DATA RETENTION POLICY

1 Policy Statement

LIV Group recognises and understands that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of the organisation.

This policy and related documents meet the standards and expectations set out by contractual and legal requirements and has been developed to meet the best practices of business records management, with the direct aim of ensuring a robust and structured approach to document control and systems.

Effective and adequate records and data management is necessary to: -

- Ensure that the business conducts itself in a structured, efficient and accountable manner
- Ensure that the business realises best value through improvements in the quality and flow of information and greater coordination of records and storage systems
- Support core business functions and providing evidence of conduct and the appropriate maintenance of associated tools, resources and outputs to clients and regulator
- Meet legislative, statutory and regulatory requirements
- Deliver services to staff and stakeholders in a consistent and equitable manner
- Assist in document policy formation and managerial decision making
- Provide continuity in the event of a disaster
- Protect the interests of the organisation and the rights of employees, clients and present and future stakeholders
- Protection personal information and data subject rights
- Avoid inaccurate or misleading data and minimise risks to personal information
- Erase data in accordance with the legislative and regulatory requirements.

Information held for longer than is necessary carries additional risk and cost and can breach data protection rules and principles. LIV Group only ever retains records and information for legitimate business reasons and use, and we comply fully with the UK data protection laws and guidance.

2 Purpose

The purpose of this document is to provide LIV Group's statement of intent on how it provides a structured and compliant data and records management system with records being defined as all documents, regardless of the format; which facilitate business activities, and are thereafter retained to provide evidence of transactions and functions.

Such records may be created, received or maintained in hard copy or in an electronic format with the overall definition of records management being a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

It constitutes a series of integrated systems related to the core processes of the organisation which ensure that evidence of, and information about, its activities and transactions are captured and maintained as viable records. Unless otherwise specified, the Data Retention Policy refers to both hard and soft copy documents.

3 Scope

The policy relates to all LIV Group staff *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents*

engaged with LIV Group in the UK or overseas) within the organisation and has been created to ensure that staff deal with the area that this policy relates to in accordance with legal, regulatory, contractual and business expectations and requirements.

This Policy applies to all personal data held by the Company and by third-party data processors processing personal data on the Company's behalf.

Personal data, as held by the above is stored in the following ways and in the following locations:

a) The Company's servers, located in G: Drive;
b) Third-party servers;
c) Computers permanently located in the Company's premises;
d) Laptop computers and other mobile devices provided by the Company to its employees;
e) Physical records stored onsite at the Company's locations and held in archive storage by an external third party;

4 General Data Protection Regulation (GDPR)

LIV Group needs to collect personal information about the people we employ, work with have a business relationship with to effectively and compliantly carry out our everyday business functions and activities, and to provide the products and services defined by our business type. This information can include *(but is not limited to),* name, address, email address, data of birth, IP address, identification number, private and confidential information, sensitive information and bank details.

In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to collecting, processing, storing and destroying all information in accordance with the ***General Data Protection Regulation***, UK data protection law and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

Our Data Retention Policy and processes comply fully with the GDPR's fifth Article 5 principle: -

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation').***

5 Data Subject Rights and Data Integrity

All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used, and how long the Company will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise

disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Company's use of their personal data, and further rights relating to automated decision-making and profiling.

6 Objectives

A record is information, regardless of media, created, received, and maintained which evidences the development of, and compliance with, regulatory requirements, business practices, legal policies, financial transactions, administrative activities, business decisions or agreed actions. It is LIV Group's objective to implement the necessary records management procedures and systems which assess and manage the following processes: -

- The creation and capture of records
- Compliance with legal, regulatory and contractual requirements
- The storage of records
- The protection of record integrity and authenticity
- The use of records and the information contained therein
- The security of records
- Access to and disposal of records

Records contain information that are a unique and invaluable resource to LIV Group and are an important operational asset. A systematic approach to the management of our records is essential to protect and preserve the information contained in them, as well as the individuals such information refers to. Records are also pivotal in the documentation and evidence of all business functions and activities.

