# DATA POLICY

We take our obligations to protect data and personal information seriously. We are bound and abide by the Australian Privacy Principles in the *Privacy Act 1988* (Cth) (**Privacy Act**) and all dealings with Data and Personal Information will be conducted in accordance with the obligations contained within this Data Policy.

1. **DEFINITIONS**

1.1. Capitalised expressions in this Policy have the corresponding meanings given in Paragraph 1.2.

1.2. **Data:** all data that we hold or have control over and therefore to which this Policy applies. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both Personal Information and Non-personal Information. In this Policy we refer to this information and these records collectively as **Data**.

a. **Data Protection Officer (DPO):** our Data Protection Officer is responsible for identifying the Data that we must or should retain and determining the proper period of retention. They also arrange for the proper storage and retrieval of Data, coordinating with outside vendors where appropriate and handling the destruction of records whose retention period has expired, in accordance with Paragraph 8.2. They are also responsible for the protection and timely destruction or de-identification of Personal Information in accordance with applicable legal and regulatory obligations for Personal Information.

b. **Data Retention Policy:** this Policy, which explains our requirements to retain Data and to dispose of Data and provides guidance on appropriate Data handling and disposal.

c. **Data Retention Schedule:** Annex A attached to this Policy which sets out retention periods for our Formal or Official Records.

d. **Disposable Information:** consists of Data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose or Data that may be safely destroyed in accordance with Paragraph 8.2 because it is not a Formal or Official Record as defined by this Policy and the Data Retention Schedule.

e. **Formal or Official Record:** certain Data is more important to us and is therefore listed in the Data Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. We refer to this as Formal or Official Records or Data.

f. **Non-personal Information:** Data which does not identify living individuals, either because it is not about living individuals (for example, the organisation's financial records) or because it has been fully anonymised.

g. **Notifiable Data Breach:** under the Notifiable Data Breaches scheme (**NDB scheme**) in the Privacy Act, any unauthorised access or disclosure of Personal Information, or risk of unauthorised access or disclosure to Personal Information that a reasonable person would conclude is likely to result in serious harm is taken to be a notifiable breach. This means that, pursuant to the NDB scheme, notification of the breach must be given to the Australian Information Commissioner (**Information Commissioner**) who is responsible for enforcing privacy regulations in Australia.

h. **Personal Information:** any information or an opinion about an identified individual or an individual who can be reasonably identified from the information or opinion. Information or an opinion may be Personal Information regardless of whether it is true. It includes special categories of Personal Information such as health information (including contact tracing information) (see Sensitive Information).

i. **Sensitive Information:** a sub-set of Personal Information defined under the Privacy Act (see section 6) which includes health information. Sensitive Information is subject to a higher level of privacy protection under the Privacy Act and additional obligations are imposed on APP entities under the APPs with regard to the collection and handling of Sensitive Information.

## 2. ABOUT THIS POLICY

2.1. The Data of NCI Group Australia Pty. Limited ABN 75 126 789 099 (**NCI**) and Assure GP Pty Ltd ABN 92 658 410 747 (**AGP**) and our subsidiaries is important to how we conduct business and manage employees.

2.2. There are legal and regulatory requirements for us to retain certain Data, usually for a specified amount of time. We also retain Data to help our business operate and to have information available when we need it. However, we do not retain all Data indefinitely. Data containing Personal Information is subject to additional legal and regulatory obligations including *APP 11* which requires an organisation to take reasonable steps to destroy or de-identify Personal Information it holds once that Personal Information is no longer needed for any purpose for which it may be used or disclosed under the Australian Privacy Principles (**APPs**) (subject to law or a court order to retain the personal information or where the personal information is contained in a Commonwealth record). Retaining Data can expose us to risk as well as be a cost to our business.

2.3. This Policy explains our requirements to retain Data and to dispose of Data and provides guidance on appropriate Data handling and disposal, destruction or de-identification. It includes and should be read together with the Data Retention Schedule in Annex A.

2.4. Failure to comply with this Policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.

2.5. This Policy does not form part of any employee's contract of employment, and we may amend it at any time.

## 3. SCOPE OF POLICY

3.1. This Policy covers all Data we hold or have control over.

3.2. This Policy covers Data that is held by third parties on our behalf, for example, cloud storage providers or offsite records storage.

3.3. This Policy explains the differences between our Formal or Official Records, documents, Disposable Information, confidential information belonging to others, Personal Information and Non-personal Information. It also gives guidance on how we classify our Data.

