## Contents

### Table of Contents



## Version History and Approvals

| Version | Approval | Date |
|---|---|---|
| 3.0 – Review and updates. | DPO & MLRO/CCO | 2017 |
| 2.0 – Review | DPO & MLRO/CCO | 2015 |
| 1.0 - Creation | DPO & MLRO/CCO | 2013 |

## Introduction

This document outlines Numis Securities Limited's and Numis Asset Management Limited's ('the Firm' or 'Numis') legal obligations and policy on data protection.

In May 2018 the Data Protection Act 1998 will be replaced by the General Data Protection Regulations ("GDPR"). This policy is designed to make sure Numis is adhering to the standards required by the GDPR, which by default will cover the existing Data Protection Act requirements.

## Scope

This policy is applicable to all UK incorporated entities and subsidiaries of Numis PLC, hereafter known as "Numis"

All members of staff including contractors and anyone authorised to act on the firm's behalf must be familiar with this policy and aware of the risks and responsibilities relating to data protection.

Failure to comply with certain requirements can incur personal criminal and/or regulatory liability as well as legal, regulatory and/or reputational risk to the firm.

This policy should be read in conjunction with the following Numis polices/procedures:

- Numis Compliance Handbook
- Data Protection Booklet
- Numis Information Security policies

Further information can be obtained by reference to the Data Protection Act 1998 ("DP ACT") and also through the Information Commissioner's website.

## Rationale

**Legal Position**

In the UK, every individual has a legal right to privacy in respect of their own personal information, the Data Protection and the General Data Protection Regulations ("DPA") set standards to make sure businesses holding and processing that information do so in accordance with the rights of individuals.

The DPA sets out the basis on which defined parties can collect and store personal data (including "sensitive personal data") and also gives individuals the right to see what information is held about them and to have it corrected if it is wrong.

Numis takes its responsibilities under the DPA seriously and to help us discharge these legal and regulatory responsibilities, the Firm has implemented a policy to help ensure that all staff (Incl. temporary staff, interns, secondees and contractors) treat personal data both lawfully and correctly.

**What are the legal consequences of a breach of the DP Act?**

The penalties for a breach of the DP Act are both criminal and civil. It is an offence to obtain or disclose personal data or procure the disclosure of that information knowingly or recklessly to another person not in accordance with the act.

The maximum penalty under the current act is £500K in fines and / or jail imprisonment. When the DPA is replaced by the General Data Protection Regulations in 2018 the maximum fine will increase to 20M Euros or 4% of annual turnover, whichever is greatest. Individuals may also seek monetary compensation from Numis if they suffer damage or distress arising from a breach.

As Numis is a registered 'Data Controller' the Information Commissioners Office ("ICO") can request to perform an audit of Numis's data protection processes at any time.

**What is data, 'personal data' and 'sensitive personal data'?**

The data protection act is concerned with personal data – Data relating to living, identifiable individuals who can be identified from:

- The data we hold
- The data & other data in possession of a data controller (Numis) and/or others

This includes opinions and indications of intention in respect to any individual in question.

For Numis purposes, data can be classed under one of the following categories

A. Automated Data (held on a computer, so digital)
B. Data that is intending to become automated

C. Not automated (hard copy) but must be part of a relevant filing system i.e. structured by reference to individuals and individual data is readily accessible (for example, a temp could find it with no prior knowledge)

There are two more categories of data under the act but these are not relevant to Numis operations. Personal data can also be classed as **sensitive personal data,** for which there has to be much stricter controls around its use. The definition of sensitive personal data is information that indicates the following:

(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c ) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The act stipulates that a data controller (i.e. Numis) must satisfy extra conditions when using sensitive personal data. It should be noted that a passport is not sensitive personal data.

Throughout this policy, references to 'personal data' relate to all types of personal data, including 'sensitive personal data', unless otherwise highlighted.