LIV Group's objectives and principles in relation to Data Retention & Records Management are to: -

- Ensure that LIV Group conducts itself in an orderly, efficient and accountable manner
- Realise best value through improvements in the quality and flow of information and greater coordination of records and storage systems
- Support core business functions and providing evidence of conduct and the appropriate maintenance of associated tools, resources and outputs to clients and 3rd parties
- Meet legislative, statutory and regulatory requirements
- Deliver services to staff and stakeholders in a consistent and equitable manner
- Provide continuity in the event of a disaster
- Protect the interests of the organisation and the rights of employees, clients and present and future stakeholders
- Ensure the safe and secure disposal of confidential data and information assets
- Ensure that records and documents are retained for the legal, contractual and regulatory period stated in accordance with each bodies rules or terms.
- Ensure that no document is retained for longer than is legally or contractually allowed
- Mitigate against risks or breaches in relation to confidential information

7 Guidelines and Procedures

LIV Group manage records efficiently and systematically, in a manner consistent with the GDPR requirements, ISO15489 and regulatory Codes of Practice on Records Management. Records management training is mandatory for all staff as part of LIV Group's statutory and compliance training programme and this policy is widely disseminated to ensure a standardised approach to data retention and records management.

Records will be created, maintained and retained in order to provide information about, and evidence of LIV Group's transactions, customers, employment and activities. Retention schedules will govern the period that records will be retained and can be found in the ***Record Retention Periods*** table at the end of this document.

It is our intention to ensure that all records and the information contained therein is: -

- **Accurate** - records are always reviewed to ensure that they are a full and accurate representation of the transactions, activities or practices that they document
- **Accessible** - records are always made available and accessible when required (*with additional security permissions for select staff where applicable to the document content*)
- **Complete** - records have the content, context and structure required to allow the reconstruction of the activities, practices and transactions that they document
- **Compliant** - records always comply with any record keeping legal and regulatory requirements
- **Monitored –** staff, company and system compliance with this Data Retention Policy is regularly monitored to ensure that the objectives and principles are being complied with at all times and that all legal and regulatory requirements are being adhered to.

8 Technical and Organisational Data Security Measures

8.1 The following technical measures are in place within the Company to protect the security of personal data. Please refer to the Company's Data Protection Policy for further details:

a) All emails containing personal data must be encrypted and/or password protected;
b) All emails containing personal data must be marked "confidential";
c) Personal data may only be transmitted over secure networks;
d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;
e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;
f) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent marked as "confidential";
g) All personal data transferred physically should be transferred in a suitable container marked "confidential";
h) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;
i) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation;
j) Personal data must be handled with care at all times and should not be left unattended or on view;
k) Computers used to view personal data must always be locked before being left unattended;
l) No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise without the formal written approval of the appropriate head of department and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;
m) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company's Data Protection Policy and the GDPR;

n) All personal data stored electronically is backed up frequently with backups stored both onsite at the Company's offices and offsite at a data centre;
o) All electronic copies of personal data should be stored securely using passwords and encryption as appropriate;
p) All passwords used to protect personal data should be changed regularly and must be secure;
q) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
r) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;
s) No software may be installed on any Company-owned computer or device without approval; and
t) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Head of Marketing to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

8.2 The following organisational measures are in place within the Company to protect the security of personal data. Please refer to the Company's Data Protection Policy for further details:

a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under the Company's Data Protection Policy;
b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;
c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;
e) All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;
f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
h) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy;
i) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy;

9.1 Retention Period Protocols

All records retained during their specified periods are traceable and retrievable. Any file movement, use or access is tracked and logged, including inter-departmental changes. All company and employee information is retained, stored and destroyed in line with legislative and regulatory guidelines.

