Data Retention Policy

Metadata Training

CONTENTS

1. Purpose, Scope and Users

I. This policy 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 Metadata Ltd (further: the “Company”).

II. This Policy applies to all business, processes, and systems of Metadata Ltd.

III. This Policy applies to all Company officers, directors, employees, agents, affiliates, contractors, consultants, advisors or service providers that may collect, process, or have access to data (including personal data and/or sensitive personal data). It is the responsibility of all of the above to familiarise themselves with this Policy and ensure adequate compliance with it.

IV. This policy applies to all information used at the Company. Examples of documents include:

- Emails
- Printed documents
- Electronic documents
- Videos
- Legal and financial documents

Reference Documents

I. EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC).

II. Privacy Policy.

2. Retention Rules

2.1. Retention General Principle

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 6 years from the date of creation of the document.

2.2. Retention General Schedule

I. The Data Protection Officer defines the time period for which the documents and electronic records should be retained through the Data Retention Schedule.

II. 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 the Company to prove compliance with any legal requirements; or
- When exercising legal rights in cases of lawsuits or similar court proceeding recognized under local law.

2.3 Safeguarding of Data during Retention Period

I. Metadata Ltd stores data using third party systems and back-up mechanisms that are password protected and saved on secured servers.

II. The third-party systems we use are constantly updated so all the software we use is kept up to date in terms of security and maintenance.

III. We use cloud systems monitored and maintained by qualified personnel and backups are taken regularly so we are protected against loss of data. Backups are also taken on other systems other than the system who store the data.

IV. During the retention period the data can be easily accessed by the person needed to access it and then it is archived.

V. The responsibility for the storage falls to the Data Protection Officer.

2.4. Destruction of Data

I. The Company and its employees should therefore, 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 retention schedule. Overall responsibility for the destruction of data falls to the Data Protection Officer.

II. Once the decision is made to dispose according to the 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.

III. 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 Schedule section below defines the mode of disposal.

IV. In this context, the employee shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Data Protection Officer subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and the Company's Privacy Policy shall be complied with.

V. Appropriate controls shall be in place that prevents the permanent loss of essential information of the company as a result of malicious or unintentional destruction of information – these controls are described in the company's IT Security Policy.

VI. The Data Protection Officer 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.

3. Breach, Enforcement and Compliance

I. The person appointed with responsibility for Data Protection, the Data Protection Officer has the responsibility to ensure that the Company's office complies with this Policy. It is also the responsibility of the Data Protection Officer to assist with enquiries from any data protection or governmental authority.

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

III. 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 to the Company'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 Company 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.

4. Document Disposal

4.1. Routine Disposal Schedule

I. 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 slip 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.
- Trade magazines, vendor catalogues, flyers and newsletters from vendors or other external organizations.

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

4.2. Destruction Method

I. Level I documents are those that contain information that is of the highest security and confidentiality and those that include any personal data. These documents shall be disposed of as confidential waste (cross-cut shredded and incinerated) and shall be subject to secure electronic deletion. Disposal of the documents should include proof of destruction.

II. Level II documents are proprietary documents 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. The documents 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.

III. Level III documents are those that do not contain any confidential information or personal data and are published Company documents. These 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.

5. Validity and document management

- This document is valid as of June 2021.

- The owner of this document is the Data Protection Officer who must check and, if necessary, update the document at least once a year.

6. Appendices

Appendix – Data Retention Schedule

6.1. Financial Records

Personal data record category	Mandated retention period	Record owner
Payroll records	6 years after audit	Finance
Supplier contracts	6 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)	6 years	Finance
Invoices	6 years	Finance

Cancelled cheques	6 years	Finance
Bank deposit slips	6 years	Finance
Business expenses documents	6 years	Finance
Check registers/books	6 years	Finance
Property/asset inventories	6 years	Finance
Credit card receipts	3 years	Finance
Petty cash receipts/documents	3 years	Finance

6.2. Business Records

Personal data record category	Mandated retention period	Record owner
Board policies	Permanent	Finance
Board meeting minutes	Permanent	Finance
Tax or employee identification number designation	Permanent	Finance
Office and team meeting minutes	3 years	Finance
Annual corporate filings	Permanent	Finance

6.3. HR and 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

6.3. 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, e.g. complaints	Permanent	Finance

6.4. Customer Data

Personal data record category	**Mandated retention period**	**Record owner**
Delegates data – inclusive of bookings, exams, contact details including address, first and second name	Deleted after 6 years or at the customer request after 1 year from the date of booking.	Customer
Live chat history	Records deleted after 1 year	Support
Email Correspondence	Manually archived. Retained for 6 years.	Support
CRM data – inclusive of Name, Email address, mobile number, address, emails and phone call summaries,	Unsubscribed customers/contacts are removed every year.	Support

6.5. 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

6.6 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 Google Drive	Reviewed quarterly, any documents containing PII deleted after 3 years	Individual employee
Local Drives & files	Moved to Google Drive monthly, then deleted from local drive	Individual employee
Google Drives, drop box	Reviewed quarterly.	Individual employee

7. Contact us

- You can write to us at Metadata Training, 13 Cropley Street, London, N17GF or you can send an email to us at info@metadatatraining.co.uk.