3.4. This Policy applies to all business units and functions of NCI and AGP in Australia.

## 4. GUIDING PRINCIPLES

4.1. Through this Policy, and our Data retention practices, we aim to meet the following commitments:

a. We comply with legal and regulatory requirements to retain Data.

b. We comply with our Data protection obligations, in particular to keep Personal Information no longer than is necessary.

c. We handle, store and dispose of Data responsibly and securely.

d. We create and retain Data where we need this to operate our business effectively, but we do not create or retain Data without good business reason.

e. We allocate appropriate resources, roles and responsibilities to Data retention.

f. We regularly remind employees of their Data retention responsibilities.

g. We regularly monitor and audit compliance with this Policy and update this Policy when required.

## 5. ROLES AND RESPONSIBILITIES

5.1. **Data Protection Officer (DPO).** The DPO is responsible for advising on and monitoring our compliance with data protection laws which regulate Personal Information. Our DPO works with our Privacy Officer on the retention requirements for Personal Information and on monitoring compliance with this Policy in relation to Personal Information.

5.2. **Responsibility of all employees.** We aim to comply with the laws, rules and regulations that govern our organisation and with recognised compliance good practices. All employees must comply with this Policy, the Data Retention Schedule, any communications suspending Data disposal, including the

destruction or de-identification of Personal Information, and any specific instructions from the DPO. Failure to do so may subject us, our employees, and contractors to serious civil or criminal liability, or both. An employee's failure to comply with this Policy may result in disciplinary sanctions, including suspension or termination. It is therefore the responsibility of everyone to understand and comply with this Policy.

5.3. **DPO.** The DPO is responsible for identifying the Data that we must or should retain, and determining the proper period of retention. It also arranges for the proper storage and retrieval of Data, coordinating with outside vendors where appropriate. Additionally, the DPO handles the destruction of records whose retention periods have expired, in accordance with Paragraph 8.2.

5.4. We have designated Darren Miller as the DPO. The DPO is responsible for:

a. Administering the Data governance program.

b. Helping department heads implement the Data governance program and related best practices.

c. Planning, developing and prescribing the Data disposal policies, systems, standards and procedures in accordance with Paragraph 8.2.

d. Providing guidance, training, monitoring and updating in relation to this Policy.

## 6. TYPES OF DATA AND DATA CLASSIFICATION

6.1. **Formal or Official Records.** Certain Data is more important to us and is therefore listed in the Data Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. Please see Paragraph 7.1 below for more information on retention periods for this type of Data.

6.2. **Disposable Information.** Disposable Information consists of Data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose or Data that may be safely destroyed in accordance with Paragraph 8.2 because it is not a Formal or Official Record as defined by this Policy and the Data Retention Schedule. Examples may include:

a. Duplicates of originals that have not been annotated.

b. Preliminary drafts of letters, memoranda, reports, worksheets and informal notes that do not represent significant steps or decisions in the preparation of an official record.

c. Books, periodicals, manuals, training binders and other printed materials obtained from sources outside of NCI and AGP and retained primarily for reference purposes.

d. Spam and junk mail.

Please see Paragraph 7.2 below for more information on how to determine retention periods for this type of Data.

6.3. **Personal Information.** Both Formal or Official Records and Disposable Information may contain Personal Information (including Sensitive Information); that is, Data that contains information or an opinion about an identified individual or an individual which is reasonably identifiable whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not (section 6, Privacy Act). We are committed to handling Personal Information in accordance with our Privacy Policy. See Paragraph 7.3 below for more information on this.

6.4. **Confidential information belonging to others.** Any confidential information that an employee might have obtained from a source outside of NCI and AGP, such as from a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted or destroyed.

## 7. RETENTION PERIODS

7.1. **Formal or Official Records.** Any Data that is part of any categories listed in the Data Retention Schedule contained in Annex A to this Policy, must be retained for the amount of time indicated in the Data Retention Schedule. A record must not be retained beyond the period indicated in the Data Retention Schedule, unless a valid legal or business reason (including a notice to preserve documents for contemplated litigation or other special situation) calls for continued retention. If you are unsure whether a certain record will be retained, contact the DPO**.**

7.2. **Disposable Information.** The Data Retention Schedule will not set out retention periods for Disposable Information. This type of Data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of in accordance with Paragraph 8.2.

7.3. **Personal Information.** The Privacy Act requires us to take reasonable steps to protect Personal Information (including Sensitive Information) and to destroy or de-identify Personal Information once it is no longer needed for any purpose for which it may be used or disclosed under the APPs (subject to legal requirements for retention of the Data, other laws and where personal information is contained in a Commonwealth record). More information can be found in our Privacy Policy.

