Privacy Policy

Contents

Privacy Policy

Purpose

The purpose of this policy is to outline how Comstar complies with applicable laws and Australian Privacy Principles as it gathers, uses, discloses, and manages **personal information** belonging to employees, contractors, customers and other parties.

See also – 'Information Security' section of the *Administration Manual - IT and Cyber Security.*

Scope

This policy applies to all Comstar Systems operations and includes the management of **personal information** communicated via Comstar' s key operational functions outlined in Table 1. This policy:

- Specifies applicable laws regarding Comstar's handling of personal information
- Specifies Comstar's obligations for handling personal information of past, present and prospective employees, contractors and customers
- Informs Comstar employees of the privacy obligations they must comply with
- Includes a Website Privacy Statement
- Outlines Comstar's process for responding to suspected data breaches and complaints from individuals and customers that their personal information has not been dealt with in accordance with this policy.

Applicable Laws

Comstar, 'as a contractor that provides services under a Commonwealth contract':

- is subject to the ***Privacy Act 1988 (Cth)***
- may be subject to the ***Freedom of Information Act (Cth)*** if the Commonwealth contract specifies FOI obligations.

The ***Fair Work Regulations 2009 (Cth)*** apply to Comstar regarding the management of employee and previous employee records and their access to the records.
The ***Privacy (Tax File Number) Rule 2015*** is a legislative instrument made under **section 17 of the Privacy Act 1988**. This rule regulates the collection, storage, use, disclosure, security and disposal of individuals' Tax File Number information.

See also: Privacy Checklist for Small Business, Office of the Australian Information Commissioner website.

Note: Employee information is exempt from provisions of the ***Personal Information Protection Act 2004 (Tas)***.

Related Documents

Website Privacy Statement	*Records Management Procedure*
Health and Exposure Monitoring Procedure	*IT and Cyber Security Policy*
Administration Manual - IT and Cyber Security	*Administration Manual - Training*
IT & Cyber Security Declaration Form	*Employment Procedure*
Incident Report Form -Quality OFI-NCR	*Drug and Alcohol Procedure*

Definitions

Personal information is any information or opinion about an identified individual, or an individual who is reasonably identifiable but does not include personal information in a publicly available record or publication.

Personal data means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.

Consent means any freely given, specific, informed and unambiguous indication of an individual's wish by which the individual, by a statement or by a clear affirmative action, signifies agreement to the collection, use or disclosure of personal or health information or the processing of personal data relating to that individual.

Processing (in relation to personal data) means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Who is Responsible for Privacy

All Comstar employees have a role to play in ensuring privacy is respected and protected.

The **HR Coordinator**, as Comstar's **Privacy Officer** shall:

1. be responsible for privacy and maintain a sound understanding of this policy and the Privacy Act
2. handle access and correction requests and complaints and enquiries about Comstar personal information handling practices

See also: 'Requesting Access to your Personal Information', 'Making a Complaint about Privacy Breaches' and 'Feedback and Complaints' (in the Website Privacy Statement).

Collection of Personal Information

In this policy, a reference to "personal information" includes "personal data". Comstar will collect personal information only where it is necessary for conducting its' functions and activities as outlined in Table 1.

Reasonably Necessary Test

The Australian Privacy Principle (APP3.18) deems that the Reasonably Necessary Test is an objective test: whether a reasonable person who is properly informed would agree that the collection is necessary. This means that, Comstar or any of our customers must be able to justify that the particular collection of personal information is 'reasonably necessary'.

Example: A Driver's Licence

A driver's Licence contains personal information with significant potential for identity theft (ie: Licence number, photo, name, DOB, address, and signature) and therefore disclosure of this information must be very limited.

Comstar has a duty of care to ensure that a person who drives a workplace vehicle is Licenced to drive that class of vehicle.

We can minimize the risk of identify theft and fulfill our duty of care with following process:

1. The employee completes and signs a declaration containing the driver's name, Licence number and expiry date.
2. An authorised Comstar representative:
    a. sights the original Licence using the Licence photo to verify the holder's identity
    b. Signs the declaration as a witness and confirming the ID is correct.
3. The only information disclosed to third parties by Comstar, is the declaration
4. The Licence holder is still required to present the Licence on demand to a representative of Comstar, or our customers.

Table 1: When is Personal Information Collected & shared?

