commtel | security

AIO5022

Data Protection and Privacy

document description

commtelns.com

Document Control

Document No:	AIO5022	**Document Author:**	Manpreet Toor
Document Title:	Data Protection and Privacy	**Company Unit Owner:**	Corporate
Document Class:	Public	**Document Status:**	Approved

Version	Approval	Revised by	Issue Date	Summary
1.0	#651 / EA088	Manpreet T, Miles H	16-Mar-2026	Updated to the latest Privacy reforms and application section. AHO4021 retired and replaced with AIO5022.

Distribution

Version	Destination	Upload Date	Location
1.0	Unity	May - 2026	Management Systems > Security Management System > Policies

Company Information

aus
29 Translink Drive
Keilor Park VIC
Australia 3042

t. (613) 8340 6100
f. (613) 9331 7121
info@commtelns.com
commtelns.com

CommTel Network Solutions Pty Ltd.
acn. 082 646 017
abn. 75 082 646 017

1 Scope

This document is intended for use by managers and employees (Permanent and Contractors) of CommTel (being the Company).

2 Purpose

CommTel is committed to data protection and privacy of information related to its company-wide business activities, and relevant legal and other requirements as they apply. This Privacy and Data Protection Policy outline CommTel's commitment to safeguarding personal information in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs). It ensures transparency in how personal data is collected, used, disclosed, and stored.

3 Application

This policy primarily applies to all CommTel business activities in relation to managing personal information about individuals in Australia (Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs). This policy also applies to other geographic locations, however if those geographic locations have stricter legislation in place, then the local laws need to be applied.

This policy applies to:

- All CommTel employees, contractors, and consultants
- Third-party vendors and service providers handling CommTel data
- CommTel's parent company, GenusPlus Group Ltd, and other Genus group companies.
- Visitors whose information is collected via ISO and GDPR complaint systems
- Any system, application, or process that stores, processes, or transmits personal information

4 Objective

To provide information about how CommTel collects, use, disclose and handle personal and sensitive information related to its business operations.

5 Target

To manage personal information to the standards of this policy.

6 CommTel Requirements

CommTel will implement and manage this policy by:

- Providing training on this policy to required internal and external stakeholders.
- Conducting audits and inspections of this policy and its implementation.
- Developing supporting documents to assist with managing this policy where required.

7 Personal Data / Information

CommTel is committed to managing personal information (including sensitive information) that it holds (information in its possession and control) and associated right-to-privacy of each individual based on the legal and other requirements in each geographic location of operation.

This is information about an individual whose identity is apparent or can reasonably be ascertained from that information.

Sensitive information is a subclass of personal information that relates to an individual's ethnic or racial origin, religious or philosophical beliefs, political opinions, trade union membership or sexual activities.

8 Personal Information Collection

CommTel may only collect (solicit), use and disclose personal information (including sensitive information) where it is justified, reasonably necessary and is done by lawful and fair means for associated business activities / functions.

Any personal information (including sensitive information) that is collected by unlawful or unfair means is deemed to have not been collected and cannot be used by CommTel or any authorised External Stakeholder for any purpose. Any unlawful or unfair means of collection is to be reported to the CommTel Human Resources Manager promptly.

CommTel will only collect personal information (including sensitive) where there is a demonstrated business, legal or other requirement. This will not occur without the individual's prior knowledge and consent.

Personal information can be collected from individuals via phone, e-mail or website, in writing, or via other method of collection. In some instances, CommTel may engage an External Stakeholder to collect information from the individual, however this will be completed only where the individual has consented.

In the management of personal information there is a primary and secondary purpose that relates to collection, use and disclosure.

- Primary purpose - Where CommTel holds personal information about an individual, it can only use or disclose the information for the particular purpose for which it was collected.
- Secondary purpose - CommTel may use or disclose the minimum amount of related personal information for the secondary purpose or for another purpose based on one or more of the exceptions below:
  - The individual has consented to a secondary use or disclosure.
  - The secondary purpose is related to the primary purpose of collection. In the case of sensitive information, it must be directly related.
  - The individual would reasonably expect the secondary use or disclosure, and that it is related to the primary purpose of collection.
  - It is permitted by laws based on the geographic locations of use.
  - It is reasonable that the secondary use or disclosure is reasonably necessary for one or more health, safety or enforcement related activities.

