

AUSTRALIAN
COMMUNICATIONS
INDUSTRY FORUM



INDUSTRY CODE
ACIF C555:2002
INTEGRATED PUBLIC NUMBER DATABASE (IPND)
DATA PROVIDER, DATA USER AND IPND
MANAGER

**ACIF C555:2002 Integrated Public Number Database (IPND)
Data Provider, Data User and IPND Manager Industry Code**

This Code was issued in draft form for comment as DR ACIF C555.

First published as ACIF C555:2000

Second edition as ACIF C555:2002

Reprinted 30 March 2006

Registered by the ACA on 22 January 2003

Disclaimers

1. Notwithstanding anything contained in this Industry Code:
 - (a) ACIF disclaims responsibility (including where ACIF or any of its officers, employees, agents or contractors has been negligent) for any direct or indirect loss, damage, claim, or liability any person may incur as a result of any:
 - (i) reliance on or compliance with this Industry Code;
 - (ii) inaccuracy or inappropriateness of this Industry Code; or
 - (iii) inconsistency of this Industry Code with any law; and
 - (b) ACIF disclaims responsibility (including where ACIF or any of its officers, employees, agents or contractors has been negligent) for ensuring compliance by any person with this Industry Code.
2. The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

Copyright

© Australian Communications Industry Forum Limited 2000

This document is copyright and must not be used except as permitted below or under the *Copyright Act 1968*. You may reproduce and publish this document in whole or in part for your or your organisation's own personal or internal compliance, educational or non-commercial purposes. You must not alter or amend this document in any way. You must not reproduce or publish this document for commercial gain without the prior written consent of ACIF. Organisations wishing to reproduce or publish this document for commercial gain (i.e. for distribution to subscribers to an information service) may apply to subscribe to the *ACIF Publications Subscription Service* by contacting the ACIF Business Manager at acif@acif.org.au. If you publish any part of this document for any purpose, you must also publish this copyright notice as part of that publication.

EXPLANATORY STATEMENT

Introduction

This Explanatory Statement is to be read with the ACIF **IPND Data Provider, Data User and IPND Manager Industry Code for Data Transfer** (the Code).

This Explanatory Statement outlines the purpose of the Code and the public interest factors which have been taken into account at the time of the registration of the Code.

Expressions used in this Explanatory Statement have the same meaning as in the Code.

Regulatory Policy and Framework

The Integrated Public Number Database (IPND) is an industry-wide database of all listed and unlisted public telephone numbers to provide information for purposes specified in clause 10 (1) of the Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997 (Licence Conditions) including the provision of directory assistance services and the publishing of telephone directories.

The IPND, therefore, is a repository of Public Number Customer Data which broadly includes the Public Number, customer name, address and directory listing information which can be used, for example, to assist the provision of emergency services and law enforcement. The IPND has the benefit of simplifying the provision of and access to information necessary to manage public safety and well being and as such provides a valuable resource to the Australian telecommunications industry and the Australian community.

The Licence Conditions (clause 10 (1)) oblige Telstra to establish and maintain the IPND. Pursuant to the *Telecommunications Act 1997 (Cth)* (the Act), Carriage Service Providers that supply a Carriage Service to an End User where the End User has a Public Number must give Telstra such information as Telstra reasonably requires in connection with Telstra's fulfilment of the obligation as the IPND Manager (Part 4, Schedule 2 of the Act).

Public Number Customer Data may only be accessed from the IPND for Approved Purposes as specified in Licence Condition 10 (1), or as specified by the ACA by written notice, which are:

- (a) providing Directory Assistance Services;
- (b) providing Operator Assisted Services or Operator Assistance Services;
- (c) publishing Public Number Directories;
- (d) providing Location Dependent Carriage Services;
- (e) the operation of Emergency Call Services or assisting Emergency Services under Part 8 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999*;
- (f) assisting Enforcement Agencies or safeguarding national security under Part 14 of the Act;
- (g) verifying the accuracy of information provided by the Data Provider and held in the database against the information Data Provider holds; and
- (h) any other activities specified by the ACA by written notice to the IPND Manager.

This list sets out the Approved Purposes, but does not imply that non Carriage Service Providers may access the data for the full range of Approved Purposes.

Part 13 of the Act deals with the protection of personal information by limiting its use, disclosure and secondary use and disclosure. Section 285 of the Act allows for specified disclosures and uses for information held in the IPND. Telstra's Licence Conditions also contains provisions about the disclosure and use of Public Number Customer Data held in

the IPND. This Code is intended to expand on the protections for Public Number Customer Data provided for by the provisions mentioned by setting principles and standards for the handling of Public Number Customer Data.

The Code was developed by the ACIF **OCRP/WC6 : IPND** Working Committee in consultation with relevant stakeholders in order to set out the procedures to be complied with by all Data Providers, Data Users and the IPND Manager. These procedures relate to the transfer of information to and from the IPND and the storage of information in the IPND.

The Code development has allowed industry Participants an opportunity to contribute to the formulation of important principles in the IPND operation that were either not covered or were insufficiently dealt with in the legislation. The principles include:

- (a) responsibility for accuracy of the information provided to the IPND; and
- (b) expectations about timeliness; and
- (c) procedures for dealing with queried and incorrect entries; and
- (d) procedures for dealing with customer and end-user issues; and
- (e) protection of confidential information and customers' listing preferences, in particular, with the protection of entries that customers do not want published in directories or made available on Directory Assistance Services.

Rationale for the Code

The Code has been developed to amplify the arrangements set out in legislation and subordinate instruments and in particular to address the interests of Participants. The Working Committee identified these interests as:

- (a) Data Provider interest in being assured that their commercially sensitive customer information is protected from misuse and that they have had the opportunity to be involved in the development of the process to meet this interest;
- (b) end user interest in being assured that the confidentiality of their information is adequately protected, especially where an end user has chosen not to be listed;
- (c) the interest of Data Users in being able to access Public Number Customer Data on clearly understood non-discriminatory terms;
- (d) the interest of the industry Participants generally in developing a Code which clearly sets out the responsibilities of each Participant and the rules for the treatment of Public Number Customer Data as it is provided to, stored in, accessed from the IPND and used by IPND Users; and
- (e) the IPND Manager's interest in being assured that Data Providers will cooperate in the provision of accurate, current and complete Public Number Customer Data to the IPND and the assurance that Data Users will only access and use Public Number Customer Data held in the IPND for Approved Purposes.

It is important for Data Providers that procedures be codified to ensure consistency and prompt provision of information to the IPND. Similarly, it is important for Data Users that procedures be codified to ensure consistency and prompt provision of information from the IPND. The Code must also address the security and privacy issues to which each IPND Participant must have regard.

A cooperatively developed self-regulatory Code was seen to be the most appropriate method of addressing these interests, and providing the assurances that IPND Users were seeking. The process of Code development has been able to maximise the participation of those representing the above interests and to take account of their interests in a more detailed way than would have been possible in subordinate instruments. Code development is consistent with the regulatory framework set in section 4 of the Act.

