

**COMMUNICATIONS
ALLIANCE LTD**



INDUSTRY CODE

C555:2024 INTEGRATED PUBLIC NUMBER
DATABASE (IPND)

C555:2024 Integrated Public Number Database (IPND) Industry Code

First published as ACIF C555:2000
Second edition as ACIF C555:2002
Third edition as ACIF C555:2007
Fourth edition as ACIF C555:2008
Fifth edition as C555:2017
Sixth edition as C555:2020

Communications Alliance Ltd was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

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

© Communications Alliance Ltd 2024

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 Communications Alliance. Organisations wishing to reproduce or publish this document for commercial gain (i.e. for distribution to subscribers to an information service) should apply to Communications Alliance by contacting the Communications Alliance Commercial Manager at info@commsalliance.com.au.

EXPLANATORY STATEMENT

This Explanatory Statement is to be read with the **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 C555:2020 **Integrated Public Number Database (IPND)** Industry Code.

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 Number Customer Data (PNCD) which facilitates the provision of information for purposes specified in the *Telecommunications (Carrier Licence Conditions (Telstra Corporation Limited) Declaration 2019* including the provision of Directory Assistance Services and the publication and maintenance of Public Number Directories.

The IPND serves as a repository of PNCD which broadly includes the Number, the Customer name, service 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, personal 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 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 Public Number Directory Data (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 Limited to establish and maintain the IPND. Pursuant to the *Telecommunications Act 1997 (Cth)* (the Act), Carriage Service Providers (CSPs) that supply a Carriage Service to an End User where the End User has a Number must give Telstra Limited such information as Telstra Limited reasonably requires in connection with Telstra Limited's fulfilment of the obligation as the IPND Manager (Part 4, Schedule 2 of the Act).

PNCD may only be accessed from the IPND 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 their use and disclosure except in limited circumstances. Section 285 and section 285A 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 Public Number Directories or made available through Directory Assistance Services.

2007 Revision

This revision sought 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.

January 2008 update

The delayed timeframe for implementation of all aspects of the Code relating to the supply and use of PNCD for Location Dependent Carriage Services (LDCS) was extended by an additional twelve months following a request from the Australian Communications Media Authority (ACMA). The February 2007 version of the Code included a six-month delay following registration to permit time to address legislative inconsistencies. The Department of Communications, Information Technology and the Arts now the Department of Communications and the Arts, released a discussion paper in June 2007

in relation to LDCS, however the matter was not resolved prior to the commencement of the caretaker period ahead of the November 2007 federal Australian election.

2017 Revision

This revision sought to deliver on three specific recommendations that came out of the 2015 IPND Review by the Department of Communications and the Arts. Broadly these were:

1. emphasis on stronger industry practices to support IPND Data Providers use of validation practices to improve data quality;
2. developing guidance for Data Providers to implement processes that allow subscribers to easily view and correct their PNCD records;
3. establishment of awareness raising measures to highlight to subscribers the importance and need for providing correct information to their CSP, in order to ensure the data held in the PNCD records is accurate.

The Code reflects practices that are the only achievable and practical approach to dealing with these matters.

Other matters addressed by this revision include:

- the IPND Manager being able to update the IPND in certain specified circumstances;
- amendments to improve the ability to identify the CSP responsible for the accuracy of the data in the IPND; and
- a requirement for Data Providers to test prior to bulk uploads or system changes (and the IPND Manager to provide feedback) preventing potential systemic errors or failures.

CSP Data Quality

The Code and Industry Guideline G619: 2017 IPND Data has set out practices to improve data quality. The industry approach does not mandate use of data validation software as there is no address data set that is specifically capable of validating the address of all premises to which utility services are provided. While there are data sets and address validation software that can identify an address for postal purposes and that a property exists for purposes of rate payments, these data sets are not suitable for identifying the physical location of premises to which services, such as utilities, are connected. For example, a rural property may be of considerable size and have either a private road or a number of street frontages. A metropolitan property may have multiple dwellings on that property (e.g., a granny flat) and in some cases of private estates there may be no 'official' address that can be validated via current data sets.

A further problem with use of address data validation software is timeliness of update. Often telecommunications services are put into place before the process of officially recognising an address. In these cases, strict use of address validation software would prohibit provision of a service, unless an override facility was in place, in which case an override facility would make the use of address validation software pointless and a regulatory cost burden for no practical benefit.

Access to PNCD

The industry process for Customer access to PNCD outlined in this Code:

- (a) contributes to security over who has access to PNCD (i.e. the Customer's CSP is in the best position to effectively identify and validate that the person seeking access to their PNCD is the actual Customer);
- (b) provides a process that is easy to use, low cost and more effective for Customers;
- (c) allows for easy correction of IPND PNCD that might arise from Customers accessing their PNCD; and
- (d) does not detract from any other right a Customer may have to access IPND PNCD.

This revision did not contemplate other recommendations in the 2015 IPND Review, such as, to broaden the range of users able to apply for access to IPND information as they had not been implemented at the time of this revision and are a matter for the Federal Government.

This revision also aligned definitions and service types with the Numbering Plan.

2019/20 Revision

This revision delivered on three Code deficiencies identified by the Australian Communications and Media Authority. Broadly these were:

1. clarify that all Numbers Issued to a Customer by a CSP are required to be listed in the IPND and give greater clarity of the number types that are required to be in the IPND;
2. set out what a CSP must do to reconcile PNCD against their own Customer data, including a mandatory obligation to review and action Changed Data Provider Reports issued by the IPND Manager; and
3. make reconciliation of PNCD compulsory between a CSP's customer systems and the IPND at least once every six months.

Previous Regulatory Arrangements

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 Australian Communications Authority (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 Act. The Bill was passed and received royal assent on 8th December 2006.

The amendments to the 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 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 the ACMA may grant authorisation enabling access to and use of information in the IPND for purposes specified in paragraph 285 (1A) (d) of the 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, Public Number Directory Publishers (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. The 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 also allows the ACMA to grant access to the IPND for research purposes specified by the Minister as being in the public interest (namely, public health, electoral matters, and research by or for the Commonwealth). Such research must not be conducted for a primarily commercial purpose.

Authorisation applications must be made in the approved form and include a privacy impact statement. An application can be made by an independent research entity or a research representative body. The ACMA can authorise a research body to disclose limited IPND data (listed number and corresponding geographic information not below postcode level) to its members provided certain requirements are met.

The Scheme sets out conditions that authorisation holders must comply with and gives the ACMA discretion to impose additional conditions. Authorisation for research purposes can be granted for a specified period or an ongoing basis.

PNDPs and researchers to whom the Scheme applies also need to apply to the IPND Manager to gain access to IPND data. PNDP's and researchers are only permitted to access Listed Numbers. Although Data Users for other Approved Purposes are only required to seek approval to access data held in the IPND from the IPND Manager, the

IPND Manager will in many cases consult with the ACMA before planning to approve access.

In addition to having obligations under the Scheme, PNDPs and researchers will be required to comply with the relevant Ministerial instruments made under the Act in relation to those approved purposes.

Further clarity is required based on operational experience with the reconciliation process and to align with changes being made to the IPND technical solution.

The Code seeks to support the new requirements of the Act and the IPND Scheme.

How the Code Builds on and Enhances 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 CSPs 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 Data Users; and
- (e) the IPND Manager's interest in being assured that CSPs and 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 Accomplishes

The stated objectives of the Code are to set out the rights and obligations of CSPs, 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) procedures treat all Data Providers on an equitable basis; and
- (c) procedures treat all Data Users in the same Approved Purpose category on an equitable basis; and
- (d) procedures do not detract from Customers' privacy rights with regard to personal information; and

- (e) procedures and processes maximise data accuracy and efficiency through the cooperation of all Participants; and
- (f) the, security, integrity and confidentiality of the PNCD that is transferred to, stored in, used and disclosed from the IPND is adequately protected.

The Code applies to all Carriers (which includes the IPND Manager) and CSPs. It also provides information and guidance for Data Providers and Data Users that are not Carriers and CSPs, to clearly establish procedures dealing with the IPND Manager. The Code relates to PNCD provided to, from and stored in, the IPND.

How the Objectives are Achieved

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

- (a) the procedure for prospective CSPs, 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 CSPs and 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.

Benefits to Consumers

The operation of the IPND indirectly benefits 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 locality 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 and respecting individual Customers' requirements to:
 - (i) have recorded, their choice of whether or 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;
- (f) the implementation of proper and lawful security and protection for the privacy of Customer data stored in the IPND;

- (g) enabling Customers through their CSP to obtain a copy of their PNCD and for the CSP to make changes that comply with the CSP's obligations; and
- (h) the provision of locality information for the emergency warning system.

Benefits to Industry

The Code is important for CSPs and 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.

The cooperatively developed self-regulatory Code is the most appropriate method of addressing these interests and providing the assurances that CSPs, Data Providers and Data Users seek. The Code revision process ensures the participation of those representing the above interests and takes account of their interests in a more detailed way than is possible in subordinate instruments. Code development is consistent with the regulatory framework set out in section 4 of the Act.

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 compliance with the Code.

There are establishment and ongoing costs incurred by CSPs, 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 from time to time. The requirement by this Code to implement and manage Unlisted Entry and Suppressed Address Entry (where a Suppressed Address entry is offered by a CSP) will result in additional costs to CSPs and Data Providers.

There are establishment and ongoing costs incurred by CSPs, Data Providers and Data Users in establishing the means by which they will transfer and access PNCD to and from the IPND, and costs incurred by CSPs to enable Customers to access their PNCD.

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

2024 Revision

This revision includes:

- clarification of a CSPs obligations relating to recording and maintaining the accuracy of the Customers List Code (clause 4.1.1 and 5.2.2);
- clarification of the use of International Numbers;
- arrangements for International Emergency Assistance Call Monitoring Centres that make International Originated Emergency Assistance Calls into Australia and information required to be included in the IPND;
- an obligation for CSPs to advise the IPND Manager if their data provision arrangements or CSP Code changes;
- updates to provisions relating to CSPs keeping the IPND Manager notified of any changes to contact details;
- clarification of the process if a CSP inadvertently overwrites another CSPs records (clause 5.2.8);

- minor updates to the reference of Telstra Limited relating to their Licence Conditions;
- updates to references, Appendix B and some definitions for clarity.

