic number — a listed number; or
- (b) if the number is a mobile telephone service number — an unlisted number.

18 Customer may change status of number

The IPND manager must amend customer data in the IPND if a data provider advises that a customer has requested that:

- (a) the customer's number be listed or unlisted; or
- (b) the customer's address be suppressed or unsuppressed.

19 IPND manager to provide daily updates

Subject to section 20, the IPND manager must, at least once every business day, transmit to data users customer data relating to:

- (a) new customers of data providers; and
- (b) amendments to the data relating to existing customers of data providers.

20 IPND manager must not disclose customer data

- (1) The IPND manager may disclose customer data to a data user only:
 - (a) for the purposes mentioned in section 12; and
 - (b) in accordance with this section.
- (2) The data may be disclosed:
 - (a) if the customer data consists only of customer contact information — only to an open data user or a restricted data user; or
 - (b) in any other case — only to an open data user.

21 IPND manager must protect customer data

The IPND manager must take all reasonable steps to ensure that customer data in his or her possession is protected from loss, or unauthorised modification, access or disclosure.

22 IPND manager to protect unlisted numbers

- (1) The IPND Manager may provide data containing an unlisted number to a data user for the following purposes:
 - (a) if the data user is a restricted data user — only for advising the user that a listed number has become an unlisted number;
 - (b) the operation of an emergency call service or assisting an emergency service under Part 8 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999*;
 - (c) assisting enforcement agencies or safeguarding national security under Part 14 of the Act;
 - (d) verifying the accuracy of information provided by the data provider and held in the IPND, against information held by the data provider;
 - (e) assisting the ACA to verify the accuracy and completeness of information held in the IPND.
- (2) The IPND manager must not provide data containing an unlisted number to a restricted data user in any other circumstances.

23 IPND manager to advise of breach

- (1) If the IPND manager becomes aware that customer data has been disclosed in breach of an obligation in Part 4, the IPND manager must, before the end of the next day, advise the following that the breach has occurred:
 - (a) the ACA;
 - (b) if the IPND manager believes that the disclosure was in breach of an obligation of a data provider under Division 4.2 — any data user that the IPND manager believes may have received the data;
 - (c) if the IPND manager believes that the disclosure was in breach of an obligation of a data user under Division 4.3 — the data provider who provided the data.
- (2) The advice to the ACA must also include the following information, to the best of the IPND manager's knowledge:
 - (a) details of customer data disclosed as a result of the breach;
 - (b) the person or persons responsible for the breach;
 - (c) the date when the IPND manager became aware of the breach;
 - (d) a statement identifying the persons required to be notified by paragraphs 23 (1) (b) or (c), and advising that those persons:
 - (i) have been notified; or
 - (ii) will be notified within the period mentioned in subsection (1).

24 IPND manager not to amend data or advise customer of another provider

If a customer requests the IPND manager to make an amendment of, or give advice about, customer data, and the IPND manager is not also the customer's carriage service provider, the IPND manager:

- (a) must not make the amendment or give the advice; and
- (b) must advise the customer to contact the customer's carriage service provider.

Division 4.2 Obligations of a data provider

25 Data provider must advise customer

Before collecting customer data from a customer, a data provider must:

- (a) provide the customer with a statement of the reasons for collecting the customer data, including the following:
 - (i) that the data is collected to enable the data provider to provide the carriage service requested by the customer;
 - (ii) that the data is collected to meet the data provider's legislative and contractual obligations; and
- (b) advise the customer that the data provider has an obligation to disclose the data to the IPND manager for inclusion in the IPND; and

-
- (c) advise the customer of the approved purposes for which the data may be used; and
 - (d) advise the customer that:
 - (i) if the telephone number contained in the data is a geographic number — the number will be a listed number if the customer does not request that it be an unlisted number; or
 - (ii) if the telephone number contained in the data is a mobile telephone service number — the number will be an unlisted number if the customer does not request that it be a listed number; and
 - (e) advise the customer that the customer may, at any time:
 - (i) request the data provider to record that the customer's telephone number is a listed number or an unlisted number, or
 - (ii) request the data provider to record that the customer's number is to become a suppressed address listing or a directory listing; and
 - (f) advise the customer that he or she must notify the data provider of any change to the data relating to the customer.