Objectives and Scope of the Code

The stated objectives of the Code are to set out rights and obligations of Data Providers, Data Users and the IPND Manager regarding the input, use, disclosure and storage of Public Number Customer Data in the IPND; and to ensure that:

- (a) agreed uniform procedures and formats are followed when Public Number Customer Data is transferred to the IPND by Data Providers and from the IPND by Data Users; and
- (b) agreed uniform procedures and formats are followed when Public Number Customer Data is transferred from the IPND by Data Users; and
- (c) IPND procedures treat Data Providers on a non-discriminatory basis; and
- (d) IPND procedures treat Data Users in the same Approved Purpose category on a non-discriminatory basis; and
- (e) IPND procedures do not detract from Customers' privacy and reasonable rights with regard to personal information; and
- (f) procedures and processes maximise data accuracy and efficiency through the cooperation of all Participants; and
- (g) the integrity and confidentiality of the Public Number Customer Data that is input to, stored in, used and disclosed from the IPND is adequately protected.

The Code applies to all CSPs, Data Providers, Data Users and the IPND Manager. The Code relates to Public Number Customer Data provided to, from and stored in the IPND.

Enhancement of Current Regulatory Arrangements

This Code enhances the current regulatory arrangements by elaborating on the following matters:

- (a) the necessary application procedure for Data Providers and Data Users to register with the IPND Manager for the provision of information to and from the IPND;
- (b) the supply and maintenance procedures for Data Providers so that Public Number Customer Data is up-to-date and is in a format and manner reasonably required by the IPND Manager as specified in the IPND Technical Requirements;
- (c) that Data Providers are responsible for the provision of accurate and current Public Number Customer Data to the IPND;
- (d) that Data Users may be provided with Public Number Customer Data which can only be used for Approved Purposes;
- (e) processes in relation to errors in Public Number Customer Data; and
- (f) processes to ensure the security, privacy and confidentiality of Public Number Customer Data.

Benefits to End-Users

The establishment and operation of the IPND will indirectly benefit end-users in a multi carrier environment. These benefits include:

- (a) continued access to comprehensive and integrated Public Number Directories;
- (b) competition in directory services, offering the possibility of increased choice and innovative directory services;
- (c) availability of comprehensive location and other information to Emergency Call Persons and emergency service organisations when emergency calls are made;
- (d) availability of comprehensive Public Number Customer Data for Enforcement Agencies and National Security agencies;

- (e) giving individual Customers the right to:
 - (i) not to be included in telephone directories and directory assistance services; or
 - (ii) have only part of their address included in telephone directories and directory assistance services; and
- (f) proper and lawful protection for the privacy of Customer data stored in the IPND.

Costs

There are costs associated with the establishment and maintenance of the IPND by the IPND Manager. These are a result of the obligations imposed by the Licence Conditions and the IPND Technical Requirements rather than from the Code.

There are establishment and ongoing costs incurred by IPND Data Providers in establishing the means by which they will provide Public Number Customer Data to the IPND as a result of the IPND Technical Requirements as provided by the IPND Manager. The requirement by this Code to implement and manage Suppressed Address where it is offered by a Data Provider will result in additional costs to that Data Provider.

There are establishment and ongoing costs incurred by IPND Data Users in establishing the means by which they will access Public Number Customer Data from the IPND.

The IPND Manager may charge all Data Users reasonable charges for access to IPND data.

Other Public Benefits or Considerations

If this Code is registered by the ACA, its rules can be enforced on producers of directories and directory services. This group is not within the scope of Part 13 of the *Telecommunications Act 1997* but having been declared as a section of the industry, will nevertheless be subject to privacy obligations set out in this Code.

A related public benefit of the IPND Code is that it sets out the operating framework within which competition in the directory and directory services market can take place. In effect, the Code contributes to the creation of a level playing field.

Bruce Lancashire
Chairman
OCR/P/WC6 : IPND Working Committee

TABLE OF CONTENTS

1	BACKGROUND	2
2	SCOPE	3
3	OBJECTIVES	4
4	EXCLUSIONS	5
5	PARTICIPANTS	6
6	DEFINITIONS AND ABBREVIATIONS	7
7	PRINCIPLES AND RULES – GENERAL APPLICATION	13
8	CONDITIONS FOR DATA USER ACCESS TO IPND DATA	14
9	PRINCIPLES FOR DATA PROVISION INTO THE IPND	16
10	PRINCIPLES RELATING TO DATA PREPARATION AND PROCESSING	17
11	IPND TRANSACTION PROCESSING	20
12	GENERAL PRINCIPLES FOR DATA TRANSFER – RULES FOR USE AND DISCLOSURE OF DATA TRANSFERRED FROM THE IPND	22
13	DATA ERRORS AND DATA QUERIES	24
14	CUSTOMER CONTACT	25
15	INFRASTRUCTURE	26
16	DATA SECURITY	27
17	CONFIDENTIALITY	28
18	BILATERAL AGREEMENTS	29
19	ADMINISTRATION AND COMPLIANCE	30
20	MONITORING	31
21	REVIEWING	32
22	AGENCY	33
APPENDIX A IPND QUALITY MANAGEMENT MEASURES		34

1 BACKGROUND

- 1.1 Telstra is obliged under Licence Conditions to establish and maintain an industry wide IPND to provide Public Number Customer Data for Approved Purposes.
- 1.2 The IPND has been developed as a resource for the telecommunications industry, directory publishing industry, Enforcement Agencies, National Security agencies and Emergency Services organisations in Australia.
- 1.3 The IPND will serve as a national central repository for the receipt, storage and distribution of Public Number Customer Data for Data Providers and Data Users.
- 1.4 While the Act and the Licence Conditions allow for the initial establishment and maintenance of the IPND by Telstra, it is contemplated that the ongoing maintenance and operation of the IPND may be transferred to another specified person or association. In that event, this Code and the Prescribed Conditions will continue to apply.
- 1.5 Part 4 of Schedule 2 of the Act specifies that if Telstra or that other person or association is under an obligation to provide and maintain an IPND, CSPs that supply a Carriage Service to an end-user, where the end-user has a Public Number, must provide Telstra or that other person or association information reasonably required in connection with the fulfilment of that obligation.
- 1.6 Where the IPND Manager is also a Carriage Service Provider, the term IPND Manager is a reference to that person in its capacity as IPND Manager and not in its capacity as a Carriage Service Provider.
- 1.7 Where a Carriage Service Provider is also the IPND Manager, the Code applies to that organisation in its role as a Carriage Service Provider.
- 1.8 This Code has been registered by the ACA.

2 SCOPE

- 2.1 This Code applies to Carriage Service Providers and Public Number Directory Producers. In terms of this Code, the application is to Data Providers, Data Users and the IPND Manager, all of whom are either Carriage Service Providers or Public Number Directory Producers.
- 2.2 This Code relates to the telecommunications activities of persons listed in Clause 2.1 in carrying on business as Carriage Service Providers, or in supplying goods and services for use in connection with the supply of a listed Carriage Service and in particular relates to the following activities:
 - (a) supplying Public Number Customer Data to the IPND;
 - (b) accessing Public Number Customer Data from the IPND; and
 - (c) managing, maintaining and administering Public Number Customer Data stored in the IPND.

3 OBJECTIVES

- 3.1 The objectives of this Code are:
- (a) to set out the rights and obligations of Data Providers, Data Users and the IPND Manager regarding the input, use, disclosure and storage of Public Number Customer Data in the IPND; and
 - (b) to ensure that agreed uniform procedures and formats are followed when Public Number Customer Data is transferred to the IPND by Data Providers; and
 - (c) to ensure that agreed uniform procedures and formats are followed when Public Number Customer Data is transferred from the IPND to Data Users; and
 - (d) to ensure that IPND procedures treat Data Providers on a non-discriminatory basis; and
 - (e) to ensure that IPND procedures treat Data Users within the same Approved Purpose category on a non-discriminatory basis; and
 - (f) to ensure that IPND procedures do not detract from Customers' reasonable rights with regard to personal information; and
 - (g) to ensure procedures and processes maximise data accuracy and efficiency through the cooperation of all Participants; and
 - (h) to ensure the Public Number Customer Data that is input to, stored in, used and disclosed from the IPND is adequately protected.

