AUSTRALIAN
COMMUNICATIONS
INDUSTRY FORUM

INTEGRATED PUBLIC NUMBER DATABASE (IPND) INDUSTRY CODE ACIF C555:2007

ACIF C555:2007 *Integrated Public Number Database (IPND)* Industry Code

First published as ACIF C555:2000
Second edition as ACIF C555:2002

Communications Alliance Ltd was formed in 2006 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services. ACIF is a division of Communications Alliance.

Disclaimers

1. Notwithstanding anything contained in this Industry Code:

   (a) Communications Alliance disclaims responsibility (including where Communications Alliance 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) Communications Alliance disclaims responsibility (including where Communications Alliance 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

EXPLANATORY STATEMENT

Introduction

This Explanatory Statement is to be read with the ACIF ***Integrated Public Number Database IPND*** Industry Code (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.

This Code replaces ACIF C555:2002 ***IPND Data Provider, Data User and IPND Manager*** Industry Code published by ACIF in April 2002.

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

Background

The Integrated Public Number Database (IPND) is an industry-wide database of all Public Numbers which facilitates the provision of information for purposes specified in the Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997 (Licence Conditions) including the provision of Directory Assistance Services and the publication and maintenance of Public Number Directories.

The IPND serves as a repository of Public Number Customer Data (PNCD) which broadly includes the Public Number, the Customer name, address and Directory Related Services' information which can be used, for example, to assist in 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. As such, it provides a valuable resource to the Australian telecommunications industry and the Australian community.

The IPND is a passive database whereby the IPND Manager facilitates the passage of data from Data Providers and to Data Users. While it is a common misconception that data is provided directly to the IPND and accessed directly from the IPND, this is not the case. Both PNCD and PNDD are made up of data that is said to be derived directly from the IPND. The use of the word derived is important as it clarifies that Data Users do not have direct access to IPND data. It is this data which can be used for the Approved Purposes contemplated by the Act, the Code and the Licence Conditions.

Current Regulatory Arrangements

The Licence Conditions 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).

PNCD may only be accessed from the IPND Manager for Approved Purposes as specified in the Licence Conditions, or as allowed by the Act or other relevant legislation.

The Approved Purposes do not imply that Data Users may access the data for the full range of Approved Purposes.

Part 13 of the Act deals with the protection of personal particulars by prohibiting its use and disclosure except in limited circumstances. Section 285 of the Act however allows for disclosures and uses for information held in the IPND for specified approved purposes. The Licence Conditions also contain provisions about the disclosure and use of PNCD held in the IPND.

2002 Version of the Code

The first IPND Code was developed in 2002 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 Manager and the storage of information in the IPND.

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

(a) responsibility for the accuracy of the information provided to the IPND Manager; 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 the Customers' listing preferences, in particular, with the protection of entries that Customers do not want published in directories or made available through Directory Assistance Services.

2007 Revision

This revision seeks to:

- bring the Code into alignment with the Act and the *Telecommunications (Section of the Telecommunications Industry) Determination 2007* and other applicable legal requirements and
- clarify matters relating to:
    - Customers;
    - operational issues; and
    - technical issues

by re-ordering the content for ease of reading and revising some clauses for improved clarity.

Why Current Regulatory Arrangements are inadequate

The IPND Manager plays a key role in providing management, access to data held in the IPND and the maintenance and security of the IPND, and copies of the IPND. The Code contains obligations to ensure that the IPND Manager acts in an equitable manner when dealing with Data Users and importantly provides that, where the IPND Manager is also a CSP, that CSP does not gain an unfair advantage over other CSPs.

In 2003 a Working Group was established to review the Approved Purposes following a request from the former ACA to address a number of perceived weaknesses in the use of IPND data in the Code. Following review by the Working Group, a Working Committee was established to revise the Approved Purposes. Later in 2003 the former ACA wrote to ACIF stating its intent to determine an Industry Standard under section 125 of the Act.

In 2006 an alternative approach was taken to define the Approved Purposes in the Act and to support the Act with the *Telecommunications (Section of the Telecommunications Industry) Determination 2007*.

In October 2006 the Australian Government introduced the *Telecommunications Amendment (Integrated Public Number Database) Bill 2006* which provided for amendments to the *Telecommunications Act 1997* (Telecommunications Act). The Bill was passed and received royal assent on 8th December 2006.

The amendments to the Telecommunications Act serve to clarify arrangements regarding access to data in the IPND through the following key additions:

- a definition of a Public Number Directory;
- a new exception to the prohibitions allowing the disclosure of IPND information for research purposes in the public interest, as specified by the Minister;
- provisions allowing for penalties for secondary disclosure of IPND information; and
- the requirement for the Australian Communications and Media Authority (ACMA) to make an IPND scheme, supported by a range of Ministerial Instruments, for granting authorisation to access data held in the IPND for specified purposes.

The IPND Scheme commenced in 2007 and details the processes by which ACMA may grant authorisation enabling access to and use of information in the IPND for purposes specified in section 285 (1A) (d) of the Telecommunications Act. Those purposes are the publication and maintenance of a Public Number Directory and the conduct of research of a kind specified by the Minister.

The IPND Scheme provides for the making of applications, the assessment of applications, the period for which an authorisation will apply and the notification of decisions under the scheme. The scheme also provides for the imposition of conditions on the granting of authorisation, and outlines the process for when an authorisation will end.

Under the Scheme, PNDPs are subject to a two phase application process for provisional and final authorisation. At each stage of the process PNDPs must also apply to the IPND Manager to seek access to a provisional IPND data source for provisional authorisation and then PNDD for final authorisation. ACMA provides authorisations to PNDPs on an ongoing basis subject to compliance with conditions of the Scheme and the Ministerial Instruments under the Act.

The Scheme compels researchers seeking access to PNDD to apply on a project by project basis for access of a fixed duration. The Scheme requires researchers to apply for access to PNDD for a period up until disaggregation and/or de-identification can occur of research findings. Researchers will also be required to seek access from the IPND Manager after authorisation has been granted by ACMA.

