Southern Communications Group

Data Retention Policy

TABLE OF CONTENTS

1. ABOUT THIS POLICY

1.1 The corporate information, records and data of Southern Communications Group is important to how we conduct business and manage employees.

1.2 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our business operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business.

1.3 This Data Retention Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

1.4 Failure to comply with this policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.

1.5 This policy does not form part of any employee's contract of employment, and we may amend it at any time.

2. SCOPE OF POLICY

2.1 This policy covers all data that we hold or have control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

2.2 This policy covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage. It also covers data that belongs to us but is held by employees on personal devices.

2.3 This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, personal data and non-personal data. It also gives guidance on how we classify our data.

2.4 This policy applies to all business units and functions of Southern Communications Group.

3. GUIDING PRINCIPLES

Through this policy, and our data retention practices, we aim to meet the following commitments:

- We comply with legal and regulatory requirements to retain data.
- We comply with our data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
- We handle, store and dispose of data responsibly and securely.
- We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason.
- We allocate appropriate resources, roles and responsibilities to data retention.

- We regularly remind employees of their data retention responsibilities.

- We regularly monitor and audit compliance with this policy and update this policy when required.

4. ROLES AND RESPONSIBILITIES

4.1 **Responsibility of all employees**. We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised compliance good practices. All employees must comply with this policy, the Data Retention Schedule, any communications suspending data disposal and any specific instructions from the Data Protection Officer (DPO) or their delegate/s. Failure to do so may subject us, our employees, and contractors to serious civil and/or criminal liability. An employee's failure to comply with this policy may result in disciplinary sanctions, including suspension or termination. It is therefore the responsibility of everyone to understand and comply with this policy.

4.2 **Records Management Department and Records Management Officer**. The DPO or their delegate/s is responsible for identifying the data that we must or should retain, and determining, in collaboration with the senior management team, the proper period of retention. They also arrange for the proper storage and retrieval of data, co-ordinating with outside vendors where appropriate.

4.3 We have designated our Chief Information and Security Officer (CISO) as the DPO. The DPO is responsible for:

- Administering the data management programme;

- Helping department heads implement the data management programme and related best practices;

- Planning, developing, and prescribing data disposal policies, systems, standards, and procedures; and

- Providing guidance, training, monitoring and updating in relation to this policy.

4.4 **Data Protection Officer.** Our Data Protection Officer (DPO) or their delegate/s is also responsible for advising on and monitoring our compliance with data protection laws which regulate personal data. This includes reviewing the retention requirements for personal data and monitoring compliance with this policy in relation to personal data.

5. TYPES OF DATA AND DATA CLASSIFICATIONS

5.1 **Formal or official records.** Certain data is more important to us and is therefore listed in the Data Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. Please see paragraph 6.1 below for more information on retention periods for this type of data.

5.2 **Disposable information**. Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Data Retention Schedule. Examples may include:

- Duplicates of originals that have not been annotated.

- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.

- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of Southern Communications Group and retained primarily for reference purposes.

- Spam and junk mail.

  Please see paragraph 6.2 below for more information on how to determine retention periods for this type of data.

5.3 **Personal data.** Both formal or official records and disposable information may contain personal data; that is, data that identifies living individuals. Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). See paragraph 6.3 below for more information on this.

5.4 **Confidential information belonging to others**. Any confidential information that an employee may have obtained from a source outside of Southern Communications Group , such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted, if received via the internet.

5.5 **Data classifications.** Some of our data is more confidential than other data. Our Data Protection Policy and Information Classification Policy explain how we classify data and how each type of data should be marked and protected. When complying with this policy, it is also important that you follow our Data Protection Policy and Information Classification Policy.

6. RETENTION PERIODS

6.1 **Formal or official records.** Any data that is part of any of the categories listed in the Data Retention Schedule contained in the Appendix to this policy, must be retained for the amount of time indicated in the Data Retention Schedule. A record must not be retained beyond the period indicated in the Data Retention Schedule, unless a valid business reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the DPO.