4 EXCLUSIONS

- 4.1 The IPND Code does not cover charging principles related to access to Public Number Customer Data within the IPND. Whilst there will be establishment and ongoing costs incurred by each Participant, these costs are outside the scope of the Code.
- 4.2 E-mail addresses are not Public Numbers under the Numbering Plan and as such are not stored in the IPND, hence the IPND Code does not deal with them.
- 4.3 The IPND contains one set of Public Number Customer Data for each Public Number. This may have implications for Public Number Directory Producers but these implications are outside the scope of this Code.

5 PARTICIPANTS

The group that developed this Industry Code consisted of the following organisations and their representatives:

Organisation	Membership	Representative
AAP Telecommunications	Non-voting	Bob Dewstow
AAP Telecommunications	Voting	Suzanne Wilson
Australian Communications Authority	Non-voting	Frances Wood
Australian Communications Authority	Non-voting	Patrick Emery
Australian Security Intelligence Organisation	Voting	(name suppressed)
Australian Telecommunications Users Group (ATUG)	Voting	John Pack
Bureau of Emergency Services Telecommunications	Voting	John Schurink
Cable & Wireless Optus	Voting	Cate Farley
Cable & Wireless Optus	Non-voting	Rajiv Jayawardena
Consumers' Telecommunications Network	Voting	Stephen Horrocks
Human Rights and Equal Opportunities Commission	Voting	Chris Cowper
NSW Police Service	Voting	Bob Jarvis
Pacific Access Pty Limited	Voting	Suzanne Towsey
Phone Directories Company	Voting	Daniel Stoten
Primus Telecommunications	Voting	Mario Verruso
Telstra Corporation	Voting	Bruce Lancashire (Chairman)
Telstra Corporation	Non-voting	Dennis Kay
Vodafone Network	Voting	Robyn Ziino

Chiang Lim provided Project Management support.

6 DEFINITIONS AND ABBREVIATIONS

For the purposes of this Industry Code, the following definitions and abbreviations apply:

ACA

means the Australian Communications Authority.

ACIF

means the Australian Communications Industry Forum.

ACIF Executive

means that group within the ACIF which is accountable for the self-regulatory process. It supports the ACIF Board, the Advisory Assembly, Reference Panels and Working Committees. It also provides the leadership, logistics, frameworks and processes required for self-regulation.

ACIF Operations Codes Reference Panel

means the body established by the ACIF Board to oversee particular areas of activity for which it is responsible in relation to inter-carrier and industry operational matters. It operates in consultation with the ACIF Executive and under the direction of the ACIF Board to provide advice to the ACIF Board, ACIF Members, and the Advisory Assembly in its assigned area of responsibility. It undertakes defined responsibilities on behalf of the ACIF and as required by the ACIF Board.

Act

means the *Telecommunications Act 1997(Cth)*.

Approved Purpose

means in respect of Public Number Customer Data stored in the IPND, the following activities as listed in Licence Condition 10 (1) and subsequently added to by the ACA by written notice on 10 June 1999:

- (a) providing Directory Assistance Services;
- (b) providing Operator Services or Operator Assistance Services;
- (c) publishing Public Number Directories;
- (d) providing Location Dependant Carriage Services;
- (e) the operation of Emergency Call Services or assisting Emergency Services under Part 8 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999*;
- (f) assisting Enforcement Agencies or safeguarding national security under Part 14 of the Act;
- (g) verifying the accuracy of information provided by the Data Provider and held in the IPND against the information the Data Provider holds; and
- (h) any other activities specified by the ACA by written notice to the IPND Manager.

Business Day

means any day from Monday to Friday (inclusive) excluding gazetted public holidays. Gazetted public holidays are limited to holidays gazetted in the Commonwealth gazette and holidays gazetted in the State or Territory from which the Data Provider normally provides the data.

Carriage Service

means a service for carrying communications by means of guided and/or unguided electromagnetic energy.

Carriage Service Provider (CSP)

has the meaning described in section 87 of the *Telecommunications Act 1997*.

Code

means the IPND Data Provider, Data User and IPND Manager Industry Code for Data Transfer except where otherwise specifically identified.

Customer

means the end-user supplied by a CSP with a Carriage Service and who has a Public Number. This includes, but is not limited to, an individual, a business entity, a government entity, a charitable entity and also includes a mobile service purchaser.

Data Provider

means a CSP who has the obligation to provide PNCD to the IPND, or an entity acting on behalf of the CSP, and who is registered with the IPND Manager under Clause 9.1.

Data Provider Error File

means files generated by the IPND and sent to Data Providers containing records of errors identified during the validation of the Data Provider's upload file to the IPND.

Data Provider Query File

means files generated by the IPND and sent to the Data Provider which highlight potential inconsistencies, identified by Data Users via Data User Query Files, in Public Number Customer Data.

Data User

means an entity which has access to Public Number Customer Data for an Approved Purpose from the IPND and which is registered with the IPND Manager as in Clause 8.3.

Data User Query File

means files generated by Data Users sent to the IPND Manager which highlight potential inconsistencies in Public Number Customer Data.

Directory Assistance Services

has the same meaning as provided by section 7 of the Act.

Emergency Call Person

has the same meaning as provided by section 7 of the Act.

Emergency Call Service

has the same meaning as provided in section 7 of the Act.

Emergency Service

means a service mentioned in paragraph (b) 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.

File Specification

means the file format (consisting of, but not limited to, data fields, the data field lengths, and the data field positions within a file) for data as set out in the IPND Technical Requirements.

Force Majeure

means an unforeseen or uncontrollable force or event, such as fire, flood, earthquake, storm or other disturbance caused by the elements, an Act of God, or war, strike, lockout, riot, explosion, insurrection, governmental action or another event of the kind enumerated above which is not reasonably within the control of the Participant.

Hard Error

means an error that prevents the upload of the file and/or Public Number Customer Data record into the IPND, that is, errors identified during the validation of the Data Provider's upload file which result in the record or file in question being rejected by the IPND and returned to the Data Provider.

Hard Reject

means Public Number Customer Data that contains a Hard Error that is rejected by the IPND and returned to the Data Provider.

Information Package

means:

- (a) a proposed standard agreement for Data Providers and/or Data Users;
- (b) in the case of Data Users, a proposal for cost structure when available;
- (c) current IPND Technical Requirements;
- (d) ACIF IPND Code; and
- (e) such other information the IPND Manager deems appropriate.

IPND

means Integrated Public Number Database pursuant to the Act and clause 10 of the Licence Conditions.

IPND Manager

means the person or association that manages, maintains and administers the IPND.

IPND Technical Requirements

means *Integrated Public Number Database (IPND) Data Users and Data Providers Technical Requirements for IPND*.

IPND Users

mean Data Providers and Data Users.

Licence Conditions

means the Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997.

Listed Entry

means Public Number Customer Data which is available for inclusion in a Public Number Directory.

