PERSONAL IDENTIFIABLE INFORMATION AND DATA MANAGEMENT POLICY

Date : 4 July 2024
Document No. : i24s-POL-039-1

CONTENTS

Document Control					
Version	Reason for Issue	Date	Prepared	Reviewed	Approved
A	Risk Management (Governance and Compliance)	15/2/2023	Anton Pickett, (Operations Manager, Civil & Construction)	Justin Kickett (Executive Director)	Angela Kickett (Executive Director)
1	Review	4/7/2024	Anton Pickett, (Operations Manager, Civil & Construction)	Justin Kickett (Executive Director)	Angela Kickett (Executive Director)

Any person(s) using i24s Group Pty Ltd's (i24s) documents or data accepts the risks of:
a) using the documents or data in electronic form without requesting and checking them for accuracy against the original hard copy version; and
b) using the documents or data for any purpose not agreed to in writing by i24s.

1 PURPOSE

i24s Group Pty Ltd ("i24s") ("the Group") (ABN 74 650 861 402), is a 100 per cent owned and operated Aboriginal business. The Group is a leading provider of talent pipeline/workforce solutions, industrial equipment hire and goods, and outreach and advocacy services, for the Mining, Resources, Energy, Infrastructure and Property sectors.

While i24s wishes to foster a culture of trust and integrity, this can only be achieved if external threats to the integrity of the Group's information and systems are controlled, and the Group is protected against risk and/or damage.

The purpose of this **Personal Identifiable Information (PII) And Data Management Policy** ("Policy") is to provide a framework for i24s to manage, maintain and continuously improve its approach to the collection, usage, management, storage, sharing and deletion of (PPI) and other data.

The governance of this Policy is overseen by the Group's Co-Founders and Officers/Executive Directors, Angela and Justin Kickett.

2 INTRODUCTION

This Policy sets out guidelines for generating, implementing and maintaining practices to protect PPI and data while being utilised within the Group's operations.
This includes ensuring PPI and data are being used for the intended purposes, via i24s' information technology and communications infrastructure, clouds, operating systems, software and applications, hardware, storage media, electronic data, and network accounts.

3 SCOPE

This Policy applies to employees, sub-contractors and other parties undertaking work for the Group.
When the following terms are referenced herein, "we", "our" or "us", we are referring to everyone at i24s. The scope of this Policy applies to all workplaces which are under the Group's control.

4 DEFINITIONS

The Australian Privacy Act provides that a "record" can be a paper document or an electronic file. Records may include physical documents, digital scans of documents, databases, and electronic files such as text, image, video, or audio files. In essence, any medium that captures and contains information constitutes a record.

For the purpose of this Policy, "data" means any information which is contained in a record, including (but not limited to) personal information.

5 POLICY

While i24s is committed to providing a reasonable level of personal privacy, users should be aware that the data they create on the Group's systems remains the property of i24s. Because of the need to protect i24s' network, the confidentiality of information stored on any network device belonging to the Group cannot be guaranteed, and as a result i24s reserves the right to audit networks and systems periodically to ensure compliance with this Policy.
Information in the possession of the Group shall be classified into different grades depending on its degree of confidentiality. Particularly sensitive information will receive special protection.
Employees, sub-contractors and other parties undertaking work for i24s will take all necessary measures to maintain the necessary cyber resilience procedures, including protecting passwords, securing access to computers, and maintaining protective software and applications.
This Policy is implemented and reviewed in accordance with the respective legislation surrounding privacy, data management and cyber security. Moreover, several of the Group's other policies are also relevant to maintain high standards of cyber resilience, including i24s' Privacy Policy and Cyber Resilience Policy.
Breaches of this Policy may result in disciplinary action, up to and including dismissal.

Information Lifecycle

The Information Lifecycle describes each phase of i24s records and data.

This Policy focuses on the Hold and Destroy phases. Hold refers to how records and data are recorded, stored, secured, backed-up and archived, while Destroy refers to how records and data are disposed of or put beyond use. For PPI, Destroy also covers the de-identification of that information so that it is no longer considered personal information.

