

# Research entity application and Privacy Impact Assessment

Telecommunications Regulations 2001



## Instructions for completion

- > This form should be used by research entities seeking authorisation from the Australian Communications and Media Authority (ACMA) to use and disclose **unlisted mobile number information** from the Integrated Public Number Database (IPND), under the Telecommunications Regulations 2001 (the Regulations).  
*NOTE:* Unlisted mobile number information can only be used for **permitted research**, as defined in the Regulations.
- > This form comprises three parts and a declaration.
  - > Sole applicants: must complete Parts 1, 2 and 3.
  - > Multiple applicants: the primary research entity must complete Parts 1, 2 and 3. Each additional applicant must complete separate Parts 2 and 3.
  - > Every applicant must sign the declaration at the end of their copy of the form.
- > In this application, terms in **bold** are defined in the Regulations. For brevity, **authorised unlisted mobile number information** is referred to as **mobile information**.
- > You can type directly into this form and attach additional material if required, clearly identifying the question(s) to which it refers.
- > This form must be accompanied by the charge (if any) determined by the ACMA (sub-paragraph 5.8(3)(d)(i) of the Regulations). Current charge: Nil.
- > Either email the completed form to [IPND@acma.gov.au](mailto:IPND@acma.gov.au) or post it to:  
IPND  
Australian Communications and Media Authority  
PO Box 13112 Law Courts  
Melbourne Vic 8010

# PART 1: Primary entity and research details

## Primary research entity details

Name of primary research entity:

Full name (if individual applicant): Click here to enter text.
Organisation name (if applicable): CROSBY TEXTOR RESEARCH STRATEGIES RESULTS PTY LTD
ABN/ACN: 58 101 934 454
Trading name/s: CROSBY TEXTOR
Registered address: Level 2, 115 Pitt Street Sydney NSW 2000
Click here to enter text.
Address (place of business, if different from registered address):
Governor Macquarie Tower, Level 26, 1 Farrer Place, Sydney, 2000
Click here to enter text.
Telephone number: (02) 9103 9200
Email: cdouglas@ctgroup.com

Name of contact for primary research entity:

Full name: Catherine Douglas
Position: Managing Director
Telephone number: [REDACTED]
Email: cdouglas@ctgroup.com

## Proposed permitted research (1.7A and 5.8 of the Regulations)

1. **Mobile information** can only be accessed for certain **permitted research**.

- a. Select the **mobile information** being sought and state why it is being sought:
- Phone number.
  - Post code.

Electoral matter research. Additional detail provided in Section 9.

- b. Indicate how many phone numbers and/or postcodes are requested, and the basis on which they will be requested (for example, random selection, geographically based):

All phone numbers for all Australian postcodes

- c. Indicate the nature of the **permitted research** for which the **mobile information** is being sought (there may be more than one type):
- Public health research (Go to Question 2).
  - Electoral matter** research (Go to Question 3).
  - Research that will contribute to public policy conducted by or on behalf of the Commonwealth or a **Commonwealth entity** (Go to Question 7).

**For research entities seeking to conduct research for *public health* purposes only:**

2. Is the proposed **permitted research** being conducted on behalf of any entities not covered by this application?

No.

Yes. If yes, please provide:

a. details of the entity/ies on whose behalf the research is being undertaken (including, as applicable, full name, ACN/ABN, registered address, website, brief description of entity and its purpose):

Click here to enter text.

b. evidence to support the **research entity's** authority to apply on behalf of each entity named at 2a above, including the name and contact details of an authorised representative of that entity:

Click here to enter text.

**For research entities seeking to conduct research for *electoral matters* only:**

3. Is any research entity a **registered political party**?

No

Yes. State the name of the party and the jurisdiction in which it is registered:

Click here to enter text.

4. Is any research entity a **political representative**?

No

Yes. State the representative's name and the relevant **Australian Parliament** or **local government authority**:

Click here to enter text.

5. Is any research entity a candidate in an election for an **Australian Parliament** or **local government authority**?

No

Yes. State the candidate's name and the relevant **Australian Parliament** or **local government authority**:

Click here to enter text.

6. Is the proposed **permitted research** to be conducted on behalf of a **registered political party**, a **political representative**, or a candidate in an election for an **Australian Parliament** or **local government authority**?

No

Yes. If yes, please state (as applicable):

a. the name of the registered political party, political representative or candidate.

Liberal Party of Australia

b. if a registered political party, the jurisdiction in which the party is registered.

Commonwealth

c. if a political representative or candidate, the **Australian Parliament** or **local government authority** the political representative represents, or for which the candidate is running in an election.

n/a

d. evidence to support the research entity's authority to apply on behalf of the registered political party, political representative, or candidate, including the name and contact details of an authorised representative of the party, representative or candidate.

Crosby Textor has been engaged by the Liberal Party to undertake this electoral matter research.

The authorised representative is Andrew Hirst, Federal Director, Liberal Party of Australia (phone: 02 6273 2564)

**For Commonwealth research entities only:**

7. Is any research entity the Commonwealth or a Commonwealth entity?

No

Yes. If yes, please state the name:

Click here to enter text.

8. Is the proposed permitted research to be conducted on behalf of the Commonwealth or a Commonwealth entity?

No

Yes. If yes:

a. please state the name of the entity on whose behalf the research will be conducted:

Click here to enter text.

b. evidence to support the research entity's authority to apply on behalf of the Commonwealth or Commonwealth entity, including the name and contact details of an authorised representative of the Commonwealth/Commonwealth entity:

Click here to enter text.