Location Dependant Carriage Service

means a Carriage Service which:

- (a) depends for its provision on the availability of information about the geographic location of the caller, and
- (b) routes telephone calls to a particular destination, normally the closest destination to the caller.

Location Dependant Carriage Service Data

means the data relevant to a Customer excluding the Customer's name but including:

- (a) the Public Number;
- (b) the address of the Customer which is:
 - (i) for a fixed service, the service address as installed, unless not technically feasible; or
 - (ii) for a mobile service, the address as provided by the customer;
- (c) a code that indicates the CSP that provides:
 - (i) service for the originating or terminating Carriage Services to the Customer; or
 - (ii) public mobile telecommunications service to the Customer; and
- (d) an indication of whether the service is to be a Listed Entry, an Unlisted Number or a Suppressed Address Record in a Public Number Directory.

Numbering Plan

means the *Telecommunications Numbering Plan 1997*.

Operator Assistance Service

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

Operator Services

means:

- (a) services for dealing with faults and service difficulties; and
- (b) services of a kind specified in regulations made under the Act.

Participants

for the purpose of this Code, means Data Providers, Data Users and the IPND Manager.

Prescribed Conditions

means in the case of Telstra, Licence Conditions, and in the event the IPND Manager is another person or association, conditions stipulated in a Ministerial Direction.

Public Number

means a number specified in the Numbering Plan as referred to in subsection 455(3) of the Act.

Public Number Customer Data

means the data relevant to a Customer and including, as referenced in Licence Condition 10 (4), and for the purposes of this Code comprises:

- (a) the Public Number; and
- (b) the name of the Customer or business; and
- (c) the directory finding name if appropriate and different to the Customer/business name; and
- (d) the address of the Customer which is:
 - (i) for a fixed service, the service address as installed unless not technically feasible;
 - (ii) for a mobile service, the address as provided by the customer; and
 - (iii) for a Listed Entry, the directory address if different; and
- (e) the name of the CSP that provides:
 - (i) services for the originating or terminating Carriage Services to the Customer; or
 - (ii) public mobile telecommunications services to the Customer; and
- (f) an indication of whether the telephone is to be used for government, business, charitable or residential purposes, if practicable; and
- (g) an indication of whether the service is to be a Listed Entry, an Unlisted Number or a Suppressed Address in a Public Number Directory.

Public Number Directory

is a document or record containing a list of telephone subscribers and their numbers. The numbers are connected to the supply of carriage services to the public in Australia. Such a document or record allows the user to search by:

- (a) the name and optionally the address (or part thereof) of a Customer; or
- (b) any other criteria (including criteria not being part of the PNCD) other than a Customer's number,

to obtain the Customer's telephone number and address, provided the directory does not enable a person who only knows a Customer's number to readily identify the Customer's name and/or address. For the avoidance of doubt and subject to any other provision of this Code, the directory may:

- (a) be in a written or electronic format or accessible by means of a website;
- (b) reproduce all or part of the PNCD; and
- (c) include information other than PNCD.

Public Number Directory Producers

are persons who:

- (a) compile, publish, maintain or produce directories of Public Numbers (whether including other or further details) in any form and using any medium; or
- (b) provide Directory Assistance Services; or
- (c) supply goods or services which are combination of (a) and (b).

Public Payphone

means a payphone in a public place that is a place where the public usually has access, or usually has access except for particular hours of the day or particular days of the week.

Residential Public Number

is any Public Number other than those tagged as business, government or charity.

Reverse Search Directory

means a directory which has the functionality to enable a person who knows only a Customer's Public Number to readily identify the Customer's name and/or other details.

Soft Error

means a potential error in a record identified during the validation of the Data Provider's upload file, at a field level, which result in the record in question being supplied to the IPND, tagged as having a Soft Error.

Soft Reject

means Public Number Customer Data that contains a potential error that is tagged by the IPND and returned to the Data Provider. These Soft Rejects are written to an error file with an appropriate error code. On investigation by the Data Provider, of the Soft Rejects, Soft Errors may not require correction.

Suppressed Address Record

is a Listed Entry whereby, at the Customer's request and if offered by the CSP, only the Customer's name, suburb, postcode and Public Number will be made public.

Unlisted Number

means a Public Number that is one of the following:

- (a) a mobile number, unless the Customer and the CSP that provides the mobile service to the Customer agree that the number will be listed;
- (b) a geographic number that the Customer and the CSP that provides services for originating and/or terminating Carriage Services to the Customer agree will not be included in a Public Number Directory;
- (c) the number of a Public Payphone; or
- (d) a number that when dialled, gives access to a private telephone exchange extension that the Customer had requested not be included in the Public Number Directory.

7 PRINCIPLES AND RULES – GENERAL APPLICATION

- 7.1 Nothing in this Code is intended to change the intellectual property rights (if any) of Data Providers, Data Users or the IPND Manager.
- 7.2 The requirements of this Code will apply equitably to all Participants, unless otherwise provided.
- 7.3 The IPND will perform minimal processing and filtering of PNCD requiring a cooperative approach to data accuracy.
- 7.4 The IPND Manager is responsible for the establishment of the IPND, its maintenance, ongoing security and data management (including disaster recovery). To the extent that these responsibilities are additional to those set out in legislation, this Code elaborates on these responsibilities.
- 7.5 The IPND Manager must take all reasonable steps to protect and secure Public Number Customer Data from misuse, loss and unauthorised access, modification or disclosure of Public Number Customer Data.
- 7.6 Where the organisation performing the role of the IPND Manager is also a Carriage Service Provider, it must not allow access either direct or indirect by any area of its organisation to IPND data for any reason other than the Approved Purposes and carrying out the responsibilities of the IPND Manager under this Code.
- 7.7 The level of service provided to each Data Provider and each Data User within the same Approved Purpose category must be non-discriminatory, that is, the same processes must apply to each relevant Participant.
- 7.8 The IPND Manager's responsibility will include quality control, for example through the provision of Data Provider Error Files, Data User Query Files and Data Provider Query Files in accordance with the IPND Technical Requirements. The IPND Manager must ensure that detected errors are promptly notified to the Data Provider.
- 7.9 The IPND must be a stand alone database system to facilitate transfer of the IPND and its management to another specified person or association. This is contemplated in section 472 of the Act.
- 7.10 While the content of the IPND Technical Requirements do not form part of this Code, processes for changing the IPND Technical Requirements are within the scope of this Code.
- 7.11 It is a general principle that in circumstances which amount to Force Majeure, all relevant Participants will without prejudice take all reasonable endeavours to address those circumstances.

8 CONDITIONS FOR DATA USER ACCESS TO IPND DATA

- 8.1 The IPND Manager must take reasonable steps to ensure that a prospective Data User is made aware of this Code and that this Code has been developed with reference to Part 6 of the Act.
- 8.2 If a person wishes to register as an IPND User, the IPND Manager must make available to that person an Information Package within 30 days from a written request for such information and/or an expression of interest in becoming an IPND User. The IPND Manager must provide an Information Package to persons applying to become IPND Users on a non-discriminatory basis.
- 8.3 Each Data User must apply to the IPND Manager before it will be considered for approval to access the IPND. In order to be accepted for registration by the IPND Manager, the Data User must provide contact information, have its registered office within Australia and be subject to Australian law, and either:
- (a) declare in writing to the IPND Manager that it commits to be bound by this Code; or
 - (b) in writing to the IPND Manager:
 - (i) agree to comply with IPND Technical Requirements and other security provisions; and
 - (ii) acknowledge the receipt of this Code; and
 - (iii) undertake not to use or supply the Public Number Customer Data other than for an Approved Purpose and in particular not to engage in the publication or maintenance of any type of Reverse Search Directory using Public Number Customer Data. A breach of this undertaking will constitute a breach of this Code.
- 8.4 The Data User may also provide information as to:
- (a) its experience as a Public Number Directory Producer who has published a Public Number Directory; and/or
 - (b) its experience in assisting Enforcement Agencies, National Security agencies, or Emergency Services; and/or
 - (c) its experience in using or supplying Public Number Customer Data for other than an Approved Purpose; and/or
 - (d) its capacity to use Public Number Customer Data for the purpose or purposes it has given
- to assist the IPND Manager in assessing the application.