26 Data provider to seek consent before forwarding customer data

- (1) The data provider must send all customer data to the IPND manager.
- (2) Before sending the data, the data provider must:
 - (a) if the telephone number contained in the data is a mobile telephone service number that is to be unlisted by default — ask the customer whether the customer wishes to consent to the number being a listed number; and
 - (b) advise the customer that, if the consent is given, it will permit:
 - (i) the IPND manager to send the customer data to data users; and
 - (ii) data users to use the data for approved purposes, including use in public number directories and directory assistance services.

27 Customer data — default listing of numbers

In recording customer data, a data provider must adopt a system that requires, as a default, the customer's number to be:

- (a) if the number is a geographic number — a listed number; or
- (b) if the number is a mobile telephone service number — an unlisted number.

28 Information required for listed numbers

If the customer's number is to be a listed number, the data provider must obtain the following information from the customer:

- (a) the customer's directory name;
- (b) the customer's directory address or suppressed address listing.

29 Customer may change status of number

A data provider must amend customer data in the possession of the data provider if a customer requests that:

- (a) the customer's number be listed or unlisted; or
- (b) the customer's number be suppressed or unsuppressed.

30 Data provider not to amend data of, or advise, customer of another provider

If a customer requests a data provider to make an amendment of, or give advice about, customer data, and the data provider is not also the customer's carriage service provider, the data provider:

- (a) must not make the amendment or give the advice; and
- (b) must advise the customer to contact the customer's carriage service provider.

31 Data provider to provide daily updates

A data provider must, at least once every business day, transmit to the IPND manager customer data relating to:

- (a) new customers; and
- (b) amendments to the data relating to existing customers.

32 Data provider must protect customer data

A data provider must take all reasonable steps to ensure that customer data in the data provider's possession is protected from loss, or unauthorised modification, access or disclosure.

Division 4.3 Obligations of a data user

33 Public number directories

If a data user produces a public number directory, the directory must contain only customer contact information.

34 Data user not to produce a directory with a reverse search function

A data user must not produce or use a public number directory that contains a reverse search function.

35 Use of public number directory

A data user must not use a public number directory to:

- (a) verify customer contact information; or
- (b) compare with or update another customer contact database;

-
- (c) build or maintain another customer contact database.

36 Data user not to contact customers

- (1) A data user may refer to customer contact information in order to contact a customer only if the following purposes are approved for the data user:
 - (a) the operation of an emergency call service or assisting an emergency service under Part 8 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999*;
 - (b) assisting enforcement agencies or safeguarding national security under Part 14 of the Act.
- (2) The data user may only use customer contact information in his or her capacity as a person for whom the purposes mentioned in paragraphs (1) (a) or (b) are approved purposes.

37 Data user must protect customer data

A data user must take all reasonable steps to ensure that customer data in the data user's possession is protected from loss, or unauthorised modification, access or disclosure.

38 Data user advised that number has become unlisted

If the IPND manager advises a data user that a listed number has become an unlisted number, the data user:

- (a) must not, after receiving that advice, disclose any customer contact information containing the unlisted number; and
- (b) must, before the end of the next day, remove the customer contact information from any public number directory for which the data user is responsible; and
- (c) must not, after that day, release or publish any document containing the customer contact information.

39 Data user advised that number has become suppressed address listing

If the IPND manager advises a data user that a number has become a suppressed address listing, the data user:

- (a) must not, after receiving that advice, disclose any customer contact information containing the customer's address; and
- (b) must, before the end of the next day, remove the address from the customer contact information in any public number directory for which the data user is responsible; and
- (c) must not, after that day, release or publish any document that includes the customer's address in customer contact information.

40 Data user not to amend data of, or advise, customer

If a customer requests a data user to make an amendment of, or give advice about, customer data, and the data user is not also the customer's carriage service provider, the data user:

- (a) must not make the amendment or give the advice; and
- (b) must advise the customer to contact the customer's carriage service provider.

41 Data user must have internal dispute resolution procedures

A data user must have in place internal dispute resolution procedures that comply with *Australian Standard AS 4269-1995 Complaints Handling* published on 5 February 1995.