Public Number Directory Publishers and researchers to whom the Scheme applies need to apply to the IPND Manager to make arrangements for giving access to data derived directly from the IPND. Data Users for other Approved Purposes are only required to seek approval to access data held in the IPND from the IPND Manager.

In addition to having obligations under the Scheme, Public Number Directory Publishers and researchers will be required to comply with the relevant Ministerial Instruments made under the Act in relation to those approved purposes.

ACMA has made the *Telecommunications (Section of the Telecommunications Industry) Determination 2007* so that this Code applies to Public Number Directory Publishers. ACMA was not able, however, to make such a determination for researchers who will access data derived directly from the IPND as the researcher's activities could not be considered telecommunications activities for the purposes of section 109 of the Act. It is intended, however, that similar rules to the Code will be adopted for researchers in the IPND Scheme or in another instrument under the Act.

The Code seeks to support the new requirements of the Act, the IPND Scheme and the *Telecommunications (Section of the Telecommunications Industry) Determination 2007*.

How the Code Builds on and Enhances the Current Regulatory Arrangements

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) the interest of Data Providers in being assured that their commercially sensitive Customer information is protected from misuse by Data Users and the IPND Manager, 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 the Customer has chosen an Unlisted Entry;

(c) the interest of Data Users in being able to access PNCD on clearly understood and equitable 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 PNCD as it is provided to, stored in and 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 PNCD to the IPND and the assurance that Data Users will only access and use PNCD held in the IPND for Approved Purposes.

What the Code will Accomplish

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

(a) agreed uniform procedures and formats are followed when PNCD is transferred to the IPND Manager by Data Providers and from the IPND Manager by Data Users; and

(b) agreed uniform procedures and formats are followed when PNCD is provided to Data Users; and

(c) procedures treat all Data Providers on an equitable basis; and

(d) procedures treat all Data Users in the same Approved Purpose category on an equitable basis; and

(e) procedures do not detract from Customers' privacy 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 PNCD 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 PNCD provided to, from and stored in the IPND.

How the Objectives will be Achieved

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

(a) the 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 PNCD 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 PNCD to the IPND;

(d) that Data Users may be provided with PNCD which can only be used for Approved Purposes;

(e) processes in relation to errors in PNCD; and

(f) processes to ensure the security, privacy and confidentiality of PNCD.

Anticipated Benefits to Consumers

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 Related 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 PNCD for Enforcement Agencies;

(e) capturing individual Customers requirement to:

    (i) not to be included in Public Number Directories and Directory Assistance Services; or

    (ii) have only part of their address included in Public Number Directories and Directory Assistance Services; and

(f) the implementation of proper and lawful protection for the privacy of Customer data stored in the IPND.

Anticipated Benefits to Industry

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

A cooperatively developed self-regulatory Code is the most appropriate method of addressing these interests, and providing the assurances that IPND Users seek. 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 out in section 4 of the Act.

Anticipated Cost to Industry

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, the IPND Technical Requirements, the IPND Scheme and related instruments, rather than from the Code.

There are establishment and ongoing costs incurred by Data Providers in establishing the means by which they will provide PNCD to the IPND Manager 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 Entry 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 Data Users in establishing the means by which they will access PNCD from the IPND.

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

Other Public Benefits or Considerations

Registration of the Code by ACMA ensures that its rules can be enforced.

Code Implementation

Discrepancies exist between the Act and the Licence Conditions in relation to Location Dependent Carriage Services. In order to allow these discrepancies to be addressed, it is necessary to have a delayed implementation of all aspects of the Code relating to the supply and use of PNCD for Location Dependent Carriage Services, until six months after registration of the Code.

Therefore the Code will be implemented in two stages:

- Immediately upon registration, the Code will become effective, with the exception of supply and use of PNCD relating to Approved Purpose (d).
- Six months after registration all code rules will become operational and enforceable for supply and use of PNCD for all Approved Purposes.

Alexander R. Osborne
Chairman
ORP/WC30 : IPND Working Committee

TABLE OF CONTENTS

1 GENERAL

1.1 Introduction

1.1.1 Section 112 of the *Telecommunications Act 1997* (the Act) sets out the intention of the Commonwealth Parliament that bodies and associations in the telecommunications industry develop industry codes relating to the telecommunications activities of those bodies.

1.1.2 The development of the Code has been facilitated by Communications Alliance through a Working Committee comprised of representatives from the telecommunications industry, Government regulatory agencies, Public Number Directory Publishers and consumer groups.

1.1.3 The Code should be read in the context of other relevant Codes, Guidelines and documents, including the ACIF G619:2007 ***IPND Data*** Industry Guideline.

1.1.4 The Code should be read in conjunction with other sources of relevant legal requirements including:

(a) the Act;

(b) the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (the TCPSS Act);

(c) the *Privacy Act 1988*;

(d) *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997* and/or any other Prescribed Conditions';

(e) the *Telecommunications Integrated Public Number Database Scheme 2007;.*

(f) the *Telecommunications (Interception and Access) Act 1979*; and

(g) the *Telecommunications (Section of the Telecommunications Industry) Determination 2007.*

1.1.5 If there is a conflict between the requirements of the Code and any requirements imposed on a Participant by law, the Participant will not be in breach of the Code by complying with the requirements of the law.

1.1.6 Statements in boxed text are a guide to interpretation only and not binding as Code rules.

1.1.7 The IPND has been developed as a resource for the telecommunications industry, Directory Related Services industry, Enforcement Agencies and Emergency Services organisations in Australia, and for any other purpose as allowed under the IPND Scheme.

1.1.8 The IPND is a national central repository for the receipt, storage and distribution of PNCD for Data Providers and Data Users.

1.1.9 Telstra is obliged under its Licence Conditions to establish and maintain an industry wide IPND.

1.1.10 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, the Code and the Prescribed Conditions will continue to apply.

