Holly McAlpine Consulting Ltd
www.hollymcalpine.com
dpo@hollymcalpine.com

Data Retention Schedule

1. Introduction

This document outlines the data retention schedule for Holly McAlpine Consulting Ltd. This schedule ensures compliance with the General Data Protection Regulation (GDPR) and relevant UK data protection laws. The schedule specifies the retention periods for different categories of personal data and provides guidance on how data should be securely disposed of once it is no longer required.

2. Principles of Data Retention

Lawfulness, Fairness, and Transparency: Personal data will be processed lawfully, fairly, and in a transparent manner.

- Purpose Limitation: Data will only be collected for specified, explicit, and legitimate purposes.
- Data Minimisation: Only data that is necessary for the specified purposes will be collected.
- Accuracy: Personal data will be accurate and kept up to date.
- Storage Limitation: Personal data will be kept in a form that permits identification of data subjects for no longer than is necessary.
- Integrity and Confidentiality: Personal data will be processed securely to protect against unauthorised or unlawful processing, accidental loss, destruction, or damage.

3. Retention Periods

Category of Data	Description	Retention Period	Reason/Justification	Action After Retention Period
Client Data	Information relating to clients, including contracts and communications.	6 years from the end of the client relationship.	Limitation Act 1980; for potential legal claims.	Securely delete or anonymise data.
Employee Data	Data relating to any employees (past and present), including payroll, performance, and disciplinary records.	6 years from the end of employment.	Employment Rights Act 1996; for potential legal claims.	Securely delete or anonymise data.
Consultancy Project Data	Data collected and created during HR consultancy projects,	3 years from the end of the engagement.	Legitimate interest for reference and case studies.	Securely delete or anonymise data.

	including reports and analyses.			
Client Employee Data	Personal information of employees and contractors collected and processed to perform the services.	1 month from the end of the engagement.	Requirement to collect and process employee data to perform the service. Ensure sufficient time for data to be returned to client at end of engagement.	Transfer to data controller or securely delete data.
Financial Records	Invoices, receipts, tax returns, and other financial records.	6 years from the end of the financial year to which they relate.	HMRC requirements.	Securely delete or anonymise data.
Marketing Data	Data collected for marketing purposes, including mailing lists and campaign data.	2 years from the last interaction with the data subject.	Legitimate interest in marketing and business development.	Securely delete or anonymise data.
Supplier Data	Information relating to suppliers, including contracts and payment details.	6 years from the end of the supplier relationship.	Limitation Act 1980; for potential legal claims.	Securely delete or anonymise data.
Health and Safety Records	Records of health and safety incidents, including risk assessments and accident logs.	6 years from the date of the incident.	Limitation Act 1980; for potential legal claims.	Securely delete or anonymise data.
Job Applicant Data	CVs, cover letters, and interview notes for unsuccessful applicants.	6 months from the date of the decision.	Legitimate interest for future reference.	Securely delete or anonymise data.
Data Subject Requests	Records of data subject access requests and related communications.	2 years from the date of the request.	GDPR compliance tracking and auditing.	Securely delete or anonymise data.
IT System Logs	Logs of system access, emails, and other IT-related data.	1 year from the date of creation.	Security monitoring and auditing.	Securely delete or anonymise data.

4. Secure Disposal of Data

When data reaches the end of its retention period, it is securely disposed of. This includes:

- Digital Data: Deleting files securely so that they cannot be recovered. This may involve using specialised software to permanently erase the data.
- Physical Data: Shredding paper documents and ensuring they are recycled or disposed of securely.

5. Regular Review and Updates

This Data Retention Schedule will be reviewed annually or whenever there are significant changes in the business processes, applicable laws, or regulations to ensure continued compliance with GDPR.

6. Data Retention Responsibilities

As the Director of Holly McAlpine Consulting Ltd, Holly McAlpine is responsible for ensuring compliance with this Data Retention Schedule and the secure management of all personal data handled by the consultancy.

By adhering to this Data Retention Schedule, Holly McAlpine Consulting Ltd ensures that personal data is managed in compliance with GDPR, thereby minimising risks associated with data breaches and maintaining the trust of clients, suppliers, and other stakeholders.

7. Document Control

Version	Date	Author	Reason
1.0	1 September 2024	Holly McAlpine	New document