**Details of proposed permitted research under this application (1.7A and 5.8 of the Regulations)**

9. Describe the nature of the proposed permitted research. Provide the following details, as applicable:

a. likely beneficiaries, direct and indirect

b. likely social benefits

c. how the research is relevant to public health (public health research)

d. the electoral matters to which the research is directed (electoral matter research)

e. how will the research contribute to the development of public policy (Commonwealth public policy research)

f. likely form of finalised research

g. any other information you consider relevant:

The proposed permitted research will be conducted through Computer Assisted Telephone Interviewing across federal and state electorates.

a) The direct beneficiaries of this research will be the Liberal Party of Australia and its associated State and Territory Divisions, including the Party's current elected representatives and candidates. The indirect beneficiaries will be the Australian electorate, as this research will be used to most accurately inform the formulation of public policy by current and prospective governments.

b) The likely social benefits to come from this research will be the formulation of public policies based on the views and preferences expressed by voters.

c) N/A

d) The electoral matters to which the research is directed include Australians' views on public policies, opinions on political parties, incumbent Members of Parliament and Senators and candidates, views of the political and current affairs environment more broadly, engagement with topical public debate, how registered voters intend to vote in upcoming elections and the factors most likely to influence their vote.

e) N/A

f) The final form of this research will be delivered in powerpoint presentation format, with accompanying anonymised data tables.

g) The conduction and final form of this research will be in full compliance with the AMRS Code of Professional Behaviour, and all local laws concerning data collection relevant to our business.

10. Is there a commercial purpose associated with the proposed **permitted research**? If so, provide details about the purpose, including what the primary purpose is. Note that if the research is being conducted for a primarily commercial purpose, it may not be 'permitted research' (see regulation 1.7A):

No

**Duration of authorisation (5.12 of the Regulations)**

11. The ACMA can specify a period of no longer than 12 months for an authorisation. An authorisation period starts on the day the IPND Manager first discloses **mobile information** to an **authorised research entity** covered by the authorisation. Detail what period is sought and why:

Twelve months. Research is conducted regularly throughout the year.

**Receipt of mobile information (5.16 of the Regulations)**

12. As the primary **research entity**, will you be receiving the **mobile information** from the IPND Manager?

No. If no, then which applicant will receive the **mobile information** from the IPND Manager?

[Click here to enter text.](#)

Yes. If yes, then describe and provide evidence of the practices, procedures, processes and systems that will be used to ensure written notice is given, within 10 business days of receiving mobile information from the IPND Manager, to:

- the ACMA; and
- each **research entity** covered by this authorisation?

The data would be shared by the IPND Manager with C|T Group's dedicated IPND contact (Michael Turner). Upon receive of the data, Michael will notify relevant parties at the ACMA.

Prior to sharing the data with the fieldhouse, the C|T Group will require anyone handling the data to sign a written acknowledgement that they understand the terms under which the data can be used, stored and eventually destroyed.

In addition to these procedures, there are a series of general points to make about general practices within the business:

The C|T Group is bound by the AMSRS Code of Professional Behaviour, which forbids the use of data for purposes other than that which it is collected for. C|T also complies with all local laws concerning data protection relevant to our business.

C|T retains information that we collect no longer than is reasonably necessary to fulfil the purposes for which it was originally collected.

C|T Group take steps to ensure information is held securely in electronic or physical form. Our security measures are supported by a variety of processes and procedures, and we store information in access controlled premises or electronic databases requiring logins and passwords.

All employees, officers or contractors of C|T Group and third party providers with access to confidential information are subject to access controls and confidentiality obligations, and we require our third-party data storage providers to comply with appropriate information security industry standards.

All C|T Group devices are password protected and equipped with software firewalls and anti-virus anti-malware.

All networked services other than those necessary for the network to function are restricted.

**End of Part 1**

## PART 2: Research entity details

### Name of research entity

Full name (if individual applicant): Crosby Textor Research Strategies Australia
Organisation name (if applicable): C T Group
ABN/ACN: 58 101 934 454
Trading name: Crosby Textor
Registered address: Level 2, 115 Pitt Street Sydney NSW 2000
Click here to enter text.
Address (place of business, if different from registered address):
Governor Macquarie Tower, Level 26, 1 Farrer Place, Sydney, 2000
Click here to enter text.
Telephone number: (02) 9103 9200
Email: cdouglas@ctgroup.com

### Details of previous authorisation/s (5.11 of the Regulations)

1. Has the **research entity** previously been granted a research authorisation under the Regulations or the Telecommunications Integrated Public Number Database Scheme 2017?

No.

Yes. If yes, then:

- a. provide evidence of the authorisation, including date, purpose and period for which it was granted:

Click here to enter text.

- b. provide details and evidence of the extent to which the entity has complied with, or is complying with, the conditions of that authorisation:

Click here to enter text.

- c. if the entity has previously been granted a research authorisation under the Regulations, provide details and evidence of the extent to which the entity has complied with the requirements regarding **mobile information** and **research information** after an authorisation ends or an entity is removed from it (5.30 and 5.31 of the Regulations).

Click here to enter text.

### Use and disclosure of mobile information (5.17 of the Regulations)

2. **Authorised research entities** must not record or use **mobile information** unless it is for **authorised research** under authorisation. Provide evidence of the practices, procedures, processes and systems that will be used to comply with this obligation:

The C|T Group is bound by the AMSRS Code of Professional Behaviour, which forbids the use of data for purposes other than that which it is collected for. C|T Group also complies with all local laws concerning data protection relevant to our business.