6.2 **Disposable information.** The Data Retention Schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of.

6.3 **Personal data.** As explained above, data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). Where data is listed in the Data Retention Schedule, we have taken into account the principle of storage limitation and balanced this against our requirements to retain the data. Where data is disposable information, you must take into account the principle of storage limitation when deciding whether to retain this data. More information can be found in in our Data Protection Policy.

6.4 **What to do if data is not listed in the Data Retention Schedule.** If data is not listed in the Data Retention Schedule, it is likely that it should be classed as disposable information. However, if you consider that there is an omission in the Data Retention Schedule, or if you are unsure, please contact the DPO.

7. STORAGE, BACK-UP AND DISPOSAL OF DATA

7.1 **Storage.** Our data must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site as set out in our Business Continuity Plan.

7.2 **Destruction**. Our DPO is responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction. The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling. The destruction of electronic data must be co-ordinated with the IT Department.

7.3 The destruction of data must stop immediately upon notification from the DPO that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation (see next paragraph). Destruction may begin again once the DPO lifts the requirement for preservation.

8. SPECIAL CIRCUMSTANCES

8.1 **Preservation of documents for contemplated litigation and other special situations.** We require all employees to comply fully with our Data Retention Schedule and procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or the DPO informs you, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until the DPO determines those records are no longer needed. Preserving documents includes suspending any requirements in the Data Retention Schedule and preserving the integrity of the electronic files or other format in which the records are kept.

8.2 If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the DPO.

8.3 In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

9. WHERE TO GO FOR ADVICE AND QUESTIONS

Questions about the policy. Any questions about retention periods relevant to your function **or** department should be raised with your line manager or function **or** department data retention lead. Any questions about this policy should be referred to the DPO dpo@scgconnected.co.uk, who is in charge of administering, enforcing, and updating this policy.

10. BREACH REPORTING AND AUDIT

10.1 **Reporting policy breaches.** We are committed to enforcing this policy as it applies to all forms of data. The effectiveness of our efforts, however, depend largely on employees. If you feel that you or someone else may have breached this policy, you should report the incident immediately to your manager. If you are not comfortable bringing the matter up with your immediate manager, or do not believe the manager has dealt with the matter properly, you should raise the matter with the manager at the next level above your direct manager or the

DPO. If employees do not report inappropriate conduct, we may not become aware of a possible breach of this policy and may not be able to take appropriate corrective action.

10.2 No one will be subject to and we do not allow, any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or co-operating in related investigations.

10.3 **Audits**. Our DPO will periodically review this policy and its procedures (including where appropriate by taking outside legal or auditor advice to ensure we are in compliance with relevant new or amended laws, regulations or guidance. Additionally, we will regularly monitor compliance with this policy, including by carrying out audits.

11. OTHER RELEVANT POLICIES

This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our:

- Quality and Information Security Policy
- IT Network Management and Security
- Privacy Policy
- Data Protection Policy
- Information Classification Policy
- Supplier Security Management
- And other IT, security and data related policies, which are available to all staff via company secure methodology.

12. CHANGES TO THIS DATA RETENTION POLICY

12.1 We reserve the right to change this Data Retention Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Data Retention Policy.

Appendix A - DEFINITIONS

Data: all data that we hold or have control over and therefore to which this policy applies. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

Data Protection Officer: the person who is responsible for advising on and monitoring compliance with data protection laws.

Data Retention Policy: this policy, which explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

Data Retention Schedule: the schedule attached to this policy which sets out retention periods for our formal or official records of Southern Communications Group:

Disposable information: disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Data Retention Schedule.

Formal or official record: certain data is more important to us and is therefore listed in the Data Retention Schedule. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. We refer to this as formal or official records or data.