The DP Act covers relevant filing systems, whereby information on a specified individual ("data subject") can be readily identified and accessed e.g. in an indexed filing system. You should note, it is not a 'relevant filing system' if there is no index, contents list or other means of finding the information. However anything held electronically is assumed to be suitably indexed and therefore will always be covered by the act.

**General Data Protection Regulations ("GDPR")**

**2018 will see the General Data Protection Regulations come into effect. Like the DPA the GDPR applies to personal data, however it provides a more expansive definition of what that is.** The most significant addition is the accountability principle. The GDPR requires firms to show **how** they

comply with the principles – for example by documenting the decisions taken about a processing activity. Numis must therefore consider all areas where it processes personal data and document and justify its processes.

The new accountability principle in Article 5(2) requires firms to demonstrate that we comply with the principles and states explicitly that this is our responsibility.

Controllers must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that they comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities.
- Where appropriate, appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
    - ❖ Data minimisation;
    - ❖ Pseudonymisation;
    - ❖ Transparency;
    - ❖ Allowing individuals to monitor processing; and
    - ❖ Creating and improving security features on an ongoing basis.
    - ❖ Use data protection impact assessments where appropriate.

## Data Protection in Numis

### Data Control

Numis collects, stores, controls and shares personal data (both electronically and manually) on a daily basis in order to operate its business. As a result Numis is classed (and registered) as a **Data Controller** with the Information Commissioners Office ("ICO") and covered by the DP Act's requirements as applicable.

Numis collects, stores, displays and shares a considerable amount of personal data during its day to day business activities; some of which may be contained within a single document. For example, a CV may contain home addresses and phone numbers, date of birth, salary, and so on. Where an employee is provided access to data, the rationale should always be considered and access only given once it has been decided there is a legitimate, reasonable reason to do so. Any access to personal data should be reviewed on a regular basis.

Numis primarily proce sses personal and/or sensitive personal data on:

- prospective, current and former employees;
- directors, shareholders and other persons who exercise significant control of prospective, current and former corporate and dealing clients;
- prospective, current and former dealing clients who are individuals (rather than legal entities)
- suppliers who are individuals (rather than legal entities).

### Registration

Since Numis processes personal and/or sensitive personal data, it is required to be registered with the Information Commissioners Office ("ICO") as a Data Controller. The ICO's register of Data Controllers is accessible to the public. The DPO is responsible for maintaining and keeping a record of the firm's registrations with the ICO.

### Data Protection Officer

Numis has an appointed Data Protection Officer ("DPO").

As of the latest policy review the Numis' Data Protection Officer is Mark Thompson. In his absence please refer to his Deputy – Tom Dyson

### Handling Personal Data

As a Data Controller, Numis must comply with the DP Act's Eight Principles for good handling of information and hence requires staff to ensure that personal data. These principles are as follows:

| | |
|---|---|
| **1** | Data is processed fairly and lawfully and, in particular, is not be processed unless it meets certain conditions, including:<br>♦ the intended use of the data has been disclosed;<br>♦ the data subject has given their consent;<br>♦ this is necessary to perform a contract to which the data subject is a party;<br>♦ it relates to a legal obligation or is in the public interest; and/or<br>♦ it is used to protect the vital interests (e.g. life or death scenarios) of the data subject. |
| **2** | Data is obtained for specified and lawful purposes and not used in other ways which may be incompatible with the purpose for which it was obtained; |
| **3** | Data is adequate, relevant and not excessive i.e. the amount of information requested is appropriate for the Firm's needs; |
| **4** | Data is accurate and, where necessary, kept up-to-date; |
| **5** | Data is not kept for longer than necessary and is destroyed once the purpose for which the information was gathered is complete and in line with the firm's record keeping requirements; |
| **6** | Data is processed in accordance with the rights of the data subjects, for example:<br>▪ they are provided with their personal data records if they so request;<br>▪ Numis must rectify data inaccuracies highlighted by the data subject; and/or<br>▪ personal data should not be used for purposes against the data subject's instruction e.g. for direct marketing; |
| **7** | Data is covered by appropriate systems and controls to provide for its protection and security and is not accessed unlawfully or inappropriately; |
| **8** | Data is not transferred outside the European Economic Area ("EEA", see Appendix 2) unless that country has an adequate level of protection for personal data or equivalent safeguards in place to protect data rights and access to information as under the DP Act (see Appendix 3 for the list of adequate data protection jurisdictions). |