For all data and records obtained, used and stored within LIV Group, we: -

- Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain

- Establish periodical reviews of data retained
- Establish and verify retention periods for the data, with special consideration given in the below areas: -

    - the requirements of LIV Group
    - the type of personal data
    - the purpose of processing
    - lawful basis for processing
    - the categories of data subjects

- Where it is not possible to define a statutory or legal retention period, as per the GDPR requirement, LIV Group will identify the criteria by which the period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices
- Have processes in place to ensure that records pending audit, litigation or investigation are not destroyed or altered
- Transfer paper based records and data to an alternative media format in instances of long retention periods (*with the lifespan of the media and the ability to migrate data where necessary always being considered*)

9.2 Designated Owners

All systems and records have designated owners (IAO) throughout their lifecycle to ensure accountability and a tiered approach to data retention and destruction. Owners are assigned based on role, business area and level of access to the data required. The designated owner is recorded on the Retention Register and is fully accessible to all employees. Data and records are never reviewed, removed, accessed or destroyed with the prior authorisation and knowledge of the designated owner.

9.3 Document Classification

LIV Group have detailed Asset Management protocols for identifying, classifying, managing, recording and coordinating LIV Group's assets (*including information*) to ensure their security and the continued protection of any confidential data they store or give access to. We utilise an ***Information Asset Register (IAR)*** to document and categorise the assets under our remit and carry out regular Information Audits to identify, review and document all flows of data within LIV Group.

The Information Audit enables us to identify, categorise and record all personal information obtained, processed and shared by our company in our capacity as a controller and processor and has been compiled on a central register which includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Retention periods
- Access level (*i.e. full, partial, restricted etc*)

Our information audits and registers enable us to assign classifications to all records and data, thus ensuring that we are aware of the purpose, risks, regulations and requirements for all data types.
How we classify data: -

All information on the LIV Group company network is classified into one of two main classifications:

Public - information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to LIV Group.

Confidential – all other information.

Confidential information is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner.

LIV Group personnel are encouraged to use common sense judgment in classifying the sensitivity of LIV Group Confidential information to the proper extent. This classification is then used to decide what access restriction needs to be applied and the level of protection afforded to the record or data. The classification along with the asset type, content and description are then used to assess the risk level associated with the information and mitigating action can then be applied.

9.4 Suspension of Record Disposal for Litigation or Claims

If LIV Group is served with any legal request for records or information, any employee becomes the subject of an audit or investigation or we are notified of the commencement of any litigation against our firm, we will suspend the disposal of any scheduled records until we are able to determine the requirement for any such records as part of a legal requirement.

9.5 Storage and Access of Records and Data

Documents are grouped together by category and then in clear date order when stored and/or archived. Documents are always retained in a secure location, with authorised personnel being the only ones to have access. Once the retention period has elapsed, the documents are either reviewed, archived or confidentially destroyed dependant on their purpose, classification and action type.

10 Expiration of Retention Period

Once a record or data has reached its designated retention period date, the designated owner should refer to the retention register for the action to be taken. Not all data or records are expected to be deleted upon expiration; sometimes it is sufficient to anonymise the data in accordance with the GDPR requirements or to archive records for a further period.

10.1 Destruction and Disposal of Records & Data

All information of a confidential or sensitive nature on paper, card, microfiche or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, clients and customers.

LIV Group is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply

with the laws and provisions made in the General Data Protection Regulation (GDPR) and that staff are trained and advised accordingly on the procedures and controls in place.

10.1.1 Paper Records

Due to the nature of our business, LIV Group retains paper based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential and compliant manner. LIV Group utilise onsite-shredding or a professional shredding service provider to dispose of all paper materials.

Employee shredding machines and confidential waste sacks are made available throughout the building and where we use a service provider for large disposals, regular collections take place to ensure that confidential data is disposed of appropriately.

10.1.2 Electronic & IT Records and Systems

LIV Group uses numerous systems, computers and technology equipment in the running of our business. From time to time, such assets must be disposed of and due to the information held on these whilst they are active, this disposal is handled in an ethical and secure manner.