## 8. STORAGE, BACK UP AND DISPOSAL OF DATA

8.1. **Storage.** Our Data must be stored in a safe, secure, and accessible manner. Any document and financial files that are essential to our business operations during an emergency must be duplicated or backed up at least once per week and maintained off-site, or both.

8.2. **Destruction.** Our DPO is responsible for the continuing process of identifying the Data that has met its required retention period and supervising its destruction. The

destruction of confidential, financial, and employee-related hard copy Data must be conducted by secure shredding. Non-confidential Data may be destroyed by recycling. The destruction of electronic Data must be coordinated with NCI and AGP's IT provider.

9. **PRESERVATION OF DOCUMENTS FOR CONTEMPLATED LITIGATION AND OTHER SPECIAL CIRCUMSTANCES**

9.1. The destruction of Data must stop immediately upon notification that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation. Destruction may begin again once the requirement for preservation is lifted.

9.2. We require all employees to comply fully with our Data Retention Schedule and procedures as provided in this Policy. All employees should note the following general exception to any stated requirements of a destruction schedule: if you believe, or you are informed that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit or other event, you must preserve and not delete, dispose, destroy or change those records, including emails and other electronic documents, until it is determined those records are no longer needed. Preserving documents includes suspending any requirements in the Data Retention Schedule and preserving the integrity of the electronic files or other format in which the records are kept.

9.3. If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the DPO.

9.4. In addition, you may be asked to suspend any routine Data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

10. **WHERE TO GO FOR ADVICE AND QUESTIONS**

10.1. **Questions about the Policy.** Any questions about this Policy should be referred to the DPO, Darren Miller at darren.m@assureglobalplus.com.au, who is in charge of administering, enforcing and updating this Policy.

11. **BREACH REPORTING AND AUDIT**

11.1. **Reporting Policy breaches.** We are committed to enforcing this Policy as it applies to all forms of Data. If you feel that this Policy may have been breached, you should report the incident to the DPO.

11.2. **Audits.** Our Legal Counsel and the DPO will review this Policy periodically and its procedures (including where appropriate by taking outside legal or auditor advice to ensure that we are in compliance with relevant new or amended laws, regulations or guidance. Additionally, we will regularly monitor compliance with this Policy, including by carrying out audits.

## 12. REGULATORY BREACH NOTIFICATION REQUIREMENTS

12.1. Certain actual or potential breaches of this Policy will require us to make formal notifications to government regulators in Australia. For example, where unauthorised access or disclosure of Personal Information has occurred, this could potentially constitute a Notifiable Data Breach under Australian legislation. If you become aware of or suspect such a breach has occurred or are unsure if a breach has occurred, you should raise the matter with the DPO, to ensure that we adequately fulfil our compliance obligations.

## 13. OTHER RELEVANT POLICIES

13.1. This Policy supplements and should be read in conjunction with our other policies and procedures in force from time to times, including without limitation our Data Retention Schedule and Privacy Policy.

# ANNEX A

## 1. DATA RETENTION SCHEDULE

1.1. NCI and AGP establish retention or destruction schedules or procedures for specific categories of data. This is done to ensure legal compliance (for example, with our data protection obligations) and to accomplish other objectives, such as protecting intellectual property and controlling costs.

1.2. Employees should comply with the retention periods listed in the data retention schedule in Clause 2 to Clause 8 below, in accordance with the NCI and AGP's Data Retention Policy above.

1.3. If you hold data not listed in Clause 2 to Clause 8 below, please refer to the Data Retention Policy above. If you still consider your data should be listed, if you become aware of any changes that may affect the periods listed below or if you have any other questions about this data retention schedule, please contact the Data Protection Officer (DPO).

## 2. COMPANY AND CORPORATE RECORDS

| TYPE OF DATA | RETENTION PERIOD | REASON | COMMENTS |
|---|---|---|---|
| Accounting records. | Seven years after the transactions covered by the records are completed. | Sections 286, 287, 288, 289 and 1306, *Corporations Act 2001* (Cth) (**CA 2001**). Best practice. | Tax requirements or other legislation may require longer. Note also that if records are kept in electronic form, they must be convertible into hard copy and available within a reasonable time. |
| Register of members, debenture holders or option holders. | Indefinitely. Entries for former members can be removed seven years after the date they ceased to be members. | Sections 173(1) and169(7), CA 2001. Best practice. | A company is required to allow any person, whether a member or non-member to inspect its registers. |
| Minutes of meetings of directors or members. | Indefinitely. | Section 198F, CA 2001. Best practice. | The CA 2001 does not specify the period for which minutes of meetings must be kept. However, as meetings are the official written record of the business transacted at a meeting, minutes should be retained permanently. Note also that current and former directors have a statutory right to inspect the books of the company (including the company's minute books) for the purposes of legal proceedings. These rights continue for seven years after the person ceases to be a director of the company. |

| | | | |
|---|---|---|---|
| Historical records and archives about the company, for example, former directors, chairpersons and employees of note. | Indefinitely. | Usual practice. | No set period in law.<br>It may be advisable to retain this information for historical purposes in the legitimate interests of the organisation. |