- 8.5 In view of the obligations of the IPND Manager under Part 13 of the Act, the IPND Manager may take into account the previous actions of a potential Data User in either complying or not complying with the Approved Purposes and the Data User's ability to use PNCD for the purpose or purposes it has given. The IPND Manager must not unreasonably deny access to a potential Data User nor give undue emphasis to a potential Data User's inexperience in their application.
- 8.6 The IPND Manager must consider an application to be a Data User without unreasonable delay. Receipt of PNCD will nevertheless be subject to agreement on terms and conditions between the IPND Manager and the Data User.
- 8.7 Data Users must ensure that contact information remains current. The IPND Manager must make current contact information available to all Participants.

9 PRINCIPLES FOR DATA PROVISION INTO THE IPND

- 9.1 Each Data Provider must register with the IPND Manager before it will be permitted to provision the IPND with Public Number Customer Data.
- 9.2 Each Data Provider must, in accordance with the Act, supply Public Number Customer Data to the IPND for each of its Public Numbers used to supply a Carriage Service to a Customer. Accordingly, a CSP that provides a service to a Customer must also provide the relevant Public Number Customer Data to the IPND in respect of each Carriage Service it supplies. This Code also applies to pre-paid Carriage Services where there is a Public Number issued that is associated with that Service.
- 9.3 Data Providers must ensure that all Public Number Customer Data transferred to the IPND is in the format specified in the IPND Technical Requirements.
- 9.4 Each Business Day, Data Providers will provide to the IPND changes to Public Number Customer Data in respect of new or existing Customers. Such data should be supplied and in the format required by the IPND Technical Requirements.
- 9.5 Each Data Provider must be responsible for the accuracy, completeness and currency of their Public Number Customer Data provided to the IPND.
- 9.6 A Data Provider must take all reasonable steps to avoid adverse impact on the accuracy, completeness and currency of another Data Provider's data.
- 9.7 The Data Provider who may have caused adverse impact on the Public Number Customer Data of another Data Provider must provide reasonable assistance in rectifying the Public Number Customer Data.
- 9.8 Each Data Provider who provides one or more Public Payphones will provide to the IPND the Public Number and location for each Payphone.
- 9.9 The IPND Manager must ensure that on-line access to the IPND is not available to Data Providers for reasons of data security.
- 9.10 In the event that a technical failure of any kind prevents a Data Provider from transferring PNCD to the IPND for more than one Business Day, the Data Provider must take all reasonable steps to provide data in another way until the technical problem is rectified.
- 9.11 In the event that a technical failure of any kind prevents the Data Provider from transferring PNCD to the IPND for more than one business day, the IPND Manager must take all reasonable steps to accommodate the Data Provider's alternate methods of transferring PNCD until the technical problem is rectified.
- 9.12 Relevant Participants must use all reasonable endeavours to rectify the technical failures referred to in Clauses 9.10 and 9.11 as soon as possible.

10 PRINCIPLES RELATING TO DATA PREPARATION AND PROCESSING

- 10.1 The Data Provider must identify each Public Number used to supply Carriage Services with a tag identifying whether the Public Number Customer Data is to be Listed or Unlisted. Where a Data Provider provides the option of Suppressed Address and a Customer has chosen that option, a Listed tag must specify Suppressed Address.
- 10.2 Where a Customer makes a request to a Data Provider for an Unlisted Number, the Data Provider must tag that PNCD as Unlisted. The IPND Manager must not pass the Unlisted PNCD onto Data Users of the IPND who are Public Number Directory Producers, except as provided for in Clause 11.8.
- 10.3 Where a Customer makes a request to a Data Provider for a Suppressed Address and that Data Provider offers that option, the Data Provider must tag that PNCD as Suppressed Address. Public Number Directory Producers must not publish street number and street name of PNCD tagged as Suppressed Address.
- 10.4 If a Customer chooses to change their CSP, the responsibility for updating the IPND with the Public Number Customer Data of the Customer will be on the gaining CSP (new Data Provider).
- 10.5 The IPND Manager must ensure that all Public Number Customer Data changes are backed up daily, and securely and safely stored. The stored data is to be kept for seven years.
- 10.6 The IPND Manager is obliged to preserve the security and confidentiality of stored Public Number Customer Data to the same level as it does for Public Number Customer Data held in the IPND.
- 10.7 Data Providers can obtain an extract of their PNCD as a full set of records or as a subset of records based on criteria agreed between the Data Provider and the IPND Manager for reconciliation purposes as a Data User (see Approved Purpose (g)). The IPND Manager must provide this information within a reasonable timeframe. In assessing a reasonable timeframe, relevant considerations include the volume and format of data requested, transmission capacity, impact on IPND operations, and the principle of non-discriminatory treatment.
- 10.8 Following agreement between the Data Provider and the IPND Manager of the relevant considerations, the IPND Manager must provide the extract of the PNCD within 30 days of that agreement.
- 10.9 Each IPND PNCD record will be identified by a Data Provider code and a Carriage Service Provider code. In an agency arrangement, the Data Provider code identifies the agent that supplies the data to the IPND on behalf of a Carriage Service Provider. In all PNCD data transfers, the IPND Manager must:
 - (a) include the Data Provider code to all Data Users;
 - (b) not include the Carriage Service Provider code to Public Number Directory Producers; and

- (c) include the Carriage Service Provider code for Approved Purposes (e) and (f).
- 10.10 The Data Provider must supply to the IPND, all Public Number Customer Data updates, that occur on one Business Day, by the next Business Day. This includes all transactions relating to pending connections or pending disconnections, and connections and disconnections.
- 10.11 The target end to end processing time from the provision of Public Number Customer Data by the Data Provider to the IPND until the availability of the Customer's Public Number Customer Data from the IPND is:
- (a) to a Data User for Approved Purpose (e) no later than 9.00 am (EST) the following day provided that the PNCD is received by 9.00 pm (EST); and
 - (b) to Data Users for Approved Purpose (f) within 24 hours; and
 - (c) to all other Data Users on the next Business Day.
- 10.12 For fixed line services the Public Number Customer Data in the IPND for Public Numbers made available by a CSP on a temporary basis to a customer for a period of up to 7 days may show the CSP as the Customer. Where the period of availability is more than 7 days, the provisions of this Code apply.
- 10.13 For other services made available for periods by a CSP to a customer, on a temporary basis:
- (a) when the CSP has made arrangements enabling queries from Emergency Services, Enforcement or National Security Agencies to be answered at any time, the Public Number Customer Data in the IPND may show the CSP as the Customer where the period of availability is 30 days or less. Where the period of availability is more than 30 days the provisions of this Code apply.
 - (b) when the CSP does not have in place arrangements as described in Clause 10.13(a), the Public Number Customer Data in the IPND may show the CSP as the Customer where the period of availability is 7 days or less. Where the period of availability is more than 7 days, the provisions of this Code apply.
- 10.14 Public Numbers associated with Customers who make those temporary services available for third parties on a short term basis (for example, hotels, hospitals, car rentals, etc.) will be entered in the IPND with the Customer information not the third party information.
- 10.15 Each Data User and Data Provider is to nominate to the IPND Manager an approved contact person(s) to manage Public Number Customer Data and deal with the IPND Manager and other parties on operational IPND issues.
- 10.16 The IPND Manager must ensure that on-line access to the IPND is not available to Data Users for reasons of data security.
- 10.17 Data Providers will provide to the IPND Manager all 1300, 1800, 190x or similar types of numbers and other equivalent services and the associated Public Number Customer Data. In the case of 1800 international numbers or equivalent services the Data Provider will provide all associated Public