C|T Group retains information that we collect no longer than is reasonably necessary to fulfil the purposes for which it was originally collected.

C|T Group take steps to ensure information is held securely in electronic or physical form. Our security measures are supported by a variety of processes and procedures, and we store information in access controlled premises or electronic databases requiring logins and passwords.

All employees, officers or contractors of C|T Group and third party providers with access to confidential information are subject to access controls and confidentiality obligations, and we required our third-party data storage providers to comply with appropriate information security industry standards.

3. An **authorised research entity** must only disclose **mobile information** (unless otherwise required to do so by or under an applicable law) to:
- its **research employees**
  - another **research entity** covered by the same authorisation
  - the ACMA, upon request.

Describe and provide evidence of the practices, procedures, processes and systems that will be used to ensure that you only disclose **mobile information** in accordance with the Regulations:

The C|T Group will dedicate an IPND contact (Michael Turner, Head of Research) as the person to receive the data from the IPND Manager. Michael, along with other relevant members of the C|T Group team and those at the fieldhouse, will be required to sign an acknowledgement that they understand the security measures that must be taken with the data as it relates to receipt, sharing, use and eventually destruction.

Additional general measures that exist within the business, include:

C|T Group take steps to ensure information is held securely in electronic or physical form.

Our security measures are supported by a variety of processes and procedures, and we store information in access controlled premises or electronic databases requiring logins and passwords.

All employees, officers or contractors of C|T Group and third party providers with access to confidential information are subject to access controls and confidentiality obligations, and we required our third-party data storage providers to comply with appropriate information security industry standards.

All C|T Group devices are password protected and equipped with software firewalls and anti-virus anti-malware.

All networked services other than those necessary for the network to function are restricted.

#### **Privacy Act (5.18 and 5.19 of the Regulations)**

4. Will the **research entity** be covered by the *Privacy Act 1988* for the duration of the authorisation? Provide supporting evidence either below or as an attachment to your response.
- Yes, as an organisation or agency within the meaning of the *Privacy Act 1988*.
- Yes, as a small business operator (within the meaning of the *Privacy Act 1988*) that has chosen to be treated as an organisation under section 6EA of that Act.
- No, the applicant is a **registered political party**.
- No, other reason specified below:

No.

Section 5.18 of the Regulations require that an authorised entity be covered by the Privacy Act, but that this does not apply if the entity is a registered political party.

CT Group has been engaged as a contractor to conduct electoral research on behalf of the Liberal Party of Australia.

Section 7c of the Privacy Act 1988 provides that certain political acts and practices are exempt from the Privacy Act. The relevant section reads as follows:

(2) An act done, or practice engaged in, by an organisation (the contractor) is exempt for the purposes of paragraph 7(1)(ee) if the act is done or the practice is engaged in:

(a) for the purposes of meeting an obligation under a contract between the contractor and a registered political party or a political representative described in subsection (1); and

(b) for any purpose in connection with one or more of the following:

(i) an election under an electoral law;

(ii) a referendum under a law of the Commonwealth or a law of a State or Territory;

(iii) the participation in another aspect of the political process by the registered political party or political representative;

(iv) facilitating acts or practices of the registered political party or political representative for a purpose mentioned in subparagraph (i), (ii) or (iii) of this paragraph.

As CT Group is contracted to, and acting on behalf of, a registered political party, the exemption from 7c of the Privacy Act applies.

However, CT Group complies with the Privacy – Market and Social Research – Code 2014 (see next section for detail), which is a registered APP Code, and by following this Code, CT Group complies with the Privacy Act 1988.

5. If an **authorised research entity** collects, uses or discloses personal information for the purposes of **authorised research** under an authorisation, it must not do an act, or engage in a practice, that breaches:
- a. an Australian Privacy Principle (APP) in relation to the personal information; or
  - b. a registered APP code that binds the entity in relation to personal information, regardless of whether:
    - it is a **registered political party**; or
    - the act or practice of the entity is exempt under section 7C of the *Privacy Act 1988* (which provides that certain political acts and practices are exempt).

Describe and provide evidence of the practices, procedures, processes and systems that will be used to ensure compliance with this requirement:

Section 5.19 of the Regulations requires that an entity must not act, or engage in a practice that breaches the Australian Privacy Principles (APP) or a registered APP code.

CT Group is a member of the Australian Market and Social Research Society (AMSRS):  
<https://www.amsrs.com.au/documents/item/2258>

CJT Group is bound by the AMSRS Code of Professional Behaviour, which mirrors the APPs on data collection, use, storage and destruction.

The AMSRS Code is a registered APP Code (the Privacy – Market and Social Research – Code 2014) and is available here: <http://www.amsro.com.au/amsroresp/wp-content/uploads/2014/03/The-Privacy-Market-and-Social-Research-Code-2014-1.pdf>

The provisions in the Code seeks to give effect to the APPs in a manner that is tailored to the research context, while providing the public and business community with the assurances needed to encourage informed and willing participation in research activities. The Code acknowledges and draws on relevant Guidelines published by the Office of the Australian Information Commissioner.

The Code forbids the use of data for purposes other than that which it is collected for. CJT also complies with all local laws concerning data protection relevant to our business.

CJT retains information that we collect no longer than is reasonably necessary to fulfil the purposes for which it was originally collected.

CJT Group take steps to ensure information is held securely in electronic or physical form. Our security measures are supported by a variety of processes and procedures, and we store information in access controlled premises or electronic databases requiring logins and passwords.

