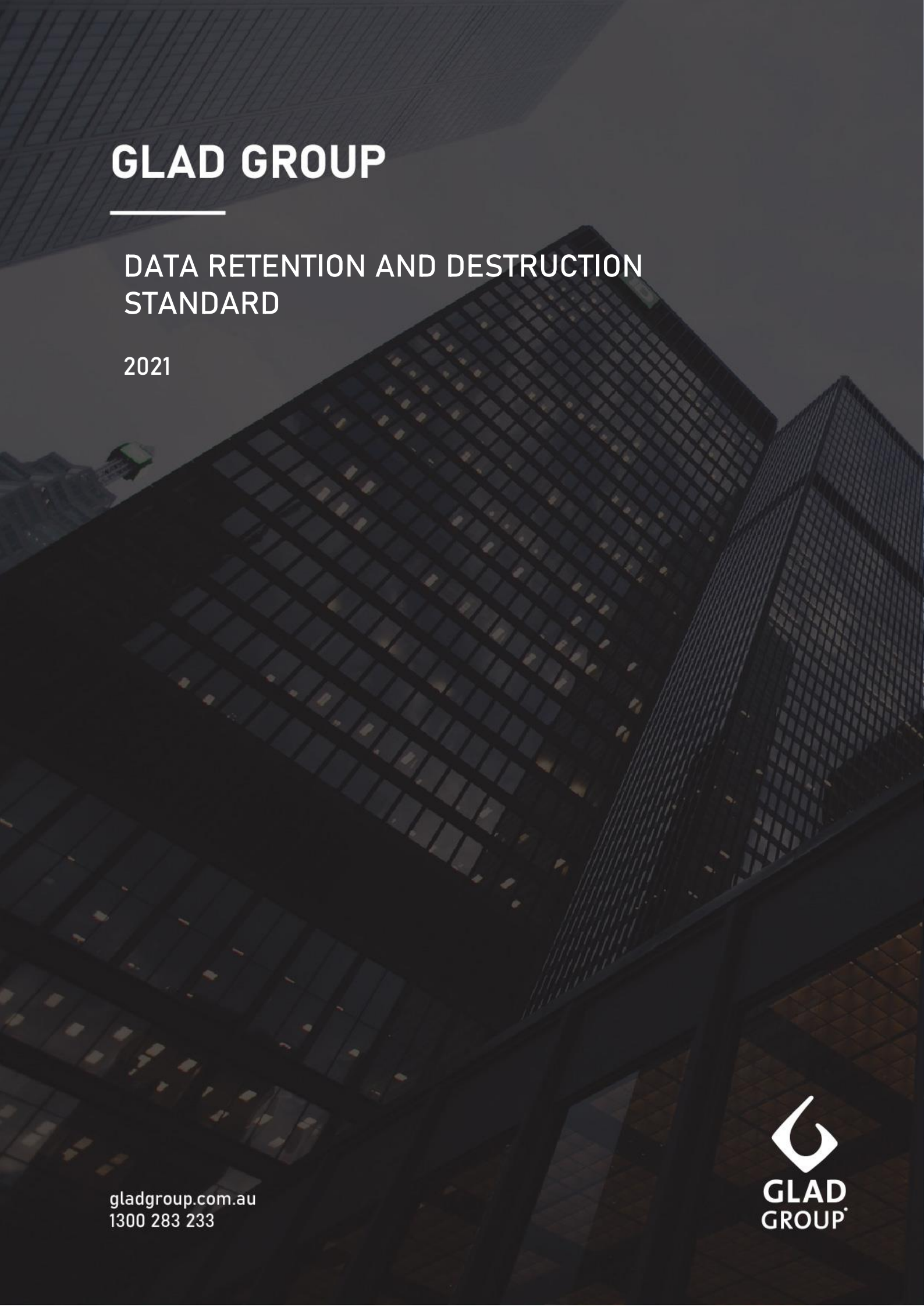


GLAD GROUP

DATA RETENTION AND DESTRUCTION STANDARD

2021

gladgroup.com.au
1300 283 233

GLAD GROUP

CONTENTS

1.0. INTRODUCTION 3
2.0. PURPOSE 3
3.0. SCOPE 3
4.0. DOCUMENTATION CLASSIFICATION 3
5.0. RESPONSIBILITIES 3
6.0. DATA RETENTION 4
6.1. PRINCIPLES 4
6.2. DATA CATEGORIES 4
6.3. RETENTION REQUIREMENTS 5
7.0. APPLICABLE DATA CLASSIFICATIONS FOR DESTRUCTION REQUIREMENTS 6
7.1. PHYSICAL 6
7.2. DIGITAL 6
8.0. PHYSICAL DATA DISPOSAL 6
8.1. SECURE DISPOSAL FACILITIES 6
9.0. IT ASSET DISPOSAL AND SANITISATION 6
9.1. IT ASSET SANITISATION AND DISPOSAL METHODS 6
9.2. SECURE IT ASSET DISPOSAL BY THIRD PARTY 7
10.0. IN-HOUSE IT ASSET SANITISATION OR DESTRUCTION 7
11.0. LITIGATION 7
12.0. OTHER INTERNAL POLICIES 7
12.1. POLICIES 7
13.0. OWNERSHIP AND VERSION CONTROL 7
14.0. APPENDIX 1 – DATA RETENTION SCHEDULE 8

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

1.0. INTRODUCTION

Data is a critical asset for Glad Group. Failure to adequately safeguard the confidentiality, integrity and availability for the lifetime of the data can result in; enforcement action from regulators including financial penalties, loss of Glad Group intellectual property, inefficient business processes and reputational damage, amongst other impacts.

This Data Retention and Destruction Standard aims to define the parameters, principles and periods for data retention in light of multiple applicable legislative and regulatory requirements.

2.0. PURPOSE

The purpose of this document is to:

- Define the high-level principles for data retention and destruction within Glad Group;
- Define the roles and responsibilities for data retention and destruction across the organisation;
- Ensure awareness of all applicable legislative and regulatory requirements relating to data retention;
- Set the retention period for all data types processed within Glad Group; and
- Define the requirements for secure destruction of Glad Group data and IT Assets.

3.0. SCOPE

This Data Retention and Destruction Standard applies to paper, electronic media and any other method used to store data that is collected, shared, stored, or otherwise processed by Glad Group.

4.0. DOCUMENTATION CLASSIFICATION