The Privacy Act requires PPI to be deleted when it is no longer required (which includes for any legal purpose), but data retention laws may require the Group to keep PPI for specific period of time. Privacy laws and data retention laws may appear to conflict, however, it is essential to consider both obligations together, and the Group has done that for the purpose of this Policy.

Guiding Principles for Managing, Retaining and Destroying Records and Data

Actively and continuously consider whether retention of data is necessary.

- Do not destroy records and data that are necessary for i24s' operations or legally required to be kept.
- Do not destroy records and data that may be relevant to ongoing or anticipated disputes, litigation or regulatory investigations. Consult with a Co-Founder/Executive Director of i24s if you have doubts about whether certain records or data should be retained for their evidentiary value.
- Retain only minimum data necessary. It is possible to have too much data. Over-collection of data is a significant risk. Only keep what is reasonably necessary fori24s' operations or to comply with our legal obligations.
- Consider whether the Group has contractual obligations to destroy certain records and data after the expiration of a contractual relationship.
- Record data in the most appropriate format and minimise paper records. Scan physical documents and save the digital scans in Document Management System. Do not use your email Inbox as a formal record filing system.

- Take steps to secure your records and data and minimise risk of corruption of data or accidental loss. Ensure that important data is securely backed-up and archive records when they are not actively being used (but which are not ready to be destroyed).
- Ensure data can be easily located and accessed (even when archived or not in active use).
- Ensure paper records are securely destroyed if appropriate. Use shredders or security bins to destroy paper records.

Managing Information and Data

Document Type	Examples (Non-Exhaustive)	Source of Obligation	Retention Requirement	Destruction Requirement
A. Governance and Financial Records				
Written financial records that: • **correctly record and explain i24s' transactions, financial position and performance; and** • **enable true and fair financial statements to be prepared and audited.**	• Documents of 'prime entry' (receipts and payment journals) • Working papers and other documents used to explain the methods by which financial statements are made up • Delivery dockets • Invoices and Statements issued • Petty Cash files • Bank Deposits.	*Corporations Act 2001* (Cth) ss 9, 286, 287 and 288	Seven years after the transaction covered by the records is completed.	Destroy after retention requirement.
Files/Folders	• Books containing the minutes or proceedings of any general meeting, or meeting of the directors.	*Corporations Act 2001* (Cth) s251A	Permanently while the company operates. For five years after the company is wound up. The liquidator must retain books for five years from date of deregistration. For three years after deregistration former directors must keep company files/folders.	
Registers	Register of members	*Corporations Act 2001* (Cth) ss 169 & 168	Permanently	Do not destroy.
Documents Relevant to	A company carrying on a business must keep records that show and explain all transactions	*Income Tax Assessment Act 1936* (Cth) s 262A	Five years after records prepared or obtained, or five	Destroy after retention requirement.

Document Type	Examples (Non-Exhaustive)	Source of Obligation	Retention Requirement	Destruction Requirement
Income and Expenditure	and other acts that are relevant for ascertaining the company's income and expenditure.	*Income Tax Assessment Act 1997* (Cth) s 121–25 *Taxation Determination* TD 2007/2	years after the completion of the transactions or act to which the records related, whichever is later (subject to limited exceptions). CGT records must be retained for five years after it becomes certain that no CGT event can happen for which those records could reasonably be expected to be relevant to working out a capital gain or loss. A taxpayer who has incurred a tax loss should retain records relevant to ascertainment of that loss until the later of the end of the statutory record retention period or the end of the statutory period of review for the assessment of the income year when the tax loss is fully deducted or applied.	
Payroll Tax	Records to demonstrate and accurately calculate liability for payroll tax.	*Payroll Tax Act 2007* (Vic) s 17C & *Taxation Administration Act 1997* (Vic) s 55 *Payroll Tax Act 2007* (NSW) *s 48 & Taxation Administration Act 1996* (NSW) s 53	At least five years after the payment was made or obtained, or the date of completion of the transaction or act to which it relates, whichever is later.	Destroy after retention requirement.