## Responsibility for Data Protection

All staff must ensure that any personal data that comes into their possession, or for which they have responsibility, is managed in accordance with this policy and the DP Act's Eight Principles.

Senior managers have additional responsibility for implementing and monitoring controls to provide for compliance with these requirements. In particular, senior managers should consider what personal data their department processes and should be able to:

- confirm the systems and controls in place to ensure that such data is securely and confidentially stored and processed under the requirements set out in this policy;
- identify excess data or data which is no longer required so that it may be destroyed in line with Numis data retention schedules; and
  outline how personal data is being kept up-to-date.

## Collecting Data and Consent

Before personal data is collected or an individual is requested to provide personal data, staff must be clear as to the purpose for which they are collecting or storing such data. The Firm may, for example, require personal data:

- to set up dealing and CB&A accounts
- For business purposes such as recording meetings, presentations or records of interactions
- to meet regulatory requirements such as for:
  - director's questionnaires for AIM companies where Numis act as the Nominated Advisor;
  - identification of potential conflicts of interest;
  - individual registrations and regulatory approvals; or
  - voice recording of transactions;
- for job applications;
- to settle an account transaction.

Where Numis is processing personal data it must either obtain consent or be able to demonstrate a legitimate interest to do so.

Individuals need to be advised when their personal data is to be stored and the purpose for which it is to be collected. Numis will principally provide this information through:

- dealing and CB&A agreements, which contain clauses covering consent to process personal data; and employment contracts, which cover collection and storage of data relating to staff.

## Data Storage

Staff should not collect and/or store personal data in excess of data required to meet the Firm's operational requirements and legal obligations.

Numis will collect personal data and store it in a variety of locations as part of normal day to day business. For example, data is stored on PCs, in 'the cloud', paper format in cupboards and so on, all of which will all fall under the scope of DP regulations (relating to a living identifiable individual and held in a retrievable filing system). Methods such as encryption, passwords and segregated hard drives should be used to protect and secure personal data held within electronic systems. To that end Numis must have information security policies that set out relevant controls and havea framework to define and set-out the controls relating to the security of stored electronic data. Where hard copies are stored physically, security methods such as locked cabinets and controls around physical access (swipe cards etc.) should be used. Data must always be stored in a robust, durable format and allow Numis employees to easily access, monitor and destroy data where necessary to do so.

## Data Sharing

Numis seeks to prevent inappropriate disclosure of information and issues arising as a consequence of poor security. Personal data must not be disclosed (whether orally, or in electronic or hard copy) unless that information is being provided for the purposes for which it was originally intended, Numis has identified that the party being disclosed to has a legitimate interest (as per DP regulations and ICO code of practice), which is recorded as part of the rationale for sharing; or there is a legal or regulatory requirement to do so.

Data can be shared in two ways: Internally or Externally.

1.) Internally

Numis will typically need to share certain amounts of personal data internally to conduct its business, for example, using an individual's e-mail address or personal phone numbers to arrange conferences or to discuss business opportunities.

Access to personal and/or sensitive personal data should be restricted to staff who have a legitimate need to access such information on a day-to-day basis. Certain data, in particular, sensitive personal data, will require more restricted access and greater data security. The DPO can advise business areas according to the type of personal data held and will carry out periodic reviews of the systems and controls in place.

The Firm would generally expect only members of the NSL Board, HR, Compliance and managers in the course of managing their team to have access to sensitive personal data.

2.) Externally

Personal data must not be disclosed, either orally, in writing or otherwise to any unauthorised third party without proper consideration and approval from the DPO.