Non-personal data: data which does not identify living individuals, either because it is not about living individuals (for example financial records) or because it has been fully anonymised.
Personal data: any information identifying a living individual or information relating to a living individual that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special categories of personal data such as health data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Data Protection Officer (DPO): The Chief Information and Security Officer (CISO) or their delegate/s is the Company's current DPO. HR will also assist the DPO with responsibility for data protection compliance.

Storage limitation principle: data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed. This is referred to in the UK GDPR as the principle of storage limitation.

Appendix B – DATA RETENTION SCHEDULE

1. **ABOUT THIS SCHEDULE**

1.1 Southern Communications Group establishes retention or destruction schedules or procedures for specific categories of data. This is done to ensure legal compliance (for example, with our data protection obligations) and accomplish other objectives, such as protecting intellectual property and controlling costs.

1.2 Employees should comply with the retention periods listed in the data retention schedule below, in accordance with the Southern Communications Group Data Retention Policy available online in the Company GDPR folder.

1.3 If you hold data not listed below, please refer to the Southern Communications Group Data Retention Policy. If you still consider your data should be listed, if you become aware of any changes that may affect the periods listed below or if you have any other questions about this data retention schedule, please contact the DPO.

1.4 This version is dated 6th February 2024.

2. **COMPANY AND CORPORATE RECORDS**

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Accounting records.	-3 years from the date they were made (private company) -6 years from the date they were made (public company)	Section 388(4) Companies Act 2006 (CA 2006)	Tax requirements or other legislation may require longer.
Register of members.	Entries for former members can be removed 10 years after the date they ceased to be members.	Section 121, CA 2006	
Register of directors.	Indefinite	Usual practice	Section 162 of the CA 2006 requires the register to be kept but legislation is not explicit about retention periods. General practice is to retain details of current and former directors, together with date of ceasing to be a director.
Register of directors' residential addresses.	Remove addresses of former directors after 10 years.	Best practice	Section 165 of the CA 2006 requires the register to be kept but there is no statutory retention period or indication whether addresses of former directors should be removed. Company

			will need to consider anything that has been told to directors and what is appropriate.
Minutes of internal directors' meetings.	10 years from the date of the meeting	Section 248, CA 2006	Statutory minimum period (no period applies to meetings held **before** 1 October 2007, but best practice is to apply a consistent standard).
Members resolutions passed other than at general meetings; minutes of general meetings, details of decisions provided by a sole director.	10 years from date of resolution, decision or meeting	Sections 355 and s358, CA 2006	Minimum period; can be extended if appropriate.
Health and safety inspections, property management and asset records.	6 years	Health and Safety at Work Act 1974 and Limitation Act 1980 (LA 1980)	
Historical records and archives about the company e.g. former directors, chairpersons, employees of note etc.	Indefinite	Usual practice	Balance data minimisation principle against the need to retain this information for historical purposes in the legitimate interests of the organisation.
Management System records including but not limited to Management Review Minutes, Audit Reports.	At least 2 years	Best practice Business need	These records will assist in demonstrating compliance and adherence to ISO standards, regulatory requirements and continuous improvement efforts within the organisation.

3. EMPLOYMENT RECORDS

Type of employment record	Retention period

Recruitment records. These may include: - Completed online application forms or CVs. - Equal opportunities monitoring forms. - Assessment exercises or tests. - Notes from interviews and short-listing exercises. - Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file.)	Six months after notifying candidates of the outcome of the recruitment exercise.
Immigration checks	Three years after the termination of employment.
Contracts. These may include: - Written particulars of employment. - Contracts of employment or other contracts. - Documented changes to terms and conditions.	While employment continues and for seven years after the contract ends.
Collective agreements Collective workforce agreements and past agreements that could affect present employees.	Any copy of a relevant collective agreement retained on an employee's record will remain while employment continues and for seven years after employment ends.
Payroll and wage records. These may include: - Payroll and wage records - Details on overtime. - Bonuses. - Expenses. - Benefits in kind.	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.