## 3. EMPLOYEE RECORDS

| TYPE OF DATA | RETENTION PERIOD | REASON | COMMENT |
|---|---|---|---|
| Records of employees as prescribed by regulation, such as date of commencement, employment contract, pay, leave particulars and termination date. | At least seven years after termination of employment. | Section 535, *Fair Work Act 2009* (Cth) (**FW Act**). Regulations 3.31 to 3.40, *Fair Work Regulations 2009* (Cth) (**FW Regulations**). | |
| Record of any superannuation contributions on behalf of an employee. | At least seven years after termination of employment. | Section 535, FW Act. Regulation 3.37, FW Regulations. | Records of contributions made to certain defined benefit funds will have different requirements as are regulated by other legislation such as the *Superannuation Industry (Supervision) Act 1994* (Cth). |
| Tax file numbers of employees. | Must take reasonable steps to securely destroy or permanently de-identify individual's tax file number information that is no longer required by law to be retained or is no longer necessary for a purpose under taxation law, personal assistance law or superannuation law. | Section 11(2), Privacy (T*ax File Number) Rule 2015* (Cth). | |

## 4. FACILITIES AND SECURITY RECORDS

| TYPE OF DATA | RETENTION PERIOD | REASON | COMMENTS |
|---|---|---|---|
| Closed-circuit television (CCTV) recordings. | As long as necessary for any investigations or claims that arise. | Best practice. | No set period in law.<br>Note also New South Wales and Australian Capital Territory have an additional requirement to inform employees before recordings take place.<br>Additionally, more complex requirements exist for recordings that include sound. |
| Visitor logs. | As long as required by relevant public health directions and orders. | Best practice. | Ordinarily, there is no set period in law. |

| | | | |
|---|---|---|---|
| | | | Note that it may be necessary to retain certain visitor logs pursuant to contact tracing requirements contained in relevant public health directions and orders relating to the [2019 novel coronavirus disease (COVID-19) **OR** COVID-19] pandemic. |
| Facilities management and building contracts and leases. | Contractual period plus six years (three years in the NT) or 12 years depending on whether the agreement is executed as a simple contract or a deed, respectively. | Limitation period, as set out by statute in each state or territory (for example, *Limitation Act 1969* (NSW)). | If agreement has been executed as a simple contract, actions are time barred six years from the date of breach of contract (three years in the NT). If the agreement is executed as a deed, actions are time barred 12 years from the accrual of the cause of action. |

## 5. INFORMATION TECHNOLOGY RECORDS

| TYPES OF DATA | RETENTION PERIOD | REASON | COMMENTS |
|---|---|---|---|
| General information about internally developed information technology (**IT**) infrastructure, software and systems for internal use. | Five years from decommissioning of system. | Business need. | No statutory period. |
| General information about externally developed IT infrastructure, software and systems for internal or external use. | Six years from decommissioning of system. | Contractual obligation.<br>Limitation period. | See also Clause 7 (Procurement records). |
| General information about internally developed IT infrastructure, software and systems for external use. | Six years from decommissioning of system. | Contractual obligation.<br>Limitation period. | Where IT infrastructure, software or systems are used externally (for example, by customers), this information may be relevant to claims and disputes. |
| Systems monitoring (for example, to detect and prevent failures, vulnerabilities and external threats). | Current year plus one year. | Business need.<br>Contractual obligation. | No statutory period.<br>It may be advisable for organisations to keep monitoring logs for as long as possible as malware or malicious code may go undetected in a system for a long period of time.<br>Where IT infrastructure, software or systems are used externally (for example, by customers), monitoring logs might also be relevant to claims and disputes. |
| Business continuity and information security plans. | Three years from when the plan is superseded. | Business need.<br>Legal or contractual obligation. | No statutory period. |

| | | | |
|---|---|---|---|
| | | Limitation period. | Consider whether the organisation is subject to any legal or contractual obligations in respect of business continuity which might necessitate a longer retention period.<br>Where IT infrastructure, software or systems are used externally (for example, by customers), business continuity plans might also be relevant to claims and disputes. |
| Technical support and helpdesk requests. | Three years from end of system. | Business need.<br>Contractual obligation.<br>Limitation period. | No statutory period.<br>Consider whether support services are provided to external customers, in which case contractual obligations and limitation periods may be relevant. |
| Technical information relating to external customer user accounts. | One year from account closure. | Business need.<br>Contractual obligation.<br>Limitation period. | No statutory period.<br>Consider whether contractual obligations and limitation periods may be relevant. |
| Contracts and agreements (for example, software licences, support agreements and hardware agreements). | Six years from expiry of the agreement. | Limitation period. | See also Clause 7 (Procurement records). |
| System back ups. | Three months. | Business need. | May be different depending on the system. |