In instances when this is required, personal data should be password protected and/or encrypted. Similar care should be taken when sending hard copy documents containing personal data (e.g. copy passports).Consideration should be given to measures for additional security of mail deliveries using third party carriers. Personal data should never be taken outside the office or stored on a laptop.

Numis' client agreements include provision for transferring information (including personal data) outside of the EEA, where necessary. Prior to sending any information outside of the EEA, staff must contact the DPO to determine if there is adequate protection and/or safeguards in place.

Numis staff are responsible for ensuring any data sharing, either internally or externally, takes place in accordance with data protection principle and this policy.

- When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) Numis employees need to identify the objective that it is meant to achieve.

- This means considering the potential benefits and risks, either to individuals or society, of sharing the data and assessment of the likely results of not sharing the data.

- What information needs to be shared? Staff shouldn't share all the personal data held about someone if only certain data items are needed to achieve the objectives.

- Who requires access to the shared personal data? Staff should work on a 'need to know' basis, meaning that other organisations should only have access to Numis data if they need it, and that only relevant staff within those organisations should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.

- When should it be shared? This includes setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular event(s).

- How should it be shared? This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.

- How can we check the sharing is achieving its objectives? Staff will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.

- What risk does the data sharing pose? For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?

- Could the objective be achieved without sharing the data or by anonymising it? It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.

- Will any of the data be transferred outside of the European Economic Area (EEA)? If so, contact the DPO.

- It is good practice to document any instances of sharing. If there are any concerns or questions the DPO should be contacted.

Consent or explicit consent for data sharing is most likely to be needed where:

- confidential or particularly sensitive information is going to be shared without a clear legal basis for doing so;
- the individual would be likely to object should the data be shared without his or her consent;
- the sharing is likely to have a significant impact on an individual or group of individuals;
- the other conditions that provide a basis for processing non-sensitive personal data include:
- The processing is necessary: – in relation to a contract which the individual has entered into; or – because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.

- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the "legitimate interests" condition. The 'legitimate interests' condition provides grounds to process personal data in a situation where an organisation needs to do so for the purpose of its own legitimate interests or the legitimate interests of the third party that the information is disclosed to. This condition cannot be satisfied if the processing is unwarranted because it prejudices the rights and freedoms or legitimate interests of the individual whose data is being processed. This condition cannot legitimise the processing of sensitive personal data.
- Considerable amount of personal data may be contained in a single document. For example, a CV may contain home addresses and phone numbers, date of birth, salary, etc. Should a colleague need to access an element of the data on such a document, the data should be supplied on a need to know basis and not in its entirety.

## Archiving

Where data is suitable for archiving it should be done so in accordance with this policy. The data is still owned by Numis and the staff member who originally filed the information for archiving is still responsible. It must be destroyed in accordance with the Numis data retention schedule (see below) where applicable. If using a third party to store Numis data they must demonstrate they have adequate data protection controls in place.

## Accuracy of data

All personal data which is stored by Numis should be accurate. The Firm is required to take reasonable steps to ensure the accuracy of the data provided and to regularly review the data for accuracy.

## Destruction

Numis staff are responsible for ensuring that personal data is not kept for longer than is necessary (and it is held in accordance with internal, legal and regulatory requirements). The requirements for record keeping are detailed and specific to each aspect of Numis' business, please see Record Retention Schedule (Appendix 1). You should liaise with your head of department for guidance or the DPO (in their absence please liaise with the Numis compliance department).

Each department should review those records which contain personal or sensitive personal data at least annually to ensure that data is retained for no longer than is necessary. Personal and sensitive personal data should be destroyed once the need for holding the data has expired.

Personal and sensitive personal data must be destroyed either by being shredded or using the CONFIDENTIAL bins provided across the office. Personal and sensitive personal data must never be thrown in the regular waste bins.

Information stored in databases or on hard drives/servers must be deleted. Note that data stored in this way is subject to the same record retention periods as paper records.