The deletion of electronic records must be organised in conjunction with the IT Department who will ensure the removal of all data from the medium so that it cannot be reconstructed. When records or data files are identified for disposal, their details must be provided to the designated owner to maintain an effective and up to date a register of destroyed records.

Only the IT Department can authorise the disposal of any IT equipment and they must accept and authorise such assets from the department personally. Where possible, information is wiped from the equipment through use of software and formatting, however this can still leave imprints or personal information that is accessible and so we also comply with the secure disposal of all assets.

In all disposal instances, the IT Department must complete a disposal form and confirm successful deletion and destruction of each asset. This must also include a valid certificate of disposal from the service provider removing the formatted or shredded asset. Once disposal has occurred, the IT Department is responsible for liaising with the information Asset Owner and updating the Information Asset Register for the asset that has been removed.

It is the explicit responsibility of the asset owner and IT Department to ensure that all relevant data has been sufficiently removed from the IT device and backed up before requesting disposal and/or prior to the scheduled pickup.

10.1.3 Internal Correspondence and General Memoranda

Unless otherwise stated in this policy or the retention periods register, correspondence and internal memoranda should be retained for the same period as the document to which they pertain or support (i.*e. where a memo pertains to a contract or personal file, the relevant retention period and filing should be observed*).

Where correspondence or memoranda that do not pertain to any documents having already be assigned a retention period, they should be deleted or shredded once the purpose and usefulness of the content ceases or at a maximum, 2 years.

Examples of correspondence and routine memoranda include (but are not limited to): -

- Internal emails
- Meeting notes and agendas
- General inquiries and replies
- Letter, notes or emails of inconsequential subject matter

10.2 Special Category Data

In accordance with GDPR requirements and Schedule 1 Part 4 of The Data Protection Bill, organisations are required to have and maintain appropriate policy documents and safeguarding measures for the retention and erasure of special categories of personal data and criminal convictions etc.

Our methods and measures for destroying and erasing data are noted in this policy and apply to all forms of records and personal data, as noted on our retention register schedule.

The Company maintains records of data processing activities in accordance with data protection legislation. Record keeping is carried out for the following processing activities:

1. Processing of personal data which includes special category data;
2. Processing of personal data which includes data about criminal convictions.

The Company creates reminder notifications on each entry of special category data uploaded onto the HR system, this ensures erasure takes place in line with the Data Retention Policy.

Special category data is deleted electronically off the system and if hard copies exist, they are destroyed by shredding.

The Company maintains a Destruction Register which is updated each time any special category data is erased or destroyed.

11 Compliance Monitoring

LIV Group are committed to ensuring the continued compliance with this policy and any associated legislation and undertake regular audits and monitoring of our records, their management, archiving and retention. Information asset owners are tasked with ensuring the continued compliance and review of records and data within their remit.

12 Responsibilities

Heads of departments and information asset owners have overall responsibility for the management of records and data generated by their departments' activities, namely to ensure that the records created, received and controlled within the purview of their department, and the systems (*electronic or otherwise*) and procedures they adopt, are managed in a way which meets the aims of this policy.

Where a DPO has been designated, they must be involved in any data retention processes and records or all archiving and destructions must be retained. Individual employees must ensure that the records for which they are responsible are complete and accurate records of their activities, and that they are maintained and disposed of in accordance with LIV Group's protocols.

13 Retention Periods

Section 11 of this policy contains our regulatory, statutory and business retention periods and the subsequent actions upon reaching said dates. Where no defined or legal period exists for a record, the default standard retention period is 6 years plus the current year (*referred to as 6 years + 1*).