Current bank details	Bank details will be deleted as soon after the end of employment as possible once final payments have been made
PAYE records	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Payroll and wage records for companies	These must be kept for six years from the financial year-end in which payments were made. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Records in relation to hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they will be retained for seven years after the working relationship ends.
Travel and subsistence	While employment continues and for seven years after employment ends.

Record of advances for loans to employees	While employment continues and for seven years after employment ends.
Personnel records. These include: - Qualifications/references. - Consents for the processing of special categories of personal data. - Annual leave records. - Annual assessment reports. - Disciplinary procedures. - Grievance procedures. - Flexible working requests and documentation; - Death benefit nomination and revocation forms. - Resignation, termination and retirement.	While employment continues and for seven years after employment ends. Any disciplinary records that have expired will be removed after the relevant timescales. Annual leave data will be held separately. Qualifications/Training records held separately.
Records in connection with working time Working time opt-out Records to show compliance, including: - Time sheets for opted-out workers. - Health assessment records for night workers.	 Three years from the date on which they were entered into. Three years after the relevant period.
Maternity records. These include: - Maternity payments. - Dates of maternity leave. - Period without maternity payment. - Maternity certificates showing the expected week of confinement.	These must be kept for three years after the end of the tax year in which the maternity pay period ends. However, given their potential relevance to pay disputes they will be retained for seven years after the working relationship ends.

For the avoidance of doubt documents relating to other forms of family leave will be retained in the same way.	
Accident records These are created regarding any reportable accident, death or injury in connection with work.	For at least four years from the date the report was made.
REASON Employment Rights Act 1996, Working Time Regulations 1998, Equality Act 2010. **Employment data comments** Where necessary, may include special categories of data, including but not limited to essential medical data, data to comply with anti-discrimination law, trade union membership.	

4. **PENSIONS RECORDS**

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Name and address of scheme or provider of the automatic enrolment scheme used to comply with the employer's duties.	6 years	Employers' Duties (Registration and Compliance) Regulations 2010 (*SI 2010/5*) (Employers' Duties Regulations 2010) (regulations 5, 6 and 8).	Minimum statutory period.
Employer pension scheme reference.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).	Minimum statutory period.
Evidence scheme complies with auto-enrolment statutory quality tests.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).	Minimum statutory period.
Name, NI number, date of birth and automatic enrolment date of all jobholders auto-enrolled (and corresponding details for non-eligible jobholders and entitled workers who have opted in or joined).	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).	Minimum statutory period.

Evidence of jobholders' earnings and contributions.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).	Minimum statutory period.
Contributions payable by employer in respect of jobholders and dates on which employer contributions were paid to scheme.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).	Minimum statutory period.
If auto-enrolment postponement period used, records of workers who were given notice of postponement including full name, NI number and date postponement notice was given.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).	Minimum statutory period.
Auto-enrolment opt-in notices, joining notices and opt-out notices (original format).	6 years (4 years for opt-out notices)	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).	Minimum statutory period. Opt-in notices, joining notices and opt-out notices must be kept in the original format, although copies of the original format or electronically stored versions are acceptable (*Pensions Regulator, Detailed Guidance Note 9, Keeping records, paragraph 8*).
If employer is (or was) sponsoring employer of an occupational pension scheme, any document relating to monies received by or owing to the scheme, investments or assets held by the scheme, payments made by the scheme, contracts to purchase a lifetime annuity in respect of scheme member and documents relating to the administration of the scheme.	For the tax year to which they relate and the following 6 years	Registered Pension Schemes (Provision of Information) Regulations 2006 (*SI 2006/567*) (regulation 18).	Minimum statutory period.
Information relating to applications for ill	While entitlement continues and for	Limitation period	Employers may also need to keep data

health early retirement benefits, including medical reports.	period of 15 years after benefits stop being paid.		relating to employees' job descriptions to assist with any ill-health application.
Death benefit nomination and revocation forms.	While entitlement continues and for period of 15 years after the death of member and their beneficiaries.	Limitation period	Longer may be required for public sector employees e.g. the National Archives suggests 100 years from date of birth.