**Third party data processors**

All third party data processors must be reviewed by the person/department responsible for the data and ultimately approved by the DPO. This review of the data processor is assessed using a 'Privacy Impact Assessment' ("PIA"), which is designed to interrogate the processors suitability to process and store Numis data; and all supporting documentation must be saved in a data processor file held by compliance.

Initial PIA documentation is available through the 'Compliance Forms' section of the Policy Hub website.

**Negotiating a contract**

The GDPR, in common with the current regime, requires that whenever processing is carried out on behalf of a controller by a third party, those parties must enter into a written contract. However, it greatly increases the list of provisions that must be included in that contract.

The required provisions are listed in Article 28(3) of the GDPR, and set out below (GDPR:
Processing by a processor must be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, categories of individuals whose data is being processed and the obligations and rights of the controller. The contract must stipulate, in particular, that the processor will:

1. process only on documented instructions, including regarding international transfers (unless, subject to certain restrictions, legally required to transfer to a third country or international organisation);
2. ensure those processing personal data are under a confidentiality obligation (contractual or

statutory);
3. take all measures required under the security provisions (Article 32) which includes pseudonymising and encrypting personal data as appropriate;
4. only use a sub-processor with the controller's consent (specific or general, although where general consent is obtained processors must notify changes to controllers, giving them an opportunity to object);
5. flow down the same contractual obligations to sub-processors;
6. assist the controller in responding to requests from individuals (data subjects) exercising their rights;
7. assist the controller in complying with the obligations relating to security, breach notification, DPIAs and consulting with supervisory authorities (Articles 32-36);
8. delete or return (at the controller's choice) all personal data at the end of the agreement (unless storage is required by EU/member state law);
9. make available to the controller all information necessary to demonstrate compliance; allow/contribute to audits (including inspections); and inform the controller if its instruction infringe data protection law

**Changes that impact personal data**

Where there is a new system to be installed, project commenced, or any other activity that may impact personal data commenced, a PIA must be completed. The PIA will initially be completed by the person/department responsible for the data and subsequently sent to Compliance for review. Compliance will decide whether or not the situation warrants a full PIA. Either way Compliance will approve and/or advise on next steps.

The completed PIA(s) and any rationale must be recorded.

## Requests for Data Access

**External Requests (subject access)**

Individuals have a legal right to access personal data that Numis may holds in relation to them.
Under the DP Act Numis is obliged to respond to any formal written request for data access and can charge a maximum administration fee of £10. Once the request has been verified, responses will be dealt with promptly and in any event must be dealt with within 40 calendar days of receipt of the request.

Requests to access personal data held by Numis must be referred to the DPO, so that the data can be collated and the response and response time monitored.

**Staff Requests**

All staff requests for access to their own personal data should be addressed to the Head of HR in the first instance.

**Incident Reporting**

A data security breach can occur for a number of reasons including (though not limited to):

1. Loss or theft of data or equipment on which data is stored;
2. Inappropriate access controls allowing unauthorised use;
3. Equipment failure;
4. Human error;
5. Unforeseen circumstances such as a fire or flood;
6. System Hacking;
7. 'Blagging' offences where information is obtained by deceiving the organisation who holds it; or
8. Employee removing data with them when they leave the Firm (in breach of Firm's policy).

Employees must notify the DPO (and in his absence the Numis compliance department) of any breaches of Numis' data protection policy in accordance with Suspicious Activity and Incident Reporting Policy which is available to all staff on the Numis Intranet.

Numis will consider the need to notify data subjects if there has been a data security breach so that they can take action to reduce any risk to them. Consideration will also be given as to whether the breach is sufficiently serious to be reported to the Information Commissioner.