All employees, officers or contractors of CJT Group and third party providers with access to confidential information are subject to access controls and confidentiality obligations, and we required our third-part data storage providers to comply with appropriate information security industry standards.

All CJT Group devices are password protected and equipped with software firewalls and anti-virus anti-malware.

All networked services other than those necessary for the network to function are restricted.

6. Describe and provide evidence of the extent to which the research entity's collection, use and disclosure of personal information complies with, or is consistent with, the *Privacy Act 1988* (whether or not that Act applies to the entity):

CT Group's collection, use and disclosure of personal information is consistent with the Privacy Act 1988, in accordance with the registered APP Code, the Privacy – Market and Social Research – Code 2014.

#### Contacting customers and compliance with the *Telecommunications Act 1997* (5.20 and 5.23 of the Regulations)

7. When contacting a person using **mobile information** for the purposes of **authorised research**, a research entity must ensure that the **contacted person** is told or asked the following during the call:
- the **research entity's** name;
  - the purpose of the research;
  - how the **research entity** obtained the mobile number used to contact the **contacted person**;
  - how the **research entity** proposes to use the **research information** relating to the **contacted person**;
  - that the use of the number by the **research entity** is authorised by the ACMA for the purposes of the **authorised research**;
  - if asked, how the **contacted person** can access any personal information about them held by the **research entity**;
  - whether the **contacted person** gives consent for the use and disclosure of the **research information** relating to the person in the research;
  - that the **contacted person** may withdraw any consent so given at any time during the call; and
  - how the research entity proposes to give the **contacted person** any other information that is required by law (for example, under the *Privacy Act 1988*).

Describe and provide evidence of the practices, procedures, processes and systems that will be used to meet this requirement:

All of CJT Group surveys are scripted and responses are supplied to interviewers in the event a question arises during the interview that is not addressed in the initial script. If a respondent shares that they would not like to continue, the call is terminated and none of the information from the interview is retained.

Examples of scripts and other relevant Q&A are included below.

#### STANDARD INTRODUCTION

Good afternoon/evening,

My name is [INSERT NAME] calling from the research firm, EMRS.

We are conducting a household survey on social issues and would like to give you the opportunity to share your opinions – May I please speak to the [REDACTED] person aged over 18, who is currently enrolled to vote and who lives in this household?

[IF YES:] The survey takes up to 15 minutes to complete.

[MUST READ OUT:] Your participation is on the understanding that both you and the end client are anonymous.

[IF ASKED WHO THE END CLIENT IS RESPOND:] I simply don't know, we are not informed of that.

[IF ASK FOR SUPERVISOR NUMBER:] [INSERT NUMBER]

This call will be monitored and recorded for quality and coaching purposes.

#### STANDARD CLOSING

Thank you for helping us with the survey. Finally may I have your first name for validation purposes only?

As this is market research, it is carried out in compliance with the Privacy Act. The information you provided will be used only for research purposes.

[IF ASKED ABOUT WHO THE RESEARCH IS BEING CONDUCTED FOR SAY:] Your participation is on the understanding that both you and the end client are anonymous.

That's the end of the interview, thank you very much for your help. Please be assured this is genuine market research. If you have any queries, you can call my supervisor on [INSERT NUMBER].

8. An authorised research entity is required to comply with all applicable laws related to unsolicited contact with another person including:
- the *Privacy Act 1988*
  - the *Spam Act 2003*
  - the *Do Not Call Register Act 2006*.

Describe and provide evidence of the practices, procedures, processes and systems that will be used to ensure compliance with the applicable laws related to unsolicited contact:

- Contractors to registered political parties are exempt from the Privacy Act by virtue of section 7c.
- Registered political parties are exempt from the Spam Act. Nonetheless the purpose of this research is to conduct anonymised public opinion polling and no unsolicited electronic messages will be sent as a result.
- Commercial or research calls from a political party (or their contractors), an independent member of parliament or a candidate for election are permitted to be made to numbers on the Do Not Call Register. However, the Telecommunications (Telemarketing and Research Calls) Industry Standard applies regardless of any exemption from the Do Not Call Register Act 2006, and CT Group's compliance with the Standards is set out below.

9. An **authorised research entity** must comply with any requirements imposed on it by the *Telecommunications Act 1997* and any legislative instrument made under that Act.

Describe and provide evidence of the practices, procedures, processes and systems that will be used to comply with this requirement (including compliance with the *Telecommunications (Telemarketing and Research Calls) Industry Standard 2017*):

Compliance with the Telecommunications Act 1997 is ensured through operational leads and automated through technology.

Additionally, C|T and its partners all participate in a formal staff induction, ongoing training and monitoring to ensure they comply with all requirements set out in the Telecommunications Act 1997.

The Telecommunications (Telemarketing and Research Calls) Industry Standard 2017 sets out the requirements for:

1. When research calls cannot be made.
2. Information that must be provided during a research call.
3. When calls must be terminated.
4. The use of call line identification.

**Contacted person does not consent to use and disclosure of research information (5.20 of the Regulations)**

5. If a **contacted person** informs an **authorised research entity** during a call that the person does not consent, or withdraws consent, to the use and disclosure of **research information** relating to them, the **authorised research entity** must comply with certain requirements.

Describe and provide evidence of the practices, procedures, processes and systems that will be used to ensure compliance with the requirement to:

- a. not record, use or disclose any **research information** relating to the **contacted person**.