The Information in this document is for the sole use of Glad Group staff and approved third parties. It is therefore classified as internal use only. This document must not be circulated outside Glad Group without consent of the information owner.

5.0. RESPONSIBILITIES

Team / Role	Responsibilities
All Users	▪ Adhere to this Standard at all times. ▪ Report any breaches of this Standard to Management. ▪ Securely handle, protect and dispose of data. ▪ Continuously monitor for changes to applicable legislation and regulations impacting data retention, and this standard.
IT Team	▪ Facilitate the underlying infrastructure for electronic data management. ▪ Perform or assist with the secure destruction/removal of expired electronic data. ▪ Implement and maintain systems to adhere to data retention

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

Team / Role	Responsibilities
	requirements defined in this standard, where possible.
Operations Team	▪ Responsible with providing Glad Group workers with the facilities to comply with this standard
Governance Committee	▪ Review this Standard annually. ▪ Monitor and enforce this Standard.
Risk & Compliance Team	▪ Review this Standard annually to ensure legislative requirements are current.

6.0. DATA RETENTION

6.1. PRINCIPLES

Data retention requirements are guided by four key principles, which set the foundations for the retention of data within Glad Group:

1) Compliance: Data will be retained to comply with relevant legislation and regulations. Legislative and regulatory requirements vary between data types, hence Glad Group has multiple legislative and regulatory requirements in relation to data retention. Appendix 1 defines all relevant legislative and regulatory data retention requirements.
2) Purpose: Data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3) Security: The confidentiality, integrity and availability of data will be protected at all times during the retention period, and data will be securely destroyed when the defined retention period is reached.
4) Capacity: Following expiry of the legislative retention period, data will be stored and retained up to a reasonable capacity that does not cause operational issues and unnecessary financial overheads.