Alexander R. Osborne
Chairman

IPND Working Committee

TABLE OF CONTENTS

1	GENERAL	2
1.1	Introduction	2
1.2	Registration with the ACMA	4
1.3	Scope	4
1.4	Objectives	5
1.5	Code review	6
2	ACRONYMS, DEFINITIONS AND INTERPRETATIONS	7
2.1	Acronyms	7
2.2	Definitions	8
2.3	Interpretations	21
3	PRINCIPLES	22
3.1	Principles of the IPND Code	22
4	RULES RELATING TO THE IPND CODE	23
4.1	Rules relating to Customers	23
4.2	Rules for data provision to the IPND Manager	24
4.3	Rules for Data Transfer – Use and disclosure of data transferred from the IPND Manager	30
5	DATA ACCURACY	34
5.1	Customer Record IPND Upload File and PNCD Data Errors	34
5.2	PNCD Data Quality	37
5.3	Data Reconciliation	39
5.4	Bulk Refresh	40
6	CONDITIONS FOR ACCESS TO IPND DATA	41
6.1	Data User access to IPND Data	41
6.2	Customer access to their IPND Data	42
7	INFRASTRUCTURE	45
7.1	IPND Interface	45
8	DATA SECURITY	47
8.1	IPND Data security	47
9	REFERENCES	50
	APPENDIX A – IPND REPORTS	52
	APPENDIX B - IPND OBLIGATIONS AND TIMELINES	53
	PARTICIPANTS	62

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 representing sections of the telecommunications industry develop industry codes relating to the telecommunications activities of participants in those sections of the industry.
- 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:
- (a) Local Number Portability Industry Code (C540);
 - (b) Number Management - Use of Numbers by Customers Industry Code (C566);
 - (c) Mobile Number Portability Industry Code (C570);
 - (d) Inbound Number Portability Industry Code (C657);
 - (e) IPND Data Industry Guideline (G619.1); and
 - (f) IPND Data Provision, Error Management and Reconciliation Processes Industry Guideline (G619.2)
- 1.1.4 The Code should be read in conjunction with related legislation and legislative instruments, including:
- (a) the Act;
 - (b) the *Telecommunications (Consumer Protection and Service Standards) Act 1999 (Cth)*;
 - (c) the *Privacy Act 1988 (Cth)*;
 - (d) *Telecommunications (Carrier Licence Conditions -Telstra Corporation Limited) Declaration 2019*, section 10 and/or any other Prescribed Conditions;
 - (e) the *Telecommunications Integrated Public Number Database Scheme 2017*;
 - (f) the *Telecommunications Numbering Plan 2015*;
 - (g) the *Telecommunications (Interception and Access) Act 1979*;
 - (h) the *Telecommunications (Emergency Call Service) Determination 2019*; and

(i) *Telecommunications Regulations 2021.*

- 1.1.5 If there is a conflict between the requirements of the Code and any requirements imposed on, or exceptions provided to, a Participant by law, the Participant will not be in breach of the Code by complying with the requirements or exceptions provided by law.
- 1.1.6 Compliance with this Code does not guarantee compliance with any legislation. The Code is not a substitute for legal advice.
- 1.1.7 Statements in boxed text are a guide to interpretation only and not binding as Code rules.
- 1.1.8 The IPND has been developed as a resource for the telecommunications industry, providers of Directory Related Services, Enforcement Agencies and ESOs in Australia, and for any other purpose as allowed under the IPND Scheme.
- 1.1.9 The IPND is a national central repository for the receipt, storage and distribution of PNCD for Data Providers and Data Users.
- 1.1.10 Telstra Limited is obliged under its Licence Conditions to establish and maintain a separate industry wide IPND.

NOTE: In maintaining the IPND, Telstra Limited also issues the Integrated Public Number Database (IPND) Data Users and Data Providers Technical Requirements for IPND (the IPND Technical Requirements) and IPND Internet Interface Service (IIS), which set out information required by the IPND Manager.

- 1.1.11 While the Act and the Licence Conditions allow for the initial establishment and maintenance of the IPND by Telstra Limited, it is contemplated that the ongoing maintenance and operation of the IPND may be transferred to another specified person or association.
- 1.1.12 Clauses 10 and 11 of Part 4 of Schedule 2 of the Act set out the obligations to provide and maintain an IPND and the CSP's responsibilities, as follows:

Clause 10 Carriage Service Providers must give information to Telstra Limited

(1) *This clause applies if Telstra Limited is obliged by a condition of a carrier licence to provide and maintain an integrated public number database.*

(2) *If;*

(a) a carriage service provider supplies a carriage service to an end-user; and

(b) the end user has a public number;

the carriage service provider must give Telstra Limited such information as Telstra Limited reasonably requires in connection with Telstra Limited's fulfilment of that obligation.

Clause 11 Carriage Service providers must give information to another person or association

(1) *This clause applies if a person or association is obliged by section 472 to provide and maintain an integrated public number database.*

(2) *If;*

(a) *a carriage service provider supplies a carriage service to an end-user; and*

(b) *the end user has a public number;*

the carriage service provider must give the person or association such information as the person or association reasonably requires in connection with the person's or association's fulfilment of that obligation.

1.1.13 Where the term Number is used in the Code it replaces the term public number as defined in the Act.

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

1.1.15 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 the ACMA

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

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; and

(b) Carriage Service Providers.

1.3.2 The Code also provides information and guidance for Data Providers and Data Users that are not Carriers and CSPs, to clearly establish procedures dealing with the IPND Manager.

NOTES:

1. *The Code is 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.*

2. *The Code has been developed and registered on the basis that it applies to Carriers and CSPs, but it also provides information and guidance for other Participants that*

interact with the IPND Manager. A Participant that is not a Carrier or CSP may be subject to other IPND related laws or instruments. For example, the Telecommunications Integrated Public Number Database Scheme 2017 sets out rules applicable to certain Data Users that are not CSPs.

- 1.3.3 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.
- 1.3.4 The Code also applies in particular to the following activities of CSPs:
- (a) supply of PNCD to the IPND Manager by a CSP 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.
- 1.3.5 The Code does not cover charging principles related to access to PNCD.

1.4 Objectives

- 1.4.1 The objectives of the Code are to ensure that:
- (a) CSPs capture and provide details of the Customer's choice of a Listed Entry, Unlisted Entry or Suppressed Address Entry (where a Suppressed Address Entry is offered);
 - (b) CSP's take reasonable steps to provide their Customers with sufficient information about the use of PNCD data;
 - (c) the rights and obligations of Participants regarding the transfer, 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 and CSPs;
 - (f) Customers have a process by which they can access their PNCD;

- (g) PNCD that is transferred to, stored in, used and disclosed from, the IPND is secure and adequately protected; and
- (h) agreed procedures:
 - a. treat CSPs on an equitable basis;
 - b. treat Data Providers on an equitable basis;
 - c. treat Data Users within the same Approved Purpose category on an equitable basis; and
 - d. do not detract from Customers' rights with regard to security and privacy of personal information; and
- (i) processes maximise data accuracy and efficiency through the cooperation of all Participants.

1.5 Code review

This Code will commence on the day of registration with the ACMA. The Code will be reviewed every 5 years, or earlier in the event of significant developments that affect the Code or a chapter within the Code.

1.6 Powers of the Telecommunications Industry Ombudsman to handle complaints under the Code

Under section 114 of the Act and subject to the consent of the TIO, the Code confers on the TIO the functions and powers of:

- (a) receiving;
- (b) investigating;
- (c) facilitating the resolution of;
- (d) making determinations in relation to;
- (e) giving directions in relation to; and
- (f) reporting on

complaints made by the end users of a Listed Carriage Service about matters arising under or in relation to the Code, including compliance with the Code by Carriers and CSPs.

2 ACRONYMS, DEFINITIONS AND INTERPRETATIONS

2.1 Acronyms

For the purposes of the Code:

ACMA

means the Australian Communications and Media Authority.

CLI

means Calling Line Identity

CSP

means Carriage Service Provider.

DUQF

means Data User Query File.

ECP

means Emergency Call Person

ESO

means Emergency Services Organisation.

IPND

means Integrated Public Number Database.

PMTS

means Public Mobile Telecommunications Service.

PNCD

means Public Number Customer Data.

PNDD

means Public Number Directory Data.

TCPSS

means *Telecommunications (Consumer Protection and Service Standards) Act 1999*.

VoIP

means Voice over Internet Protocol.

2.2 Definitions

For the purposes of the Code:

Act

means the *Telecommunications Act 1997 (Cth)*.

Alternate Address Flag

has the same meaning as given by the definition in section 6 of the *Telecommunications (Emergency Call Service) Determination 2019*.

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.

A-Party

means the individual or entity initiating the communication.

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 ESOs under Part 8 of the TCPSS Act;
- (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 CSP via the Data Provider and held in the IPND against the information the CSP holds;
- (h) undertaking research of a kind specified in the *Telecommunications (Integrated Public Number Database – Permitted Research Purposes) Instrument 2017 and Telecommunications Regulations 2001*;
- (i) assisting the ACMA, or its nominee, to verify the accuracy and completeness of information held in the IPND; and
- (j) any other purposes permitted by the Act, or any other relevant laws.

Authorities

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

Business Day

means any day from Monday to Friday (inclusive) excluding gazetted public holidays. A Business Day goes from 12:00 am to 11:59 pm on that day, unless otherwise specified. 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.

Business Hours

means the hours commencing at 8.00 am and ending at 5.00 pm on any Business Day. All times specified in this Code are based on Australian Eastern Standard Time (AEST).

Carriage Service

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

Carriage Service Provider

has the same meaning as given by section 87 of the Act.

NOTE: CSPs include internet service providers and VoIP service providers that supply a Carriage Service using an Issued Number.

If an entity is supplying a Carriage Service directly to a Customer, using a Number, the entity is considered to be a CSP under this Code and the obligations relating to a CSP in this Industry Code will apply.

If an entity is a CSP and is providing a Carriage Service using a Number, the CSP has an obligation to supply information to the IPND consistent with cl10 (2) of Part 4 of Schedule 2 to the Act.

For example:

1) an entity provides a Carriage Service associated with a voice service, or a data service such as an alarm or IOT monitoring service, where they Issue the Number associated with it to another person nor for further resale then the person that provides that Carriage Service is a CSP and has an obligation to provide information to the IPND Manager informing that they are supplying a Listed Carriage Service to that Number.

Carrier

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

CLI

means the CLI injected into the A-Party communication.

CSP Code

means the unique CSP Code generated and allocated by the IPND Manager on receipt of an application from a CSP that provides Carriage Services to Customers using a Number.

Customer

means a person to whom a CSP Issues a Number in conjunction with supply of a Listed Carriage Service and which is not for resale.

NOTES: Depending on whether the Customer of the CSP is another CSP or end user of the Listed Carriage Service will determine who is required to provide information to the IPND. For example:

1. Where an entity uses the Listed Carriage Service which has a Number Issued and associated to it itself it is the Customer. The CSP providing the Listed Carriage Service and the associated Number has the obligation to provide information to the IPND Manager.

2. If the Customer uses the Listed Carriage Service associated to a Number Issued to them to resell the Listed Carriage Service to provide a service (e.g. a voice or data service) to another person and they have Issued the Number associated to that Listed Carriage Service to another person, they have become a CSP and have the obligation to provide information to the IPND Manager.

3. Where a Customer has Issued a Number that was Issued to them to another person, they become a CSP, and they have the obligation to provide information to the IPND Manager.

4. If the Customer does not Issue the Number associated to the Listed Carriage Service to another person (e.g. their customer is unaware of the Number associated to the Listed Carriage Service), or it is made clear in contractual arrangements that their customer only has limited use of that Number for the purposes of the supplied service they are not a CSP.

If an entity is a CSP (refer definition above) and is providing a Listed Carriage Service using a Number they have the obligation to supply information to the IPND consistent with Schedule 2, Part 4, s10 (2) of the Act.