5. FACILITIES AND SECURITY RECORDS

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
CCTV recordings.	30 days for routine recordings. As long as necessary for any investigations or claims that arise	Best practice	No set period in law but as these can contain personal data, should be kept for no longer than is necessary for the purpose. Relevant authorities must comply with the Surveillance Camera Code of Practice.
Visitor logs.	6 months	Best practice	No set period in law but as these can contain personal data, should be kept for no longer than is necessary for the purpose.
Property management and asset records.	6 years or 12 years depending on whether the agreement is executed as a simple contract or a deed respectively	Limitation period	If agreement has been executed as a simple contract, actions are time barred 6 years from the date of breach of contract (*section 5, Limitation Act 1980*). If the agreement is executed as a deed, actions are time barred 12 years from the accrual of the cause of action (*section 8, Limitation Act 1980*).
Building contracts.	12 years from practical completion when executed as a deed	Limitation period	Consideration may be given where appropriate to professional appointment, building contract, collateral warranty, third-party rights, development

			agreement and novation or assignment documents. Also potentially to related documents such as insurance and finance, for example, bonds and parent company guarantees. In addition, consideration may be given to other records relating to the building works, such as correspondence, which may be required in the event of a dispute.
Leases.	6 or 12 years depending on the issue	Limitation period	If the tenant has not paid rent, the landlord is time barred from recovering the same 6 years from the date the rent became due (*section 19, LA 1980*). Otherwise because a lease is usually executed as a deed, actions under leases are time barred 12 years from the accrual of the cause of action (section 8, LA 1980).
Health and safety files for building works.	6 years from completion	Limitation period	Organisations may wish to retain for longer to assist with future works and maintenance.
Environmental related records including but not limited to Waste Transfer notes and Consignment notes.	At least 3 years	General Waste Regulations, Hazardous Waste Regulations, WEEE Legislation, RoHS	Signed 'Transfer Notes' (or 'Consignment Notes' if the waste is hazardous) must be kept for a minimum of three years for Consignment Notes and two years for any waste received or transferred

6. IT RECORDS

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
General information about internally developed IT infrastructure, software and systems for internal use.	5 years from decommissioning of system	Business need	No statutory period so organisation can balance need to retain these records against data minimisation principle.
General information about externally developed IT infrastructure, software and systems for internal or external use.	7 years from decommissioning of system	Contractual obligation Limitation period	See also Procurement section
General information about internally developed IT infrastructure, software and systems for external use.	7 years from decommissioning of system	Contractual obligation Limitation period	Where IT infrastructure, software or systems are used externally (for example, by customers) then this information may be relevant to claims and disputes.
Systems monitoring, (for example, to detect and prevent failures vulnerabilities and external threats).	Current year plus 1 year Consider whether records can be fully anonymised after this period (or no personal data collected in first place) where there is a need to keep these logs for longer or indefinitely	Business need Contractual obligation Limitation period	No statutory period so organisation can balance need to retain these records against data minimisation principle. It may be advisable for an organisation to keep monitoring logs for as long as possible as malware or malicious code may go undetected in a system for a long period of time. Where IT infrastructure, software or systems are used externally (for example, by customers), monitoring logs might also be relevant to claims and disputes.
Business continuity and information security plans.	3 years from when the plan is superseded Consider whether record can be fully anonymised after this period (or no personal	Business need Legal or contractual obligation Limitation period	No statutory period so organisation can balance need to retain these records against data minimisation principle.