Number Customer Data including foreign addresses, if permitted by the customer. The national C party translation, that is, the number or numbers associated with these services will be entered into the IPND as Unlisted Numbers. Where 1800 or equivalent numbers are used as private indial numbers Data Providers may exclude the Public Number Customer Data from the IPND.

11 IPND TRANSACTION PROCESSING

- 11.1 Where Public Number Customer Data contains a Hard Error:
 - (a) the IPND Manager must not add PNCD to the IPND; and
 - (b) the IPND Manager must produce a Hard Reject within 24 hours for retrieval by the Data Provider.
- 11.2 Where Public Number Customer Data contains a Soft Error:
 - (a) the IPND Manager must add PNCD to the IPND and must tag it to indicate the presence of a Soft Error; and
 - (b) the IPND Manager must produce a Soft Reject within 24 hours for retrieval by the Data Provider.
- 11.3 On receipt of a Hard Reject, the Data Provider must take reasonable steps to resolve the matter and supply the corrected Public Number Customer Data to the IPND within 1 Business Day.
- 11.4 On receipt of a Soft Reject, the Data Provider must take reasonable steps to resolve the matter and supply the corrected Public Number Customer Data to the IPND within 2 Business Days.
- 11.5 Relevant considerations in the correction of errors include, but are not limited to whether it is necessary to contact the Customer, technical difficulties, agency arrangements, time zones and file transfer times.
- 11.6 When the IPND receives a record from one Data Provider that will over write the existing record of another Data Provider within the IPND the IPND Manager will notify the original Data Provider of the event within 2 Business Days of this change.
- 11.7 Where the Data Provider has taken all possible steps to resolve a Hard Error and is still unable to enter Public Number Customer Data into the IPND, the IPND Manager and the Data Provider must take reasonable steps to identify and resolve the issue.
- 11.8 When a Data Provider sends an update to the IPND that causes a Public Number to change status from Listed to Unlisted the following action will be taken for Public Number Directory Producers:
 - (a) the IPND Manager must accept this update as valid;
 - (b) the IPND Manager must notify relevant Data Users that a particular Public Number has become Unlisted. The notification will only include:
 - (i) the Public Number;
 - (ii) date of unlisting; and
 - (iii) Data Provider code.

The IPND Manager must not provide any other PNCD associated with the Public Number to those Public Number Directory Producers; and

 - (c) those Data Users will ensure that all Public Number Customer Data associated with that Public Number is not disclosed to the Public. Those Public Number Directory Producers must update their

databases within 1 Business Day to remove and update all Public Number Customer Data associated with the Public Number prior to the next publication or use of the relevant Public Number Directory including Operator Assistance Services.

- 11.9 Data Users may only use the Listed to Unlisted IPND transaction to contact the Customer or the CSP to confirm the change in listing status.
- 11.10 When a Data Provider sends an update to the IPND that causes Public Number Customer Data to go from Listed to Suppressed Address, the following action will be taken for Public Number Directory Producers:
 - (a) the IPND Manager must accept this transaction as valid.
 - (b) the IPND Manager must provide to Public Number Directory Producers, a transaction that tags this Public Number Customer Data as Suppressed Address as per Clause 10.3.
 - (c) those Public Number Directory Producers must update their databases within 1 Business Day to remove and update all relevant PNCD associated with the Public Number prior to the next publication or use of the relevant Public Number Directory including Operator Assistance Services.

12 GENERAL PRINCIPLES FOR DATA TRANSFER – RULES FOR USE AND DISCLOSURE OF DATA TRANSFERRED FROM THE IPND

- 12.1 The IPND must have in-built functionality to deny provision of tagged unlisted Public Number Customer Data to Data Users except for:
 - (a) as provided for in Clause 11.8;
 - (b) an Emergency Call Service or an Emergency Services; or
 - (c) assisting Enforcement Agencies or National Security agencies.
- 12.2 In supplying PNCD to Location Dependant Carriage Services Data Users, the IPND Manager must withhold the name of the Customer.
- 12.3 The IPND must have in-built functionality to indicate that Public Number Customer Data has a Suppressed Address.
- 12.4 Data Users must not use IPND Public Number Customer Data to contact Customers, with the exception of the following:
 - (a) an Emergency Call Person; or
 - (b) Public Number Directory Producers.
- 12.5 This Code prohibits the use of IPND Public Number Customer Data for publishing or maintaining a Reverse Search Directory.
- 12.6 This Code prohibits use and/or disclosure of IPND Public Number Customer Data for any purpose other than an Approved Purpose. Examples of use of Public Number Customer Data by Data Users which would contravene this Code include but are not limited to:
 - (a) use of unlisted Public Number Customer Data for purposes other than assisting Enforcement Agencies, Emergency Services, National Security agencies, and for the provision of Location Dependant Carriage Services consistent with Clause 12.2; or
 - (b) selling or providing Public Number Customer Data to any other entity for any purpose except as a Public Number Directory Producer or as required by law; or
 - (c) analysing or collating information such that it could be used to obtain information about new services or moved services; or
 - (d) obtaining information about movement between CSPs or for establishment of marketing databases.

- 12.7 The IPND Manager will make available daily updates of the IPND database as indicated by the IPND Technical Requirements to Data Users within the same Approved Purpose category on a non-discriminatory basis.
- 12.8 Where a Data User requests data to be provided by particular fields, the IPND Manager must provide advice to that Data User regarding the cost and time involved. Where the Data User decides to proceed, the IPND Manager must respond in a reasonable timeframe and on a non-discriminatory basis.
- 12.9 All data transferred from the IPND will be via electronic means as specified via file transfer protocol, unless under exceptional circumstances where an alternate process is negotiated.
- 12.10 The IPND Technical Requirements document provided by the IPND Manager will contain a description of the standard file transfer mechanisms and formats.
- 12.11 Each Data Provider will receive details of file processing, completion or where appropriate, rejection, after each data transfer from the IPND has been processed.
- 12.12 A Data User may request a download of all the data contained in the IPND relevant to it at a specific point in time, that is, a bulk data refresh. A bulk data refresh may be arranged on request to the IPND Manager. Requests should be made in advance. The IPND Manager must provide this information within a reasonable timeframe. In assessing a reasonable timeframe relevant considerations include the volume of data requested, transmission capacity, impact on IPND operations, and the principle of non discriminatory treatment.