For the benefit of doubt, the details provided to the IPND Manager always requires the details of the end Customer that has been Issued the Number, and this should be noted as not always being the end user of the Listed Carriage Service

Data Provider

means a person who is registered with the IPND Manager and has received authorisation from the IPND Manager to send PNCD to the IPND on behalf of the CSP.

NOTE: A person is not classified as a Data Provider until this authorisation process is completed.

A Data Provider may be:

- the CSP or*
- may act on behalf of a CSP.*

Where a Data Provider acts on behalf of one or more CSPs, it must be registered to send PNCD to the IPND Manager for each CSP.

Data Provider Code

means a unique Data Provider Code, generated and allocated by the IPND Manager, on receipt of an application from a Data Provider.

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 CSP via the Data Provider which highlights potential inconsistencies in PNCD, identified by Data Users via Data User Query Files.

Data User

means an entity that has been granted authorisation from the ACMA and / or IPND Manager to receive PNCD from the IPND 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 Address

means the address provided for Listed Entries in Public Number Directories.

NOTE: Refer to G619 IPND Data Industry Guideline.

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

has the same meaning as given by the *Telecommunications (Emergency Call Service) Determination 2019*.

Emergency Call Person

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

Emergency Call Service

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

Emergency Management Person

has the same meaning as given by section 275B of the Act.

Emergency Service Organisation

has the same meaning as given by subsection 147 (11) in the TCPSS Act.

Enforcement Agency

means a government agency that 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.

Finding Name

means the name used for Directory Related Services.

NOTE: Refer to G619.1 *IPND Data Industry Guideline*.

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.

Gaining CSP

means the CSP to which a Number has been or is to be Ported.

Geographic Number

has the same meaning as given by the Numbering Plan.

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.

Held

has the same meaning as Hold defined in the *Number Management – Use of Numbers by Customers* industry code (C566).

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;
- (c) current IPND Technical Requirements;
- (d) the C555 **Integrated Public Number Database** Industry Code;
- (e) the G619.1 **IPND Data** Industry Guideline;
- (f) the G619.2 **IPND Data Provision, Error Management and Reconciliation Processes** Industry Guideline; and
- (g) 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.

International Emergency Assistance Call Monitoring Centre

means a call centre outside of Australia that provides an International Originated Emergency Assistance Call service – to initiate a request for emergency assistance on behalf of a person in Australia via an International Originated Emergency Assistance Call Transit CSP.

NOTE: For example, an international call centre operating on behalf of a multinational company (e.g. a vehicle manufacturer) that initiates a request for emergency assistance following a vehicle emergency or a mobile phone user out of terrestrial coverage sending an SOS message via satellite.

International Originated Emergency Assistance Call Transit CSP

means a CSP that provides an Australian communications entry point for an International Emergency Assistance Call Monitoring Centre to receive an International Originated Emergency Assistance Call and transfers that call to the Relevant Termination Point as an Emergency Call after performing appropriate number translations.

International Originated Emergency Assistance Call

means an emergency request for assistance originating from outside of Australia.

IPND Manager

means the person or association or delegate(s) that manages, maintains, and administers the IPND.

IPND Scheme

means the *Telecommunications Integrated Public Number Database Scheme 2017*.

IPND Technical Requirements

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

Issued

has the meaning as given by the *Number Management – Use of Numbers by Customers* industry code (C566).

Licence Conditions

means the additional conditions that apply to Telstra Limited (ACN 086 174 781) as set out in the *Telecommunications (Carrier Licence Conditions - Telstra Corporation Limited) Declaration 2019*.

Listed Carriage Service

has the same meaning given by section 16 of the Act.

Listed Entry

means an entry in the IPND relating to a Listed Number, containing PNDD that will be available in Directory Related Services and includes a Standard Telephone Service with:

- (a) a Geographic Number or Mobile Number that the Customer has agreed to be included in Directory Related Services; or
- (b) any other Number that the Customer has specifically requested to being included in Directory Related Services.

Listed Number

means a Number other than an Unlisted Number.

List Code

means the identifier for use of data in a Directory Related Service.

NOTE: Options are a Listed Entry, an Unlisted Entry or a Suppressed Address Entry (where a Suppressed Address Entry is offered).

Local Service

has the same meaning given by 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 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) a 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 a Suppressed Address Entry is offered) in a Public Number Directory.

Losing CSP

means the CSP from which a Number has been or is to be Ported.

Mobile Number

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

Number

means a number specified in the Numbering Plan that has been Issued to a CSP or a Customer to be used in conjunction with the supply of a Listed Carriage Service.

NOTE: For avoidance of doubt, a Number that can be Issued to a Customer only includes:

- *calling card numbers (i.e., 18 9)*
- *freephone numbers (i.e., 18x);*
- *Geographic Numbers (i.e., 02x, 03x, 07x, 08x);*
- *International Numbers (Numbers Issued by a CSP operating within Australia for use within Australia);*
- *local rate numbers (i.e., 13 and 1300);*
- *Mobile Numbers (i.e., 04x);*
- *premium rate numbers (i.e., 19x); and*
- *satellite numbers (i.e., 014)*

Numbering Plan

means the *Telecommunications Numbering Plan 2015*.

Operator Assistance Service

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

Operator Services

means services:

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

as per the Act and any specific Licence Conditions.

Participants

means Data Users, CSPs, Data Providers and the IPND Manager.

Port

means the movement of a Number, declared as Portable under the Numbering Plan, between CSPs on different carrier networks using a Porting solution as defined by the relevant Industry Code. The words Porting, Ported and Portability have corresponding meaning.

NOTE: The Numbering Plan sets out which Numbers are Portable. Portable Numbers and the relevant Industry Code include:

- *Inbound Numbers (i.e. 13xx and 18xx) refer to C657 Inbound Number Portability;*
- *local (geographic) Numbers refer to C540 Local Number Portability;*
- *mobile Numbers refer to C570 Mobile Number Portability*

Prescribed Conditions

means in the case of Telstra Limited, 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 same meaning given by section 32 of the Act.

Public Number Customer Data

means data required under the Licence Conditions and as otherwise reasonably required by the IPND Manager as follows:

- (a) (Public) Number;
- (b) Service Status Code;
- (c) Customer name and associated details;
- (d) Finding Name for a Listed Entry or Suppressed Address Entry (where a Suppressed Address Entry is offered); and
- (e) 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 a Suppressed Address Entry is offered), the Directory Address; and
- (f) List Code;
- (g) Usage Code;
- (h) Type of Service (optional);
- (i) Customer contact;
- (j) CSP Code;
- (k) Data Provider Code;
- (l) Transaction Date;
- (m) Service Status Date;
- (n) Alternate Address Flag; and
- (o) prior (Public) Number (optional).

*NOTE: For additional information on the above data sets see G619.1 **IPND Data** Industry Guideline.*

Public Number Directory

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

Public Number Directory Data

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

- (a) the Number of the Customer;
- (b) the name of the Customer;
- (c) the directory finding name for a Listed Entry or Suppressed Address Entry (where a Suppressed Address Entry is offered);
- (d) the directory address of the Customer for a Listed Entry or Suppressed Address Entry (where a Suppressed Address Entry is offered);
- (e) Usage Code and
- (f) List Code;
- (g) or as otherwise authorised pursuant to the IPND Scheme.

Public Number Directory Publishers

has the same meaning given by the *Telecommunications Integrated Public Number Database Scheme 2017*.

Public Payphone

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

Reconciliation

means the comparison and correction by a CSP of the PNCD held by the IPND Manager associated to that particular CSP, with the CSPs own data for a Number that is: -

1. associated with an active service in its customer records data base that does not have a corresponding customer 'connected' PNCD record in the IPND for that Number;
2. associated with an active service in its customer records data base for which the corresponding PNCD record in the IPND for that Number has a 'disconnected' status;
3. associated with a disconnected service in its customer records data base for which the corresponding PNCD record in the IPND has a 'connected' status in the IPND; and
4. associated with a service that does not present in its customer records data base for which there is a PNCD record for that Number in a 'connected' status in the IPND.

Relevant Termination Point

has the same meaning given by the *Telecommunications (Emergency Call Service) Determination 2019*.

Service Address

means the address of the Customer which is:

- (a) for a Local Service, the physical address at which the service is installed, unless not technically feasible; or
- (b) for a PMTS, the physical address, where practicable, as provided by the Customer.

NOTE: For avoidance of doubt, a Service Address can only be a physical address where an emergency service vehicle can find a building or other facility, such as a dwelling, office building, marina, manufacturing or storage facility etc. and the Customer has an association to that premises. Postal addresses such as Roadside Mail Box, Post Boxes etc. are not considered to be a physical address.

Service Status Code

means the identifier used to advise the IPND Manger that the Carriage Service is active (connected) or disconnected.

Service Status Date

means the date the service was activated or disconnected on the CSP's system.

Soft Error

means a potential error in a CSP 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 CSP via the Data Provider.

Standard Telephone Service

has the same meaning given by section 6 of the TCPSS.

Sub Address

means the additional physical address data that identifies a Service Address or Directory Address at a more specific level, such as the unit number, floor level, building identification, or other addressing within a building / complex, marina etc.

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 Number will be made public in Directory Related Services.

Transaction Date

means the date and time at which the transaction occurred on the CSP's system.

Triple Zero

means the ECS for calls to 000 and 112.

Type of Service

means the optional value used to identify the type of Carriage Service being provided.

*NOTE: common examples include MOBIL, FIXED, etc.
Refer to G619.1 IPND Data Industry Guideline.*

An exception to this optional value is the use of the value TPSP – refer to clause 4.2.36.

Unlisted Entry

means an entry in the IPND containing PNDD relating to an Unlisted Number.

Unlisted Number

means a Number of one of the following kinds:

- (a) a Mobile Number, unless the Customer and the CSP that provides the PMTS to the Customer agree that the Number will be a Listed Number;
- (b) the number of a Public Payphone;
- (c) a Number that the Customer and the CSP that provides services for originating or terminating Carriage Services to the Customer agree will not be included in a PND;
- (d) any other Number that may be treated as an Unlisted Number because of a change to a law.

Usage Code

means the indicator of whether the service is to be used for government, business, charitable or residential purposes, if practicable.

NOTE: Refer to G61.1 IPND Data Industry Guideline for Usage Codes.

Voice over Internet Protocol

means technology used to transmit voice conversations over a data network using the Internet Protocol.

2.3 Interpretations

In the Code, unless the contrary appears:

- (a) headings are for convenience only and do not affect interpretation;
- (b) a reference to a statute, legislative instruments, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them;
- (c) words in the singular includes the plural and vice versa;
- (d) words importing persons include a body whether corporate, politic or otherwise;
- (e) where a word or phrase is defined, its other grammatical forms have a corresponding meaning;
- (f) mentioning anything after include, includes or including does not limit what else might be included;
- (g) words and expressions which are not defined have the meanings given to them in the Act; and
- (h) a reference to a person includes a reference to the person's executors, administrators, successors, officers, employees, subcontractors, agents, assignees and novatees.