The script used is as follows that provides assurance as to how the information will be used:

**Introduction:**

**Good afternoon/evening,**

**My name is .... calling from the research firm, EMRS.**

**We are conducting a household survey on New South Wales issues and would like to give you the opportunity to share your opinions - May I please speak to the [REDACTED] person aged over 18, who is currently enrolled to vote and who lives in this household?**

**[IF YES:] The survey takes up to 8 minutes to complete.**

**[MUST READ OUT:] Your participation is on the understanding that both you and the end client remain anonymous.**

**[IF ASKED WHO THE END CLIENT IS RESPOND:] I simply don't know, we are not informed of that.**

[IF ASK FOR SUPERVISOR NUMBER: [REDACTED]

**QA. The call will be monitored and recorded for quality and coaching purposes.**

**Closing Statement:**

Thank you for helping us with the survey. Finally may I have your first name for validation purposes only?

As this is market research, it is carried out in compliance with the Privacy Act. The information you provided will be used only for research purposes.

[IF ASKED ABOUT WHO THE RESEARCH IS BEING CONDUCTED FOR SAY:] Your participation is on the understanding that both the individual information that you provide and the end client remain anonymous.

[IF ASKED WHO THE END CLIENT IS, RESPOND:] I simply don't know, we are not informed of that.

That's the end of the interview, thank you very much for your help. Please be assured this is genuine market research. If you have any queries, you can call my supervisor on [REDACTED]

[RECORD FIRST NAME]

- b. not use the **mobile information** relating to the **contacted person**.

In this instance, participants are added to an internal "do not call" register operated by the fieldhouse, meaning on any future projects even if the fieldhouse inadvertently tried to call the number, the dialler and system will not allow it to go through as it would have been blacklisted.

- c. as soon as reasonably practicable, take all reasonable steps to destroy any **research information** relating to the person within 10 business days after the **contacted person** refuses to give, or withdraws, consent.

All data we receive is deidentified. It is retained for quality control and dispute resolution purposes. Should a contacted person or research participant lodge a complaint via our complaints procedure or request to withdraw their consent to provide their details and data provided, we will destroy all associated data collected from that person from the primary data source held securely on our servers and from an quality control or validation data sources.

- d. give written notice to all other **authorised research entities** that the **mobile information** relating to the **contacted person** must not be used.

All employees, officers or contractors of C|T Group and third party providers with access to confidential information are subject to access controls and confidentiality obligations, and we required our third-part data storage providers to comply with appropriate information security industry standards.

6. If one **authorised research entity** notifies another **authorised research entity** that consent to use **mobile information** has been refused or withdrawn, the entity which receives that notification must not use the **mobile information** of the person who has refused to give, or withdrawn, consent.

Describe and provide evidence of the practices, procedures, processes and systems that will be used to ensure you do not use the **mobile information** after notification that consent has not been given or was withdrawn.

All employees, officers or contractors of C|T Group and third party providers with access to confidential information are subject to access controls and confidentiality obligations, and we required our third-part data storage providers to comply with appropriate information security industry standards.

7. If a **contacted person** refuses or withdraws consent to the use and disclosure of **research information** relating to them, what practices, procedures, processes and systems will be in place to deal with that request?

If a respondent shares that they would not like to continue, the call is terminated and none of the information from the interview is retained.

C|T conducts extensive training and ongoing monitoring to ensure compliance with all policies and procedures.

No undue pressure is placed on anyone we contact to undertake the survey and should they decline at the outset we end the call. In this instance, no information has been recorded.

Should a respondent contacted agree to begin the survey but at some point request that the call ceases, we oblige ending the call. In this circumstance, incomplete surveys are not recorded in our system and therefore no data is held on that individual.

Only completed surveys that reach the end successfully and the telephone interviewer submits the data to the system are held as records of calls with all refusals, incompletes and terminated calls having no data stored other than the outcome of the call.

8. An **authorised research entity** must have internal dispute resolution procedures to deal with inquiries or complaints from a **contacted person** about the entity's use or disclosure of any **research information** relating to the person.

Describe and provide evidence of internal dispute resolution procedures that will be used to:

- a. deal with inquiries or complaints from a contacted person about the use or disclosure of any **research information** relating to the person.

If a respondent shares that they would not like to continue, the call is terminated and none of the information from the interview is retained.

C|T conducts extensive training and ongoing monitoring to ensure compliance with all policies and procedures.

EMRS treats all complaints or queries regarding privacy and the AMSRS code seriously and will investigate with due diligence to ensure the matter is resolved appropriately to the satisfaction of all parties.

To lodge a complaint or request further information, any parties wishing to do so are directed to our privacy policy on the website that outlines the complaint procedure.

We will respond and advise whether we agree with your complaint or not. If we do not agree, we will provide reasons. If we do agree, we will advise what (if any) action we consider it appropriate to take in response.

If research participants are still not satisfied, then we suggest they contact the Office of the Australian Information Commissioner.

- b. provide the ACMA's contact details to a **contacted person** who wants to escalate their complaint.

On the two or three occasions we have needed to contact the ACMA to resolve a matter in the past 10 years, we have gone through the channels provided (typically in response to an email they sent to our field agency).

- c. provide reasonable assistance to the ACMA in relation to any such complaint if requested by the ACMA to do so.

On the very few instances where this has been necessary in the last 15 years of operation, we have had a positive and constructive relationship and dealings with ACMA to resolve any legitimate complaints or enquiries they have contacted us in regard to.

#### **Disclosure of research information (5.21 of the Regulations)**

9. An **authorised research entity** must not disclose **research information** unless it is for the purposes of **authorised research** under the authorisation.

Describe and provide evidence of the practices, procedures, processes and systems that will be used to ensure that **research information** is not disclosed, except for the **authorised research**.