1.1.11 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 with all information reasonably required in connection with the fulfilment of that obligation.

1.1.12 Where the term IPND Manager is used in the Code, the term applies only to that person in its capacity as the IPND Manager.

1.1.13 Where the term CSP is used in the Code, and a CSP is also the IPND Manager, the term applies to that organisation in its role as a supplier of Carriage Services and not in its capacity as IPND Manager.

1.2 Registration with ACMA

The Code is to be submitted to the Australian Communications and Media Authority for registration pursuant to section 117 of the *Telecommunications Act 1997* (Cth).

1.3 Scope

1.3.1 The Code is applicable to the following sections of the telecommunications industry under section 110 of the Act:

(a) Carriers;

(b) Carriage Service Providers; and

(c) Public Number Directory Publishers.

For the purposes of the Code these are specifically Data Providers and Data Users (collectively known as IPND Users) and the IPND Manager.

NOTE: The Code is also applicable to the IPND Manager as:

- *this role is currently performed by a Carrier; and*
- *the IPND Manager carries out the telecommunications activities listed in Clause 1.3.3.*

1.3.2 The Code deals with the following telecommunications activities as defined in Section 109 of the Act:

(a) carrying on business as a Carrier; or

(b) carrying on business activities as a Carriage Service Provider; or

(c) supplying Goods or Service(s) for use in connection with the supply of a Listed Carriage Service.

1.3.3 The Code applies to the telecommunication activities of Participants listed in Clause 1.3.1, and in particular relates to the following activities:

(a) supply of PNCD to the IPND Manager by a Data Provider pursuant to Part 4 of Schedule 2 of the Act;

(b) accessing of PNCD from the IPND Manager by Data Users pursuant to the Act and other relevant law; and

(c) managing, maintaining and administering PNCD stored in the IPND by the IPND Manager pursuant to the Prescribed Conditions.

1.3.4 The Code does not cover charging principles related to access to PNCD.

1.4 Objectives

The objectives of the Code are to ensure that:

(a) Data Providers capture and provide details of the Customer's choice of a Listed Entry, Unlisted Entry or where offered, Suppressed Address Entry;

(b) Data Providers take reasonable steps to provide Customers with sufficient information about the use of PNCD data;

(c) the rights and obligations of Participants regarding the input, use, disclosure and storage of PNCD in the IPND are clear;

(d) agreed uniform procedures and formats are followed when PNCD is transferred to the IPND Manager by Data Providers;

(e) agreed uniform procedures and formats are followed when PNCD is transferred from the IPND Manager to Data Users;

(f) procedures treat Data Providers on an equitable basis;

(g) procedures treat Data Users within the same Approved Purpose category on an equitable basis;

(h) procedures do not detract from Customers' rights with regard to privacy of personal information;

(i) procedures and processes maximise data accuracy and efficiency through the cooperation of all Participants; and

(j) PNCD that is input to, stored in, used and disclosed from the IPND is adequately protected.

1.5 Code review

Review of the Code will be conducted after five years of the Code being registered by the Australian Communications and Media Authority.

1.6 Code Implementation

1.6.1 Provisions of this Code will take effect immediately upon registration of this Code by ACMA, with the exception of supply and use of PNCD relating to Approved Purpose (d) for Location Dependent Carriage Services.

1.6.2 Provisions of the Code relating to supply and use of PNCD relating to Approved Purpose (d) will take effect six months from the date of registration of this Code by ACMA.

2 ACRONYMS, DEFINITIONS AND INTERPRETATIONS

2.1 Acronyms

For the purposes of the Code, the following acronyms apply:

ACIF	Australian Communications Industry Forum
ACMA	Australian Communications and Media Authority
CSP	Carriage Service Provider
IPND	Integrated Public Number Database
PMTS	Public Mobile Telecommunications Service
PNCD	Public Number Customer Data
PNDD	Public Number Directory Data

2.2 Definitions

For the purposes of the Code, the following definitions apply:

Act

means the *Telecommunications Act 1997(Cth)*.

Amalgamated Query File

means a file containing potential inconsistencies in PNCD raised by all Data Users, and is a mechanism whereby a Data User can directly verify that a query is active for a particular service.

NOTE: A query for any service flagged as an Unlisted Entry will only be sent to Enforcement Agencies and Emergency Services.

Approved Purpose

means in respect of PNCD stored in the IPND, the following activities :

(a) providing Directory Assistance Services;

(b) providing Operator Services or Operator Assistance Services;

(c) publishing and maintaining 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 in accordance with Part 14 of the Act, or any other applicable legal requirement;

(g) verifying the accuracy of information provided by the Data Provider and held in the IPND against the information the Data Provider holds;

(h) undertaking research of a kind specified in the *Telecommunications (Integrated Public Number Database – Permitted Research Purposes) Instrument 2007 (No.1);*

(i) assisting ACMA, or its nominee, to verify the accuracy and completeness of information held in the IPND; and

(j) any other purposes where permitted by the Act, and any other relevant laws.

Authorities

includes but is not limited to ACMA, the Office of the Privacy Commissioner and an Enforcement Agency.

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

has the same meaning as in the Act.

Carriage Service Provider

has the meaning given by section 87 of the Act.

NOTE: CSPs include internet service providers and VoIP service providers.

Customer

means the person who is contracted to the CSP for the supply of a Carriage Service in association with a Public Number.

Data Provider

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

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 a file generated by the IPND and sent to the Data Provider which highlight potential inconsistencies in PNCD, identified by Data Users via Data User Query Files.

Data User

means an entity which has access to PNCD or PNDD for an Approved Purpose.

Data User Query File

means a file generated by a Data User and sent to the IPND Manager to highlight one or more potential inconsistencies in PNCD.

Directory Assistance Services

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

Directory Assistance Service Provider

means a provider of Directory Assistance Services and includes Operator Assistance Services.

Directory Related Services

means Directory Assistance Services, Operator Assistance Services, Operator Services and the publication and maintenance of Public Number Directories.