13 DATA ERRORS AND DATA QUERIES

- 13.1 The IPND Manager must produce information for each Data Provider which summarises the total number of its Public Number Customer Data records successfully processed and the number of those records rejected. This information must be made available to the Data Provider on a daily basis for reconciliation purposes except on days where no file is submitted.
- 13.2 The Data Provider must download the information referred to in Clause 13.1, and investigate the success or failure of the data transfer. The Data Provider must amend and transmit any corrections via daily upload files to the IPND in accordance with Clauses 11.3 and 11.4.
- 13.3 If a Data User discovers a new potential error or queries the content of an IPND data record, that Data User will notify the IPND Manager, without undue delay, of this query in the manner set out in the IPND Technical Requirement.
- 13.4 On receipt of potential error notifications the IPND Manager must make available a daily file of these notifications to the relevant Data Provider within one Business Day of receipt.
- 13.5 The IPND Manager must make available a daily file to all Data Users of all listed potential errors within one Business Day of receipt.
- 13.6 The IPND Manager must make available a daily file of all potential errors including those which relate to unlisted Public Number Customer Data to Data Users who assist Enforcement Agencies, Emergency Services and National Security agencies within one Business Day of receipt.
- 13.7 The receipt of an updated data record in response to the Data User Query File will clear the query tag in the IPND.

14 CUSTOMER CONTACT

14.1 A Data Provider must take reasonable steps to inform the Customer of the type of use and the type of disclosure of their Public Number Customer Data under this Code. These steps should be consistent with relevant privacy obligations. Examples of reasonable steps include, but are not limited to, inclusion in standard forms of agreement, provision of written material to Customers, provision of verbal advice to Customers or information via public media.

14.2 If a Customer contacts any of the following in relation to Public Number Customer Data:

- (a) the IPND Manager; or
- (b) a Data Provider who is not the Customer's CSP; or
- (c) a Data User who is not the Customer's CSP,

then the IPND Manager, the Data Provider, the CSP and the Data User, as the case may be, must advise the Customer that changes to their Public Number Customer Data can only be effected by that Customer's CSP.

14.3 A Data Provider must take reasonable steps to ensure that the Customer understands that at any time they wish to have their basic IPND data altered in any way that they will be required to contact their CSP to arrange the alteration of their Public Number Customer Data. Examples of reasonable steps include, but are not limited to, inclusion in standard forms of agreement, provision of written material to Customers, provision of verbal advice to Customers or information via public media.

14.4 By agreeing to this Code, each Participant agrees to be bound by the Customer's choice to have their Public Number Customer Data tagged as either Listed or Unlisted.

14.5 Customer contact may arise from indirect use of Public Number Customer Data within the IPND by Enforcement Agencies or a National Security agency or an Emergency Service Organisation.

15 INFRASTRUCTURE

- 15.1 Data Providers are responsible at their cost for the provision and maintenance of their own data provision links and medium to the IPND. The Data Provider is responsible for ensuring that technical compatibility with the IPND is achieved.
- 15.2 Data Users are responsible at their cost for the provision and maintenance of their own data extraction links and medium to the IPND. The Data User is responsible for ensuring that technical compatibility with the IPND is achieved.
- 15.3 The IPND Manager is also responsible for facilitating the implementation of the IPND Technical Requirements with all Participants.
- 15.4 The IPND Manager will provide an encryption device and undertake to replace or repair any such encryption device which ceases to function.
- 15.5 A CSP may contract with another CSP or Data Provider to act as its agent to arrange for the provision of the required information to the IPND.
- 15.6 IPND Users may propose changes to the IPND interface which will be considered by the IPND Manager and other IPND Users.
- 15.7 The IPND Manager must consider all reasonable requests of a Data Provider and/or Data User for additional technical enhancements to the IPND.
- 15.8 The IPND Manager must consult relevant Data Users and Data Providers about proposed changes to the IPND Technical Requirements and seek the agreement of the majority of relevant Participants. Participants must not unreasonably delay in responding or unreasonably withhold consent. Where the IPND Manager judges that the change to the File Specification is necessary and urgent, a timeframe for response may be specified.
- 15.9 The IPND Manager must provide to all Data Providers and Data Users on a non discriminatory basis at least six months advance written notification of changes to the IPND interface and to technical specifications having a material impact on them.
- 15.10 The IPND Manager must consider all reasonable comments of the Data Providers and Data Users in relation to any proposal by the IPND Manager to change the IPND interface.
- 15.11 All IPND Users will implement changes referenced in Clause 15.9 within an agreed specified timeframe enabling compliance with the IPND Manager's reasonable requirements.

16 DATA SECURITY

- 16.1 The IPND will be located within a secure building and must be independent from any other of the IPND Manager's IT systems apart from those needed to maintain and support the IPND.
- 16.2 To maintain data security and integrity, on-line access to the IPND is not available with the exception of Clause 17.1.
- 16.3 Data Users are responsible to ensure that data received from the IPND is maintained securely against loss, or against unauthorised access, use, modification or disclosure, in accordance with relevant privacy obligations.
- 16.4 An IPND User who becomes aware of any breach of security within their organisation which may reasonably be foreseen to have an impact on the integrity and confidentiality of the Public Number Customer Data residing in the IPND must advise the IPND Manager who will advise relevant IPND Users. The IPND User must take any other reasonable steps to minimise the effects of the breach.
- 16.5 If the IPND Manager has reasonable grounds to believe that a Data User has breached the Code or other law in its use or disclosure of Public Number Customer Data, in such a way as to impact on the integrity or confidentiality of the Public Number Customer Data, the IPND Manager must immediately notify all Data Providers whose Public Number Customer Data may be compromised by the suspected breach so that they may take appropriate steps to mitigate their loss, and provide reasonable assistance to Data Providers in such mitigation. This Clause does not imply that the IPND Manager has a responsibility to identify all breaches.
- 16.6 Where the IPND Manager becomes aware of any breach of security of the Public Number Customer Data stored in and archived from the IPND, which may reasonably be considered to have an impact on the integrity and confidentiality of the Public Number Customer Data stored in and archived from the IPND, the IPND Manager must advise relevant IPND Data Users and all Data Providers. The IPND Manager must take all other reasonable steps to minimise the effects of the breach, including cooperating with IPND Users in action they need to take in respect of the breach.

17 CONFIDENTIALITY

- 17.1 To preserve confidentiality the IPND Manager's access to the Public Number Customer Data is limited to that necessary for maintenance, administration and to carry out the responsibilities of the IPND Manager under this Code.
- 17.2 Where the responsibility of the IPND Manager involves necessary viewing of IPND data beyond that normally required for maintenance, administration, fault identification, auditing and reporting, the IPND Manager must notify all relevant Data Providers. The IPND Manager must specify the reason for such viewing and a description of the activities in relation to that viewing. Notification must occur within seven Business Days after the event.

18 BILATERAL AGREEMENTS

- 18.1 This Code contains the minimum requirements for data transferred to and from and stored in the IPND. While parties may agree on alternative arrangements in bilateral agreements, such alternative arrangements must not diminish any requirements or principles in this Code.
- 18.2 If bilateral arrangements are entered into between the IPND Manager and Data Providers they should incorporate:
 - (a) indemnities against risk arising from the requirements set out in this Code; and
 - (b) the intent of the provisions of Clauses 7.1, 7.6 and 12.6, and Sections 16 and 17 of this Code.
- 18.3 If bilateral arrangements are entered into between the IPND Manager and Data Users they should incorporate:
 - (a) indemnities against risk arising from the requirements set out in this Code; and
 - (b) the intent of the provisions of Clauses 7.1 and 12.6 and Sections 16 and 17 of this Code.