3 PRINCIPLES

3.1 Principles of the IPND Code

- 3.1.1 Nothing in this Code is intended to change the intellectual property rights (if any) of Participants.
- 3.1.2 The requirements of this Code will apply equitably to all Participants, unless otherwise provided.
- 3.1.3 The IPND Manager will perform minimal processing and filtering of PNCD, requiring a cooperative approach amongst Participants to data accuracy.
- 3.1.4 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.
- 3.1.5 The level of service provided to each Data Provider and each Data User within the same Approved Purpose category must be equitable.
- 3.1.6 The IPND Manager will assist in quality control, for example through the provision of Data Provider Error Files, Data User Query Files, Data Provider Query Files and address (locality, state and postcode) validation in accordance with the IPND Technical Requirements.
- 3.1.7 The IPND must be a stand-alone database system to facilitate the transfer of the IPND and its management to another specified person as contemplated by section 472 of the Act.
- 3.1.8 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.
- 3.1.9 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 of principles in this Code or the *G619.1 IPND Data* Industry Guideline.
- 3.1.10 The IPND should contain one set of current PNCD for each Number Issued to a Customer.

4 RULES RELATING TO THE IPND CODE

4.1 Rules relating to Customers

- 4.1.1 A CSP must provide the Customer with a choice of either a Listed Entry, Unlisted Entry or a Suppressed Address Entry (where a Suppressed Address Entry is offered), for any primary voice service, and make arrangements to record the Customers preference in the IPND.

NOTES: A secondary voice service (e.g. smart watch) is dependent on a primary voice service being connected and is not the Carriage Service of the associated Number that is required for a directory listing and therefore the List Code may be set as Unlisted Entry.

A CSP providing a data only Carriage Service (e.g., IoT, M2M, machine sensors) may set the List Code as Unlisted Entry.

A CSP providing a PMTS may set the List Code as Unlisted Entry.

Where a CSP providing a voice Carriage Service offers their Customers an option of a Suppressed Address Entry, only the Customer's name, locality, state, postcode and Number will be made public in Directory Related Services.

- 4.1.2 CSPs must take reasonable steps to inform their Customers about the provision of their PNCD to the IPND and its uses, including the type of Data Users who may have access to PNCD from the IPND.

NOTE: This IPND specific information may be provided to Customers as part of the privacy related materials which need to be drawn to Customer's attention when initially collecting personal information, and otherwise made readily available, in order to comply with Australian Privacy Principle 5.

Types of Data Users that may be referred to could include (but not limited to) Directory Related Service Providers, Emergency Call Service Operators and Enforcement Agencies.

- 4.1.3 CSPs must take reasonable steps to inform their Customers of the importance of their PNCD being kept up to date and accurate and must encourage them to contact their CSP if their information changes. For example, if a Customer changes their service address, they should advise their CSP.

- 4.1.4 If a Customer contacts any of the following in relation to their 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 or the Data User as the case may be, must advise the Customer that changes to their PNCD can only be made by that Customer's CSP.

NOTE: This clause does not affect any other obligations Participants may have under law, such as under the Australian Privacy Principle 13, to correct inaccurate data.

- 4.1.5 A CSP must take reasonable steps to ensure that their Customers understand that if at any time they wish to have their PNCD altered in the IPND 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 of information in standard forms of agreement, provision of written material to Customers, provision of verbal advice to Customers or information via public media.

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

- (a) an Emergency Call Person;
- (b) Directory Assistance Service Providers and Public Number Directory Publishers as allowed under the Act; or
- (c) as allowed under the Act, or another legislative instrument.

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

4.2 Rules for data provision to the IPND Manager

- 4.2.1 Each CSP that provides a Carriage Service to a Customer using a Number must provide the IPND Manager the relevant PNCD, including transaction updates, in respect of each Carriage Service it supplies, that occur on one Business Day, by the end of the next Business Day. This includes all transactions relating to connections or disconnections.

NOTES: Reasonable time to register with the IPND Manager prior to commencement of supply of services to Number and testing timeframes should also be considered.

CSPs should design and maintain their systems and processes to keep the PNCD provided to the IPND Manager up to date.

CSPs should note that in order to meet their obligation to provide PNCD by the next business day if they have a Data Provider uploading for them, they need to allow sufficient time for their Data Provider to upload their data.

Details of IPND obligations and their corresponding timelines can be found in Appendix B.

- 4.2.2 Each CSP that has an obligation under clause 4.2.1 must register with the IPND Manager in order to be authorised to supply PNCD to the IPND. Such registration must occur in a timely manner to consider subsequent activity (e.g. IPND connectivity, testing, etc) to meet the obligations under clause 4.2.1.
- 4.2.3 To register with the IPND Manager, a CSP must submit a written application of intent, and must provide its name, address and contact details, including a valid email contact that is monitored daily to receive and action important communications from the IPND Manager and other IPND Stakeholders, to the IPND Manager.
- 4.2.4 The IPND Manager must acknowledge receipt of the application of intent within 2 Business Days.
- 4.2.5 CSPs must ensure that the information provided pursuant to clause 4.2.3 remains current.
- 4.2.6 CSPs must ensure that in the case of organisational change or consolidation with another CSP the IPND Manager must be advised within a reasonable timeframe of the updated details.
- 4.2.7 The IPND Manager must make an Information Package available on the IPND Manager website.
- 4.2.8 Following on from clause 4.2.3, a CSP must then either:
- (a) register with the IPND Manager as its own Data Provider before providing the IPND Manager with PNCD; or
 - (b) contract with a Data Provider, to act on its behalf to provide PNCD to the IPND Manager.
- 4.2.9 The IPND Manager must only register a person as a Data Provider after receiving a completed application of intent from the person, and where the person has:
- (a) provided any necessary supporting material requested by the IPND Manager relating to their role as a Data Provider, including details of any CSP for whom they are acting as Data Provider;
 - (b) provided contact information, including a valid email contact that is monitored daily to receive and action important communications from the IPND Manager and other IPND Stakeholders;
 - (c) details of their registered office; and
 - (d) any other information as required by the IPND Manager to register the person as a Data Provider, including technical information and testing, etc.

NOTE: This application of intent applies only for the purposes of commencing formal approval, registration and acceptance testing for intending Data Providers of the IPND.

- 4.2.10 Following on from clause 4.2.9 the IPND Manager must consider the application of intent and respond to the prospective Data Provider within 10 Business Days with a decision on whether the applicant will be registered as a Data Provider by the IPND Manager.
- 4.2.11 The IPND Manager may request further time to assist and supply any further information required in the establishment of arrangements with the prospective Data Provider to enable the Data Provider to submit a file to the IPND Manager for evaluation and testing.
- 4.2.12 A Data Provider must nominate to the IPND Manager an approved contact person(s) to manage the CSP's PNCD and engage with the IPND Manager and other parties on IPND operational issues.
- 4.2.13 Data Providers must ensure that the information provided pursuant to clause 4.2.9 remains current.
- 4.2.14 Where a new Data Provider is intending to transfer PNCD to the IPND Manager, the Data Provider must first successfully complete system testing in the IPND testing environment.

NOTE: The IPND Manager will be notified on completion of the successful testing in the IPND testing environment and will then authorise the Data Provider to connect to the IPND production environment.

- 4.2.15 A Data Provider must use its Data Provider Code to identify itself as the agent that supplies PNCD to the IPND Manager on behalf of a CSP or group of CSPs.
- 4.2.16 Data Providers must ensure that all PNCD records provided to the IPND Manager include the unique Data Provider Code, CSP Code and file source combination as assigned by the IPND Manager that identifies the CSP responsible for ensuring accurate, complete and up to date PNCD and the Data Provider responsible for uploading the PNCD to the IPND Manager.
- 4.2.17 Where a CSP uses a new Data Provider they must provide the IPND Manager within a reasonable timeframe, with the details of the new Data Provider.

NOTE: Example; A CSP may change the Data Provider it uses to upload PNCD on its behalf or it may use an additional Data Provider.

As the IPND Manager validates the combination of CSP Code and Data Provider Code if a CSP does not advise the IPND Manager of a change to Data Provider arrangements, the records will error.

- 4.2.18 Where a CSP advises the IPND Manager of a new Data Provider Code the IPND Manager must make that CSP Code and Data Provider Code a valid combination and respond to the CSP

confirming the CSP Code and Data Provider Code as a valid combination and the date upon which that combination may be used to upload PNCD within 2 Business Days of notice from the CSP.

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

NOTES: On receipt of PNCD the IPND Manager will undertake analysis of the PNCD in accordance with the IPND Technical Requirements and provide a report containing details of any errors found. Details of IPND reports can be found in Appendix A.

The IPND Manager undertakes limited checks of address data quality and only validates a valid combination of locality/state/postcode fields. CSPs should ensure that they have their own arrangements to validate address data quality.

- 4.2.20 Each CSP must ensure that the PNCD provided to the IPND Manager is accurate and complete at the time of data provision (subject to any obligations in accordance with section 5).

*NOTE: In order to meet this obligation in relation to accurate address data and ensure the highest level of quality of address data that is vital to many IPND Data Users, and in conjunction with clause 4.2.1, it is highly recommended that the CSP follows the guidance provided in G619.1 **IPND Data Industry Guideline** and uses address validation tools such as specific address validation software to validate the correct entry and supply of address data to the IPND Manager.*

- 4.2.21 A Data Provider or any other party in the chain of suppliers leading from the CSP to the Data Provider, acting on behalf of a CSP must ensure that the PNCD that is supplied to the IPND Manager is an accurate reflection of the PNCD supplied by the CSP.

- 4.2.22 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 and in the correct sequence and format after the technical failure has been rectified.

- 4.2.23 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 (with a focus on ensuring the protection and privacy of IPND data) to accommodate the Data Provider's alternate methods of transferring PNCD until the technical problem is rectified.

- 4.2.24 If a Customer chooses to change their CSP, the responsibility for providing the updated PNCD to the IPND Manager rests with the Gaining CSP.

NOTE: This includes asking and recording the Customers preference for an Unlisted, Listed or Suppressed Address Entry (where a Suppressed Address Entry is offered).

- 4.2.25 If a CSP is merged or taken over by another CSP, the responsibility for providing updated PNCD to the IPND Manager rests with the new CSP.
- 4.2.26 A Gaining CSP must not send a 'Connect' PNCD transaction to the IPND Manager until the Port has been completed as set out in the applicable Portability industry code for the Number.
- 4.2.27 A Losing CSP must not send a 'Disconnect' PNCD transaction to the IPND Manager until the Port has been completed as set out in the applicable Portability industry code for the Number.

NOTES: Clauses 4.2.26 and 4.2.27 seek to avoid a situation whereby the IPND could otherwise contain incorrect data if the Port is withdrawn or expires.

Relevant industry codes include:

C540 Local Number Portability;

C570 Mobile Number Portability; and

C657 Inbound Number Portability.

- 4.2.28 CSPs must identify each Number used to supply a Carriage Service with a List Code in the PNCD identifying whether the Number is to be a Listed Entry, Suppressed Address Entry (where a Suppressed Address Entry is offered) or an Unlisted Entry.
- 4.2.29 CSPs must identify, by the use of an Alternate Address Flag in the PNCD, 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 ESOs 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.