Emergency Call Person

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

Emergency Call Service

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

Emergency Service

has the same meaning as given in section 7 in the Act.

Enforcement Agency

means a government agency who requires access to information stored in the IPND for the law enforcement or national security purposes described in the Licence Conditions.

File Specification

means the file format (consisting of, but not limited to, data fields, data field lengths, and 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.

Geographic Number

means a number that has been allocated under the Numbering Plan to a CSP for the provision of a Local Service.

Hard Error

means an error that prevents the upload of the file and/or PNCD 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.

Hard Reject

means PNCD 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) the ACIF C555:2007 ***Integrated Public Number Database*** Industry Code;

(e) the ACIF G619:2007 ***IPND Data*** Industry Guideline; and

(f) such other information the IPND Manager deems appropriate.

Integrated Public Number Database

means the Integrated Public Number Database created pursuant to the Act and the Licence Conditions.

IPND Manager

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

IPND Scheme

means the *Telecommunications Integrated Public Number Database Scheme 2007*.

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 PNDD that will be available in Directory Related Services and includes a Standard Telephone Service with:

(a) a Geographic Number that the Customer has not requested to be excluded from Directory Related Services;

(b) a Mobile Service Number, that the Customer has agreed to be included in Directory Related Services;

(c) a Public Number that when called, gives access to a private telephone exchange extension that the Customer has specifically requested to be included in Directory Related Services; or

(d) any other Public Number that the Customer has specifically requested to being included in Directory Related Services.

Local Service

has the same meaning as in the Numbering Plan.

Location Dependent Carriage Service

means a Carriage Service which:

(a) depends for its provision on the availability of information about the street address of the caller, and

(b) routes calls to a particular destination, normally the closest destination to the caller.

Location Dependent 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 Local Service, the service address as installed, unless not technically feasible; or

(ii) for a PMTS, the physical address, where practicable, as provided by the Customer;

(c) a code that can be used to identify the CSP that provides:

(i) service for the originating or terminating Carriage Services to the Customer; or

(ii) PMTS to the Customer; and

(d) an indication of whether the service is to be a Listed Entry, an Unlisted Entry or a Suppressed Address Entry (where offered) in a Public Number Directory.

Mobile Service Number

means a number that has been allocated under the Numbering Plan to a CSP for the provision of a PMTS.

Numbering Plan

means the *Telecommunications Numbering Plan 1997*.

Operator Assistance Service

means a service involving the connection of a telephone call by an operator, as per the Licence Conditions.

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;

as per the Act and Licence Conditions.

Participants

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

Prescribed Conditions

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

Public Mobile Telecommunications Service

has the meaning given in section 32 of the Act.

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 the Licence Conditions, and for the purposes of this Code comprises:

(a) the Public Number; and

(b) the name of the Customer; and

(c) the directory finding name as appropriate; and

(d) the address of the Customer which is:

  (i) for a Local Service, the service address as installed unless not technically feasible;

  (ii) for a PMTS, the physical address, where practicable, as provided by the Customer; and

  (iii) for a Listed Entry or Suppressed Address Entry (where offered), the directory address; and

(e) the name of the CSP that provides:

  (i) services for the originating Carriage Services to the Customer; or

  (ii) PMTS to the Customer; and

(f) an indication of whether the service 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 Entry or a Suppressed Address Entry (where offered) in a Directory Related Service.

Public Number Directory

has the meaning given by section 285(2) of the Act.

Public Number Directory Data

means a sub-set of PNCD derived directly from the IPND including:

(a) the Public Number of the Customer;

(b) the name of the Customer;

(c) the directory finding name for a Listed Entry or Suppressed Address Entry;

(d) the directory address of the Customer for a Listed Entry or Suppressed Address Entry (where offered);

(e) an indication of whether the service is to be used for government, business, charitable or residential purposes, if practicable; and

(f) an indication of whether the service is to be Listed Entry, an Unlisted Entry or a Suppressed Address Entry (where offered) in a Directory Related Service;

(g) or as otherwise authorised pursuant to the IPND Scheme.

Public Number Directory Publisher

has the same meaning as given in *Telecommunications (Section of the Telecommunications Industry) Determination 2007*.

Public Payphone

means a public payphone as defined in the *Licence Conditions* which is operated by a Carrier or CSP.

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 PNCD that contains a potential error that is tagged by the IPND and returned to the Data Provider.

Standard Telephone Service
has the same meaning as in the *Telecommunications (Consumer Protection and Service Standards) Act 1999.*

Suppressed Address Entry

means a Listed Entry whereby at the Customer's request, and if offered by the CSP, only the Customer's name, locality, State, postcode and Public Number will be made public in Directory Related Services.

Unlisted Entry

means PNDD that will not be available in Directory Related Services and includes a Standard Telephone Service with:

(a) a Geographic Number that the Customer has specifically requested to be excluded from Directory Related Services;

(b) a Mobile Service Number that the Customer has not agreed to be included in Directory Related Services;

(c) the number of a Public Payphone;

(d) a Public Number that when called, gives access to a private telephone exchange extension that the Customer had not specifically requested be included in Directory Related Services; or

(e) any other Public Number, that the Customer has not specifically requested to be included in Directory Related Services.

2.3 Interpretations

In the Code, unless the contrary appears:

(a) a reference to a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them;

(b) words in the singular includes the plural and vice versa;

(c) a verb used in the present tense includes that verb used in other tenses;

(d) words importing persons include a body whether corporate, politic or otherwise; and

(e) a reference to a person includes a reference to the person's executors, administrators, successors, officer, employee, volunteer, agent and/or subcontractor (including but not limited to, persons taking by novation) and assigns.

3 PRINCIPLES

3.1 Nothing in this Code is intended to change the intellectual property rights (if any) of Participants.

3.2 The requirements of this Code will apply equitably to all Participants, unless otherwise provided.

3.3 The IPND will perform minimal processing and filtering of PNCD, requiring a cooperative approach amongst Participants to data accuracy.