Function	Personal information required / potentially required

Employment of staff	Comstar HR / administration personnel:
	• Name
	• Address (residential, postal and email)
	• Phone number
	• Gender
	• Bank account details
	• Tax file number
	• Superannuation fund details
	• Police Checks /Criminal Record – see **Sensitive Information** section.
	• Health information where it can affect the individual's health and safety or health and safety of others in the workplace eg:
	  ○ 'fit to climb' medical certificate
	  ○ drug and alcohol testing
	• Hazard exposure and health monitoring eg:
	  ○ Audiometric testing
	  ○ Allergies which might potentially affect a worker and which could be aggravated by the work environment / activities.
	• Education and employment history details
	• Emergency contact details
	• Academic records, certificates of achievement/ competency, inductions
	• Licences & ID Cards:
	  ○ Driver's Licence (Licence #, photo, name, DOB, address, and signature)
	  ○ Construction Industry White Card (Card #, name, DOB and signature)
	  ○ High Risk Work Licence (Licence #, photo, name, DOB and signature)
	
	Records
	All Comstar records for this function are retained in the Administration area in secured filing cabinets. Electronic records are retained in the P drive with restricted access permissions in accordance with the *Records Management Procedure* and the *IT & Cyber Security Procedure.* All archived records are retained in the locked archive store in accordance with the *Records Management Procedure.*
	See also - **Disclosing Personal Information to Third Parties**.

Development and delivery of projects & related services	Clients/Customers will have access to the following personal information:
	• Name
	• Certificates of competency & inductions
	• Training records eg: refresher training for tower rescue
	• Police Checks (unless this is unfavorable eg: the person has a Criminal Record – in which case, the information would be withheld) – see also **Sensitive Information** & **Disclosing Personal Information to Third Parties.**
	• Licences & ID Cards:
	  ○ Driver's Licence (Licence #, photo, name, DOB, address, and signature)
	  ○ Construction Industry White Card (Card #, name, DOB and signature)
	  ○ High Risk Work Licence (Licence #, photo, name, DOB and signature)
	• Logs and registers eg: training information
	
	Records
	All Comstar records for this function are retained in the Administration area in secured filing cabinets. Electronic records are retained in the P drive with restricted access permissions in accordance with the *Records Management Procedure* and the *IT & Cyber Security Procedure.* All archived records are retained in the locked archive store in accordance with the *Records Management Procedure.*
	See also - **Disclosing Personal Information to Third Parties**.

Table 1 - continued

Function	Personal information required & disclosed to 3rd Parties
Management of wages/ salaries & related financial matters	The following entities will have access to personal information: Tax office: • Tax file number • Salary, income and taxation details Superannuation Funds: • Information related to Superannuation payments TasBuild: • Information related to Long Service leave payment Company accountants & Xero/Workflowmax (payroll service provider): • Name • Address (residential, postal and email) • Phone number • Gender • Bank account details • Tax file number • Superannuation fund details • Salary, income and taxation details **Records** All Comstar records for this function are retained in the Administration area in secured filing cabinets. Electronic records are retained in the P drive with restricted access permissions in accordance with the *Records Management Procedure*; and off-site in Xero/Workflowmax cloud-based software. All archived records are retained in the locked archive store in accordance with the *Records Management Procedure.* See also - **Disclosing Personal Information to Third Parties**.

On-boarding of sub-contractors	Clients/Customers will have access to the following personal information:
	• Name of sub-contractor employee
	• Certificates of competency & inductions
	• Insurance certificates – professional indemnity, Income protection etc
	• Training records eg: refresher training for tower rescue
	• Licences & ID Cards:
	  ○ Driver's Licence (Licence #, photo, name, DOB, address, and signature)
	  ○ Construction Industry White Card (Card #, name, DOB and signature)
	  ○ High Risk Work Licence (Licence #, photo, name, DOB and signature)
	• Photographs of individuals at worksites
	• Logs and registers eg: training information
	
	Records
	All Comstar records for this function are retained in the Administration area in secured filing cabinets. Electronic records are retained in the P drive with restricted access permissions in accordance with the *Records Management Procedure.* All archived records are retained in the locked archive store in accordance with the *Records Management Procedure.*

Table 1 - continued

Function	Personal information required / potentially required

Audits – including: External audits by 3rd Parties, Internal management systems audits & field audits	External & internal auditors are required to verify that information and records are correct and will have access to the following personal information:
	• Name
	• Certificates of competency & inductions
	• Training records eg: refresher training for tower rescue
	• Licences & ID Cards:
	  ○ Driver's Licence (Licence #, photo, name, DOB, address, and signature)
	  ○ Construction Industry White Card (Card #, name, DOB and signature)
	  ○ High Risk Work Licence (Licence #, photo, name, DOB and signature)
	• Random drug and alcohol test results
	• Photographs of individuals at worksites and on ID cards
	• Logs and registers eg: training information
	
	Records
	All Comstar records for this function are retained in the Administration area and with the QEHS Manager. Electronic records are retained in the P drive with restricted access permissions in accordance with the *Records Management Procedure.* All archived records are retained in the locked archive store in accordance with the *Records Management Procedure.*
	See also - **Disclosing Personal Information to Third Parties**.

