GDPR Data Retention Policy

Policy Number	16
Version	1.0
Policy Contact	Matthew Betteridge
Date Issued	19th May 2018
Review Date	19th May 2019
Target Audience	Staff
Approved by	OneCall24 Policy Team

This Document defines OneCall24's Data Retention Policy ("Policy") and is to be used in conjunction with OneCall24's Data Privacy Policy to adhere to the General Data Protection Regulation (GDPR) 2018.

It sets the required retention periods for specified categories of personal data and sets out the minimum standards to be applied when destroying certain information within OneCall24.

The Policy consists of the following sections and applies to all staff without exception.

1. Retention Rules.
2. Safeguarding of Data during Retention Period.
3. Destruction of Data.
4. Breach, Enforcement and Compliance.
5. Document Disposal.
6. Appendix – Data Retention Schedule.

Adherence forms part of the employee's terms and conditions of employment and any breaches of policy may be considered a disciplinary offence and could lead to dismissal.

OneCall's Policy Lead Susanna Caddeo has overall responsibility for the Policy, its implementation and the effect it has on all staff.

1. Retention Rules.

OneCall24's GDPR Owner Matthew Betteridge defines the time period for which the documents and electronic records should to be retained through the Data Retention Schedule.

In the event, for any category of documents not specifically defined elsewhere in this Policy (and in particular within the Data Retention Schedule) and unless otherwise mandated differently by applicable law, the required retention period for such document will be deemed to be 10 years from the date of creation of the document.

As an exemption, retention periods within Data Retention Schedule can be prolonged in cases such as:

- Ongoing investigations from Member States authorities, if there is a chance records of personal data are needed by OneCall24 to prove compliance with any legal requirements; or
- When exercising legal rights in cases of lawsuits or similar court proceeding recognized under local law.

2. Safeguarding of Data during Retention Period.

The possibility that data media used for archiving will wear out shall be considered. If electronic storage media are chosen, any procedures and systems ensuring that the information can be accessed during the retention period (both with respect to the information carrier and the readability of formats) shall also be stored in order to safeguard the information against loss as a result of future technological changes. The responsibility for the storage falls to the GDPR Owner.

3. Destruction of Data.

OneCall24 and its employees will, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant. See Appendix for the Data Retention Schedule. Overall responsibility for the destruction of data falls to the GDPR Owner.

Once the decision is made to dispose according to the Data Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding. The Document Disposal section below defines the mode of disposal.

The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the GDPR Owner subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and OneCall24's Data Protection Policy shall be complied with.

Appropriate controls shall be in place that prevents the permanent loss of essential information of OneCall24 as a result of malicious or unintentional destruction of information.

The GDPR Owner shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

4. Breach, Enforcement and Compliance.

The GDPR Owner has the responsibility to ensure that each of OneCall24's offices comply with this Policy. It is also the responsibility of the GDPR Owner to assist any local office with enquiries from any local data protection or governmental authority.

Any suspicion of a breach of this Policy must be reported immediately to GDPR Owner. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate.

Failure to comply with this Policy may result in adverse consequences, including, but not limited to, loss of customer confidence, litigation and loss of competitive advantage, financial loss and damage OneCall24's reputation, personal injury, harm or loss. Non-compliance with this Policy by permanent, temporary or contract employees, or any third parties, who have been granted access to OneCall24 premises or information, may therefore result in disciplinary proceedings or termination of their employment or contract. Such non-compliance may also lead to legal action against the parties involved in such activities.

5. Document Disposal.

Records which may be routinely destroyed unless subject to an on-going legal or regulatory inquiry are as follows:

- Announcements and notices of day-to-day meetings and other events including acceptances and apologies.
- Requests for ordinary information such as travel directions.
- Reservations for internal meetings without charges / external costs.
- Transmission documents such as letters, fax cover sheets, e-mail messages, routing slips, compliments slips and similar items that accompany documents but do not add any value.
- Message slips.
- Superseded address list, distribution lists etc.
- Duplicate documents such as CC and FYI copies, unaltered drafts, snapshot printouts or extracts from databases and day files.
- Stock in-house publications which are obsolete or superseded.
- Trade magazines, vendor catalogues, flyers and newsletters from vendors or other external organizations.