## Appendix 1 – Record Retention Schedule

| Category | Retention Period | Reason | Detail |
|---|---|---|---|
| CORPORATE DOCUMENTS | | | |
| Minutes of Committees or Board Meetings (Official Copy) | At least 10 years | Legal | Companies Act 2006 - Sec 248 |
| Written resolutions of the Board | At least 10 years from the date of the resolution | Legal | Companies Act 2006 - Sec 355 |
| Minutes of general and class meetings | At least 10 years from the date of the meeting | Legal | Companies Act 2006 - Sec 355 |
| Notices of general and class meetings (signed copy) | At least 10 years from the date of the meeting | Legal | Companies Act 2006 - Sec 355 |
| Certificate of Incorporation | Permanently (recommended) | Legal | No statutory retention period. |
| Certificate to commence business (plc. only) | Permanently (recommended) | Legal | No statutory retention period. |
| Printed copies of resolutions filed at Companies House | Min 10 years | Legal | Companies Act 2006 - Sec 355 |
| Company Registers (including, but not limited to, register of directors and secretaries, register of directors' interests in shares and debentures, register of directors' declarations of interest, register of charges, register of members) | Permanently (recommended) | Legal | Companies Act 2006 - Sec 113 |
| Company Organisation Papers (if significant) | Permanently (recommended) | Commercial | No statutory retention period. |
| Memorandum of Association | Permanently (recommended) | Legal | No statutory retention period. |
| Articles of Association | Permanently (recommended) | Legal | No statutory retention period. |
| Annual Return | 3 years | Legal | Companies Act 2006 - Sec 388(4)(a)(b) |
| Change of Name | Permanently (recommended) | Legal | No statutory retention period - results in new Certificate of Incorporation. |
| Contract for purchase of own shares | 10 years from date of purchase | Legal | Companies Act 2006 - Sec 702 |
| Annual Reports and Accounts | Archive one copy – at least one copy should be kept for the life of the organisation | Legal | 3 years private company / 6 years public limited company according to the Companies Act 1985 Section 221 as modified by the Companies Act 1989 and the Companies Act 2006 |
| Circulars to Shareholders | Permanently retain one master copy of each. | Commercial | No statutory retention period. |
| Forms of share application, forms of acceptance, renounced letters of acceptance and allotment, renounced share certificates | Minimum of 12 years (recommended) | Legal | No statutory retention period. |

| | | | |
|---|---|---|---|
| Annual Meeting Proxy and Polling Cards | 1 months after meeting if no poll demanded, 1 year if poll is demanded or meeting convened by court | Commercial | No statutory retention period. |
| Share and stock transfer forms | 12 years after transfer (recommended) | Legal | No statutory retention period. |
| Trade and Service Marks Documents | Permanently or at least 6 years after cessation of registration | Legal | No statutory retention period. |
| Copyright Protection | 50 years after author's death (recommended) | Copyright Act | No statutory retention period. |
| **FINANCIAL: ACCOUNTING RECORDS** | | | |
| Cheques | 6 +1 years | Legal | Companies Act 2006 - Sec 388 |
| Invoices | 6 +1 years | Legal | Companies Act 2006 - Sec 388 |
| Invoices (Capital) | 10 years | Commercial | Companies Act 2006 |
| Purchase Orders | 4 years | Audit | No statutory retention period. |
| Quotations (Capital) | 12 years | Audit | No statutory retention period. |
| Quotations (Revenue) | 7 years | Audit | No statutory retention period. |
| Customs & Excise Returns | 6 +1 years | Legal | https://www.gov.uk/guidance/archiving-your-trade-documents#archiving-your-vat-and-excise-documents |
| Expense Claims | 6 years | Legal | Taxes Management Act 1970 |
| Redundancy Payments | 6 years after employment ceased | Legal | Data Protection Act |
| Accounts | 3 years from date on which made (Private Company)<br>6 years from date on which made (Public Company) | Legal | Companies Act 2006 - Sec 388(4)(a)(b) |
| Bank Instruction | 6 years after ceasing to be effective | Legal | Companies Act 2006 - Sec 388 |
| VAT records | 6 +1 years | Legal | VAT Act 1994 - Schedule 11 Sec 6 |
| **FINANCIAL: CASH RECORDS** | | | |
| Bank Paying In Counterfoils | 6 +1 years | Legal | Companies Act 2006 - Sec 388 |
| Bank Statements | 6 +1 years | Legal | Companies Act 2006 - Sec 388 |
| Bank Reconciliation | 6 +1 years | Legal | Companies Act 2006 - Sec 388 |
| Banking Returns | 6 +1 years | Legal | Companies Act 2006 - Sec 388 |
| Petty Cash Records | 6 +1 years | Legal | Companies Act 2006 - Sec 388 |
| Main Cash Book | 6 +1 years | Legal | Companies Act 2006 - |