Incident investigations & performance management	Comstar and/or customer investigator, HR consultants and sometimes the regulator eg: WorkSafe will have access to the following personal information:
	• Name
	• Certificates of competency & inductions
	• Training records eg: refresher training for tower rescue
	• Licences & ID Cards:
	  ○ Driver's Licence (Licence #, photo, name, DOB, address, and signature)
	  ○ Construction Industry White Card (Card #, name, DOB and signature)
	  ○ High Risk Work Licence (Licence #, photo, name, DOB and signature)
	• Photos of individuals, signatures on site documents, Licences etc
	• Drug and alcohol test results
	• Observed information about the conduct or activities of a person
	• Photographs or video recordings (including CCTV footage)
	• Logs and registers eg: training information
	• IT access logs
	• Identifiable data (eg IP address) collected via a website, mobile application, email, wifi or online service, including by cookies or related technology, location information from a mobile device (because it can reveal user activity patterns and habits)
	
	Records
	All Comstar records for this function are retained in the Administration area in secured filing cabinets (incident report forms are retained by the QEHS Manager). Electronic records are retained in the P drive with restricted access permissions in accordance with the *Records Management Procedure.* All archived records are retained in the locked archive store in accordance with the *Records Management Procedure.*
	See also - **Disclosing Personal Information to Third Parties**.

Table 1 - continued

Function	Personal information required / potentially required
Management of sick leave information	Sick leave applications are submitted to the administration office and are processed with restricted access, in most cases only the Executive Assistant, Accountant, line manager and MD, will have access to the following personal information: • Medical Certificates – for more than 2 consecutive days leave In some cases where a person needs special consideration (eg: restricted functional capacity) requiring task restrictions and if this can be accommodated by the business, other Comstar personnel on a 'need to know' basis only), will have access to the following personal information: • Functional capacity details – eg: restricted duties • Relevant injury details **Records** All Comstar records for this function are retained in the Administration area in secured filing cabinets. Electronic records are retained in the P drive with restricted access permissions in accordance with the *Records Management Procedure.* All archived records are retained in the locked archive store in accordance with the *Records Management Procedure.*
Return to Work (RTW) & Injury Management, **Workers Compensation Claims & health monitoring**	Comstar RTW Coordinator, insurance company representative, Rehabilitation service providers, treating medical practitioners, independent medical practitioners as required, (and other Comstar personnel on a **'need to know' basis only**), will have access to the following personal information: • Name • Address (residential, postal and email) • Phone number • Gender • Medical Certificates, limited treatment and medications information • Functional capacity details – eg: restricted duties • Relevant injury details **Records** All Comstar records for this function are retained in the Administration area in secured filing cabinets. Electronic records are retained in the P drive with restricted access permissions in accordance with the *Records Management Procedure.* All archived records are retained in the locked archive store in accordance with the *Records Management Procedure.* See also - **Disclosing Personal Information to Third Parties**.

Table 1 - continued

Function	Personal information required / potentially required

Hazard exposure monitoring	To meet our WHS duty of care to **monitor hazard exposures in the workplace**, measurements are sometimes required eg: noise levels and EME exposure when working near RF equipment. Our workers have a right to information regarding hazards and the results of hazard exposure monitoring shall be anonymized where practicable before distribution to our Workers. The QEHS Manager and RTW Coordinator shall have full access (and other Comstar personnel on a **'need to know' basis only**), will have access to the following personal information:
	• Hazard exposure and health monitoring eg:
	  ○ Records of exposure to noise, RF/EME etc
	  ○ Audiometric testing
	  ○ Allergies which might potentially affect a worker and which could be aggravated by the work environment / activities.
	
	This information will be shared with customers if it is incident related – see also 'Incident investigations & performance management'.
	Records
	All Comstar records for this function are retained in the Administration area in secured filing cabinets. Electronic records are retained in the P drive with restricted access permissions in accordance with the *Records Management Procedure.* All archived records are retained in the locked archive store in accordance with the *Records Management Procedure.*
	
	See also - **Disclosing Personal Information to Third Parties**.