For PMTS, the Alternate Address Flag is set to 'False'.

- 4.2.30 A Number Issued to a Customer who makes the Number available to third parties (for example hotels, hospitals, car rentals etc) on a short-term basis (less than 30 calendar days) must be provided to the IPND with the Customer details in the PNCD, not the third-party user information.

NOTES: For a Standard Telephone Service made available to a person by a CSP on a short-term basis (less than 30 calendar days) either when the CSP has made arrangements enabling queries from ESOs or Enforcement Agencies to be answered at any time, or when the CSP does not have these arrangements in place, the PNCD in the IPND may show the CSP as the Customer.

A CSP may be identified as the Customer for services that are provided to end users on a short-term basis, including on a per call basis such as those from VoIP outbound only services.

- 4.2.31 Where a Data Provider is making a relevant system change, it must undertake an assessment of whether the change will impact the delivery of PNCD being sent to the IPND Manager.
- 4.2.32 If the Data Provider believes, because of the assessment in clause 4.2.31, that there is potential for an impact of this kind, then the Data Provider must successfully complete system testing in the IPND testing environment before their system change can be put into effect, i.e., prior to including any such change in PNCD sent to the IPND production environment.
- 4.2.33 The Data Provider must request access to the IPND testing environment from the IPND Manager in order to conduct the tests referred to in clause 4.2.32.

NOTE: The IPND Manager will be notified on completion of the successful testing in the IPND testing environment and will then authorise the Data Provider to connect to the IPND production environment.

INTERNATIONAL EMERGENCY ASSISTANCE CALL MONITORING CENTRES

An International Emergency Assistance Call Monitoring Centre that initiates requests for emergency assistance on behalf of a third party in Australia is expected to have a commercial arrangement with an International Originated Emergency Assistance Call Transit CSP to provide the Number translations and routing for the International Originated Emergency Assistance Call and ensure that the ECP and ESOs have the necessary information to provide assistance.

- 4.2.34 An International Originated Emergency Assistance Call Transit CSP responsible for delivery of International Originated Emergency Assistance Calls on behalf of an International Emergency Assistance Call Monitoring Centre must populate the IPND with the relevant PNCD as follows:
- (a) The Customer's name must be the name of the International Originated Emergency Assistance Call Transit CSP and the International Emergency Assistance Call Monitoring Centre (e.g., [Name of the International Originated Emergency Assistance Call Transit CSP] – Supporting [name of International Emergency Assistance Call Monitoring Centre]).

- (b) The Number must be the Number Held by the International Originated Emergency Assistance Call Transit CSP and Issued to the International Emergency Assistance Call Monitoring Centre for use as the A-Party CLI presented for International Originated Emergency Assistance Calls.
- (c) The Customer contact number must be the Australian contact number of the International Emergency Assistance Call Monitoring Centre that the ECP or ESOs can call back if the call drops out or is terminated prematurely.
- (d) The address must be the address of the International Originated Emergency Assistance Call Transit CSP in Australia.
- (e) The Alternate Address Flag must be set as 'True' – to indicate the caller is not at the Service Address supplied in the PNCD.
- (f) Type of Service must be set to TPSP1 to indicate International Originated Emergency Assistance Calls.

4.3 Rules for Data Transfer – Use and disclosure of data transferred from the IPND Manager

DATA PROVISIONING

- 4.3.1 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 the Approved Purpose (e) no later than 9:00am (AEST) the following day, provided that the PNCD is received by 9:00pm (AEST);
 - (b) to Data Users for Approved Purpose (f), within 24 hours; and
 - (c) to all other Data Users, on the next Business Day.
- 4.3.2 In PNCD and PNDD transfers, the IPND Manager must provide the following additional associated data:
 - (a) Data Provider and CSP codes to Enforcement Agency, Emergency Call Service and Emergency Management Person Data Users; and
 - (b) CSP codes to Location Dependent Carriage Service Data Users.
- 4.3.3 When a Data Provider sends an update to the IPND Manager that causes the List Code of a PNCD Number to change from Listed Entry to Unlisted Entry, or Suppressed Address Entry (where a Suppressed Address Entry is offered) to Unlisted Entry, the IPND Manager must:
 - (a) accept this update as valid;

- (b) notify relevant Data Users that the List Code of a PNCD Number has changed to an Unlisted Entry by a notification that will only include:
 - (i) the PNCD Number;
 - (ii) date of change to an Unlisted Entry;
 - (iii) the List Code; and
- (c) not provide any other PNCD associated with the Number to providers of Directory Related Services.

NOTE: Refer to clause 4.3.12 for Data Users' obligations.

4.3.4 When a Data Provider sends an update to the IPND Manager that causes the List Code of a PNCD Number to change from a Suppressed Address Entry (where a Suppressed Address Entry is offered) to Listed Entry, or Unlisted Entry to Listed Entry the IPND Manager must:

- (a) accept this update as valid; and
- (b) provide relevant PNCD or PNDD to Data Users.

NOTE: Refer to clause 4.3.12 for Data Users' obligations.

4.3.5 When a Data Provider sends an update to the IPND Manager that causes the List Code of a PNCD Number to change from Listed Entry to Suppressed Address Entry (where a Suppressed Address Entry is offered), or Unlisted Entry to Suppressed Address Entry (where a Suppressed Address Entry is offered), the IPND Manager must:

- (a) accept this update as valid; and
- (b) provide relevant PNCD or PNDD to Data Users.

NOTE: Refer to clause 4.3.12 for Data Users' obligations.

USE AND DISCLOSURE

4.3.6 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 4.3.3;
- (b) provision to an Emergency Call Service or an ESO;
- (c) assisting Enforcement Agencies; or
- (d) Approved Purposes (g), (i) and (j).

4.3.7 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 4.3.3.

- 4.3.8 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 (where a Suppressed Address Entry is offered) has become an Unlisted Entry.
- 4.3.9 Upon receiving notification that the List Code of a PNCD Number has changed, providers of Directory Related Services (except printed publications) must reflect the List Code changes for PNCD Numbers by updating all relevant records within two Business Days of Public Number Directory Data (PNDD) being made available by the IPND Manager.

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

- 4.3.10 The IPND must have in-built functionality to indicate that PNCD relates to a Suppressed Address Entry (where a Suppressed Address Entry is offered).
- 4.3.11 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 (where a Suppressed Address Entry is offered).
- 4.3.12 Data Users must not:
- (a) use or disclose Unlisted Entry data for purposes other than assisting Enforcement Agencies and ESOs and for approved purposes under the *Telecommunications Regulation 2021*;
 - (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.
- 4.3.13 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.
- 4.3.14 Where a Data User requests data to be provided using bespoke business rules to meet their Approved Purpose, for example random sampling for specific volume of Customer Numbers, the

IPND Manager must respond on an equitable basis within a reasonable timeframe with advice to the Data User regarding cost and estimated time involved.

- 4.3.15 All Customer Numbers, PNCD and PNDD provided by the IPND Manager must be encrypted and transferred via secure electronic means as specified in the IPND Technical Requirements and the Access to Internet Interface Service documents provided by the IPND Manager to Data Users and Data Providers, unless under exceptional circumstances where an alternate secure process and costs are negotiated and accepted by the Data User and chargeable by the IPND Manager.
- 4.3.16 The IPND Technical Requirements and the Access to Internet Interface Service documents provided by the IPND Manager to Data Users and Data Providers must contain a description of the standard file transfer mechanisms and formats.
- 4.3.17 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.
- 4.3.18 The IPND Manager must provide information referred to in clause 4.3.17 within a reasonable timeframe.

NOTE: In assessing a reasonable timeframe, relevant considerations include:

- *the volume of data requested;*
- *format and media;*
- *transmission capacity;*
- *methods of secure delivery;*
- *impact on IPND operations; and*
- *the principle of equitable treatment.*

- 4.3.19 The IPND Manager must maintain a register of current IPND Data Provider, CSP and Data User unique Codes and contact information (entity name, address and contact details).
- 4.3.20 The IPND Manager must make available upon request and on a regular basis (at least monthly) a current register per clause 4.3.19 to relevant CSPs, Data Users, Data Providers, Enforcement Agencies, Communications Alliance and the ACMA.

5 DATA ACCURACY

5.1 Customer Record IPND Upload File and PNCD Data Errors

- 5.1.1 Where the Customer Record IPND Upload File has failed:
- (a) the IPND Manager must not add any PNCD contained in the Customer Record IPND Upload File to the IPND; and
 - (b) the IPND Manager must produce a File Reject notification within 24 hours for retrieval by the Data Provider.

NOTE: See section 6 of the IPND Technical Requirements for details of the Customer Record IPND Upload File.

- 5.1.2 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 notification within 24 hours for retrieval by the Data Provider.

- 5.1.3 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 notification within 24 hours for retrieval by the Data Provider.

- 5.1.4 Where PNCD is identified by a Data User as potentially incorrect, contains an error or queries the content of the PNCD, the Data User will create a Data User Query File (DUQF) and make it available to the IPND Manager, as set out in the manner specified in the IPND Technical Requirements.

- 5.1.5 The IPND Manager must produce a Data Provider Query File notification under clause 5.1.4 within 24 hours for retrieval by the Data Provider.

- 5.1.6 The IPND Manager must make available feedback with all error notifications to Data Providers in response to each Customer Record IPND Upload File which contained errors.

NOTE: Refer to G619.2 IPND Data Provision, Error Management and Reconciliation Processes Industry Guideline.

- 5.1.7 Data Providers must download all error notifications on the same Business Day that they are made available by the IPND Manager, or no later than 8:00am (AEST) the following Business Day if the notification is made available by the IPND Manager after 9:00pm (AEST).

- 5.1.8 If the Data Provider and CSP are different entities, the Data Provider must communicate all error notifications downloaded in clause 5.1.7 to relevant CSPs on the same Business Day, or no

later than 8:00am (AEST) the following Business Day where the error notification is made available by the IPND Manager after 9:00pm (AEST).

- 5.1.9 Data Providers must take reasonable steps to resolve Customer Record IPND Upload File fail notifications referred to in clause 5.1.3 and supply the corrected Customer Record IPND Upload File to the IPND Manager within one Business Day or notify the IPND Manager of a Technical Failure as referred to in clause 4.2.22.
- 5.1.10 CSPs must take reasonable steps to remediate and provide corrected PNCD to the IPND Manager within 1 Business Day following PNCD Hard Error (clause 5.1.2) or User Query (clause 5.1.4 and 5.1.5) notifications being made available by the IPND Manager.

NOTE: The receipt of an updated data record from the Data Provider in response to a DUQF will clear the query tag in the IPND. Details of IPND reports can be found in Appendix A.

- 5.1.11 CSPs must take reasonable steps to remediate and provide corrected PNCD to the IPND Manager within 2 Business Days following PNCD Soft Error (clause 5.1.3) or User Query (clause 5.1.4 and 5.1.5) notifications being made available by the IPND Manager.