Personal information may be collected for the following purposes:

- Recruitment of Workers.
- To confirm the identity of individuals.
- To perform services for, or receipt services from, External Stakeholders (Customers, suppliers and others).
- To perform internal business services, such as:
  - Travel services (including family members).
  - Social functions.
- Marketing activities.
- When required by law.
- Personal Information that may be collected:
- Employee information (Name, mailing address, email, landline and mobile telephone), age and gender, passport, visa documents, taxation, remuneration, leave entitlements, superannuation, bank details, emergency contacts, health records).
- Visitor information relating to site identification (Name, phone number, picture, employer).
- Job candidate information (work history, experience, qualifications, memberships, referees, personal references, interview summary responses).
- Employee performance information (Reviews, feedback, disciplinary activities).
- Other external parties (Name, e-mail, mailing, landline, mobile, telephone).

Prior to any personal information collection, CommTel's authorised individual involved with the collection will ensure:

- There is a justification and reasonable necessity for the information, including consideration of the consequences (for the individual and CommTel) if the information is not obtained.
- The primary purpose of collection has been made clear, questions do not exceed any stated purpose, collection is for a current activity and not a future need, and any secondary use or disclosure is known.
- The individual has been adequately informed before giving any consent for information to be collected.
- The individual has the capacity to understand and communicate their consent and understands how the information will be protected, used and disclosed.

In occasional instances it may not be practical to provide prior notification of collection or ensure awareness at the time of collection. CommTel will retain records as to why this prior notification could not be achieved and must take reasonable steps to provide notification, or ensure the individual is aware, as soon as practicable after the collection.

Any sensitive information that may be collected will have a clear and direct primary purpose and have written approval from the CommTel Human Resources Manager, prior to any collection being considered and occurring.

CommTel may need to verify personal information (including sensitive information) for accuracy and completeness. This could include contacting other businesses or External Stakeholders, however will only be completed when it is required for legitimate business activities.

All personal information (including sensitive) that is legitimately collected (by lawful means) will be stored by CommTel and authorised External Stakeholders for a required retention period in defined information systems.

Sensitive information is classified as, but not limited to the following:

- Race, ethnic origin, philosophical beliefs, religious beliefs or affiliations.
- Membership of a political association or political opinions.
- Membership of a professional or trade association or trade union.
- Sexual orientation or practices.
- Criminal record that is also personal information.
- Health information about an individual.
- Genetic information about an individual that is not otherwise health information.
- Biometric information that is to be used for the purpose of automated biometric identification or verification, or biometric templates.

9 Personal Information Use and Disclosure - Overview

CommTel may use or disclose personal information (including sensitive information) for:

- The primary purpose it was collected,
- Other related purposes that would be reasonably expected, and
- For legitimate business purposes.

This includes disclosure to CommTel's authorised External Stakeholders (Suppliers and other business affiliates). CommTel individuals authorised to use or disclose information must only do so to CommTel authorised External Stakeholders. In the event that an External Stakeholder cannot be verified, personal information must not be disclosed in any form.

It is considered that CommTel has 'disclosed' personal information where it makes it accessible to any External Stakeholder and releases the subsequent handling of the information from its effective control. Those External Stakeholders are then required under contract or through some other mechanisms to abided by the relevant parts of the Australian Privacy Principles.

In the context of 'use', it is defined where CommTel or an External Stakeholder handles the personal information or undertakes an activity with the personal information that is within its effective control.