Function	**Personal information required / potentially required**
Monitoring security of Comstar Premises	Comstar use security cameras and video recording systems to manage security at work premises. Signage is displayed at each area where cameras are in use and the video monitors are only viewable in the front administration office. **Records** All Comstar video records for this function are retained in the Comstar IT Server with access only with Managing Director authorization and it is restricted to the IT Supervisor, Executive Assistant & Managing Director. All archived records are retained in the locked archive store in accordance with the *Records Management Procedure.* See also - **Disclosing Personal Information to Third Parties**.
Function	**Personal information required / potentially required**
Identification of visitors to the Comstar website.	Comstar Systems may collect personal information and other data from visitors to our website through the use of a Cookie or other automated means including server logs. A Cookie is a packet of data that our website puts on the visitor's computer hard drive to identify them as a visitor to that website. The information may include the visitor's server address; domain name; IP address; the date and time of the visit; the pages accessed and documents downloaded; the previous site visited; the type of browser used. Visitors may choose to disallow Cookies through their web browser settings. **Records** All Comstar records for this function are retained in the Comstar IT Server with access restricted to the IT Supervisor. All archived records are retained in accordance with the *Records Management Procedure.* See also - **Disclosing Personal Information to Third Parties**.

Access to Personal Information

Comstar shall take reasonable steps to protect personal information from misuse, loss, disclosure and unauthorised access. Personal information **shall only be disclosed to persons on a 'need to know' basis**:

- For the purpose for which it was collected
- For a related purpose which you might reasonably expect
- As otherwise required by law.

Anonymised Information & De-Identification

Comstar will make reasonable efforts to anonymise personal information before disclosure to a wider audience eg:

- Incidental site photos (no faces displayed)
- hazard exposure monitoring records

This means that an individual will not be identified by the records if they must be disclosed to a customer for contractual reasons.
However, the small workforce at Comstar means that an individual may be easily identified by other means eg: Co- workers who were present on the worksite at the time of hazard monitoring.

De-Identification

Comstar will make reasonable efforts to de-identify personal information before disclosure to a wider audience. See - Example: A Driver's Licence

Sensitive Information

Sensitive information generally requires **a higher level of privacy protection** than other personal information. Inappropriate handling of sensitive information can have adverse consequences for an individual or those associated with the individual. Sensitive Information includes:

1) information or an opinion (that is also personal information) about an individual's:
   a) racial or ethnic origin
   b) political opinions
   c) membership of a political association
   d) religious beliefs or affiliations
   e) philosophical beliefs
   f) membership of a professional or trade association
   g) membership of a trade union
   h) sexual orientation or practices, or
   i) criminal record
2) health information about an individual
3) genetic information (that is not otherwise health information)
4) biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or

5) biometric templates

Comstar does not collect personal information concerning items 1a-h and items 3, 4 & 5.
See Table 1 for how health information is managed.

Disclosing Personal Information to Third Parties

Before disclosing personal information to a third party (eg customer), Comstar shall specify in writing (eg: email) the following conditions required of the recipient:

- That they will take reasonable steps to protect personal information from misuse, loss, disclosure and unauthorised access; and
- That they manage personal information in accordance with the *Privacy Act 1988 (Cth)* and Australian Privacy Principles (or an equivalent regulatory framework).
- Any information regarding a person's criminal records shall not be disclosed to third parties without authorisation from the Managing Director.

As a minimum, all Comstar emails shall contain a footer that includes the conditions specified above.

Data Security

Comstar will take reasonable steps to protect personal information from misuse, loss, interference, unauthorised access or modification, and disclosure.

IT and Cyber Security

Comstar manages IT and cyber security in accordance with AS27001 – Information Technology – Security techniques – information security management systems – requirements. We are committed to the responsible management of access to our IT network as well as access to client networks. This is achieved using data management protocols, restricted access permission levels, backup processes, secure firewalls and facilities. Employees and other Comstar IT network users are required to sign the IT & Cyber Security Declaration Form which outlines their confidentiality and intellectual property (IP) obligations. For details refer to:

- *IT and Cyber Security Policy*
- *Administration Manual - IT and Cyber Security*
- *IT & Cyber Security Declaration Form*
- *Records Management Procedure*

Destruction of Personal Information

In accordance with the *Records Management Procedure,* hard copy and electronic records containing personal information are retained by Comstar for a period of 7 years and sometimes longer if required by legislation eg: asbestos related health records.

When the records retention (archive) period has expired, hard copy documents, including expired archival documents, shall be placed by an authorised person, directly into a locked security bin for destruction by a specialist contractor.

Electronic records containing personal information shall be destroyed by the IT & Cyber Security Specialist in accordance with the *Administration Manual - IT and Cyber Security*, Media Handling section which requires destruction by either overwriting, use of specialist software to destroy the data or by physical destruction of the drive.