3.4 The IPND Manager is responsible for the ongoing maintenance, security and data management of the IPND (including disaster recovery). To the extent that these responsibilities are additional to those set out in legislation, this Code elaborates on these responsibilities.

3.5 The level of service provided to each Data Provider and each Data User within the same Approved Purpose category must be equitable..

3.6 The IPND Manager will assist in 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.

3.7 The IPND must be a stand-alone database system to facilitate transfer of the IPND and its management to another specified person as contemplated by section 472 of the Act.

3.8 It is a general principle that in circumstances which amount to Force Majeure, all relevant Participants will without prejudice use all reasonable endeavours to address those circumstances.

3.9 The IPND contains one set of current PNCD for each Public Number.

4 RULES RELATING TO CUSTOMERS

4.1 Each CSP must provide Customers with the choice of either a Listed Entry or an Unlisted Entry.

4.2 Where Data Providers offer Customers an option of a Suppressed Address Entry, only the locality, State and Postcode components of the directory address may appear in Directory Related Services.

4.3 A Data Provider must take reasonable steps to inform the Customer of the type of use and the type of disclosure of their PNCD.

NOTE: 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.

4.4 If a Customer contacts any of the following in relation to PNCD:

(a) the IPND Manager;

(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 PNCD can only be effected by that Customer's CSP.

NOTE: This clause does not affect any other obligations Participants may have under law to correct inaccurate data.

4.5 A Data Provider must take reasonable steps to ensure that the Customer understands that if at any time they wish to have their PNCD altered in any way they will be required to contact their CSP to arrange this.

NOTE: 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.

4.6 Data Users must not use PNCD to contact Customers, with the exception of the following:

(a) an Emergency Call Person; or

(b) Directory Assistance Service Providers as allowed under the Act; or

(c) as allowed under the IPND Scheme.

NOTE: Customer contact may arise from indirect use of PNCD within the IPND by Enforcement Agencies or an Emergency Service Organisation.

5 RULES FOR DATA PROVISION TO THE IPND MANAGER

5.1 Each Data Provider must, in accordance with the Act, supply PNCD to the IPND Manager for each Public Number it uses to supply a Carriage Service to a Customer.

5.2 Accordingly, a CSP that provides a Carriage Service to a Customer must also provide the relevant PNCD to the IPND Manager in respect of each Carriage Service it supplies.

> *NOTE: This Code also applies to calling card, internet and pre-paid Carriage Services where there is a Public Number issued that is associated with that Service.*
>
> *In the case of 1800 international numbers or equivalent Carriage Services the Data Provider will provide all associated PNCD including foreign addresses, if permitted by the Customer. The national C party translation, that is, the number or numbers associated with these Carriage 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 PNCD from the IPND.*

5.3 Each Data Provider who provides one or more Public Payphones will provide to the IPND Manager the Public Number and location for each Public Payphone.

5.4 Each Data Provider must register with the IPND Manager before commencing providing the IPND Manager with PNCD.

5.5 Each Data Provider must nominate to the IPND Manager an approved contact person(s) to manage its PNCD and deal with the IPND Manager and other parties on IPND operational issues.

5.6 Data Providers must ensure that the contact information provided pursuant to Clause 5.5 remains current.

5.7 Data Providers must ensure that all PNCD transferred to the IPND Manager is in the format specified in the IPND Technical Requirements.

5.8 In the event that a technical failure of any kind prevents a Data Provider from transferring PNCD to the IPND Manager for more than one Business Day, the Data Provider must take all reasonable steps to provide data to the IPND Manager as soon as practicable.

5.9 In the event that a technical failure of any kind prevents a Data Provider from transferring PNCD to the IPND Manager 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.

5.10 If a Customer chooses to change their CSP, the responsibility for providing the updated PNCD to the IPND Manager rests with the gaining CSP (new Data Provider).

5.11 Each Data Provider must send a disconnect transaction to the IPND Manager for each Public Number upon ceasing to supply Carriage Service to a Customer on that Public Number.

5.12 Each Data Provider must ensure that the information provided to the IPND Manager is accurate, complete and up to date.

NOTE: It is recommended that Data Providers use address validation software to validate the correct entry of address data.

5.13 A Data Provider must take all reasonable steps to avoid adverse impact on the accuracy, completeness and currency of another Data Provider's data.

5.14 Any Data Provider who may have caused adverse impact on the PNCD of another Data Provider must provide reasonable assistance in resolving the problem.

5.15 The Data Provider must identify each Public Number used to supply a Carriage Service with a tag identifying whether the Public Number is to be a Listed Entry, Suppressed Address Entry (where offered) or an Unlisted Entry.

5.16 Data Providers must identify, by the use of an alternate address flag, those services where the service address provided may not be the physical address from where the customer is calling.

NOTE: The alternate address flag is a mandatory field in the IPND that assists Emergency Service organisations in their communications with the caller. The flag should be set to 'True' where calls are made from a telephone service connected to a PABX, when using nomadic services such as VOIP, or when calling from Geographic Numbers used to relay Emergency Services.

5.17 The Data Provider must ensure that all PCND records provided to the IPND Manager includes their Data Provider code and the relevant CSP code.

5.18 In an agency arrangement, the Data Provider must use its Data Provider code to identify itself as the agent that supplies the data to the IPND Manager on behalf of a CSP.

5.19 The Data Provider must supply to the IPND Manager, all PNCD 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 or disconnections.

5.20 For a Standard Telephone Service made available by a CSP on a temporary basis:

(a) when the CSP has made arrangements enabling queries from Emergency Services or Enforcement Agencies to be answered at any time, the PNCD in the IPND may show the CSP as the Customer where the period of availability is 30 calendar days or less.

(b) when the CSP does not have in place arrangements as described in Clause 5.20 (a), the PNCD in the IPND may show the CSP as the Customer where the period of availability is seven calendar days or less.