10 Personal Information Use and Disclosure – With Consent

Personal and sensitive information may be used and disclosed between authorised CommTel individuals and External Stakeholders in all geographic locations subject to:

- The local laws in the specific geographic location allowing this section of the policy to proceed.
- The use or disclosure is required / authorised by laws in the specific geographic location.
- The individual's consent for all required use and disclosure for legitimate business activities has been obtained.
- The disclosure of the information being directly related to the primary purpose for which the information was collected.
- There is no reason to consider that the individual concerned would object to the disclosure.

- The individual providing consent for another individual to act on their behalf.

11 Personal Information Use and Disclosure – Without Consent

Personal and sensitive information may be used and disclosed between authorised CommTel individuals and External Stakeholders in all geographic locations without an individual's consent based on the following limited aspects:

- The local laws in the specific geographic location allowing this section of the policy to proceed.
- There is no reason to consider that the individual concerned would object to the disclosure.
- The use or disclosure is required / authorised by laws in the specific geographic location.
- It being necessary to:
  - Deal with a serious and imminent threat to any individual's life or health.
  - Lessen or prevent a serious threat to public health or safety.
- Where disclosure relates to law enforcement, government agency and related matters:
  - For the purpose of ascertaining the location of an individual who has been reported as a missing person.
  - Where it would be unreasonable or impracticable to collect directly from the individual as it may jeopardise the purpose of collection or the integrity of the personal information collected.
  - To prevent, detect, investigate or correct an offence where there are reasonable grounds to believe that an offence / improper conduct may have been (or is about to be) committed.
  - To assist with punishment of criminal offences, confiscation of the proceeds of crime, breaches of law imposing a penalty, sanction, diplomatic or consular functions, proceedings to or implementation of court / tribunal orders or any other allowed and legitimate purposes that relates to CommTel and the individual.

Any disclosure of information where the individual has not consented must be documented in detail, including (but not limited to) exactly what was released, the communication methods, who approved the release, the date and to whom it was released, and other information that relates to the disclosure.

12 Unsolicited Personal Information

This relates to personal information where CommTel has taken no active steps to collect the personal information, however, has received it through some form of communication.

If information becomes available through misdirection, CommTel will make a decision if the personal information is either retained, destroyed or de-identified (if lawful and reasonable) within a reasonable period of time with communication to the sender about the outcome. The decision will also consider whether the information could have been collected by CommTel directly.

In the event that personal information is provided to CommTel that is in addition to the information that has been requested, this information is treated as unsolicited personal information until further notice.

If there is difficulty deciding if the personal information received is solicited / unsolicited CommTel will review the situation within a reasonable period based on:

- The nature of the additional personal information and the connection it has with the request.
- Always being conservative and treat the personal information as unsolicited if a decision cannot be reached.

All individuals being the subject of authorised and legitimate personal information collection are to ensure that they only provide the minimum information requested. In the event that an individual believes that the information request does not meet the stated purpose, it can be raised with the CommTel Human Resources Manager.

Where a reasonable period of time is not achieved in the destruction or de-identification of the unsolicited personal information, CommTel will need to justify why the action was not taken in a reasonable period of time.

13 Trans-border Communication of Personal Information

As business requirements change and CommTel expands its operations, CommTel may need to disclose or store personal information to businesses (including parent or sister companies) or government agencies located in other geographic locations. In these instances, CommTel will comply with the personal information privacy requirements as required by legal and other requirements, including all reasonably foreseeable expectations to ensure that all personal information has sufficient protection from misuse, unauthorised access and disclosure.

For the purposes of this section, a 'geographic location' is a person or entity that receives personal information that is located outside the Commonwealth of Australia.

Personal information (including sensitive information) can be transferred / communicated about an individual to another geographic location subject to:

- The transfer is necessary for the performance of defined and legitimate business activities.
- The individual consenting to the transfer of the specific information to other geographic locations and the end use and disclosure is known to the consenting individual.
- The recipient being subject to laws that are substantially similar to the Australian Privacy Principles legislation.
- Checking that the recipient in other geographic locations has taken reasonable steps to ensure that the recipient does not breach the privacy principles in relation to the information.
- Providing conditions to the recipient on the storage, use and disclosure of the information, as well as breach reporting requirements.
- Where CommTel discloses personal information to a recipient in another geographic location, it is accountable for any acts or practices of the recipient in relation to the information that would breach the Australian Privacy Principles, except where the following exists.
- CommTel obtains valid consent from the individual whose information is being 'disclosed' and where it is (a) expressly obtained (b) plainly evident that the individual was aware that CommTel would not be taking steps to ensure the recipient complies with the Australian Privacy Principles.
- CommTel has a reasonable belief that the person or entity outside Australia is subject to laws substantially similar to the Australian Privacy Principles.