The C|T Group is bound by the AMSRS Code of Professional Behaviour, which forbids the use of data for purposes other than that which it is collected for. C|T Group also complies with all local laws concerning data protection relevant to our business.

C|T retains information that we collect no longer than is reasonably necessary to fulfil the purposes for which it was originally collected.

C|T Group take steps to ensure information is held securely in electronic or physical form. Our security measures are supported by a variety of processes and procedures, and we store information in access controlled premises or electronic databases requiring logins and passwords.

All employees, officers or contractors of C|T Group and third party providers with access to confidential information are subject to access controls and confidentiality obligations, and we required our third-part data storage providers to comply with appropriate information security industry standards.

10. Except as outlined at question 14 above, an **authorised research entity** must not disclose **research information** except to its **research employees** (unless required to do so by or under a law that applies to it).

Describe and provide evidence of the practices, procedures, processes and systems that will be used to ensure compliance with this requirement.

The C|T Group is bound by the AMSRS Code of Professional Behaviour, which forbids the use of data for purposes other than that which it is collected for. C|T Group also complies with all local laws concerning data protection relevant to our business.

C|T retains information that we collect no longer than is reasonably necessary to fulfil the purposes for which it was originally collected.

C|T Group take steps to ensure information is held securely in electronic or physical form. Our security measures are supported by a variety of procedures, which are outlined in the employee handbook. Additionally, we store information in access controlled premises or electronic databases requiring logins and passwords.

All employees, officers or contractors of C|T Group and third party providers with access to confidential information are subject to access controls and confidentiality obligations, and we required our third-part data storage providers to comply with appropriate information security industry standards.

11. An **authorised research entity** may disclose **research information** relating to a **contacted person** if:
- the information is de-identified (that is, it does not identify the person, and the person is not reasonably identifiable from the information), and
  - the information does not include the person's public number.

Describe and provide evidence of the practices, procedures, processes and systems that will be used to ensure the **research information** is de-identified and does not include the person's public number before it is disclosed.

After data collection has concluded and prior to any data being made available internally to researchers or sent to externally to clients, all identifying information (including phone number) is removed from the data file to be used. This guarantees the anonymity of each respondent to be surveyed. This practice even extends to reviewing all written comments or answers provided to ensure no phone numbers or identifying details (names, addresses etc) are included in the final data file.

#### Technical systems (5.22 of the Regulations) and data security

12. An **authorised research entity** must have technical systems to receive **mobile information** in accordance with any method specified by the IPND Manager.

Describe and provide evidence of the processes and technical systems that will be used to receive the **mobile information from the IPND Manager**.

CT Group will comply with the IPND Data File Guidelines and the Technical Requirements as set out by the IPND manager, in accordance with the Standard IPND Data Access Agreement.  
<https://www.telstra.com.au/content/dam/tcom/personal/consumer-advice/ipnd/standard-ipnd-data-access-agreement-2017.pdf>

13. What technical security measures will be used to protect **mobile information** and **research information** that is stored or transferred in **electronic** format from misuse, loss, unauthorised access, modification or disclosure?

All C|T Group devices are password protected and equipped with software firewalls and anti-virus anti-malware. All networked services other than those necessary for the network to function are restricted.

14. What physical security measures will be in place to protect any **mobile information** and **research information** that is contained in **hardcopy** records from misuse, loss, unauthorised access, modification or disclosure?

C|T Group take steps to ensure information is held securely in electronic or physical form.

Hardcopies are shredded immediately after use or placed in locked secure shredding bins. No material is left unattended either in the office or outside.

Entry to the office requires an electronic pass. Additionally, areas of the premises where hard copies may be found are access via additional electronic access or keys.

All employees are briefed extensively on confidentiality upon starting with the firm. It is also a condition of each employee's contract.

15. Specify and provide evidence of:
- what internal security measures will be used to ensure access is restricted only to **research employees** who need to handle **mobile information** and **research information**.

C|T Group take steps to ensure information is held securely in electronic or physical form. Our security measures are supported by a variety of processes and procedures, and we store information in access controlled premises or electronic databases requiring logins and passwords.

All employees, officers or contractors of C|T Group and third party providers with access to confidential information are subject to access controls and confidentiality obligations, and we required our third-part data storage providers to comply with appropriate information security industry standards.

All C|T Group devices are password protected and equipped with software firewalls and anti-virus anti-malware. All networked services other than those necessary for the network to function are restricted.

All employees are briefed extensively on confidentiality upon starting with the firm. It is also a condition of each employee's contract.

- b. whether audit trails will be used to monitor who accesses and manipulates the **mobile information** and **research information**.

C|T conducts 6 monthly security reviews

- c. what measures will be in place to ensure that unauthorised copies of the **mobile information** and **research information** cannot be made, that is, copies that are not required for the authorised research.

The information is stored on a device that is only accessible by a couple of C|T employees

16. Will the **mobile information** and/or **research information** be accessible to or handled by persons or organisations outside of Australia at any time?

No

17. If yes:

- a. provide the name and contact details of the overseas person or entity:

Not applicable

- b. describe and provide evidence of the relationship between that person/s or entity and you (for example, contract):

Not applicable

- c. for what purpose(s) will the **mobile information** and/or **research information** be accessed or handled by the overseas entity?

Not applicable

- d. describe and provide evidence of the measures to be taken to ensure that appropriate privacy and security protections are in place to protect the **mobile information** and/or **research information** from misuse, loss and unauthorised access, modification or disclosure while it is accessed or handled by the overseas entity.