6.2. DATA CATEGORIES

For the purpose of defining data retention requirements, all data will be categorised into one of the below categories. Appendix 1 defines the full data retention schedule for all data categories.

- Personal Data – Any data that permits identification of an individual e.g. name, email address, date of birth. This category also includes sensitive personal data such as an individual's medical/health details, religious beliefs, political opinions, trade union membership, sexual orientation, etc.
- Financial Data – Accounts and other financial records such as but not limited to forecasts, budgets, P&L statements, balance sheets, etc.
- Legal Data – All data related to legal agreements including leases, agreements for the purchase/sale of assets, customer/supplier contracts, insurance documentation, etc.
- Capital Transaction Data – Data pertaining to the sale or acquisition of assets, such as heads of agreement, Investment Committee papers, etc.

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

- Tax Data – All records relating to tax such as but not limited to tax returns, activity statements,fringe benefits tax (FBT) returns, GST and invoices.
- Corporate Data – All data that relates to general governance activities of the organisation e.g.board and board committee meeting minutes, AML and CTF documentation, minutes of the Disclosure Committee, Compliance Plans, audit reports, etc.
- Technology Data – Data and metadata that relates to the management and configuration of information technology such as but not limited to system logs, system configurations, data backups, etc.
- Health and Environmental Data – Data that relates to Glad Group's management and tracking of sustainability, (such as asset energy consumption) and data that relates to working environments (such as health and safety assessments).
- Operational Data – General data relating to the operational activities of business units includingsupplier management.
- Unstructured Data – Various data types retained in repositories in various formats which cannotbe accurately identified and categorised.
-

6.3. RETENTION REQUIREMENTS

Retention period

The minimum retention period for all data types will be the legislative or regulatory requirement, whilethe maximum requirement will be the minimum retention period + 1 year, to allow sufficient time for operational activities associated with destroying the data.

Where there are no legislative or regulatory retention requirements for the data, the following criteriawill be applied:

- Australian Privacy Principle 11 (APP 11) (as per Australian Privacy Act 1988) will be applied to ensure personal information is destroyed or de-identified once it is no longer needed. Where possible, no data types will be retained in perpetuity.
- Subject to the application of APP 11, the Limitations of Actions Act 2008 (NSW) period of 6 years will be applied where retention periods are undefined. Six years represents the statute of limitations for tortious claims in New South Wales.

Retention trigger

The retention trigger defines the point in time in at which the specified retention periods become applicable. The clock for the minimum and maximum retention periods starts upon occurrence of thetrigger event. For example, if the retention trigger is the end of the year in which the records were prepared and the maximum retention period is eight (8) years, if the records were prepared in 2020, they must be disposed of by year end 2028.

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

7.0. APPLICABLE DATA CLASSIFICATIONS FOR DESTRUCTION REQUIREMENTS

7.1. PHYSICAL

Any Glad Group Information that can be classified as Internal Use or Highly Sensitive must be disposed of in a secure manner as defined within this standard.

7.2. DIGITAL

Any Electronic Media devices that contain or have contained data classified as Internal Use or Highly Sensitive in line with the Glad Group Data Classification Standard must be sanitised by an approved supplier before the device is disposed of

See the Glad Group Data Classification Standard, Appendix A to the Information Management Policy, for more detail on the Glad Group Data Classifications.

8.0. PHYSICAL DATA DISPOSAL

8.1. SECURE DISPOSAL FACILITIES

The following requirements define the facilities that must be available at all Glad Group locations wheredata classified as Internal Use or Highly Classified will be handled, stored or processed.