Requesting Access to your Personal Information

Access and amendment requests, complaints and other privacy enquiries will be managed in accordance with the process outlined below and should be directed to:

Privacy Officer (HR Coordinator)
17 Brisbane Street Hobart, Tasmania Australia 7000
P: (03) 6231 0150
F: (03) 6231 0219
E: contact@comstarsystems.com.au

You can request a copy of your employment records from a current or former employer (Fair Work Regulations 2009).

You can also request amendment to personal information if you believe that it is incorrect or make complaints about the information handling practices of Comstar or breaches of your privacy by Comstar.

Making a Complaint about Privacy Breaches

Complaints Process

Complaints will be investigated and where possible a response provided **within 7 working days**. If delays occur the complainant will be kept informed of progress and when a response is likely to be given.

Step 1 – Receiving the complaint

Privacy complaints should be directed to the **Privacy Officer** who will take all complaints seriously and collect the necessary details to address the matter appropriately. Informal (verbal) complaints may be accepted but the Managing Director reserves the right to require that a complaint be made in writing before proceeding further.

Step 2 – Investigating the complaint

The **Privacy Officer** will investigate the complaint in a timely manner, liaising with Comstar personnel and others as required. The investigation shall take into account:

- The reasons why the information needed to be collected and disclosed
- The effectiveness and appropriateness of the collection and disclosure process
- The immediate causes and root of the problem
- The corrective actions required to address issues raised by the complaint
- Any necessary changes or improvements to the collection and disclosure process to prevent a similar situation arising again

Step 3 – Presentation of Findings

The **Privacy Officer** will verbally inform the complainant of the investigation findings of the and any corrective actions proposed/already taken.

The investigation findings shall be documented by the Privacy Officer, who shall ensure that root causes of the privacy breach and that corrective measures are identified. At the discretion of the Managing Director, a copy of the report may be provided to the complainant upon request.

Step 4 – Record Keeping

Records of all privacy complaints shall be maintained by the **Privacy Officer** in the P: drive at P:/Human Resources/Privacy/……. Records of privacy complaints shall include any documents including all correspondence and minutes of discussions/meetings associated with the complaint.

Using IT access permission levels, **access to these records is restricted** to the Privacy Officer, Executive Assistant and Managing Director.

Malicious or Vexatious Complaints

All complaints will be treated with the utmost seriousness, however if a complaint is found to be **malicious or vexatious**, or it is a repeated complaint to which a response has previously been given, no further action may be taken on the complaint. **The Managing Director may deem it appropriate to avoid any further communication with the complainant or refer the matter to the Office of the Australian Information Commissioner for a ruling.**

Website Privacy Statement

All personal information collected by Comstar Systems through our website shall be used, stored and disclosed in accordance with the with the *Privacy Act 1988 (Cwth)*, Personal Information Protection Act 2004 (Tas), the Comstar Systems Privacy Policy, and this privacy statement.

The Comstar Systems Privacy Policy is available from Comstar's Privacy Officer upon request.

Personal information is any information or opinion about an identified individual, or an individual who is reasonably identifiable but does not include personal information in a publicly available record or publication.

Comstar Systems is not responsible for the privacy practices of web sites external to Comstar Systems.

Automatic Collection of Personal Information

Comstar Systems may collect personal information and other data from visitors to our website through the use of a Cookie or other automated means including server logs. A Cookie is a packet of data that our website puts on the visitor's computer hard drive to identify them as a visitor to that website. The information may include the visitor's server address; domain name; IP address; the date and time of the visit; the pages accessed, and documents downloaded; the previous site visited; the type of browser used. Visitors may choose to disallow Cookies through their web browser settings.

Disclosure of Information to Third Parties

Comstar Systems may disclose personal information to a third party if the disclosure is necessary to prevent or lessen a serious and imminent threat to health and safety or to manage cyber security risks. More detailed information about how Comstar Systems manages personal information is provided in our *Privacy Policy*.

Feedback and Complaints

If you believe that Comstar is holding personal information that is inaccurate, incomplete or out of date, please contact Comstar's Privacy Officer and we will revise the relevant information. Make sure that you provide a name, phone number and email address for the purpose of receiving a reply. This information will only be used for the purpose for which it was provided and your name and email address will not be added to any mailing list by Comstar Systems.

Feedback and Complaints should be directed to:

Privacy Officer (HR Coordinator)

17 Brisbane Street Hobart, Tasmania Australia 7000
P: (03) 6231 0150
F: (03) 6231 0219
E: contact@comstarsystems.com.au