Not applicable

#### Employees of authorised research entity (5.24 of the Regulations)

18. An **authorised research entity** must take all reasonable steps to ensure that **research employees** are aware of and comply with the conditions of the authorisation, and notify the entity of actions that may result in a contravention of a condition.

Describe and provide evidence of the practices, procedures, processes and systems that will be used to ensure that each **research employee**:

- a. is made aware of the conditions of the authorisation (including any additional conditions specified by the ACMA):

The C|T Group is bound by the AMSRS Code of Professional Behaviour, which forbids the use of data for purposes other than that which it is collected for. C|T also complies with all local laws concerning data protection relevant to our business.

CJT retains information that we collect no longer than is reasonably necessary to fulfil the purposes for which it was originally collected.

CJT Group take steps to ensure information is held securely in electronic or physical form. Our security measures are supported by a variety of processes and procedures, and we store information in access controlled premises or electronic databases requiring logins and passwords.

All employees, officers or contractors of CJT Group and third party providers with access to confidential information are subject to access controls and confidentiality obligations, and we required our third-part data storage providers to comply with appropriate information security industry standards.

All CJT Group devices are password protected and equipped with software firewalls and anti-virus anti-malware. All networked services other than those necessary for the network to function are restricted.

All employees are briefed extensively on confidentiality upon starting with the firm. It is also a condition of each employee's contract.

- b. cooperates with the entity in complying with those conditions:

Privacy and confidentiality requirements are detailed in the employee handbook and are also a condition of each employees contract

- c. will notify the entity in writing as soon as reasonably practicable after the **research employee** becomes aware of an act or omission that would result in a contravention of a condition:

Employees will be made aware of the specific requirements relating to IPND data at the commencement of the research engagement, including processes to alert team leaders of any contravention

#### **Contravention of authorisation conditions (5.25 of the Regulations)**

19. The Regulations set out requirements in the event of a contravention of a condition of the authorisation (including any additional conditions specified by the ACMA).

Describe and provide evidence of the practices, procedures, processes and systems to ensure that if you become aware that you (or another research entity under the same authorisation), contravene a condition then, as soon as reasonably practicable, you:

- a. give written notice to the ACMA:

If the CT Group becomes aware that it has contravened a condition, either the fieldhouse or relevant member of the CT Group team will advise the IPND liaison (and CT Head of Research) Mike Turner. Once we are aware of the contravention all activity relating to use of the IPND database will cease, pending communication with the ACMA. Mr Turner will then provide written correspondence to the ACMA.

- b. take reasonable steps to minimise the effects of the contravention:

Once we are aware of the contravention all activity relating to use of the IPND database will cease, pending communication with the ACMA.

**No use or disclosure of mobile information by former authorised research entities (5.30 of the Regulations)**

20. When an authorisation ends, or if an authorised research entity is removed from an authorisation, a **former research entity** must:

- a. not make a record, or use, the **mobile information**
- b. not disclose the **mobile information**, unless authorised, or required to do so by request of the ACMA
- c. take all reasonable steps to destroy the **mobile information** within 10 business days after the authorisation ends or the **research entity** is removed from the authorisation.

Describe and provide evidence of what practices, procedures, processes and systems will be used to ensure that these requirements are met:

All employees will be made aware of the specific requirements related to IPND data at the start of the engagement. On completion of the engagement, there will be a requirement to destroy all information.

21. During the authorisation period, will **mobile information** be linked to other data from another source?

- No
- Yes. If yes, specify how the **mobile information** will be separated from the other data, and destroyed, when the authorisation ends or revoked to ensure compliance with the Regulations.

No.

**Use or disclosure of authorised research information by former authorised research entities (5.31 of the Regulations)**

22. When an authorisation ends, or if an authorised research entity is removed from an authorisation, a **former research entity** must not:

- a. make a record, or use, the **research information**
- b. disclose the **research information**, unless authorised, or required to do so by request of the ACMA; unless the information does not identify the **contacted person**, the person is not reasonably identifiable from the **research information** and does not include the person's public number.

Describe and provide evidence of the practices, procedures, processes and systems that will be used to ensure that when you become a **former authorised research entity**, you will not:

- a. make a record of, or use, the **research information**:

The CT Group will require all employees and EMRS sign an acknowledgment that that will not record or use the research information once the authorisation has ended. At the end of the contract the CT Group IPND liaison will remind all relevant parties of their obligation.

- b. disclose the **research information**, unless it is **de-identified** and does not include the contacted person's number:

The CT Group will require all employees and EMRS sign an acknowledgment that that will not record or use the research information once the authorisation has ended. At the end of the contract the CT Group IPND liaison will remind all relevant parties of their obligation.

**Removal from research authorisation (5.31 of the Regulations)**

23. An **authorised research entity** which is removed by the ACMA from a research authorisation must:
- a. not make a record of, or use, the **research information**
  - b. not disclose the **research information**, unless authorised, or required to do so by or under an applicable law
  - c. take all reasonable steps to destroy the **research information** within 10 business days after the authorisation ends or the entity is removed from the authorisation.

Describe and provide evidence of the practices, procedures, processes and systems that will be used to ensure that you meet this obligation if it becomes applicable to you:

The CT Group will require all employees and EMRS sign an acknowledgment that that will not record or use the research information once the authorisation has ended. At the end of the contract the CT Group IPND liaison will remind all relevant parties of their obligation.

**End of Part 2**

## PART 3: Privacy Impact Assessment

An application must be accompanied by a Privacy Impact Assessment. The Office of the Australian Information Commissioner provides a Guide to undertaking privacy impact assessments (the PIA Guide), available at: <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments>.