Document Type	Examples (Non-Exhaustive)	Source of Obligation	Retention Requirement	Destruction Requirement
		Payroll Tax Act 2009 (NT) s 74 & *Taxation Administration Act 2008* (NT) s 79 *Payroll Tax Act 1971* (Qld) s 114 & *Taxation Administration Act 2001* (Qld) s 118 *Payroll Tax Act 2008* (Tas) s 60 & *Taxation Administration Act 1997* (Tas) s 63 *Payroll Tax Act 2002* (WA) s 87 & *Taxation Administration Act* 2003 (WA) s 89		
Stamp Duty and Duties	Records, books, documents and working papers relating to: • transfer of property; • mortgages and other security documents; • leases; • transfer of motor vehicles; and • insurance.	*Duties Act 2000* (Vic) ss 21B & 21C *Duties Act 1999* (ACT) & *Taxation Administration Act 1999* (ACT) s64 *Duties Act 1997* (NSW) & *Taxation Administration Act 1996* (NSW) s53 *Stamp Duty Act 1978* (NT) & *Taxation Administration Act 2007* (NT) s79 *Duties Act 2001* (Qld) & *Taxation Administration Act 2001* (Qld) s118 *Stamp Duties Act 1923* (SA) s48 & *Taxation Administration Act 1996* (SA) s53	At least five years after the date payment was made or obtained, or the date of completion of the transaction or act to which it relates, whichever is later.	Destroy after retention requirement.

Document Type	Examples (Non-Exhaustive)	Source of Obligation	Retention Requirement	Destruction Requirement
		Duties Act 2001 (Tas) & *Taxation Administration Act 1997* (Tas) s63 *Duties Act 2008* (WA) & *Taxation Administration Act* 2003 (WA) s87		
GST	Records relevant to taxable supply, taxable importation or creditable acquisitions and importations.	*Taxation Administration Act 1953* (Cth) ss 385-5	At least five years after the completion of the transaction or acts to which they relate.	Destroy after retention requirement.
Personal Property Security Documents	Any security agreement or contract that provides for the security interest.	*Personal Property Security Act 2009* (Cth) ss 275–277	The security agreement or contract which creates the security must be retained for the term of the security.	Destroy after retention requirement.
Documents Required as Evidence (in legal proceedings)	The types of documents that could be captured are broad. State and territory-based legislation imposes offences in relation to the destruction of documents that a person knows are reasonably likely to be required as evidence in a legal proceeding.	E.g. *Crimes Act 1958* (Vic) ss 83 & 254	Necessary to determine on a case-by-case basis. Where litigation is on foot, or is reasonably anticipated, relevant documents must not be destroyed (even if this results in their retention for periods in excess of the time limits imposed by taxation, corporation or other legislation).	i24s would take steps as are reasonable in the circumstances not to destroy documentation that could be required as part of a legal proceeding.
B. Information About Individuals				
PPI	Any document which records information or an opinion about an identified individual or an individual who is reasonably identifiable. For example, personal information may include:	*Privacy Act 1988* (Cth) APP 11	Retain until the personal information is no longer required for any purpose and the organisation is not legally	i24s would take steps as are reasonable in the circumstances to destroy the personal information or to ensure that the personal information is de-identified when it is no

Document Type	Examples (Non-Exhaustive)	Source of Obligation	Retention Requirement	Destruction Requirement
	• name, date of birth, postal address or email address of an individual • a government issued identifier (Medicare, passport or concession card number) • feedback provided in relation to an unsuccessful applicant's job interview • professional qualifications held by an individual. Documents such as: • an application to attend a i24s function or conference • job applications, reference letters • those created for, or collected through, disciplinary hearings and practice audits.		required to retain the information.	longer needed, and retention is not required.
Sensitive Information (including health information)	'Sensitive information' is a subset of 'personal information' and includes information about a person's: • racial or ethnic origin • religious beliefs or affiliations • sexual preferences or practices • criminal record • health • political opinions • membership of a political , professional or trade association trade union. Documents that might contain sensitive personal information include: • application for attendance at a i24s function which includes religious or cultural information	*Privacy Act 1988* (Cth) APP 11	Retain until the sensitive information is no longer required for any purpose for which it may be used or disclosed under the Privacy Act and the organisation is not legally required to retain the information. i24s would destroy or de-identify records and data that is no longer needed for the purpose for which it was collected or authorised under the Health Records Act.	I24s would take steps that are reasonable in the circumstances to destroy the documents containing sensitive information or to ensure that the documents containing sensitive information are de-identified when they are no longer needed, and retention is not required.