## 6. SALES, MARKETING AND CUSTOMER RECORDS

| TYPE OF DATA | RETENTION PERIOD | REASON | COMMENTS |
|---|---|---|---|
| Bought in mailing lists and associated contracts. | One year for mailing lists.<br>Six years from expiry or termination for contracts (12 years for contracts executed as a deed). | Best practice for mailing lists.<br>Limitation period for contracts. | See *APP guidelines on Direct marketing* from the Office of the Australian Information Commissioner (OAIC). |
| Marketing database records (for example, lead generation, marketing feedback and contact data). | Two years from last contact. | Business need. | Depends on the nature of the business. |
| Customer relations database records (for example, call centre records, queries, meeting feedback and account history). | Six years from last contact. | Business need and limitation period. | |
| Order fulfilment records. | Six years from completion. | Limitation period and accounting requirement. | |

| | | | |
|---|---|---|---|
| Opt-out or suppression lists. | Indefinite. | Business and compliance need. | Only sufficient information to enable the opt-out should be retained. |
| Evidence of consent to marketing (including electronic marketing). | While consent valid.<br>Six years from date consent was withdrawn or ceases to be valid. | Business need and limitation period. | Consent can be withdrawn at any time and may not necessarily remain valid indefinitely, although how long it remains valid will depend on the context. |
| Market research and marketing campaigns. | Two years from completion. | Business need. | |
| Press releases. | Five years from publication. | Business need. | |
| Customer complaints handling. | Six years from settlement or closure. | Business need and limitation period. | |
| Website analytics reports from cookies and other similar technology. | Two years. | Business need. | Cookies themselves may be set for different periods depending on the function of the cookie. |

## 7. PROCUREMENT RECORDS

| TYPE OF DATA | RETENTION PERIOD | REASON | COMMENTS |
|---|---|---|---|
| Unsuccessful tenders. | Two years. | Business need. | Businesses that have a large number of tenders may prefer to only retain for one year but will depend on the nature of the business. |
| Successful tenders. | Contract period plus six years (12 years for contracts executed as a deed). | Limitation period. | |
| Contractual documents. | Contract period plus six years (12 years for contracts executed as a deed). | Limitation period. | |

## 8. LEGAL RECORDS

| TYPE OF DATA | RETENTION PERIOD | REASON | COMMENT |
|---|---|---|---|
| Legal advice and opinions (non-litigation). | Seven years after the life of the service or the matter the advice relates to. | Rule 14.2, *Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015* (LPULASCR 2015) (does not apply in the Northern Territory (NT) and Western Australia (WA)). | Except where there are client instructions or legislative provisions to the contrary.<br>For provisions governing NT, see Rule 6.2, *Rules of Professional Conduct and Practice*.<br>For provisions governing WA, see Rule 28, *Legal Profession Conduct Rules 2010*. |

| | | | |
|---|---|---|---|
| Legal advice and other records relating to specific litigation or claim. | Seven years from settlement or withdrawal of the claim. | Rule 14.2, LPULASCR 2015 (does not apply in NT and WA). | Except where there are client instructions or legislative provisions to the contrary.<br>For provisions governing NT, see Rule 6.2, *Rules of Professional Conduct and Practice*.<br>For provisions governing WA, see Rule 28, *Legal Profession Conduct Rules 2010*. |
| Previous versions of policies, including IT policy, privacy policy and retention policy. | Six years from being superseded. | Business need and limitation period in the event of a related claim. | |
| Monitoring and investigation requests. | Six years from closure of investigation. | Limitation period. | |
| Insurance claims. | Six years after settlement of claim. | Limitation period. | |
| Records of each notifiable incident. | Five years from the day the notice of the incident is given to the regulator. | Section 38(7), *Work Health and Safety Act 2011* (Cth). | Australian businesses are required to notify the work health and safety regulator immediately becoming aware of any death, serious injury or dangerous incident arising out of the conduct of their business occurs. |