| | | | |
|---|---|---|---|
| | | | Sec 388 |
| **FINANCIAL: LOAN RECORDS** | | | |
| Debtor Accounts Control Report | 6 +1 years | Legal | |
| Individual Debtor Accounts | 6 +1 years after clearance of debt | Legal | |
| Listing of Wage Deductions | 6 years | Audit | Taxes Management Act 1970 |
| Statement of Loan Account | 6 +1 years | Commercial | |
| **HEALTH AND SAFETY** | | | |
| Accident Books | 3 years from date of each entry | Legal | The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 |
| Equipment Inspection Records | Until the next Inspection report is recorded. | Legal | The Provision and Use of Work Equipment Regulations 1998 |
| Asbestos Register and Asbestos Disposal Certificate | Permanently | Legal | Control of Asbestos at Work Regulations 2012 |
| Control of Substances Hazardous to Health (COSHH) – list of employees exposed to group 3 and 4 biological agents | 40 years | Legal | http://www.hse.gov.uk/coshh/ |
| Risk Assessments | Until superceded by updated assessment. | Legal | The Management of Health and Safety at Work Regulations 1999 |
| Safe Systems of Work | At least 6 months after completion of work | Commercial | |
| Health and Safety policy | Permanently. | Commercial | Implied by Health and Safety at Work Act 1974 - Sec 2(3) |
| Assessment of risks under health and safety regulations (including routine assessment monitoring and maintenance records for aspects in workplace such as air quality, levels of pollution, noise level, use of hazardous substances etc.) | Until revised (statutory) Permanently (old and current copies) (recommended) | Commercial | Management of Health & Safety at Work Regulations 1992 - Sec 1 (1992/2051) |
| **HUMAN RESOURCES** | | | |
| Personnel Records (including Directors' contracts) | 7 years after employment ceases | Legal | No statutory retention period. |
| Employment contract, including personnel and training records, written particulars of employment, changes to terms and conditions. | 6 years after employment ceases | Commercial | Limitation Act 1980 (Sec 5) and Data Protection Act 1998 |
| Senior Executive Records | Permanently | Commercial | No statutory retention period. |
| Consents for the processing of personal and sensitive data | For as long as the data is processed and held in respect of a living individual | Legal | Data Protection Act 1998 |
| Staff Appraisals | 6 years after employment ceases | Commercial | Limitation Act 1980 (Sec 5) and Data Protection Act 1998 |
| Consolidated Sickness Records showing dates and causes of sick leave | 6 years after employment ceases | Commercial | Limitation Act 1980 (Sec 5) and Data Protection Act 1998 |
| Vacancies and Applications (Unsuccessful) | 6 months - 1 year after notifying unsuccessful candidates | Commercial | Disability Discrimination Act 1995 and Race Relations Act 1976 |