Document Type	Examples (Non-Exhaustive)	Source of Obligation	Retention Requirement	Destruction Requirement
	regarding dietary preferences • records that include the criminal history of a client, contractor or job applicant • records that include medical or health information about an individual.			
Government Related Identifiers	Tax File Number	*Privacy Act 1988* (Cth) ss 17 & 18 *Privacy (Tax File Number) Rule 2015 r 11*	Reasonable steps must be taken to protect the TFN information from misuse, loss, unauthorised access, modification or disclosure. Access to such documents must be restricted to individuals who need to handle the information for taxation law, personal assistance or superannuation law purposes.	A TFN recipient must take reasonable steps to securely destroy or permanently de-identify TFN information of an individual where it is no longer: • required by law to be retained • necessary for a purpose under taxation law or superannuation law.
	Documents that fall within the concept of personal information where the identity of the individual is reasonably identifiable, including: • Medicare number • driver's licence number • passport number • Centrelink number	*Privacy Act 1988* (Cth) APP 9 & 11	See above as for Personal Information.	See above as for Personal Information.
C. Employee Records				
Records of Employee Information (as prescribed by Fair Work Legislation)	Must keep records containing prescribed information, including: • employee's name, employer's name, employee status (full-time/part-time; permanent/casual; date employment began)	*Fair Work Act 2009* (Cth) s 535, Ch 3, Part 3-6, Division 3 *Fair Work Regulations 2009* (Cth)	Seven years after termination of employment.	Destroy after retention requirement. The Privacy Act 1988 (Cth) requirements relating to personal information and sensitive information do not apply to prescribed employee records or non-prescribed employee records (e.g.

Document Type	Examples (Non-Exhaustive)	Source of Obligation	Retention Requirement	Destruction Requirement
	• records relating to pay, bonuses, allowances etc • records relating to leave • records relating to overtime • records relating to averaging of hours • records relating to superannuation contributions • records relating to termination and how employment was terminated • records relating to individual flexibility arrangements and guarantees of annual earnings.			routine performance appraisals) generally.
Fringe Benefits Tax	Documents such as: • invoices, receipts, logbooks etc • employee declarations	*Fringe Benefits Tax Assessment Act 1986* (Cth) s 132	Five years after the completion of the transactions or acts to which the records relate.	Destroy after retention requirement.
Superannuation Guarantee	Documents such as: • superannuation guarantee calculations; • superannuation guarantee contributions; and • choice of superannuation fund forms/nomination forms.	*Superannuation Guarantee (Administration) Act 1992* (Cth) s 79	Five years after the records were prepared or obtained, or the transactions or acts to which those records relate, whichever is later.	Destroy after retention requirement.
Notifiable Incidents	Records of deaths, serious injuries or illness and dangerous incidents.	*Occupational Health and Safety Act 2004* (Vic) s 38 *Work Health and Safety Act 2011* (NSW) s 38 *Work Health and Safety Act 2012* (Tas) s 38 Work Health and Safety Act 2011 (ACT) s 38	Five years from the day notice of the incident is given to the regulator.	Destroy after retention requirement.

Document Type	Examples (Non-Exhaustive)	Source of Obligation	Retention Requirement	Destruction Requirement
		Work Health and Safety (National Uniform Legislation) Act 2011 (NT) s 38 *Work Health and Safety Act 2011* (Qld) s 38 *Work Health and Safety Act 2012* (SA) s 38		

6 GOVERNANCE

The governance of this Policy is overseen by the Group's Officer, Angela Kickett. For further information about this Policy and/or other health, safety, environmental or quality management matters, please contact i24s on +61 8 9209 2090 or admin@i24s.com.au

Justin Kickett

Justin Kickett

Co-Founder/Executive Director