In all cases, disposal is subject to any disclosure requirements which may exist in the context of litigation.

Confidential documents (i.e. those that contain information that is of the highest security and confidentiality and those that include any personal data) shall be disposed of as confidential waste (cross-cut shredded and incinerated) and shall be subject to secure electronic deletion.

Proprietary documents (i.e. those that contain confidential information such as parties' names, signatures and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal data) should be cross-cut shredded and then placed into locked rubbish bins for collection by an approved disposal firm, and electronic documents will be subject to secure electronic deletion.

All other documents (i.e. those that Level do not contain any confidential information or personal data and are published OneCall24 documents) should be strip-shredded or disposed of through a recycling company and include, among other things, advertisements, catalogues, flyers, and newsletters. These may be disposed of without an audit trail.

If you require further information regarding any aspect of this policy, please contact your line manager.

Appendix – Data Retention Schedule

Financial Records

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

Credit card receipts	Seven 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	Permanent	Finance
Office and team meeting minutes		Finance
Annual corporate filings	Permanent	Finance

HR: Employee and Candidate Records

Personal data record category	**Mandated retention period**	**Record owner**
Disciplinary, grievance proceedings records, oral/verbal, written, final warnings, appeals	As per legal requirement; for such period as required by policies or potential legal claim arising from same	HR
Applications for jobs, interview notes – Recruitment/promotion panel Internal: Where the candidate is unsuccessful and has not been made compliant Where the candidate is successful	 Archived as 'Do Not Use' after six months. Seven years after last assignment	HR
Payroll input forms, wages/salary	Seven years after last	HR

records, overtime/bonus payments Payroll sheets, copies	assignment	
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	Seven years after last assignment	HR
Employee address details	Seven years after last assignment	HR
Expense claims	As per legal requirement	HR
Annual leave records	Seven years after last assignment	HR
Accident books Accident reports and correspondence	As per legal requirement	HR
Certificates and self-certificates relating to Compliance and Competencies	Seven years after last assignment	HR
Pregnancy/childbirth certification	Seven years after last assignment	HR
Parental leave	Seven years after last assignment	HR
Maternity pay records and calculations	Seven years after last assignment	HR
Redundancy details, payment calculations, refunds, notifications	Seven years after last assignment	HR
Training and development records	Seven years after last assignment	HR

CRM data – inclusive of Name, Photo, Email address, mobile number, address, emails and phone call summaries, DPO information	Seven years after signing contract, compliance lapsing or request from Candidate to delete.	Registration & Compliance

Contracts

Personal data record category	**Mandated retention period**	**Record owner**
Signed	Permanent	Finance
Contract amendments	Permanent	Finance
Successful tender documents	Permanent	Finance
Unsuccessful tenders' documents	Permanent	Finance
Tender – user requirements, specification, evaluation criteria, invitation	Permanent	Finance
Contractors' reports	Permanent	Finance
Operation and monitoring, eg complaints	Permanent	Finance

Customer Data

Personal data record category	**Mandated retention period**	**Record owner**
CRM data – inclusive of Name, Email address, mobile number, address, emails and phone call summaries, DPO information	Seven years after last assignment or request from Customer to delete records.	Business Systems Administrator
Metrics data	Seven years after last assignment or request from Customer to delete.	Business Systems Administrator

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 & 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 attachments deleted after three years.	Individual employee
Deleted Emails	Cleared monthly	Individual employee
Personal Network Drive	Reviewed quarterly, deleted after ten years.	Individual employee
Local Drives & files	Moved to network drive monthly, then deleted from local drive.	Individual employee
Shared Drives, Drop box	Reviewed quarterly, deleted after seven years.	Individual employee

Review

This policy statement will be reviewed annually as part of our commitment to upholding professional standards. It may be altered from time to time in the light of legislative changes, operational procedures or other prevailing circumstances.