- All Glad Group staff must dispose of physical documents in the secure paper disposal bins provided.
- All Glad Group work spaces are provided a lockable paper disposal bin.
- All staff must have access to the bin for day to day use.
- The contents of the secure paper disposal bins must be restricted to authorised individuals only.
- Secure paper disposal bins must be locked at all times.
- The bin's opening where paper will be pushed though must not be large enough to allow access to the documents within.
- Bins must be emptied routinely into a paper shredder by an approved supplier who must provide certification/ conformation of bin collection and paper destruction.
- Documents must be shredded to a size as to make recovery of the document unfeasible.
- Access to the paper bins outside of the routine emptying must be recorded and the procurement manager must be informed.
- If a document's classification cannot be identified. It must be disposed of in the secure disposalbins.

9.0. IT ASSET DISPOSAL AND SANITISATION

Any Electronic Media devices that contain or have contained data classified as Internal Use or Highly Sensitive in line with the Glad Group Data Classification Standard must be sanitised by an approved supplier before the device is disposed of securely.

9.1. IT ASSET SANITISATION AND DISPOSAL METHODS

All Glad Group IT Assets that are to be sanitised or disposed of must only do so through the approved sanitising or disposal supplier. For guidance on the approved supplier contact the Glad Group Team Leader - IT Infrastructure.

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

9.2. SECURE IT ASSET DISPOSAL BY THIRD PARTY

Any IT Assets to be sanitised and or disposed must adhere to the following:

Corporate electronic media devices must be returned to the Glad Group IT Service Team

- Electronic media devices must be transported securely to reduce the risk of IT Asset theft, loss or compromise during transit, use an approved carrier any time an IT Asset is being transported by anyone other than the system owner or manager.
- Only an approved 3rd party IT Asset Disposal provider must be used. For guidance contact the Glad Group Team Leader - IT Infrastructure.

Sanitisation or destruction certificate must be produced and retained for all IT Assets sanitised and or disposed of. This certificate must have an itemised list of the assets processed. A copy ofthe certificate should be provided to the Glad IT Service Team for catalogue and storage.

10.0. IN-HOUSE IT ASSET SANITISATION OR DESTRUCTION

Glad Group does not approve the use of in-house sanitisation or destruction of assets. Any request to do so must be approved by the Glad Group Chief Operating Officer.

11.0. LITIGATION

Where Glad Group is involved in actual or impending litigation, all internal documents and records relatingto that litigation must be retained until otherwise advised by the General Counsel, regardless of anyretention or destruction requirements defined in this Standard.

12.0. OTHER INTERNAL POLICIES

The following policies also apply in relation to data retention and should be read in conjunction with this Standard. The policies can be found on the Glad Intranet.

12.1. POLICIES

- Information Security Policy
- Information Management Policy

13.0. OWNERSHIP AND VERSION CONTROL

If you require additional information about this Standard and/or you have any questions, concerns or suggestions for improvements to this Standard, contact the Manager IT & Innovation.

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

14.0. APPENDIX 1 – DATA RETENTION SCHEDULE

DATA TYPE	RETENTION TRIGGER	MINIMUM RETENTION PERIOD	MAXIMUM RETENTIONPERIOD	SOURCE
Personal Data				
Employee records: ▪ Personnel files, payslips, background screening information, performance appraisals, training, disciplinary information, medical certificates, contact details, etc.	Termination of employment	7 years	15 years	Fair Work Act 2009, S535F
Job applications: ▪ Unsuccessful candidates; CVs, references, interview notes, etc.	Data of employment decision	N/A	6 years	Criteria defined in Section 2.3 ofthis Standard
Customer / Client information: ▪ Name, email address, phone number, etc. ▪ Customer queries, complaints, etc.	Date of collection	N/A	6 years	Criteria defined in Section 2.3 ofthis Standard
Marketing data: ▪ Personal information collected during and for marketing related activities – Mailing lists, business cards, marketing event attendance lists, etc.	Date of last interaction with individual	N/A	6 years	Criteria defined in Section 2.3 ofthis Standard
Marketing data: ▪ Cookies revealing user IP address, location data, other identifiable data types.	Date of collection	N/A	6 years	Criteria defined in Section 2.3 ofthis Standard