14 How to contact us

If you maintain any types of records that are not listed in the table in the Appendix, and it is not clear from the existing record types in the table what retention period should apply, or if you have any questions about this policy, please contact our Data Protection Administrator:

Address: Whitehall Waterfront, 2 Riverside Way, Leeds, LS1 4EH

You can also call us on 0113 244 2444 or email DataProtectionAdmin@liv-group.co.uk

Document Control

Issue:	Date of Issue:	Comment	Approved by
1	18.05.18	Original Document – First Issue	Helen Peace
2	06.06.18	Insertion of Section 14	Helen Peace
3	14.06.18	Update to Appendix – Data Retention Schedule – Marketing Data & Non-Client Data	Helen Peace

Appendix – Data Retention Schedule

Financial Records

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

Business Records

Personal data record category	Mandated retention period	Record owner
Article of Incorporation to apply for corporate status	Permanently	Finance
Board policies	Permanently	Finance
Board meeting minutes	7 years	Finance
Tax or employee identification number designation	7 years	Finance
Office and team meeting minutes	7 years	Finance
Annual corporate filings	7 years	Finance

HR: Employee Records

Personal data record category	Mandated retention period	Record owner
Disciplinary, grievance proceedings records, oral/verbal, written, final warnings, appeals	In most cases may not be used once warnings are spent but should be retained for 2 years	HR
Applications for jobs, interview notes – Recruitment/promotion panel Internal Where the candidate is unsuccessful Where the candidate is successful	1 year following date of appointment 6 years after employment ceases	HR
Payroll input forms, wages/salary records, overtime/bonus payments Payroll sheets, copies	6 years following year end	HR
Bank details – current	6 years after employment ceases	HR
Payrolls/wages	6 years following year end	HR
Job history including staff personal records:	6 years after employment ceases	HR

contract(s), Ts & Cs; previous service dates; pay and pension history, pension estimates, resignation/termination letters		
Employee address details	6 years after employment ceases	HR
Expense claims	6 years following year end for public companies	HR
Annual leave records including, compassionate leave, time off for public duties or for dependants	2 years	HR
Accident books Accident reports and correspondence	40 years 3 years from date of last entry for claims under F2508(revised); longer period recommended because of risk of personal injury claims or claims under the Equality Act 2010	HR
Health and safety records	40 years	HR
Risk assessments and records of consultations with safety reps and committees	Permanently	HR
Statutory and Regulatory Training	6 years after leaving	HR
First Aid Training	6 years after leaving	HR
Fire Warden Training	6 years after leaving	HR
H&S representatives training	6 years after leaving	HR
H&S training - employees	5 years after leaving	HR
Medical reports (general)	6 years after leaving	HR
Medical records and details of biological tests as specified by the COLW Regulations	40 years from date of last entry	HR
Medical records as specified by COSHH regulations	40 years from date of last entry	HR
Records of tests and examinations of control systems and protective equipment under the COSHH regulations	5 years from date of the test	HR
Sickness records, Certificates and self-certificates unrelated to workplace injury; statutory sick pay forms	40 years after employment ends	HR
Pregnancy/childbirth certification	Until the child reaches the age of 21	HR
Parental leave	5 years from first request (18 years for disabled child)	HR
Maternity leave, pay records and calculations	3 years after end of tax year in which the maternity period ends	HR
Paternity leave and pay records	3 years after end of tax year in which the paternity period ends	HR
Adoption leave and matching certificate	3 years after end of tax year in which the adoption period ends	HR
Redundancy details, payment calculations, refunds, notifications	6 years after employment ceases	HR
Redundancy correspondence	6 years after employment ceases	HR
Redundancy - less than 20 - facts relating to	3 years	HR

this		
Redundancy - more than 20 - facts relating to this	12 years	HR
Documents proving the right to work in the UK	2 years after employment ceases	HR
Training and development records	6 years after employment ceases	HR

Contracts

Personal data record category	Mandated retention period	Record owner
Signed	7 years	Finance
Contract amendments	7 years	Finance
Successful tender documents	7 years	Finance
Unsuccessful tenders' documents	1 year past the audit completion	Finance
Tender – user requirements, specification, evaluation criteria, invitation	7 years	Finance
Contractors' reports	7 years	Finance
Operation and monitoring, eg complaints	7 years	Finance