A Privacy Impact Assessment for the permitted research project must be conducted for each **research entity** covered by this application. A report on the assessment should be provided below or as an annexure. If provided as an annexure, it must include the below information at a minimum. Terms in the following table have the same meanings as they have in the PIA Guide.

Section heading	Content
Executive summary	<p>A brief executive summary, including:</p> <ul style="list-style-type: none"> <li>the purpose of the Privacy Impact Assessment</li> <li>brief project description and key information flows</li> <li>summary of findings</li> <li>recommendations or existing strategies to address identified privacy risks.</li> </ul>
Privacy Impact Assessment methodology	<p>This section should outline the approach taken to undertake the Privacy Impact Assessment Methodology, including any stakeholder consultation.</p> <p>(Refer to Plan the PIA and Identify and consult with stakeholders in the PIA Guide.)</p>
Project description	<p>This section should describe the key features of the project, including any relevant background or the rationale for the project. Outline how personal information will be handled in the project, including through diagrams illustrating information flows, if appropriate. Information flows can also be addressed in more detail in the next section if required.</p> <p>This section should be kept brief and should not contain any analysis of privacy implications, as these will be addressed in later sections.</p> <p>(Refer to Describe the project and Map the information flows in the PIA Guide.)</p>
Analysis	<p>This section should identify:</p> <ul style="list-style-type: none"> <li>the project's impacts (positive and negative) on privacy</li> <li>privacy risks that may arise from the project, including whether the project complies with privacy legislation</li> <li>any strategies that are in place to remove, minimise or mitigate privacy risks</li> <li>recommendations about additional strategies required to remove, minimise or mitigate privacy risks.</li> </ul> <p>It may be appropriate to present an assessment of the project against each of the Australian Privacy Principles or any other legal obligations relating to privacy. It is important to remember, however, that the Privacy Impact Assessment is more than a compliance check, and that other questions may also need to be addressed. If the analysis is lengthy due to the complexity of the project or significant privacy impacts, it may be appropriate to split this information into separate sections.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>including information on privacy impacts and risks, existing strategies, and recommendations in separate sections</li> <li>presenting separate analyses for discrete parts of the project or information flows.</li> </ul> <p>(Refer to Privacy impact analysis and compliance check, Privacy management—addressing risks and Recommendations in the PIA Guide.)</p>

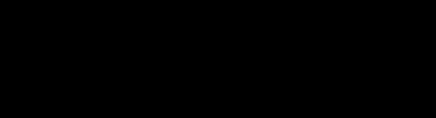
Section heading	Content
Conclusion	<p>This section should summarise the overall findings and outline the conclusions of the Privacy Impact Assessment, including whether the privacy safeguards currently in place or identified in the recommendations will be sufficient to protect personal information handled in the project.</p> <p>It should also outline the next and ongoing steps in the Privacy Impact Assessment process (refer to Respond and review in the PIA Guide).</p>
Appendices	<p>If required, appendices can be used to provide more detailed information. For example, the nature of consultation, who participated in consultation and the anticipated outcomes of the project.</p>

**End of Part 3**

## Declaration

I declare that:

1. The contents of this application, and any enclosures or annexures to this application, are true and correct.
2. I am aware that the ACMA may:
  - a. request the research entity to provide further information within 90 days of the ACMA's request
  - b. treat the application as if it did not specify the research entity, if the research entity does not provide the requested information within 90 days of the ACMA's request.
3. If this authorisation is granted, the research entity that completes this declaration will:
  - a. comply with all conditions of authorisation, including any additional conditions specified by the ACMA when the authorisation is granted, or subsequently specified or varied
  - b. act in accordance with the Privacy Impact Assessment.
4. If this authorisation is granted, the applicant will not use or disclose information obtained pursuant to the Regulations except for the purpose for which authorisation is sought.
5. The applicant will be covered by the *Privacy Act 1998* for the duration of the authorisation (unless the applicant is a registered political party).
6. The applicant will not act, or engage in a practice, that breaches an Australian Privacy Principles (APP) in relation to personal information about an individual, or a registered APP code that binds the entity in relation to personal information about an individual.
7. I am aware that the applicant must comply with any requirements imposed on the entity by the *Telecommunications Act 1997* and any legislative instrument made under that Act, and with all applicable laws related to unsolicited contact with another person.
8. I am aware that the ACMA may consult any person or body that the ACMA considers appropriate (including the Office of the Australian Information Commissioner) in connection with certain decisions under the Regulations, and that information provided in this authorisation may be disclosed for the purpose of that consultation.
9. I am aware the ACMA may remove an authorised research entity from a research authorisation if the ACMA is satisfied that a condition of any research authorisation that covers the entity has been contravened.
10. I have the authority to sign this application on behalf of the applicant.
11. I am aware that under section 137.1 of the *Criminal Code Act 1995*, it is an offence to knowingly provide false or misleading information to a Commonwealth entity in connection with the performance of functions under a law of the Commonwealth.

Sig		
Print full name	<i>Director, Privacy &amp; Data Protection</i>	

Position in organisation (if applicable)
<i>Director</i>
Date <i>21/12/2019</i> a date.

## Privacy

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

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

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

Under the Regulations, the ACMA may consult any person or body that the ACMA considers appropriate before deciding to grant an authorisation; specify, vary or revoke an additional condition; remove an entity from an authorisation; and make a decision on a reconsideration request. Details of this application may be disclosed as part of consultation.

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