Privacy impact assessment form—Public number directory publishers

**Instructions for completion**

* Complete this privacy impact assessment (PIA) form if you are seeking an authorisation to use and disclose customer data for the purpose of publishing and maintaining a public number directory under the Telecommunications Integrated Public Number Database Scheme 2017 (the IPND Scheme). This form identifies how you will handle customer data and will assist the ACMA to consider the privacy impact of your proposal for the authorisation you are seeking.
* You can type directly into this form and attach additional material, clearly identifying the question(s) to which it refers. Email the completed form to IPND@acma.gov.au or post it to:

IPND Scheme

Australian Communications and Media Authority

PO Box 13112 Law Courts

Melbourne Vic 8010

**Acronyms and abbreviations**

* CA IPND Code: Industry Code *C555:2008 Integrated Public Number Database* (IPND).
* IPND Scheme: Telecommunications Integrated Public Number Database Scheme 2017.
* Privacy impact assessment form: PIA form.

**Definitions**

* ‘Approved purpose’ has the same meaning as that given by the IPND Code.
* ‘Customer’ has the same meaning as that given by the IPND Scheme.
* ‘Customer data’ has the same meaning as that given by the IPND Scheme.
* ‘Public number directory’ (PND) means the public number directory to which your application relates.

A reference to whether customer data *will* be handled in a specified manner includes a reference to whether it *may* be handled in that manner—that is, it should include information-handling practices that will occur regularly as well as those that may only occur in special circumstances.

**Applicant details**

Applicant name:

|  |
| --- |
| Registered name Click here to enter text.  |
| Trading name Click here to enter text. |
| ABN / ACN Click here to enter text. |
| Address (place of business, if different from registered address) Click here to enter text. |
| Telephone Click here to enter text. |
| Website address Click here to enter text. |

Name of person completing this form:

|  |
| --- |
| Full name Click here to enter text. |
| Position within company (if business) Click here to enter text.  |
| Telephone Click here to enter text.  |
| Mobile Click here to enter text. |
| Email Click here to enter text. |

**Collection**

1. Outline what steps, if any, you will take to notify customers, or to enable them to find out (for example, through a publicly available privacy statement) about the following:
2. the identity of your organisation and how to contact it
3. whether customers are able to access the data you hold about them
4. why the customer data is/has been collected (for example, to produce a PND)
5. the organisations, or the types of organisations, to which you will usually disclose the customer data.

|  |
| --- |
| Click here to enter text. |

**Use**

1. Specify the primary purpose for collecting (seeking authorisation to use and disclose) customer data.

**Note:** This will be for the purpose stated on your application form.

*Example: To publish and maintain a public number directory.*

|  |
| --- |
| Click here to enter text. |

1. Unless there is a pre-existing business relationship with that customer, what measures will be in place to ensure that the customer data will not be used to contact a customer who has an unlisted number in the IPND?

|  |
| --- |
| Click here to enter text. |

**Disclosure**

1. Will any customer data be disclosed to a third party, including a related body corporate, at any time? List ALL third parties to whom you intend to disclose customer data, as well as the profession of any third parties. If the answer is ‘No’, go to Question 6.

*Example: PND Web Design Pty Ltd; a web programming contractor.*

|  |
| --- |
| Click here to enter text. |

1. What will be the reason(s) for the disclosure(s)?

*Example: To enable the web designer to provide systems design and web programming services relating to the development of an electronic directory.*

|  |
| --- |
| Click here to enter text. |

1. What measures, if any, will be in place to ensure that customer data is not disclosed except for publishing and maintaining PNDs?

|  |
| --- |
| Click here to enter text. |

1. If customer data (or copies of that data) is disclosed to a third party (for example, a contractor), what measures will be taken to:
2. inform the third party and its relevant staff of their obligations under the IPND Scheme?

|  |
| --- |
| Click here to enter text. |

1. keep records of all copies of customer data made or held by the third party?

|  |
| --- |
| Click here to enter text. |

1. ensure the third party securely destroys the copies once they are no longer required for the relevant purpose(s) for which they were provided?

|  |
| --- |
| Click here to enter text. |

**Data linkage**

1. Do you intend to link customer data to data from another source?

|  |
| --- |
| Click here to enter text. |

1. If the answer to Question 6 is ‘No’, go to Question 8. If the answer to Question 6 is ‘Yes’, describe:
2. what types of information will the other data include?

*Example: A customer’s opening hours where the customer operates a business.*

|  |
| --- |
| Click here to enter text. |

1. will the other data be included in the PND and, if so, what types of data will this include?

|  |
| --- |
| Click here to enter text. |

1. how will the other data be obtained?

|  |
| --- |
| Click here to enter text. |

1. why is the data linkage necessary for publishing or maintaining the PND?

|  |
| --- |
| Click here to enter text. |

**Data quality**

1. What measures will be in place to ensure:
2. That customer data contained in the PND will be updated?

|  |
| --- |
| Click here to enter text. |

1. compliance with obligations on the updating of an individual entry if a listed number becomes unlisted?

|  |
| --- |
| Click here to enter text. |

**Data security**

1. In what form will the PND be published—for example, as a hard-copy book or online? What measures will be in place to prevent reverse-searching, data theft or unlawful extraction of customer data from the PND?

|  |
| --- |
| Click here to enter text. |

1. What technical security measures will be used to protect the customer data that is stored or transferred in electronic format from misuse, loss and unauthorised access, modification or disclosure?