14 Access to Personal Information

CommTel allows each individual to access their own personal information. However, there are occasions where this access may be denied by CommTel, including situations where:

- Providing access would pose a serious and imminent threat to the life or health of any individual
- Providing access would have an unreasonable impact upon the privacy of other individuals
- There are existing or anticipated legal proceedings between CommTel and the individual, and the information would not be accessible by the process of discovery in those proceedings
- Providing access would reveal the intentions of CommTel in relation to negotiations with the individual in such a way as to prejudice those negotiations
- Providing access would be unlawful, and/or denial of access is required or authorised under law
- Providing access would be likely to prejudice an investigation of possible unlawful activity.

Where providing access would reveal evaluative information generated within CommTel in connection with a commercially sensitive decision-making process, CommTel may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Where CommTel is not required to provide the individual with access to the information then CommTel must, if reasonable to do so, consider whether the use of mutually agreed mediators would allow sufficient access to meet the needs of both parties.

If CommTel charges for providing access to personal information, those charges must not be excessive, and any cost must be informed up front.

15 Working with Personal Information

CommTel Individuals working with any personal information (including sensitive) will:

- Maintain confidentiality of all information regarding individual's information retained or known.
- Protect information in their control and report any breaches of this policy.

- Only disclose information to CommTel authorised External Stakeholders.
- Contact the Human Resources Manager immediately if they are unsure about any use or disclosure of personal information (including sensitive information).
- Inform any External Stakeholder of the privacy requirements related to:
  - Not disclosing information to any other unauthorised individual.
  - How the information is to be managed.

It is a breach of this policy to discuss / share confidential information (verbal, written or and any other transmissible format) with individuals that are not authorised to have access.

16 Maintaining Personal Information

CommTel will ensure that the personal information it retains is kept up to date as required for business, External Stakeholder, legal and other requirements. Each individual can also request or provide an update to their personal information.

In the event that a disagreement occurs between the individual and CommTel in relation to the accuracy of the information, a written note will be retained on the individuals file pertaining to the accuracy and disagreement.

All access and updates (correction, change, addition or other) to personal information are to be directed to the CommTel Human Resources Manager.

17 Retention and Disposal of Personal Information

All personal information (including sensitive information) will be retained as required by legal or other requirements, as outlined in the company Retention Schedule.

All personal information (including sensitive information) will be disposed of securely when no longer required for business or legal reasons.

18 Outsourced Personal Information Management

When approval to release / outsource personal information to an External Stakeholder for management exists, a contract should be considered to allow CommTel to retain the right to access and amend it if required. The contract will also need to cover the storage, disclosure, access and use within the External Stakeholder to ensure that the Australian Privacy Principles are maintained.

Where CommTel engages a recipient contractor located in another geographic location to perform services on its behalf, the personal information to that contractor is a disclosure. This means that CommTel will need to comply with Trans-borders provisions before making that disclosure. Where a subcontractor may be engaged by the recipient contractor, they should also take reasonable steps to ensure that the subcontractor does not breach the Australian Privacy Principles in relation to the personal information.

19 Direct Marketing

This involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services for promotion, information or sale. In the event CommTel is permitted to use or disclose personal information for the purpose of direct marketing, it will:

- Allow an individual to request not to receive direct marketing communications by allowing an opt-out or unsubscribe.
- Comply with the communicated request with a reasonable time after a request is made.
- On request and where practicable and reasonably justifiable, CommTel will provide its source for an individual's personal information. Factors related to the following areas may impact disclosure:
- Possible adverse consequences for the individual if they are not notified of the source.
- Length of time that has elapsed since the information was collected.
- Time, inconvenience and cost involved for retrieval.
- Direct marketing can be accepted where the:

- Individual would have reasonably expected their personal information to be used for the purpose of direct marketing.
- Collection and use has occurred with permission from the individual directly.