NOTE: Soft Errors are written to an error file with an appropriate error code. On investigation by the Data Provider or CSP of the Soft Errors, Soft Errors may not require correction.

Relevant considerations in the correction of errors include, but are not limited to, whether it is necessary to contact the Customer for e.g. additional name or address details, technical difficulties, agency arrangements, time zones and file transfer times.

- 5.1.12 The IPND Manager must provide Data Users with an Amalgamated Query File (AQF) on a monthly basis.

NOTE: The AQF will list all Active User Query files awaiting PNCD update in the IPND by their respective Data Provider. AQFs will not be produced if there are no Active User Query Files. This report can be used to directly verify that a query is for a particular service.

Details of IPND reports can be found in Appendix A.

- 5.1.13 Where the IPND Manager receives record(s) from one CSP that over write the existing record(s) of another CSP within the IPND (or within the IPND test environment), and the IPND Manager has become aware that this has occurred in error and/or is not a normal IPND operation, the IPND Manager must notify the CSP's Data Provider submitting the change and the original Data Provider of the event within one Business Day of becoming aware of the error.

NOTE: Data Providers and Data Users are encouraged to make use of the IPND test environment to assist in the identification and resolution of potential issues that may prevent the transfer of PNCD to the IPND, and prior to uploading data to or receiving data from the IPND. Details of IPND reports can be found in Appendix A.

- 5.1.14 If the Data Provider and CSP are the same entity, the Data Provider must check their monthly changed data provider report to ensure their PNCD records have not been incorrectly overwritten.

NOTES: All CSPs have the potential to overwrite an existing PNCD record of another CSP.

The changed data provider report is issued on the 1st of each month, or daily if a change of DP code has occurred in the prior 24 hours. DPs are encouraged to make use of the daily changed data provider report to ensure their PNCD records maintain accuracy. Refer to G619.2 for information on the use of the daily changed data provider report.

Due to the current limitations the CSP Code is not included in the changed data provider report.

A change of CSP Code report will identify a change to a CSP Code.

Details of IPND reports can be found in Appendix A.

- 5.1.15 Where a CSP has identified its PNCD record(s) has / have been incorrectly overwritten or has been advised that its PNCD has incorrectly overwritten another CSP, the CSP must take action to correct its incorrect PNCD held by the IPND Manager within 7 Business Days.

NOTES: If a CSP's PNCD records have been incorrectly overwritten by another CSP's PNCD, the CSP whose PNCD is incorrect will send a refresh with the latest record to the IPND via their Data Provider.

It is understood that a Data Provider and a CSP can be the same entity.

- 5.1.16 If a CSP incorrectly overwrites another CSP's PNCD record(s), they must contact the CSP (whose PNCD has been overwritten and provide the Number (s) associated to the overwritten PNCD, in order to resolve the matter.
- 5.1.17 If the Number of the overwritten PNCD record is to be shared between CSPs, in order to resolve the matter identified in clause 5.1.16, this must be made available through a secure method.
- 5.1.18 For any secure method used in clause 5.1.17 that includes use of a password, the password must be sent separately.

- 5.1.19 Where a CSP and / or DP has taken steps to resolve a repeated instance of a Hard Error and its resolution remains unsuccessful, the CSP and /or DP must engage the IPND Manager for assistance to resolve the Hard Error.
- 5.1.20 If the IPND Manager is engaged as per clause 5.1.19, the IPND Manager must take all reasonable steps to assist the CSP and / or DP to resolve repeated instances of a Hard Error failure.
- 5.1.21 The IPND Manager may perform limited maintenance of a complete PNCD or PNDD record in the IPND where:
- (a) PNCD Numbers that may no longer be in use by any CSP and requires the Service Status Code to be changed to Disconnected; or
 - (b) PNCD Numbers do not comply with the Numbering Plan.
- 5.1.22 Where the IPND Manager undertakes maintenance of a complete PNCD or PNDD record beyond what is normally required for maintenance and integrity of the IPND, administration, fault identification, auditing and reporting, the IPND Manager must:
- (a) take all reasonable steps to obtain permission from the relevant CSP before amending any records;
 - (b) specify the reason for such maintenance activity;
 - (c) provide a description of the maintenance activity;
 - (d) maintain a record (for a period of three years) of all maintenance activities undertaken, who authorised or requested the maintenance activities and the reason (s) for the maintenance activities; and
 - (e) notify the ACMA within five Business Days in the event a CSP is no longer available to provide permission for limited maintenance to a PNCD or PNDD record.

5.2 PNCD Data Quality

- 5.2.1 A CSP, upon confirming that a Customer's PNCD is incorrect, must take reasonable steps to ensure that incorrect PNCD information is corrected and sent to the IPND Manager within two Business Days, subject to operational limitations, such as requesting and receiving Customer information to correct the data.

NOTE: This does not include PNCD found to be incorrect through the Data Reconciliation process.

- 5.2.2 In accordance with clauses 4.2.20 and clause 4.2.21 a CSP must have a process to ensure the ongoing accuracy of the List Code in the PNCD held by the IPND Manager.

NOTES: In order to identify where the List Code in the PNCD held by the IPND Manager may be inaccurate a CSP may use the data reconciliation process under clause 5.3.4 to achieve the outcome outlined above.

List Code information is included in the extract of PNCD made available to a CSP by the IPND Manager under clause 5.3.4 to assist in maintaining List Code accuracy.

Customer data for a service which is disconnected in the CSP's customer records database but incorrectly flagged as connected in PNCD held by the IPND Manager has the potential to be published if it has a Listed Entry List Code. If the Listed Entry List Code is incorrect, and should be Unlisted Entry, there may be impacts on the Customer.

- 5.2.3 Where a CSP identifies any discrepancies in List Code of PNCD held by the IPND Manager identified under clause 5.2.2 the CSP must take reasonable steps to amend any discrepancies and provide updated PNCD to the IPND Manager within 1 Business Day of the discrepancy being identified.
- 5.2.4 Where a CSP has identified a discrepancy in the PNCD held by the IPND Manager under clause 5.2.2 they must keep the following records:
- (a) total number of Numbers with a List Code discrepancy;
 - (b) total number of Numbers with a Listed Entry List Code in the CSP's customer records database but an Unlisted Entry List Code in PNCD held by the IPND Manager;
 - (c) total number of Numbers with an Unlisted Entry List Code in the CSP's customer records database but a Listed Entry List Code in PNCD held by the IPND Manager;
 - (d) date/s the discrepancies were identified; and
 - (e) date/s the updated PNCD was sent to the IPND Manager in accordance with clause 5.2.3.
- 5.2.5 A CSP that has identified discrepancies in the PNCD held by the IPND Manager under clause 5.2.2 must keep the records required in clause 5.2.4 for at least 12 months from the date the discrepancy is identified.
- 5.2.6 A Data Provider must take all reasonable steps to avoid adverse impact on the operation of the IPND and on becoming aware of a problem must immediately notify the IPND Manager of the impact and provide reasonable assistance in resolving the problem.
- 5.2.7 A Data Provider must take all reasonable steps to avoid adverse impact on the accuracy, completeness and currency of the PNCD it provides on behalf of a CSP.

- 5.2.8 A Data Provider must take all reasonable steps to avoid adverse impact on the accuracy, completeness and currency of another Data Provider's PNCD.
- 5.2.9 Any Data Provider or CSP who becomes aware or is made aware of having caused adverse impact on the PNCD of another Data Provider or CSP must immediately notify the IPND Manager and provide all reasonable assistance in resolving the problem.

5.3 Data Reconciliation

- 5.3.1 For Reconciliation purposes, Data Providers who are the same entity as the CSP must 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 at least once every six months.
- 5.3.2 Where a Data Provider performs the role of providing PNCD to the IPND on behalf of a CSP, the Data Provider must:
 - (a) obtain an extract of the relevant CSP, PNCD as a full set of records or as a subset of records based on criteria agreed between the CSP, Data Provider and the IPND Manager at least once every six months;
 - (b) provide the relevant CSP with their PNCD extract, as soon as practicable, after the extract has been made available to the Data Provider by the IPND Manager.
- 5.3.3 The IPND Manager must extract PNCD referred to in clauses 5.3.1 and 5.3.2 at a date and time agreed to with the Data Provider and provide the PNCD to the Data Provider within a reasonable timeframe, not exceeding 5 Business Days from the agreed date of the PNCD extract.
- 5.3.4 CSPs must undertake a Reconciliation of the extract of the PNCD referred to in clause 5.3.1 and 5.3.2 and take reasonable steps to amend any discrepancies between the PNCD held by the IPND Manager and the CSP's own data by sending updated PNCD to the IPND Manager within 30 Business Days of the PNCD extract being made available by the IPND Manager.

NOTE: Refer to G619.2 IPND Data Provision, Error Management and Reconciliation Processes Industry Guideline for further details on the reconciliation process.

The reconciliation process under clause 5.3.4 should identify mismatches of Connection status.

- 5.3.5 CSPs must keep records for each PNCD extract Reconciliation referred to in clause 5.3.4 and retain that data for at least the past year. The records must contain the:
 - (a) total number of Numbers associated with a CSP's active service that do not have a corresponding customer record in the IPND;

- (b) total number of Numbers associated with a CSP's active services for which the corresponding customer record in the IPND has a 'disconnected' status;
- (c) total number of PNCD associated with a CSP with a 'connected' status in the IPND for which the Number is designated as 'disconnected' in a CSP's Customer Systems; and
- (d) total number of PNCD associated with a CSP with a 'connected' status in the IPND for which the Number is not present in a CSP's Customer Systems.

5.4 Bulk Refresh

- 5.4.1 Where a Data Provider intends to undertake a large data or bulk refresh of PNCD they supplied to the IPND, they must notify the IPND Manager at least two Business Days before this activity is undertaken.
- 5.4.2 If a Data Provider intends to send more than 20 files per day for each filesource, they must inform the IPND Manager in advance to arrange a suitable timeframe.

NOTE: Each individual file has a size constraint of 100,000 records per file.

6 CONDITIONS FOR ACCESS TO IPND DATA

6.1 Data User access to IPND Data

6.1.1 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 Customer Numbers, PNCD or PNDD.

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

NOTE: This Information is made available on the IPND Manager and ACMA websites.

6.1.3 If a person wishes to register as an IPND Data User, the IPND Manager must make available to that person an Information Package within 2 Business Days of receiving a written request for such information and/or an expression of interest in becoming an IPND Data User. The IPND Manager must provide an Information Package to persons wishing to register as an IPND Data User on an equitable basis.

NOTE: Under the IPND Scheme and the Telecommunications Regulations 2021, 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 sub-section 285(3) of the Act, must apply to the ACMA for an authorisation, and to the IPND Manager for access. Other parties who require access should contact only the IPND Manager who may consult the ACMA.

6.1.4 The IPND Manager may only register a person as a Data User after receiving an application from the person, and where the person has:

- (a) advised the Approved Purpose for use of PNCD or PNDD;
- (b) provided any necessary supporting material relating to the intended Approved Purpose;
- (c) provided contact information;
- (d) authorisation from the ACMA where required at law, and provided a copy of that authorisation (including any relevant conditions) to the IPND Manager; and
- (e) their registered office within Australia.