*Example 1: Firewalls and access controls will prevent unauthorised access.*

*Example 2: Staff who do not need to amend information will be restricted to read-only access to prevent unauthorised modification.*

|  |
| --- |
| Click here to enter text. |

1. What physical security measures will be in place to protect any customer data that is contained in hard-copy records from misuse, loss and unauthorised access, modification or disclosure?

*Example: Dedicated secure storage areas or cabinets with combination locks.*

|  |
| --- |
| Click here to enter text. |

1. Specify:
2. what internal security measures will be introduced to ensure access is restricted only to staff members who need to handle customer data?

*Example: User permissions and passwords.*

|  |
| --- |
| Click here to enter text. |

1. which persons, according to position or work function, will be permitted to access the customer data?

*Example: IT staff and IT contractors.*

|  |
| --- |
| Click here to enter text. |

1. whether audit trails will be used to monitor who accesses and manipulates the customer data?

|  |
| --- |
| Click here to enter text. |

1. Specify what measures will be taken to ensure that unauthorised copies of the customer data cannot be made, that is, copies that are not required for the publication of a PND?

|  |
| --- |
| Click here to enter text. |

1. If you become aware of a security breach within your organisation that may reasonably be foreseen to have an impact on the integrity and confidentiality of the customer data, what measures will you take to:
2. minimise the effects of the breach?

|  |
| --- |
| Click here to enter text. |

1. ensure the breach does not re-occur?

|  |
| --- |
| Click here to enter text. |

1. What steps will be taken to securely destroy or permanently de-identify customer data that is no longer required for any purpose?

*Example: Hard-copy records will be shredded and electronic records will be erased via degaussing.*

|  |
| --- |
| Click here to enter text. |

**Openness**

1. Will you make publicly available a document (for example, a privacy statement) that sets out clearly expressed policies on your information-handling practices for customer data? If so, where will this information be made available? Please attach a copy of this document if you answered ‘Yes’.

|  |
| --- |
| Click here to enter text. |

**Access and correction**

1. How will customers be provided with rights of access to customer data you hold about them, as well as a way to correct it?

|  |
| --- |
| Click here to enter text. |

1. What steps will be taken if customers ask you to correct their data?

|  |
| --- |
| Click here to enter text. |

1. What systems, if any, will be in place to ensure that:
2. all customer data for a customer can be identified?

|  |
| --- |
| Click here to enter text. |

1. corrections or amendments to customer data are made across all divisions of your organisation?

|  |
| --- |
| Click here to enter text. |

(c) external parties that have been provided customer data for the customer are notified of corrections or amendments?

|  |
| --- |
| Click here to enter text. |

1. Will there be an audit trail of corrections or amendments that are made to the customer data?

|  |
| --- |
| Click here to enter text. |

**Transborder data flows**

1. (a) Will the customer data be accessible to or handled by persons or organisations outside of Australia at any time, for example, made available for storage on a web-server located in a foreign country or to a foreign contractor?

|  |
| --- |
| Click here to enter text. |

(b) Will persons or organisations who are not subject to Australian law have access to the customer data or handle it?

|  |
| --- |
| Click here to enter text. |

1. If the answer to Question 21 is ‘No’, go to Question 23. If the answer to Question 21 (a) or (b) is ‘Yes’, specify:

(a) who will have access to the information and what is your relationship with the person(s) or organisation?

|  |
| --- |
| Click here to enter text. |

(b) For what purpose(s) will the information be made accessible or handled?

|  |
| --- |
| Click here to enter text. |

(c) What measures will be taken to ensure that appropriate privacy and security protections are in place to protect the information from misuse, loss and unauthorised access, modification or disclosure while it is stored overseas?

|  |
| --- |
| Click here to enter text. |

**Declaration**

I declare that:

1. The content of this application and any enclosures or annexures to this application are true and correct to the best of my knowledge and belief.
2. I have the authority to sign this report on behalf of the authorised user.
3. I am aware that under section 137.1 of the *Criminal Code Act* *1995*, it is an offence to knowingly provide false or misleading information to a Commonwealth entity in connection with the performance of functions under a law of the Commonwealth.

|  |  |  |
| --- | --- | --- |
| Signature |  | Position in organisation (if applicable) Click here to enter text. |
| Print full name Click here to enter text. |  | Date Click here to enter a date. |

**Note:** The information provided on or with this form is being sought in accordance with section 295A of the *Telecommunications Act 1997*, which authorises the ACMA to administer the IPND Scheme. The information may also be used to report to the minister on the IPND Scheme in accordance with section 295U of the *Telecommunications Act 1997* and to enable the ACMA to perform a number of its telecommunications functions under section 8 of the *Australian Communications and Media Authority Act* *2005.* If you do not provide the information, your application will not be reviewed.

**Privacy**

The *Privacy Act 1988* (Cth) (the Privacy Act) imposes obligations on the ACMA in relation to the collection, security, quality, access, use and disclosure of personal information. These obligations are detailed in the Australian Privacy Principles.

The ACMA may only collect personal information if it is reasonably necessary for, or directly related to, one or more of the ACMA’s functions or activities.

The ACMA will not use the information for any other purpose, nor will we disclose it, unless we have your consent or we are otherwise permitted to do so under the Privacy Act.

Further information on the Privacy Act and the ACMA’s Privacy Policy is available at [www.acma.gov.au/privacypolicy](http://www.acma.gov.au/privacypolicy). The Privacy Policy contains details about how you may access personal information about you that is held by the ACMA, and seek the correction of such information. It also explains how you may complain about a breach of the Privacy Act and how we will deal with such a complaint. If you have any questions, please contact the ACMA’s privacy contact officer by email at privacy@acma.gov.au.