20 Information Security

CommTel is committed to protecting personal information and privacy through various safeguards and will take reasonable steps to keep personal and business information protected from loss, misuse, unauthorised access, modification and disclosure.
CommTel uses a variety of physical and electronic security measures. These include restricting physical access to its offices and electronically using firewalls, routers, network and host intrusion detection systems, appropriate encryption, and secure databases.
Access to personal information is restricted to authorised personnel and related external stakeholders that have permission.

The Internet and any electronic transmission to CommTel may occur in an unsecure environment. Any information sent to CommTel through the Internet or other electronic methods are to consider if encryption of information is required. Information either sent physically or electrically is sent at the sender's own risk.

21 Data Security

CommTel maintains administrative, technical, and physical safeguards that are designed to be appropriate to its operating environment and risk profile, which may include:

- Logical access controls and authentication measures to limit access to authorised personnel
- Use of encryption and other protective technologies where appropriate to reduce the risk of unauthorised access.
- Security monitoring, testing, and review activities to help identify and manage vulnerabilities
- Policies, procedures, and training to support staff awareness of privacy and data protection obligations.

Specific safeguards may vary depending on the system, service, or data set involved, and are reviewed periodically to ensure they remain appropriate.

22 Cross Border Disclosure

CommTel ensures that any overseas data transfers comply with APP 8, verifying that the recipient country has adequate data protection laws or obtaining consent from the individual.

23 Data Breach Response

CommTel follows the Notifiable Data Breaches (NDB) scheme:

- Assess suspected breaches promptly.
- Notify affected individuals and the Office of the Australian Information Commissioner (OAIC) and relevant EU supervisory authorities if required
- Mitigate risks and prevent recurrence.

24 Access and Correction

Individuals may request access to or correction of their personal information by contacting CommTel's Security Manager. Requests will be handled in accordance with APP 12 and 13.

25 Training and Awareness

CommTel provides regular training to employees on privacy obligations, data handling procedures, and breach response protocols.

26 CommTel's Website

CommTel's website (extranet / main business website) provides external hyperlinks to other websites owned and controlled by others. These external websites are governed by their own privacy policy and each individual using these links do so at their own discretion.
Each individual using CommTel's website consents to the collection, use and disclosure of personal information as defined in this policy.

27 Use of Cookies

Cookies provide information to CommTel about recognising any device (Desktop, laptop, tablet, mobile phone or any other equipment or device) that connects to its website, however it does not identify the individual.
Information is collected about an individual's use of the CommTel website for improvement purposes and does not access any information stored on the access device. Cookies are installed on the device to obtain information only where the individual consents.

CommTel may use cookies to:

- Count visitors to the website, movement around the website, residence time, date, number of clicks and page visits and other attributes.
- Define the geographic location of the source access.
- Collect information about the device (IP address, operating system, Web browser and other available attributes).

28 Complaints and Further Information

If any individual has questions or concerns related to data protection and privacy, contact the CommTel Human Resources Manager or General Manager.

29 Records

Monitoring and measurement of this policy is completed through the version control and documented reviews.

30 Legislation, Codes of Practice & Standards

Legislation	Codes of Practice	Standards
Privacy Act 1988 (Cth), as amended, most recently by the Privacy and Other Legislation Act 2024 (Cth)	**VIC** – None issued **ACT** – None issued **NSW** - None issued **QLD** - None issued **NT** - None issued **WA** – None issued **SA** – None issued **TAS** - None issued	• ISO9001-2015 Quality management systems • ISO45001-2018 OHS management system • ISO14001-2015 Environmental management system • ISO27001-2022 Information Security management system