5.21 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.) must be entered in the IPND with the Customer information not the third party information.

5.22 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.

5.23 The IPND Manager must provide the information referred to in Clause 5.22 within a reasonable timeframe, not exceeding 15 Business Days.

6 CONDITIONS FOR DATA USER ACCESS TO IPND DATA

6.1 The IPND Manager must treat prospective Data Users within the same Approved Purposes category in an equitable manner with regards to the terms and conditions of access to PNCD or PNDD.

6.2 The IPND Manager must take reasonable steps to ensure that a prospective Data User is made aware of this Code.

6.3 If a person wishes to register as an IPND User, the IPND Manager must make available to that person an Information Package within 30 calendar days of receiving 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 an equitable basis.

NOTE: Under the IPND Scheme, prospective Data Users who wish to use PNCD or PNDD for Public Number Directories or research in the public interest as determined by the Minister under section 285(3)of the Act, must apply to ACMA for an authorisation, and to the IPND Manager for access. Other parties who require access should contact only the IPND Manager.

6.4 In order to be registered by the IPND Manager, the prospective Data User must apply to the IPND Manager and:

(a) advise the Approved Purpose for use of PNCD or PNDD;

(b) provide any necessary supporting material relating to the intended Approved Purpose;

(c) provide contact information;

(d) have its registered office within Australia and be subject to Australian law.

6.5 The prospective Data User must also:

(a) declare in writing to the IPND Manager that it commits to be bound by this Code;

(b) in writing to the IPND Manager:

(i) agree to comply with IPND Technical Requirements and other security provisions as notified in writing by the IPND Manager from time to time;

(ii) acknowledge the receipt of this Code; and

(iii) undertake not to use or supply the PNCD or PNDD other than for the specific Approved Purpose for which it has applied; and

(c) if subject to the IPND Scheme, have authorisation from ACMA, and provide a copy of that authorisation (including any relevant conditions) to the IPND Manager.

6.6 The IPND Manager must not unreasonably deny access to a prospective Data User nor give undue emphasis to a potential Data User's inexperience in their application.

NOTE: In view of the obligations of the IPND Manager under Part 13 of the Act and other applicable laws, 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 or PNDD for the purpose or purposes it has given.

6.7 On receipt of the Data User application from a prospective Data User and all information reasonably requested by the IPND Manager needed in considering the Data User's application, the IPND Manager must consider the application and respond to the prospective Data User within 30 Business Days with a decision on whether the applicant will be registered as a Data User by the IPND Manager.

NOTE: The receipt of PNCD or PNDD will be subject to agreement on the terms and conditions between the IPND Manager and the prospective Data User.

6.8 Each Data User must nominate to the IPND Manager an approved contact person(s) to manage communications with the IPND Manager and other parties on IPND operational issues.

6.9 Data Users must ensure that contact information remains current.

7 RULES FOR DATA TRANSFER – USE AND DISCLOSURE OF DATA TRANSFERRED FROM THE IPND MANAGER

7.1 The target end to end processing time from the provision of PNCD by the Data Provider to the IPND Manager until the availability of the Customer's PNCD 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);

(b) to Data Users for Approved Purpose (f) within 24 hours; and

(c) to all other Data Users on the next Business Day.

7.2 In all PNCD and PNDD transfers, the IPND Manager must provide:

(a) the Data Provider code to all Data Users, excluding researchers; and

(b) the CSP code to all Data Users, excluding providers of Directory Related Services and researchers.

7.3 When a Data Provider sends an update to the IPND Manager that causes a Public Number to change status from Listed Entry, or Suppressed Address Entry to Unlisted Entry the IPND Manager must:

(a) accept this update as valid;

(b) notify relevant Data Users that a particular Public Number has become an Unlisted Entry. The notification will only include:

(i) the Public Number;

(ii) date of change to an Unlisted Entry; and

(iii) the Data Provider code.

(c) not provide any other PNCD associated with the Public Number to providers of Directory Related Services.

NOTE: Refer to Clause 7.9 for Data Users' obligations.

7.4 When a Data Provider sends an update to the IPND Manager that causes a Public Number to change status from a Suppressed Address Entry, or Unlisted Entry to Listed Entry the IPND Manager must:

(a) accept this update as valid;

(b) notify relevant Data Users that a particular Public Number has become a Listed Entry. The notification will only include:

(i) the Public Number;

(ii) date of change to a Listed Entry; and

(iii) PNCD or PNDD including the Data Provider code.

NOTE: Refer to Clause 7.9 for Data Users' obligations.

7.5 When a Data Provider sends an update to the IPND Manager that causes a Public Number to go from Listed Entry, or Unlisted Entry to Suppressed Address Entry, the IPND Manager must:

(a) accept this transaction as valid.

(b) notify relevant Data Users that a particular Public Number has become a Suppressed Address Entry. The notification will only include:

(i) the Public Number;

(ii) date of change to a Suppressed Address Entry; and

(iii) PNCD or PNDD including the Data Provider code.

NOTE: Refer to Clause 7.9 for Data Users' obligations.

7.6 The IPND Manager must ensure that the IPND has in-built functionality to deny provision of PNCD identified as an Unlisted Entry to Data Users except for:

(a) as provided for in Clause 7.3;

(b) an Emergency Call Service or an Emergency Service;

(c) assisting Enforcement Agencies; or

(d) Approved Purposes (g), (i) and (j).

7.7 The IPND Manager must not disclose any PNCD contained in an Unlisted Entry to any Data User that provides Directory Related Services except as permitted by the Act or any other applicable laws, or in accordance with the procedure set out in Clause 7.3.

7.8 The IPND Manager must only provide data containing an Unlisted Entry to providers of Directory Related Services for the purpose of informing those providers that a Listed Entry or Suppressed Address Entry has become an Unlisted Entry.

7.9 Upon receiving notification that a Public Number has changed listing type, providers of Directory Related Services must reflect that change by updating all relevant records within one Business Day of receiving that notification.