6.1.5 Data Users must:

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

- (b) not transfer, copy, use or supply the Customer Numbers, PNCD or PNDD other than for the specific Approved Purpose for which it has applied.

- 6.1.6 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 consider the previous actions of a potential Data User and any advice from the ACMA about the potential Data User's compliance or non-compliance with the Approved Purposes, and the Data User's ability to use Customer Numbers, PNCD or PNDD for the purpose or purposes it has given.

- 6.1.7 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 prospective 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 Customer Numbers, PNCD or PNDD will be subject to agreement on the terms and conditions as between the IPND Manager and the prospective Data User.

- 6.1.8 Each Data User must nominate to the IPND Manager an approved contact person(s) (including outside of Business Hours) to manage communications with the IPND Manager and other parties on IPND operational issues.

- 6.1.9 Data Users must ensure that contact information remains current.

6.2 Customer access to their IPND Data

Under the *Privacy Act 1988 (Cth)*, Customers who are individuals are entitled to obtain access to their PNCD and, if that data is incorrect, to seek correction.

For practical purposes, this Code sets out an industry agreed process for Customers to obtain their PNCD and / or seek correction of that data through the CSP of which they are a Customer.

NOTES 1: The process set out in this Code for Customers to seek access to their PNCD is the industry preferred process but does not detract from the Customers' rights (where the Customers are individuals) to seek access to their personal information under the Privacy Act 1988 (Cth) and other privacy laws, including from the IPND Manager.

The industry preferred approach recognises the practical issues associated with the IPND Manager being unable to confirm the identity of a person seeking access to PNCD as the person with

a right to seek access to that data. The industry has agreed that the process set out in the Code is the preferred approach as it reduces the potential risk of PNCD being provided to an unauthorised individual and resulting in a breach of privacy laws.

2. Where a person has services with more than one CSP they should approach each CSP of which they are a Customer to access the relevant PNCD.

- 6.2.1 Where the Customer seeks access to their PNCD, the Customer should contact their CSP directly, through the communication method advised by their CSP.

NOTE: Responsibility for the accuracy of the Customer's PNCD lies with both the Customer and the Customer's CSP.

- 6.2.2 Upon request by the Customer for their PNCD, the CSP must: -

- (a) verify their Customer's request and identity;
- (b) record their Customer's PNCD request;
- (c) agree with their Customer the method(s) for providing their PNCD to them;
- (d) arrange to obtain a copy of their Customer's PNCD; and
- (e) provide their Customer's current PNCD to their Customer once it has been received from the IPND Manager.

NOTE: For existing Customer Authentication processes refer to Telecommunications Service Provider (Customer Identity Authentication) Determination 2022.

- 6.2.3 The CSP must respond to their Customer's request for a copy of their PNCD by supplying the requested PNCD within 20 Business Days, subject to clause 6.2.2 (a) and 6.2.2 (c).

NOTE: Under Australian Privacy Principle 12.8, the process of arranging access to PNCD relating to services supplied by that CSP to their Customer may be undertaken on a cost recovery basis between the CSP and their Customer. Any charges involved must not be excessive.

- 6.2.4 The IPND Manager must ensure that requests from CSPs for PNCD are processed in a timely manner and that relevant PNCD is supplied to the CSP within 10 Business Days of receiving the PNCD request.

NOTE: Under Australian Privacy Principle 12.8, the process of arranging access to PNCD relating to services supplied by that CSP to their Customer may be undertaken on a cost recovery basis between the CSP and the IPND Manager. Any charges involved must not be excessive.

6.2.5 A CSP may submit single or multiple PNCD record requests for the same Customer.

6.2.6 Where a Customer identifies that their PNCD is inaccurate, the customer's CSP must correct the inaccurate PNCD subject to the CSP's assessment as to whether the Customer's requested changes comply with the CSP's regulatory obligations, including the IPND Code and IPND Data Guideline for the supply of PNCD to the IPND Manager.

NOTE: For example, a request to change the name, or the spelling of the name should be cross checked against a form of identification, such as a driver's licence. A request to change the service address or locality should be checked to ensure that such an address exists, and that the Customer has an association to that service address. If the service address is not recognised by an address validation source, and the Customer appears to be attempting to use a vanity address, the PNCD service address should not be changed.

6.2.7 A CSP must not charge a Customer for correcting PNCD that is inaccurate.

7 INFRASTRUCTURE

7.1 IPND Interface

- 7.1.1 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.
- 7.1.2 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.
- 7.1.3 The IPND Manager must facilitate the implementation of the IPND Technical Requirements with all Data Users and Data Providers.
- 7.1.4 Data Users and Data Providers must comply with the reasonable requirements of the IPND Manager in implementing the IPND Technical Requirements and the IPND Internet Interface Service (IIS).
- 7.1.5 The IPND Manager must provide a method of data encryption/data decryption to each Data User and Data Provider and undertake to maintain any such method of data encryption/data decryption.
- 7.1.6 Data Users and Data Providers may propose changes to the IPND interface to the IPND Manager, which will be considered by the IPND Manager and other Data Users and Data Providers.
- 7.1.7 The IPND Manager must consider all reasonable requests of Data Users and Data Providers for additional technical enhancements to the IPND.
- 7.1.8 The IPND Manager must consult relevant Data Users and Data Providers about proposed changes to the IPND Technical Requirements or to the IPND interface and obtain the agreement of the majority of relevant Data Users and Data Providers.
- 7.1.9 Data Users and Data Providers must not unreasonably delay in responding, or unreasonably withhold consent to proposed changes to the IPND Technical Requirements or to the IPND interface.
- 7.1.10 The IPND Manager must consider all reasonable comments of the Data Users and Data Providers in relation to any proposal by the IPND Manager to make changes to the IPND Technical Requirements or to the IPND interface.
- 7.1.11 Where the IPND Manager proposes to make changes to the IPND interface, or to the IPND Technical Requirements, and those changes would have a material impact on Data Users or Data Providers, the IPND Manager must notify, in writing, all affected Data Users and Data Providers of the changes:

(a) on an equitable basis; and

(b) at least six months in advance of the change;

to the extent that such notification is possible.

7.1.12 All Data Users and Data Providers must implement changes referenced in clause 7.1.11 within an agreed specified timeframe.

8 DATA SECURITY

8.1 IPND Data security

8.1.1 Where practical all parties subject to this Code are responsible for ensuring the security of IPND data in transit between themselves and the IPND Manager.

8.1.2 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.

NOTE: The IPND Manager at times may be served with a lawful request / direction from the ACMA or other authorised agencies to cease the provision of PNCD to a Data User for whatever reason.

8.1.3 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.

8.1.4 Where the organisation performing the role of the IPND Manager is also a CSP, it must not allow access either directly or indirectly 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 (Cth)* and, where the IPND Manager is Telstra Limited, also as allowed under the Licence Conditions.

NOTE: 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 8.1.13.

8.1.5 The IPND Manager must ensure that all PNCD changes are backed up daily, and securely and safely stored.

NOTE: PNCD is stored for three years on the IPND file system after which it becomes archived.

8.1.6 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.

8.1.7 A Data User or Data Provider 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 Data Users and Data Providers; and
- (b) take reasonable steps to minimise the effects of the breach.

NOTE – All parties subject to the Code should be aware of their compliance obligations with the Notifiable Data Breaches (NDB) Scheme under Part III C of the Privacy Act.
<https://www.oaic.gov.au/>

8.1.8 A Data User that has reasonable grounds to believe that another Data User has breached the Code or other law in its use or disclosure of PNCD must advise the IPND Manager or the ACMA.

8.1.9 Where the IPND Manager becomes aware that a Data User is using or disclosing PNCD for a purpose other than that authorised by the ACMA or allowed by law, the IPND Manager must immediately notify the ACMA, the Office of the Australian Information Commissioner and all Data Providers whose CSP 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.

8.1.10 The IPND Manager must take all reasonable steps to minimise the effects of a breach of clause 8.1.7 and 8.1.8, including cooperating with CSPs, their Data Providers and Authorities in any action in respect of the breach.

8.1.11 Where the IPND Manager becomes aware of any breach of security of the PNCD stored in and archived from the IPND or any Force Majeure, power loss or link failure, 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, CSPs, Data Users and Data Providers.

8.1.12 The IPND Manager must take all reasonable steps to minimise the effects of a breach or threat to the operation or integrity of the IPND, including:

- (a) cooperating with Data Users in any action in respect of the breach; and
- (b) disconnecting Data Users and / or Data Providers to protect the integrity of the IPND;

until such effects have been rectified or mitigated by Data Users and / or Data Providers and reconnection has been agreed with the IPND Manager.

- 8.1.13 To preserve confidentiality, the IPND Manager must not access the PNCD except:
- (a) to the extent necessary for maintenance, administration and to carry out the responsibilities of the IPND Manager under the Code and the Prescribed Conditions; or
 - (b) to comply with any requirements of, or as permitted by, the Act or any other relevant laws.

9 REFERENCES

Publication	Title
Industry Codes	
C540	Local Number Portability
C566	Number Management – Use of Numbers by Customers
C570	Mobile Number Portability
C657	Inbound Number Portability
Industry Guidelines and other documents	
G619.1	IPND Data
G619.2	IPND Data Provision, Error Management and Reconciliation Processes
IPND Data Users and Data Providers Technical Requirements for IPND	
Legislation	
<i>Privacy Act 1988</i>	
<i>Telecommunications Act 1997</i>	
<i>Telecommunications (Carrier Licence Conditions -Telstra Corporation Limited) Declaration 2019</i>	
<i>Telecommunications (Consumer Protection and Service Standards) Act 1999</i>	
<i>Telecommunications (Emergency Call Service) Determination 2019</i>	
<i>Telecommunications (Integrated Public Number Database – Permitted Research Purposes) Instrument 2017</i>	
<i>Telecommunications (Integrated Public Number Database- Public Number Directory Requirements) Instrument 2017</i>	
<i>Telecommunications (Integrated Public Number Database – Public Number Additional Information) Instrument 2017</i>	
<i>Telecommunications (Integrated Public Number Database Scheme – Conditions for Authorisations) Determination 2017</i>	
<i>Telecommunications Integrated Public Number Database Scheme 2017</i>	
<i>Telecommunications (Integrated Public Number Database Scheme – Conditions for Deciding Authorisation Applications) Instrument 2017</i>	
<i>Telecommunications (Interception and Access) Act 1979</i>	
<i>Telecommunications Numbering Plan 2015</i>	

Telecommunications Regulations 2021

Telecommunications Service Provider (Customer Identity Authentication) Determination 2022

