ALLIOTTS
PART OF THE SHAW GIBBS GROUP

Alliotts LLP

Data Retention and Deletion Policy

---

1. Purpose

This policy establishes the standards and procedures for the retention and destruction of personal data collected and processed by Alliotts LLP as part of the Shaw Gibbs Group ("the Firm") in relation to its clients and employees. The policy aims to ensure compliance with applicable data protection laws while balancing business needs, professional obligations, and individual rights.

2. Scope

This policy applies to all personal data processed by the Firm, including:

- Client personal data
- Employee and contractor personal data
- Job applicant data
- Data of client representatives and contacts
- Data of third-party service providers and vendors

It covers personal data in all formats, including electronic records, paper documents, emails, and other communication records.

3. Policy Statement

The Firm is committed to retaining personal data only for as long as necessary for the purposes for which it was collected, or as required by applicable laws, regulations, or professional standards. Once the retention period has expired, personal data shall be securely destroyed or anonymized in accordance with this policy.

4. Roles and Responsibilities

4.1 Data Protection Officer

- Overall responsibility for compliance with this policy
- Regular review and update of retention schedules
- Approval of exceptions to standard retention periods
- Oversight of data destruction processes
- Liaison with regulatory authorities regarding retention matters

4.2 Department Heads

- Implementation of retention periods for their respective departments
- Ensuring compliance with retention schedules
- Coordination of periodic data clean-up operations
- Training staff on retention requirements
- Reporting retention issues to the Data Protection Officer

4.3 IT Department

- Implementation of technical solutions for automatic archiving and deletion
- Secure destruction of electronic data
- Maintenance of destruction logs and certificates
- Regular backup system purging
- Technical support for data retrieval and restoration

4.4 All Staff

- Adherence to retention schedules
- Proper classification of documents and data
- Reporting retention issues to the Data Protection Officer
- Participation in training programs
- Compliance with data handling procedures

5. Retention Periods

5.1 Client Data

Category	Retention Period	Trigger for Retention Period
Client identification and KYC data	7 years	From end of client relationship
Engagement/matter files	7 years	From closure of matter/engagement
Billing and financial records	7 years	From end of financial year
Client communications	6 years	From date of communication
Contracts and agreements	6 years	From contract expiry/termination
Special category data	3 years	From collection or last use
Regulated client data	As per regulatory requirements	As per regulatory requirements
Marketing preferences	Until withdrawn	From collection or last confirmation

5.2 Employee Data

Category	Retention Period	Trigger for Retention Period
Personnel files	6 years	From end of employment
Payroll and tax information	7 years	From end of relevant tax year
Recruitment data (successful)	Duration of employment + 6 years	From end of employment
Recruitment data (unsuccessful)	1 year	From notification of decision
Performance reviews	5 years	From date of review
Disciplinary records	2 years	From resolution of issue
Health and safety records	3 years	From date of record
Training records	5 years	From completion of training
Employment contracts	6 years	From end of employment
Immigration status documents	2 years	From end of employment
Pension records	Duration of scheme membership + 6 years	From end of scheme membership

5.3 Special Cases and Exceptions

The following circumstances may extend or modify standard retention periods:

- **Litigation holds:** Data subject to litigation holds will be retained until the hold is lifted
- **Regulatory investigations:** Data relevant to ongoing investigations will be retained until resolution
- **Contractual requirements:** Where client agreements specify longer retention periods
- **Professional liability concerns:** Extended retention may apply where professional liability risks exist
- **Precedent value:** Anonymized versions may be retained indefinitely for reference purposes

6. Data Destruction

6.1 Electronic Data Destruction

Electronic data destruction must follow these procedures:

- Deletion from active systems using secure deletion methods
- Decommissioning of storage media using industry standards (e.g., DOD 5220.22-M)
- Regular purging of backup systems according to backup rotation policy
- Verification processes to confirm complete destruction
- Documentation of destruction in destruction logs
- Overwriting of data multiple times to prevent recovery

6.2 Physical Document Destruction

Physical document destruction requirements:

- Paper shredding to at least Level P-4 (DIN 66399)
- Use of certified destruction service providers
- Certificates of destruction to be maintained for audit purposes
- Secure storage pending destruction
- On-site shredding for highly sensitive materials
- Witnessed destruction for confidential documents

6.3 Third-Party Service Providers

When using third-party destruction services:

- Contractual obligations for data destruction must be established
- Right to audit destruction processes must be maintained
- Certification of destruction must be obtained
- Regular compliance reviews must be conducted
- Chain of custody documentation must be maintained

7. Documentation and Compliance

7.1 Retention Documentation

The Firm shall maintain comprehensive records including:

- Data inventory and retention schedule
- Destruction certificates and logs
- Exception requests and approvals
- Compliance audit reports
- Training records and attendance logs

7.2 Regular Reviews

The following review schedule shall be maintained:

- **Annual review** of retention schedules and policy effectiveness
- **Regular compliance audits** to ensure adherence to procedures
- **Regular staff training** on retention requirements and updates
- **Monthly monitoring** of destruction activities and logs

8. Data Subject Rights

8.1 Right to Erasure

Requests for erasure will be handled according to the Firm's Data Subject Access Rights procedure, taking into account:

- Legal and professional obligations to retain certain data
- Legitimate interests for retention
- Technical limitations and feasibility
- Contractual obligations to clients or third parties
- Regulatory requirements and professional standards

8.2 Right to Access

Data subjects have the right to access their personal data, including:

- Information about retention periods applicable to their data
- Rationale for retention decisions
- Expected deletion dates where applicable
- Details of any exceptions to standard retention periods

9. Archiving

9.1 Archiving Process

Data archiving procedures include:

- Transfer of data not actively needed but within retention period to archive systems
- Archive access limited to authorized personnel only
- Regular integrity checks of archived data
- Clear restoration procedures for archived data
- Documented chain of custody for archived materials

9.2 Archive Security

Archive security measures include:

- Encryption of archived electronic data
- Physical security for stored media and documents
- Access logging and monitoring systems
- Regular security assessments and updates
- Environmental controls for physical storage areas

10. Training and Awareness

10.1 Training Requirements

All staff should receive:

- Initial training on this policy during onboarding
- Annual refresher training on retention requirements
- Department-specific training based on data handling responsibilities
- Communication on policy updates and changes
- Specialized training for staff with elevated data handling responsibilities

10.2 Training Records

The Firm should maintain records of:

- Training completion by all staff members
- Training content and materials used
- Assessment results where applicable
- Refresher training schedules and completion

11. Policy Review and Updates

11.1 Review Schedule

This policy should be reviewed bi-annually or whenever there are significant changes to:

- Applicable laws and regulations
- Professional standards and industry best practices
- Business operations and data processing activities
- Risk assessments and threat landscapes
- Technology systems and capabilities

11.2 Update Process

Policy updates will follow these procedures:

- Draft revisions prepared by the Data Protection Officer
- Consultation with relevant department heads
- Legal review where necessary
- Approval by senior management
- Communication to all staff as appropriate
- Implementation with appropriate training

12. Non-Compliance

12.1 Consequences

Failure to comply with this policy may result in:

- Disciplinary action up to and including termination
- Regulatory penalties and fines
- Reputational damage to the Firm
- Legal liability and potential litigation
- Loss of professional certifications or licenses

12.2 Reporting

All instances of non-compliance must be reported to the Data Protection Officer immediately for investigation and remediation.

13. Related Policies and Procedures

This policy should be read in conjunction with:

- Data Protection Policy
- Data Security Policy
- Employee Privacy & Data Protection Policy
- Third-Party Data Processing Agreements (as applicable)
- DPIAs (as applicable)
- ROPAs (as applicable)

14. Contact Information

For questions or concerns regarding this policy, contact:

Data Protection Officer – Tania Bennett
Email: tania.bennett@shawgibbs.com
Phone: +44 (0)1865 262200

Policy Owner - Mark Ferguson
Email: mark.ferguson@shawgibbs.com
Phone: +44 (0)1865 262200