NOTE: Change of listing type includes any change from: Listed Entry, Suppressed Address Entry (where offered) or Unlisted Entry to any other listing type.

7.10 The IPND must have in-built functionality to indicate that PNCD relates to a Suppressed Address Entry.

7.11 Providers of Directory Related Services must not publish or otherwise disclose address details other than the locality, State and Postcode of PNDD tagged as Suppressed Address Entry.

7.12 Data Users must not:

(a) use or disclose Unlisted Entry data for purposes other than assisting Enforcement Agencies and Emergency Services;

(b) sell or provide PNCD to any other entity for any purpose except as required by law;

> *NOTE: PNDD can be used for Directory Related Services to develop products which can then be sold or provided.*

(c) analyse or collate information such that it could be used to obtain information about new services or moved services; or

(d) obtain information about movement between CSPs or for establishment of marketing databases.

7.13 The IPND Manager will make available daily updates of the IPND as indicated by the IPND Technical Requirements to Data Users within the same Approved Purpose category on an equitable basis.

7.14 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 an equitable basis.

7.15 All PNCD and PNDD will be transferred via electronic means as specified via file transfer protocol, unless under exceptional circumstances where an alternate process is negotiated.

7.16 The IPND Technical Requirements document provided by the IPND Manager to IPND Users must contain a description of the standard file transfer mechanisms and formats.

7.17 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 by the IPND Manager upon request. Data Users should provide a reasonable timeframe of advance notification when making such requests.

7.18 The IPND Manager must provide information referred to in Clause 7.17 within a reasonable timeframe.

> *NOTE: In assessing a reasonable timeframe, relevant considerations include:*
>
> *- the volume of data requested;*
> *- transmission capacity;*
>
> *- impact on IPND operations, and*
>
> *- the principle of equitable treatment.*

7.19 The IPND Manager must make current Data User contact information available to all Data Providers and ACMA upon request.

7.20 The IPND Manager must make current Data Provider contact information available to all Data Users and ACMA upon request.

8 DATA ERRORS AND DATA QUERIES

8.1 Where PNCD contains a Hard Error:

(a) the IPND Manager must not add the PNCD to the IPND; and

(b) the IPND Manager must produce a Hard Reject within 24 hours for retrieval by the Data Provider.

8.2 Where PNCD contains a Soft Error:

(a) the IPND Manager must add the 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.

8.3 The Data Provider must download the information referred to in Clauses 8.1 and 8.2, and investigate the reason for the error.

8.4 On receipt of a Hard Reject, the Data Provider must take reasonable steps to resolve the matter and supply the corrected PNCD to the IPND Manager within one Business Day.

8.5 On receipt of a Soft Reject, the Data Provider must take reasonable steps to resolve the matter and supply the corrected PNCD to the IPND Manager within two Business Days.

Note: 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.

8.6 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.

8.7 When the IPND Manager 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 two Business Days of this change.

8.8 Where the Data Provider has taken all possible steps to resolve a Hard Error and is still unable to provide PNCD to the IPND Manager, the IPND Manager and the Data Provider must take reasonable steps to identify and resolve the issue.

8.9 The IPND Manager must produce information for each Data Provider which summarises the total number of its PNCD 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.

8.10 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 Requirements via the Data User Query File.

8.11 The IPND Manager must make available a Data Provider Query File of the notifications in Clause 8.10 to the relevant Data Provider within one Business Day of receipt.

8.12 The IPND Manager must make available an Amalgamated Query File to all Data Users of all potential errors related to Listed Entries within one Business Day of receipt

8.13 The IPND Manager must make available an Amalgamated Query File of all potential errors including those which relate to Unlisted Entries to Enforcement Agencies and Emergency Services within one Business Day of receipt.

*NOTE**:** The receipt of an updated data record from the Data Provider in response to a Data User Query File will clear the query tag in the IPND.*

9 INFRASTRUCTURE

9.1 Data Providers are responsible at their cost for the provision and maintenance of their own data provision links and medium to the IPND. Data Providers are responsible for ensuring that their own technical compatibility with the IPND is achieved.

9.2 Data Users are responsible at their cost for the provision and maintenance of their own data extraction links and medium to the IPND. Data Users are responsible for ensuring that their own technical compatibility with the IPND is achieved.

9.3 The IPND Manager must facilitate the implementation of the IPND Technical Requirements with all IPND Users.

9.4 IPND Users must comply with the reasonable requirements of the IPND Manager in implementing the IPND Technical Requirements.

9.5 The IPND Manager must provide a method of encryption to each IPND User and undertake to maintain any such method of encryption.

9.6 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 Manager.

9.7 IPND Users may propose changes to the IPND interface to the IPND Manager which will be considered by the IPND Manager and other IPND Users.

9.8 The IPND Manager must consider all reasonable requests of IPND Users for additional technical enhancements to the IPND.

9.9 The IPND Manager must consult relevant IPND Users about proposed changes to the IPND Technical Requirements and seek the agreement of the majority of relevant IPND Users.

9.10 IPND Users must not unreasonably delay in responding or unreasonably withhold consent to proposed changes to the IPND Technical Requirements.

9.11 Where the IPND Manager judges that any change to a File Specification is necessary and urgent, a timeframe for response may be specified.

9.12 The IPND Manager must consider all reasonable comments of the IPND Users in relation to any proposal by the IPND Manager to change the IPND interface.

9.13 The IPND Manager must provide all IPND Users with written notification of changes to the IPND interface and to technical specifications having a material impact on them on an equitable basis for at least six months in advance of such change to the extent that such notification is possible.

9.14 All IPND Users must implement changes referenced in Clause 9.13 within an agreed specified timeframe enabling compliance with the IPND Manager's reasonable requirements.

10 DATA SECURITY

10.1 The IPND Manager must take all reasonable steps to protect the security and confidentiality of PNCD held in the IPND, or stored, against:

(a) loss,

(b) unauthorised access, use, modification or disclosure; and

(c) other misuse.