APPENDIX A – IPND REPORTS

IPND Report Name	Description	Frequency	Who sees the Report
.err file	Reports success or failure of corresponding upload file	One file/ upload file	Data Provider
Changed Carriage Service Provider report	Informs Data Providers of all PNCD gained and lost during the reporting period.	Daily /Monthly	
Changed Data Provider report	Informs Data Providers of all PNCD Numbers gained and lost in the last month	Daily/Monthly	Data Provider and the CSP if the same entity
Data Provider Snapshot	Snapshot of PNCD uploaded to the IPND	On Request	Data Provider
Data Provider Query File	File produced by DUQF processes containing issues raised by Data Users against the number uploaded to the IPND	Daily (if active UQF issues)	CSP and Data Provider
Data User Query File (DUQF)	Contains numbers, codes and description of issues being raised by Data Users	As Required	CSP and Data User
Data User Reports	Reports such as Book Close for publishers of Public Number Directories and Bulk Data Refreshes for all Data User types	On Request	CSP and Data User
Amalgamated Query file	File containing all active issues submitted by all Data Users	Monthly	Data User
DUQF.err file	Feedback file – reports on success or failure of a DUQF file loaded by the Data User	Correlates directly with an uploaded DUQF file	Data User

APPENDIX B - IPND OBLIGATIONS AND TIMELINES

Activity	Day 1 (within 24 hours)	Day 2 (within 48 hours)	Day nnn
Register as an IPND Data Provider			<p>4.2.1 Each CSP that provides a Carriage Service to a Customer using a Number must provide the relevant PNCD to the IPND Manager in respect of each Carriage Service it supplies that occur on one Business Day, by the end of the next Business Day.</p> <p>4.2.2 Each CSP that has an obligation under clause 4.2.1 must register with the IPND Manager in order to be authorised to supply PNCD to the IPND. Such registration must occur in a timely manner to consider subsequent activity (e.g. IPND connectivity, testing, etc) to meet the obligations under clause 4.2.1.</p>
Register as an IPND Data User			<p>6.1.3 If a person wishes to register as an IPND Data User, the IPND Manager must make available to that person an Information Package within 2 Business Days of receiving a written request for such information and/or an expression of interest in becoming an IPND Data User. The IPND Manager must provide an Information Package to persons wishing to register as an IPND Data User on an equitable basis.</p> <p>6.1.7 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 prospective 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.</p>

Data User IPND technical failure	<p>4.2.22 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 and in the correct sequence and format after the technical failure has been rectified.</p> <p>4.2.23 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 (with a focus on ensuring the protection and privacy of IPND data) to accommodate the Data Provider's alternate methods of transferring PNCD until the technical problem is rectified.</p>		
---	---	--	--

<p>Data Provider sends data to IPND Manager</p>	<p>4.2.1 Each CSP that provides a Carriage Service to a Customer using a Number must provide the IPND Manager the relevant PNCD, including transaction updates, in respect of each Carriage Service it supplies, that occur on one Business Day, by the end of the next Business Day. This includes all transactions relating to connections or disconnections.</p>	<p>5.2.1 A CSP, upon confirming that a Customer's PNCD is incorrect, must take reasonable steps to ensure that incorrect data is corrected and sent to the IPND Manager within two Business Days, subject to operational limitations, such as requesting and receiving Customer information to correct the data.</p>	
<p>IPND Manager uploads received PNCD for Data Users</p>	<p>4.3.1 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 the Approved Purpose (c) , no later than 9:00am (AEST) the following day, provided that the PNCD is received by 9:00pm (AEST); (b) to Data Users for Approved Purpose (f), within 24 hours;</p>	<p>4.3.1 (c) to all other Data Users, on the next Business Day.</p>	

IPND Manager uploads and makes available error files for Data Provider			5.1.6 The IPND Manager must make available feedback with error notifications to Data Providers in response to each file uploaded which contained errors.
Data Provider pulls error files and processes errors	<p>5.1.7 Data Providers must download all error notifications on the same Business Day that they are made available by the IPND Manager, or no later than 8:00am (AEST) the following Business Day if the notification is made available by the IPND Manager after 9:00pm (AEST).</p> <p>5.1.8 If the Data Provider and CSP are different entities, the Data Provider must communicate all error notifications downloaded in clause 5.1.7 to relevant CSPs on the same Business Day, or no later than 8:00am (AEST) the following Business Day where the error notification is made available by the IPND Manager after 9:00pm (AEST).</p>		Note: 5.1.2 refers to hard errors, 5.1.4 refers to DPQF and 5.1.5 refers to feedback with error notifications in response to each file with errors.

Hard errors	<p>5.1.2 Where PNCD contains a Hard Error:</p> <p>(a) the IPND Manager must not add the PNCD to the IPND; and</p> <p>(b) the IPND Manager must produce a Hard Reject within 24 hours for retrieval by the Data Provider.</p> <p>5.1.10 CSPs must take reasonable steps to remediate and provide corrected PNCD to the IPND Manager within 1 Business Day following PNCD Hard Error (clause 5.1.2) and User Query (clause 5.1.4 and 5.1.5) notifications being made available by the IPND Manager.</p>		
Soft errors	<p>5.1.3 Where PNCD contains a Soft Error:</p> <p>(a) the IPND Manager must add the PNCD to the IPND and must tag it to indicate the presence of a Soft Error; and</p> <p>(b) the IPND Manager must produce a Soft Error within 24 hours for retrieval by the Data Provider.</p>	<p>5.1.11 CSPs must take reasonable steps to remediate and provide corrected PNCD to the IPND Manager within 2 Business Days following PNCD Soft Error (clause 5.1.3) and User Query (clause 5.1.4 and 5.1.5) notifications being made available by the IPND Manager.</p>	

<p>Data Provider Query File</p>	<p>5.1.4 Where PNCD is identified by a CSP or Data User as potentially incorrect, contains an error or queries the content of the PNCD, the Data User will create a Data User Query File (DUQF) and make it available to the IPND Manager, as set out in the manner specified in the IPND Technical Requirements.</p> <p>5.1.5 The IPND Manager must produce a Data Provider Query File notification under clause 5.1.4 within 24 hours for retrieval by the Data Provider.</p>		
<p>Amalgamated query file</p>			<p>5.1.12 The IPND Manager must provide Data Users with an Amalgamated Query File (AQF) on a monthly basis.</p>
<p>PNCD incorrect</p>		<p>5.2.1 A CSP, upon confirming that a Customer's PNCD is incorrect, must take reasonable steps to ensure that incorrect data is corrected and sent to the IPND Manager within two Business Days, subject to operational limitations, such as requesting and receiving Customer information to correct the data.</p>	

<p>Data Reconciliation file requests</p>			<p>5.3.1 For Reconciliation purposes, Data Providers who are the same entity as the CSP must 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 at least once every six months.</p> <p>5.3.2 Where a Data Provider performs the role of providing PNCD to the IPND on behalf of a CSP, the Data Provider must:</p> <p>(a) obtain an extract of the relevant CSP, PNCD as a full set of records or as a subset of records based on criteria agreed between the CSP, Data Provider and the IPND Manager at least once every six months;</p> <p>(b) provide the relevant CSP with their PNCD extract, as soon as practicable, after the extract has been made available to the Data Provider by the IPND Manager.</p> <p>5.3.3 The IPND Manager must extract PNCD referred to in clauses 5.3.1 and 5.3.2 at a date and time agreed to with the Data Provider and provide the PNCD to the Data Provider within a reasonable timeframe, not exceeding 5 Business Days from the agreed date of the PNCD extract.</p>
<p>List Code Process</p>	<p>5.2.3 Where a CSP identifies any discrepancies in List Code data held by the IPND Manager identified under clause 5.2.2 the CSP must send updated PNCD to the IPND Manager within 1 Business Day of the discrepancy being identified.</p>		

<p>Data Reconciliation processing</p>			<p>5.3.4 CSPs must undertake a Reconciliation of the extract of the PNCD referred to in clause 5.3.1 and 5.3.2 and take reasonable steps to amend any discrepancies between the PNCD held by the IPND Manager and the CSP's own data by sending updated PNCD to the IPND Manager within 30 Business Days of the PNCD extract being made available by the IPND Manager.</p>
<p>Mass data uploads</p>	<p>5.1.13 Where the IPND Manager receives record(s) from one CSP that over write the existing record(s) of another CSP within the IPND (or within the IPND test environment), and the IPND Manager has become aware that this has occurred in error and/or is not a normal IPND operation, the IPND Manager must notify the CSP's Data Provider submitting the change and the original Data Provider of the event within one Business Day of becoming aware of the error.</p>	<p>5.4.1 Where a Data Provider intends to undertake a large data or bulk refresh of PNCD they supplied to the IPND, they must notify the IPND Manager at least two Business Days before this activity is undertaken.</p>	
<p>PNDP – change of Listing Type</p>		<p>4.3.9 Upon receiving notification that a Number has changed listing type, providers of Directory Related Services (except printed publications) must reflect changes to Listing Status for Numbers by updating all</p>	

		relevant records within two Business Days of Public Number Directory Data (PNDD) being made available by the IPND Manager.	
CSP supply of PNCD to Customers			6.2.3 The CSP must respond to their Customer's request for a copy of their PNCD by supplying the requested PNCD within 20 Business Days, subject to clause 6.2.2 (a) and 6.2.2 (c).
IPND supply of PNCD to CSP			6.2.4 The IPND Manager must ensure that requests from CSPs for PNCD are processed in a timely manner and that relevant PNCD is supplied to the CSP within 10 Business Days of receiving the PNCD request.
IPND Manager maintenance of PNCD or PNDD			<p>5.1.22 Where the IPND Manager undertakes maintenance of a complete PNCD or PNDD record beyond what is normally required for maintenance and integrity of the IPND, administration, fault identification, auditing and reporting, the IPND Manager must:</p> <ul style="list-style-type: none"> (a) take all reasonable steps to obtain permission from the relevant CSP before amending any records; (b) specify the reason for such maintenance activity; (c) provide a description of the maintenance activity; (d) maintain a record (for a period of three years) of all maintenance activities undertaken, who authorised or requested the maintenance activities and the reason (s) for the maintenance activities; and (e) notify the ACMA within five Business Days in the event a CSP is no longer available to provide permission for limited maintenance to a PNCD or PNDD record.

PARTICIPANTS

The Working Committee responsible for the revisions made to this Code consisted of the following organisations and their representatives:

Organisation	Membership	Representative
ACCAN	Non-voting	Samuel Kininmonth
ACMA	Non-voting	Emma Bain
Aussie Broadband	Voting	Eric Erickson
Aussie Broadband	Non-voting	Bryan Coulson
IPND Manager (Telstra Limited)	Voting	Penny Waite
Optus	Voting	Tom Forwood
Optus	Non-voting	Warren Hudson
Paradigm One	Voting	Devendra Gupta
Symbio	Voting	Michelle Costa
Telstra Limited	Voting	David Fabbian
Telstra Limited	Non-voting	Spiro Zantiotis
Telstra Limited	Non-voting	Robert Lansbury
TPG Telecom	Voting	Annie Leahy
TPG Telecom	Non-voting	Alexander R. Osborne
Vocus	Voting	John Sexton

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

Communications Alliance was formed in 1997 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 25
100 Mount Street
North Sydney
NSW 2060 Australia**

**Correspondence
PO Box 444
Milsons Point
NSW 1565**

**T 61 2 9959 9111
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 Communications Alliance