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

DATA TYPE	RETENTION TRIGGER	MINIMUM RETENTION PERIOD	MAXIMUM RETENTIONPERIOD	SOURCE
CCTV	Date of collection	N/A	4 weeks	Criteria defined in Section 2.3 ofthis Standard
Visitor sign-in logs	Date of collection	N/A	2 years	Criteria defined in Section 2.3 ofthis Standard
Financial Data				
Financial statements: ▪ Statements of financial position, P&L statements, statement of cash flows, notes or documents relating to financial statements, etc.	End of financial year	7 years after the end of the transactions to which the document relates	8 years	Corporations Act 2001 Financial Transaction Reports Act 1988
Records of purchase, sale or othercosts associated with business assets: ▪ Property, vehicles, equipment, payment card details etc.	End of financial year	7 years	8 years	Financial Transaction Reports Act 1988
Debt financing information: ▪ Bank debt information, debt capital market transactions, etc.	Date of final repayment of debt	6 years	7 years	Criteria defined in Section 2.3 ofthis Standard
Payroll information, bank details of former employees	Termination of employment	1 year	2 years	Criteria defined in Section 2.3 ofthis Standard
Superannuation information	End of financial year last superannuation transaction was complete	5 years	6 years	Superannuation Guarantee (Administration) Act 1992
Legal Data				

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

DATA TYPE	RETENTION TRIGGER	MINIMUM RETENTION PERIOD	MAXIMUM RETENTIONPERIOD	SOURCE
Contract documentation with suppliers / clients and associateddocuments: ▪ Design and construction contracts, consultancy deed, master services agreements, etc.	Termination of contract	6 years	7 years	Criteria defined in Section 2.3 ofthis Standard
Insurance documentation	Expiration of policy	6 years	7 years	Criteria defined in Section 2.3 ofthis Standard
Personal Property Securities	Beginning of the term of the security	For the term of the security	1 Year following the term of the security	Personal Property Securities Act 2009 (Cth)
Licences, confidentiality deeds, and associated documentation	Termination of licence or deed	6 years	7 years	Criteria defined in Section 2.3 of this Standard
Capital Transaction Data				
Lease / purchase of asset contractsand associated documentation	When asset is divested,or upon closure of any warranty claim on sale	6 years	7 years	Criteria defined in Section 2.3 ofthis Standard
Tax Data				
Tax returns and related documentation	End of financial year	5 years	6 years	Income Tax Assessment Act 1997
Receipts and invoices for goods and services	End of financial year	5 years	6 years	Income Tax Assessment Act 1997
Capital Gains Tax	Completion of the transactions to which the records relate	5 years after the completion of the transactions to which the records	6 years	Income Tax Assessment Act 1997

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

DATA TYPE	RETENTION TRIGGER	MINIMUM RETENTION PERIOD	MAXIMUM RETENTIONPERIOD	SOURCE
		relate		
Fringe Benefits Tax	The date they are prepared, or the transactions are completed	5 years after the date they are prepared, or the transactions are completed	6 years	Income Tax Assessment Act 1997
Payroll Tax, Land Tax, Stamp Duty	The date they are prepared, or the transactions are completed	5 years	6 years	Criteria defined in Section 2.3 ofthis Standard
Corporate Data				
Board meeting minutes and Papers	Date of meeting	7 years	8 years	Corporations Act 2001
Records of Board resolution voting	Date resolution under vote is passed	7 years	8 years	Corporations Act 2001
External audit reports	Date of report publication	6 years	7 years	Criteria defined in Section 2.3 ofthis Standard
Powers of Attorney documentation	End of relevant litigation	6 years	7 years	Criteria defined in Section 2.3 ofthis Standard
Subscription agreements: ▪ Accession deeds, side letters, unit transfer forms, pre-emptive offer letters, etc.	Date subscription agreement ends, or dateof issue of letter	6 years	7 years	Criteria defined in Section 2.3 ofthis Standard
Register of members of the Company	Entry on the register	5 years after the last entry onto the	6 years	Corporations Act 2001