	data collected in first place) where there is a contractual or legal obligation to keep these plans for a longer period.		However, consider whether organisation is subject to any legal or contractual obligations in respect of business continuity which might necessitate a longer retention period, for example, under the NIS Regs. Where IT infrastructure, software or systems are used externally (for example, by customers), business continuity plans might also be relevant to claims and disputes.
Technical support and help-desk requests.	3 years from end of system Consider whether record can be fully anonymised after this period (or no personal data collected in first place) where there is a need to keep these requests for a longer period (for example, 7 years to align with limitation periods)	Business need. Contractual obligation. Limitation period.	No statutory period so organisation can balance need to retain these records against data minimisation principle. Consider whether support services are provided to external customers, in which case contractual obligations and limitation periods may be relevant.
Technical information relating to external customer user accounts.	1 year from account closure. Consider whether record can be fully anonymised after this period (or no personal data collected in first place) where there is a need to keep these plans for a longer period.	Business need Contractual obligation Limitation period	No statutory period so organisation can balance need to retain these records against data minimisation principle. Consider whether contractual obligations and limitation periods may be relevant.
Contracts and agreements (software licences, support agreements, hardware agreements etc.).	7 years from expiry of the agreement	Limitation period	See also Procurement section.
System backups.	3 months	Business need	May be different depending on the system.

7. SALES, MARKETING AND CUSTOMER RECORDS

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Bought in mailing lists and associated contracts.	1 year for mailing lists. 6 years from expiry or termination for contracts (12 years for contracts executed as a deed).	Best practice for mailing lists Limitation period for contracts	Consult ICO *guidance* on bought-in lists; ICO *Direct Marketing Code* recommends that organisations should not rely on indirect consent given more than 6 months ago.
Marketing database records (e.g. lead generation, meeting feedback, contact data etc.).	2 years from last contact	Business need	Depends on the nature of the business.
Customer relations database records (e.g. call centre records, queries, meeting feedback, account history etc.).	6 years from last contact	Business need and limitation period.	
Order fulfilment records.	6 years from completion	Limitation period and accounting requirement.	
Opt-out/suppression lists.	Indefinite	Business and compliance need.	Only sufficient information to enable the opt out should be retained.
Evidence of consent to marketing (including electronic marketing).	While consent valid 6 years from date consent withdrawn or ceases to be valid	Business need Limitation period	Consent can be withdrawn at any time and may not necessarily remain valid indefinitely although how long it remains valid will depend on the context.
Market research, marketing campaigns	2 years from completion	Business need	DMA suggests two years from last campaign.
Press releases	5 years from publication	Business need	
Customer complaints handling	6 years from settlement or closure	Business need and limitation period	
Website analytics reports from cookies and other similar technology	2 years	Business need	This refers to the output from information obtained via cookies. No firm period recommended by the ICO, although the French regulator recommends 25 months from collection and, for Google

			Analytics the DMA recommends 2 years. Cookies themselves may be set for different periods depending on the function of the cookie.

8. **PROCUREMENT RECORDS**

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Unsuccessful tenders	2 years	Business need	Businesses that have a large number of tenders may prefer to only retain for 1 year but will depend on the nature of the business.
Successful tenders	Contract period plus 6 years (12 years for contracts executed as a deed).	Limitation period	
Contractual documents	Contract period plus 6 years (12 years for contracts executed as a deed).	Limitation period	

9. **LEGAL RECORDS**

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Legal advice and opinions (non-litigation).	6 years after life of the service or matter the advice relates to	Business need	
Legal advice and other records relating to specific litigation or claim.	6 years from settlement or withdrawal of claim	Limitation period	
Data subject rights requests	6 years from closure of request	Limitation period	
Previous versions of policies, including IT policy, privacy policy, retention policy etc.	6 years form being superseded	Business need and limitation period in the event of a related claim	
Monitoring and investigation requests	6 years from closure of investigation [LINK TO ORGANISATION'S MONITORING POLICY]	Limitation period	
Insurance claims	3 years after settlement	Limitation period	