19 ADMINISTRATION AND COMPLIANCE

19.1 ACIF Code Administration and Compliance Scheme

Under ACIF Industry Code Signatory arrangements, Signatories to this Industry Code are subject to the ACIF G524:2001 **Code Administration and Compliance Scheme** Industry Guideline (*the Scheme*). Accordingly, all Signatories who are bound by this Code are also bound by the Scheme.

19.2 Powers to handle industry complaints under this Code

19.2.1 Complaints may be made under this Code to ACIF by a member of the industry (*or a voluntary or non-profit consumer organisation or similar body*) (*an "Industry Complaint"*) about a contravention of this Code by a Signatory to this Code.

19.2.2 Complaints by a member of the industry (*or a voluntary or non-profit consumer organisation or similar body*) about a contravention of this Code by a Signatory to this Code may be referred from the ACA under the power granted to the ACA in section 514 of the Telecommunications Act 1997, subject to ACIF's agreement to accept the referral. Without limiting the grounds on which ACIF may withhold its agreement to accept a referral, ACIF may withhold its agreement where it considers that the complaint can be more conveniently dealt with in another forum or that handling the complaint may impose an unreasonable cost burden on ACIF.

19.2.3 ACIF must handle complaints under 19.2.1 or 19.2.2 in accordance with the provisions of the ACIF G514:2001 Code Administration and Compliance Scheme.

19.3 If the IPND Manager or an IPND User has reasonable grounds to believe that another IPND User has breached the Code or other law in its use or disclosure of Public Number Customer Data, the IPND Manager or that IPND User, as appropriate, must immediately refer the suspected breach to ACIF, where it involves a Code signatory, and/or ACA, where the Code is registered.

20 MONITORING

- 20.1 The IPND Manager must assist the ACIF Executive in administering and monitoring of this Code by providing reports as requested including the quality measures in Appendix A – IPND Quality Management Measures.
- 20.2 The IPND Manager will make recommendations to the ACIF Operations Codes Reference Panel where there are industry developments or practices which will impact on the Code or require a separate code to be drafted.

21 REVIEWING

- 21.1 The ACIF Operations Code Reference Panel will review this Code no later than the last day of the month, 12 months after the date of publication by ACIF. The IPND Manager will assist the ACIF Operations Code Reference Panel by providing reports as requested. In addition the Code must be reviewed under Clause 21.2 and subsequent reviews under the ACIF Code Administration and Compliance Scheme.
- 21.2 The Code must be reviewed when:
- (a) the ACA by written notice specifies a change in Approved Purposes or requires additional information for Public Number Customer Data; or
 - (b) regulations are made under the Act which change the extent of Operator Services; or
 - (c) any other relevant changes in legislation that impact the operation of the IPND.

22 AGENCY

- 22.1 Although Participants may enter into agency arrangements with regard to the IPND, the existence of agency arrangements does not diminish the rights and obligations of Participants that exist under this Code.

APPENDIX A

IPND QUALITY MANAGEMENT MEASURES

REPORT	SUB REPORT	PROVIDED BY	REPORT FREQUENCY	RECIPIENT	CODE REFERENCE
List of registered IPND Users					
This list will show company name, company address, contact name, contact telephone number.	IPND Register	IPND Manager	As required	IPND Users	8.1; 8.3,10.15, 20.1
		IPND Manager	Yearly	ACA, ACIF, IPND Users	
Upload and Download transactions					
Records received/sent This report shows the daily transactions per IPND User. It shows the number of records received from a data provider, or the number of records sent to a data user. This report is incorporated in the error report generated per transfer activity.	Daily Error Report	IPND application	Daily	Data Provider or Data User.	7.8, 9.4, 13.1; 13.5
Activity Report A summary of transactions uploaded by Data Provider	A summary of file transfer activity. Exception report by IPND user	IPND Manager	Weekly	IPND User	9.4, 12.7

REPORT	SUB REPORT	PROVIDED BY	REPORT FREQUENCY	RECIPIENT	CODE REFERENCE
or downloaded by Data User.	A summary of file transfer activity by IPND user	IPND Manager	Monthly	IPND Users ACA, ACIF notified if failure to transfer is more than 30 days.	9.4, 12.7
Services Connected Report This report shows a snapshot of the status of the IPND.	Monthly snapshot of the number of records tagged as connected/disconnected per CSP.	IPND Manager	Monthly	Data Provider	10.10
	Yearly snapshot of the number of records tagged as connected/disconnected per CSP. An aggregated report.	IPND Manager	Yearly	ACA, ACIF, IPND Users	20.1
Error Reports					
Each upload file received by the IPND will generate an error report to the data provider. This report will indicate: * the number of records received per file; * the number of hard error records per file; * the number of soft errors per file; * the number of warnings per file Each download file sent by the IPND will generate a file		IPND application	Per file received	IPND Users as appropriate	7.8, 9.4, 11.1, 11.2, 12.11, 13.1

REPORT	SUB REPORT	PROVIDED BY	REPORT FREQUENCY	RECIPIENT	CODE REFERENCE
record count which indicates the number of records contained in the download file.					
Soft Error Report					
A report which provides analysis of the type of Soft Errors against a record in the IPND per CSP.	CSP Report	IPND Manager	Monthly	Data Providers	11.2
	Amalgamated report	IPND Manager	Yearly	ACA and IPND users	11.2
User error query file management					
This report will show the number of outstanding queried services per Data Provider.	CSP Report	IPND Manager	Monthly	Data Providers	13.4, 13.6
	Amalgamated report	IPND Manager	Yearly	ACA and IPND Users	20.1
Security Notification					
An exception report of a breach of security to the IPND	Security Notification	IPND Manager	Exception	IPND users, ACA	16.4, 16.5, 16.6

The policy objective of the greatest practicable use of industry self-regulation without imposing undue financial and administrative burdens on industry is central to the regulatory scheme of the *Telecommunications Act 1997*.

ACIF was established to implement the policy of industry self-regulation. It is a company limited by guarantee and is a not-for-profit membership-based organisation. Its membership comprises carriers/carriage service providers, business and residential consumer groups, industry associations and individual companies.

ACIF's mission is to develop collaborative industry outcomes that foster the effective and safe operation of competitive networks, the provision of innovative services and the protection of consumer interests. In the development of Industry Codes and Technical Standards as part of its mission, ACIF's processes are based upon its principles of openness, transparency, consensus, representation and consultation. Procedures have been designed to ensure that all sectors of Australian society are reasonably able to influence the development of Standards and Codes. Representative participation in the work of developing a Code or Standard is encouraged from relevant and interested parties. All draft Codes and Standards are also released for public comment prior to publication to ensure outputs reflect the needs and concerns of all stakeholders.



Published by:
**THE AUSTRALIAN
COMMUNICATIONS
INDUSTRY FORUM LTD**

Level 9
32 Walker Street
North Sydney
NSW 2060 Australia

Correspondence:
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
TTY 61 2 9923 1911
E acif@acif.org.au
www.acif.org.au
ABN 56 078 026 507

Care should be taken to ensure that material used is from the current version of the Standard or Industry Code and that it is updated whenever the Standard or Code is amended or revised. The number and date of the Standard or Code should therefore be clearly identified. If in doubt please contact ACIF.