Capital Life Funeral Planning Limited

Data Retention Policy

Content

1. Introduction

This policy has been established to set the minimum standards for achieving and maintaining appropriate records management of CLFP and customer information assets ("data records") on any media during any part of its lifecycle.

Compliance with this policy supports CLFP in meeting its business objectives and to balance the needs of customers, colleagues, commercial partners and other stakeholders. This policy is to ensure compliance with the General Data Protection Regulation ('GDPR') on storage limitation, in terms of how long the data is retained.

The legal requirements, Article 5(e) of the GDPR states that personal data shall be kept for no longer than is necessary for the purposes for which it is being processed.

All data records must be managed in accordance with this policy.

2. Definition

In the context of this policy, Data Retention is defined as:

The storage, management and timely disposal, anonymisation of data records in order to meet all legal, regulatory, contractual or operational obligations of CLFP.

Personal data records can only be considered anonymised when the individual/customer can no longer be identified, and the data used in their preparation is deleted at the same time. If not, they continue to be considered 'personal data' as the source data could be used to re-identify the individual/customer.

Failure to operate appropriate data retention procedures can lead to various issues including (but not limited to):

- Breach of legal, regulatory or contractual obligations;
- Reputational damage and loss of revenue;
- Loss or corruption of data;
- Disruption to business working; or
- Loss of resources and assets

3. Scope

This policy applies to all individuals working for or on behalf of CLFP at all times, and other persons, entities, or organisations (3rd parties) that have access to CLFP data records. Failure to comply with this policy may lead to the initiation of disciplinary procedures in line with CLFP's Disciplinary Policy.

4. Principles

CLFP must ensure that it is meeting its legal and regulatory requirements for retaining data and documented records, specifically ensuring that it is meeting GDPR regulation on storage limitation.

The sections below set out the key principles with which CLFP must comply:

4.1 Retention Periods

CLFP will operate processes to ensure data records are regularly backed up to protect against loss or destruction. The IT Team will ensure backup schedules are in place which complement the retention periods.

4.2 Record Keeping

Each Business Area that retains data records, either electronically or on paper, onsite or offsite, will maintain a list which shows, as a minimum:

- Record type / category
- Whether it is retained due to legal or regulatory need
- How long it will be retained
- Where it is stored
- Who is allowed access, and the extent of that access (view only, add, change, delete)
- Who is responsible for housekeeping / maintenance
- Data records sent for offsite storage should also show: When it was sent for offsite storage and the number or reference allocated to it by the offsite facility or Document Management and the destruction date

4.3 Storage Considerations

When storing data records on computer media (disk, CD/DVD, tape, cloud etc.) particular consideration should be given to the media to ensure that:

- It does not degrade before the retention period expires.
- The required technology to recover the information is available throughout the retention period.
- The data can be recovered in a manner acceptable to a court of law e.g. within an acceptable timeframe and format.
- Where the Business Area is not clear on whether the above will be satisfactorily addressed, they should consult with the Information Security team

4.4 Destruction / Disposal

Data records which are no longer required should be destroyed or erased (i.e. irrecoverably purged) securely. Appropriate methods should be used to avoid accidental disclosure of information

Where this is performed by a 3rd party a destruction certificate is to be obtained and retained.

In relation to data records that contain personal data, if there is a legitimate reason for these to be retained beyond the retention period, the IT Team, instead of fully deleting or destroying them, amend the data records so that they are irreversibly anonymised and therefore no longer constitute personal data.

5. Supporting Documentation/Legislation

• Data Protection Policy

• Data Protection Act 2018

• General Data Protection Regulation (EU) 2016/679

- Limitation Act 1980
- Taxes Management Act 1970

Appendix A – Data Retention Schedule

Financial Records

Personal data record category	Mandated retention period	Record owner
Payroll records	Seven years after audit	Finance
Supplier contracts	Seven years after contract is terminated	Finance
Chart of Accounts	Permanent	Finance
Fiscal Policies and Procedures	Permanent	Finance
Permanent Audits	6 years	Finance
Financial statements	6 years	Finance
General Ledger	Permanent	Finance
Investment records (deposits, earnings, withdrawals)	7 years	Finance
Invoices	7 years	Finance
Cancelled cheques	7 years	Finance
Bank deposit slips	7 years	Finance
Business expenses documents	7 years	Finance
Property/asset inventories	7 years	Finance
Credit card receipts	3 years	Finance
Petty cash receipts/documents	3 years	Finance

Business Records

Personal data record category	Mandated retention period	Record owner
Article of Incorporation to apply for corporate status	Permanent	Finance
Board policies	Permanent	Finance
Board meeting minutes	Permanent	Finance
Tax or employee identification number designation	6 years after employment finishes	Finance
Annual corporate filings	Permanent	Finance

HR: Employee Records

Personal data record category	Mandated retention period	Record owner
Disciplinary, grievance proceedings records, oral/verbal, written, final warnings, appeals	As per legal requirement	HR
Applications for jobs, interview notes – Recruitment/promotion panel Internal Where the candidate is unsuccessful Where the candidate is successful	Deleted immediately Duration of employment	HR
Payroll input forms, wages/salary records, overtime/bonus payments Payroll sheets, copies	7 years	HR
Bank details – current	Duration of employment	HR
Payrolls/wages	Duration of employment	HR

Job history including staff personal records: contract(s), Ts & Cs; previous service dates; pay and pension history, pension estimates, resignation/termination letters	As per legal requirement	HR
Employee address details	Duration of employment	HR
Expense claims	As per legal requirement	HR
Annual leave records	Duration of employment	HR
Accident books Accident reports and correspondence	As per legal requirement	HR
Certificates and self-certificates unrelated to workplace injury; statutory sick pay forms	As per legal requirement	HR
Pregnancy/childbirth certification	As per legal requirement	HR
Parental leave	Duration of employment	HR
Maternity pay records and calculations	As per legal requirement	HR
Redundancy details, payment calculations, refunds, notifications	As per legal requirement	HR
Training and development records	Duration of employment	HR

Contracts

Personal data record category	Mandated retention period	Record owner
Signed	Permanent	Finance

Contract amendments	Permanent	Finance
Successful tender documents	Permanent	Finance
Tender – user requirements, specification, evaluation criteria, invitation	Permanent	Finance

Customer Data

Personal data record category	Mandated retention period	Record owner
Live chat history	Until no longer needed or requested to be deleted	Technology
CRM data – inclusive of Name, Email address, mobile number, address, emails and phone call summaries	For a period of 7 years or until no longer needed or requested to be deleted, active funeral plans keep until time of death	Technology

Non – Customer Data

Personal data record category	Mandated retention period	Record owner
Name, email address	Kept until person unsubscribes / requests to be removed from system	Marketing
Call recordings	Automatically deleted after 6 months	Sales

IT

Personal data record category	Mandated retention period	Record owner
Recycle Bins	Cleared monthly	Individual employee
Downloads	Cleared monthly	Individual employee
Inbox	All emails containing PII attachments deleted after 3 years.	Individual employee
Deleted Emails	Cleared monthly	Individual employee
Local Drives & files	Moved to network drive weekly, then deleted from local drive	Individual employee
Google Drives, drop box	Reviewed monthly, any record/file containing PII deleted by employee after maximum of 3 years, or as soon as no longer needed	Individual employee