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

DATA TYPE	RETENTION TRIGGER	MINIMUM RETENTION PERIOD	MAXIMUM RETENTIONPERIOD	SOURCE
		register		
Records electronically registered with ASIC	Lodgement with ASIC	7 years	8 years	Corporations Act 2001
Registers required by ASFL Licensees (e.g. complaints, disputes, breach registers, training register, authorised representatives register)	Entry on the register	5 years after the last entry in the register	6 years	Corporations Act 2001
Disclosure Documents (PDS)	Issue of PDS	7 years after the date of the PDS	8 years	Corporations Act 2001, Part 7
Technology Data				
System and network logs	Date of logging	6 months	18 months	Criteria defined in Section 2.3 ofthis Standard
System backups	Date of backup	7 days	10 years	Criteria defined in Section 2.3 ofthis Standard
Service request tickets	Tickets closure	7 year	8 years	Criteria defined in Section 2.3 of this Standard
Public network data / logs (Wi-Fi)	Date of capture	2 years	3 years	Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015
Health and Environmental Data				
Sustainability and energy consumption information	End of the reporting yearin which the activities recorded took place	7 years	30 years	National Greenhouse and Energy Reporting Act 2007

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

DATA TYPE	RETENTION TRIGGER	MINIMUM RETENTION PERIOD	MAXIMUM RETENTIONPERIOD	SOURCE
Health and Safety incident reports including exposure records	Date of creation	30 years	31 years	Work Health and Safety Act 2011 (NSW) Occupational Health and SafetyAct 2004 (Vic) Work Health and Safety Act 2011(Qld) Work Health and Safety Act 2011 (National Uniform Legislation) Criteria defined in Section 2.3 ofthis Standard
Incidents notified to WorkSafe	Date of creation	5 years	6 years	Criteria defined in Section 2.3 ofthis Standard
Radiation risk assessments and management documentation	Date asset life	1 year	2 years	Criteria defined in Section 2.3 ofthis Standard
Hazardous materials registers and incident data	Data of collection	30 years	31 years	Criteria defined in Section 2.3 ofthis Standard
Energy and sustainability reports(incl. cooling tower reports, complaints, etc.)	Date collection	7 years	8 years	National Greenhouse and Energy Reporting Act 2007
Operational Data				
AML records: ▪ Customer KYC records; background checks, identification documentation, etc. ▪ CTF records e.g. reports to regulators.	Date last designated service is provided to customer	7 years	8 years	Anti-Money Laundering and Counter-Terrorism Financing Act 2006
Supplier management details	18 months from date supplier was last used in	6 years	7 years	Criteria defined in Section 2.3 ofthis Standard

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)

DATA TYPE	RETENTION TRIGGER	MINIMUM RETENTION PERIOD	MAXIMUM RETENTIONPERIOD	SOURCE
	SAP			
Asset development and construction documentation: ▪ Development plans, construction blueprints, etc.	Date of development completion	6 years	15 years	Criteria defined in Section 2.3 ofthis Standard
Professional event managementdata: ▪ Hosted event information, attendee lists, competitions, etc.	End of event or competition	1 year	6 years	Criteria defined in Section 2.3 ofthis Standard
Internal audit, risk & compliance reports	Date of creation	6 years	7 years	Criteria defined in Section 2.3 ofthis Standard
Unstructured Data				
Email and Email Archive (IncludingSkype voicemail)	Date of receipt	8 years	Indefinite	Criteria defined in Section 2.3 ofthis Standard
Instant messaging	Date of receipt of message	N/A	1 year	Criteria defined in Section 2.3 ofthis Standard
Unstructured Data backup ▪ Including but not limited to File Server Backup, Local drives Backups	Date of backup	7 days	20 years	Criteria defined in Section 2.3 ofthis Standard
File share data (SharePoint, OneDrive, etc.) ▪ Data stored in file shares which does not fall into any of the categories of data specified in this Standard.	Date of last access	6 years	10 years	Criteria defined in Section 2.3 ofthis Standard

© COPYRIGHT GLAD GROUP (ALL RIGHTS RESERVED)


GLAD
GROUP