10.2 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.

10.3 Where the organisation performing the role of the IPND Manager is also a CSP, it must not allow access either direct or indirect by any area of its organisation to data held in the IPND for any reason other than as allowed under the Act or the *Telecommunications (Interception and Access) Act 1979* and, where the IPND Manager is Telstra, also as allowed under the Licence Conditions.

10.4 The IPND Manager must ensure that all PNCD Data changes are backed up daily, and securely and safely stored. Stored data is to be kept for seven years.

10.5 To maintain data security and integrity, on-line access to the IPND is not available with the exception of the activity allowed for in Clause 11.1.

10.6 Data Users must take all reasonable steps to protect the security and confidentiality of data derived directly from the IPND against:

(a) loss,

(b) unauthorised access, use, modification or disclosure; and

(c) other misuse.

10.7 An IPND User who becomes aware of any substantive or systemic breach of security within their organisation, which may reasonably be foreseen to have an impact on the integrity and confidentiality of the PNCD residing in the IPND, must:

(a) advise the IPND Manager who will advise relevant Authorities and IPND Users; and

(b) take reasonable steps to minimise the effects of the breach.

10.8 An IPND User that has reasonable grounds to believe that a Data User has breached the Code or other law in its use or disclosure of PNCD must advise the IPND Manager.

10.9 Where the IPND Manager becomes aware that a Data User is using or disclosing PNCD for a purpose other than that for which they are approved the IPND Manager must immediately notify the relevant

Authorities and all Data Providers whose PNCD may be compromised by the suspected breach.

NOTE: This Clause does not imply that the IPND Manager has a responsibility to identify all breaches.

10.10 The IPND Manager must take all reasonable steps to minimise the effects of the breach, including cooperating with Data Providers and Authorities in any action they need to take in respect of the breach.

10.11 Where the IPND Manager becomes aware of any breach of security of the PNCD stored in and archived from the IPND, which may reasonably be considered to have an impact on the integrity or confidentiality of the PNCD stored in and archived from the IPND, the IPND Manager must advise relevant Authorities and IPND Users. The IPND Manager must take all other reasonable steps to minimise the effects of the breach, including cooperating with IPND Users in any action they need to take in respect of the breach.

11 CONFIDENTIALITY

11.1 To preserve confidentiality, the IPND Manager's access to the PNCD is limited to that necessary for maintenance, administration and to carry out the responsibilities of the IPND Manager under the Code and the Prescribed Conditions.

11.2 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 and ACMA. 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.

12 BILATERAL AGREEMENTS

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 or the ACIF G619:2007 ***IPND Data*** Industry Guideline.

13 CODE ADMINISTRATION AND COMPLIANCE

13.1 ACIF Code Administration and Compliance Scheme

Under ACIF Industry Code Signatory arrangements, signatories to this Industry Code are subject to the ACIF G514:2003 ***Code Administration and Compliance Scheme*** Industry Guideline (*the Scheme*). Accordingly, all signatories who are bound by this Code are also bound by the Scheme.

13.2 Powers to handle industry complaints under this Code

13.2.1 Complaints may be made under this Code to Communications Alliance 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.

13.2.2 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 ACMA under the power granted to the ACMA in section 514 of the *Telecommunications Act 1997*, subject to the agreement of Communications Alliance to accept the referral. Without limiting the grounds on which Communications Alliance may withhold its agreement to accept a referral, Communications Alliance 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 Communications Alliance.

13.2.3 Communications Alliance must handle complaints under Clause 13.2.1 or 13.2.2 in accordance with the provisions of the ACIF G514:2003 Code Administration and Compliance Scheme.

14 REFERENCES

Publication	**Title**
Industry Guidelines	
ACIF G514:2003	Code Administration and Compliance Scheme
ACIF G619:2007	IPND Data

Legislation
Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997
Privacy Act 1988
Telecommunications Act 1997
Telecommunications (Consumer Protection and Service Standards) Act 1999
Telecommunications (Integrated Public Number Database – Permitted Research Purposes) Instrument 2007 (No.1)
Telecommunications Integrated Public Number Database Scheme 2007
Telecommunications (Interception and Access) Act 1979
Telecommunications Numbering Plan 1997
Telecommunications (Section of the Telecommunications Industry) Determination 2007

PARTICIPANTS

The Working Committee that revised this Code consisted of the following organisations and their representatives:

Organisation	Membership	Representative
Acxiom	Voting	Jodie Sangster
Australian Communications and Media Authority	Non-voting	Julia Cornwell
Australian Privacy Foundation	Voting	Nigel Waters
Baycorp Advantage	Voting	Melissa Stratton/ Matthew Walker
Consumers' Telecommunications Network	Voting	Annie McCall
FCS OnLine	Voting	Margo Fitzgibbon
Hutchison Telecoms	Voting	Brian Currie
Hutchison Telecoms	Non-voting	Alexander R. Osborne
Optus	Voting	Melina Rohan/Tracey Mason
Telstra Corporation	Voting	Michael J. Ryan
Telstra Corporation	Non-voting	Brett Born
Telstra Corporation	Non-voting	Sanjay Prem
Vodafone Network	Voting	Van Le

This Working Committee was chaired by Alexander R. Osborne. Margaret Fleming of Communications Alliance provided project management support.

Communications Alliance was formed in 2006 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

In pursuing its goals, Communications Alliance offers a forum for the industry to make coherent and constructive contributions to policy development and debate.

Communications Alliance seeks to facilitate open, effective and ethical competition between service providers while ensuring efficient, safe operation of networks, the provision of innovative services and the enhancement of consumer outcomes.

It is committed to the achievement of the policy objective of the *Telecommunications Act 1997* - the greatest practicable use of industry self-regulation without imposing undue financial and administrative burdens on industry.

Published by:
COMMUNICATIONS
ALLIANCE 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 info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507

Care should be taken to ensure the 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