Tenancy Data

Personal data record category	Mandated retention period	Record owner
Yardi tenancy record including personally identifiable information about the tenant(s) and further information or attachments which may include the following – AST; tenancy deposit certificate; proof of ID; Visa; References, Bank statements; Utility Bills; Credit checks; Standing Order and Direct Debit madnates; Let Agreed forms; email commiumincations and other copy correspondence; Deposit return bank details; Forwarding address	Details are held on the Yardi database platform whilst tenancy is live and for a period of 6 years following the end of tenancy then deleted.	BTR Team
Reapit tenancy record including personally identifiable information about the tenant(s) and further information or attachments which may include the following – AST; tenancy deposit certificate; proof of ID; Visa; References, Bank statements; Utility Bills; Credit checks; Standing Order and Direct Debit madnates; Let Agreed forms; email commiumincations and other copy correspondence; Deposit return bank details; Forwarding address	Details are held on the Reapit database platform whilst tenancy is live and for a period of 6 years following the end of tenancy then deleted.	PRS Team

Non - Customer Data

Personal data record category	Mandated retention period	Record owner
Name, email address	Kept for 19 months on phased developments 13 months on non-phased unless requests to be removed from system at any stage. Housekeeping of stages within	Marketing and PRS Inbound Team PRS Inbound Team

	Zoho CRM system needs to be done weekly to ensure prospects are changed to resident where appropriate.	
Call recordings	Automatically deleted after 6 months	Sales

Special Category Data

Personal data record category	Mandated retention period	Record owner
Special category data relating to employees	6 years after employment ceases	HR
Special category data relating to unsuccessful job applicants	1 year following end of recruitment process	HR
Special category data relating to tenants	1 year after end of tenancy period (unless relevant to an ongoing claim, dispute or complaint)	Customer Service Delivery Manager
Special category data relating to unsuccesful tenancy applications	Deleted 3 months after end of unsuccesful application process	Customer Service Delivery Manager

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
Personal Network Drive	Reviewed quarterly, any documents containing PII deleted after 3 years	Individual employee
Local Drives & files	Moved to network drive monthly, then deleted from local drive	Individual employee
Google Drives, drop box	Reviewed quarterly, any documents containing PII deleted after 3 years	Individual employee
Onsite CCTV Recording	Footage overwritten automatically no more than 30 days after recording	CCTV system overwites footage automatically

Marketing Data

Personal data record category	Mandated retention period	Record owner
Online personal data (from websites, platforms, data capture forms, direct emails, PRS Inbox, etc.)	Zoho storage – to be kept for 19 months on phased developments 13 months on non-phased unless requests to be removed from system at any stage. Digital storage – deletion at point of request from website, PRS Inbox, server, mail chimp, etc. Otherwise deleted after 13	Marketing then PRS Inbound Team Marketing Team

	months.	
Drop box	4 years. If shared with client password protect (although no personal data involved).	Marketing Team
Supplier agreements	Length of contract plus 12 months	Marketing Team
Client details	Retain while a client	Marketing Team
Supplier details	Retain while a supplier	Marketing Team
Mail chimp/similar	Delete campaign within 3 months	Marketing Team
Social media posts	Permanent	Marketing Team

Block Management

Personal data record category	Mandated retention period	Record owner
Service Charge History	12 years after disinstruction (Source ARMA Guidance note F09)	Block Management department
Tenant's QUBE Record and associated saved documents	12 years after disinstruction (Source ARMA Guidance note F09)	Block Management department
Customer Complaints	6 years after the conclusion of the complaint (source ARMA Guidance note F09)	Block Management department
Copy Correspondence	3 years (source ARMA Guidance note F09) – This assumes that any correspondence which may be needed to defend a dispute is saved as part of the tenant record	Block Management department
RMC Information Articles and company minutes Share dealings Company register and seal Proxies / polling and voting records Director Specific Information (used for procuring insurance for example)	 Lifetime of the company (to be client on disinstruction) 12 years after the transaction Lifetime of the company 1 year 6 years following disinstruction	 Where LIV acts as director – Block Management department Or the client where they are director