| | | | |
|---|---|---|---|
| | | | recommend six months. One year limitation for defamation actions under Limitations Act |
| Disciplinary | 6 years after employment ceases (recommended) | Commercial | Data Protection Act 1998 |
| Leave (Adoption, Annual, Flexi, Sick, Special, Time Off in Lieu) | 3 years after tax year end in which period ends | Commercial | The Statutory Maternity Pay (General) and Statutory Sick Pay (General) (Amendment) Regulations 2005. This is outlined in Sick Pay Guide (HMRC) |
| Group Health/Accident Policies | 12 years after benefit ends | Legal | Limitation Act 1980 |
| Early Retirement/Redundancy Documents | 6 years after date of retirement/redundancy | Legal | The Retirement Benefits Schemes (Information Powers) Regulations 1995 |
| Travel and subsistence claims and authorisations | 6 years | Commercial | Implied in Taxes Management Act 1970 - Part IV (34) |
| Working time opt out forms | 2 years after the opt-out has been rescinded or has ceased to apply | Legal | The Working Time Regulations 1998 (SI 1998/1833) |
| Records to show compliance with Working Time Regulations 1998 including time sheets for opted out workers | 3 years | Legal | 3 years after pay reference period end following period that records cover \| HM Revenue & Customs Guide |
| **INSURANCE** | | | |
| Public/Employers/Product Liability/PI | 40 years | Commercial | Employers' Liability ( Compulsory Insurance) Regulations 1998 |
| Claims correspondence | 3 years after settlement | Commercial | Data Protection Act 1998 |
| Settlements | 7 years after claim | Legal | |
| Insurance Schedules | 10 years | Commercial | |
| **LEGAL** | | | |
| Contracts/Agreements | 6 years after expiry/termination | Legal | Limitation Act 1980 - Sec 5 |
| Contracts executed as a deed | 12 years after expiry/termination | Legal | Limitation Act 1980 |
| Standard terms and conditions | 7 years after expiry | Legal | |
| Tenders | 6 years | Commercial | |
| Trade Marks | 7 years from date of termination | Commercial | https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/581672/PDTMD-Retention-and-Disposal-Policy.pdf |
| Lease (signed copies) | 15 years after expiry of lease | Legal | Limitation Act 1980 |

| | | | |
|---|---|---|---|
| Landlord's consents | 15 years after surrender, expiry or termination of lease or memoranda of terms | Legal | |
| Planning Permission | 3 years after property interest ceased | Legal | Town and Country Planning Act 1990 |
| Contracts relating to building, building maintenance, repairs etc | 13 years | Legal | Data Protection Act 1998 |
| **COMPLIANCE** | | | |
| PA Dealing Records | 7 years | Legal & Regulatory | FCA SYSC 9.1 |
| Insider Lists and external (market sounding) insider lists | 7 years | Legal & Regulatory | FCA SYSC 9.1 - Disclosure Guidance and Transparency Rules sourcebook Chapter 2 5 year minimum |
| Bloomberg and internal chat data, e-mails | 7 years | Legal & Regulatory | FCA SYSC 9.1 |
| STOR/Near Misses/RO | 7 years after submission/investigation closes | Legal & Regulatory | FCA SYSC 9.1 |
| SAR records | 7 years after submission/investigation closes | Legal & Regulatory | Money Laundering Regulations 2007 (5 years). No statute of limitations in UK for indictable offences |
| **CUSTOMER KYC RECORDS** | | | |
| Client Due Diligence and any investigation material | 7 years after termination of the client relationship or end of the investigation | Legal & Regulatory | Money Laundering Regulations 2007 (5 years). No statute of limitations in UK for indictable offences |
| Client files and all related information | 7 years after termination of the client relationship | Legal & Regulatory | Money Laundering Regulations 2007 (5 years). No statute of limitations in UK for indictable offences |
| **PENSIONS** | | | |
| Trust Deeds and Rules | Permanently | Legal | Companies Act 2006, Pensions Act 2014 |
| Pension Payments | 6 years after last payment of benefits | Legal | Taxes Management Act 1970 |
| Members' Records | 6 years | Audit | http://www.thepensionsregulator.gov.uk/docs/detailed-guidance-9.pdf |
| Valuation Working Papers | Review every 10 years | Audit | |
| Actuarial Certificates | Permanently | Audit | Companies Act 2006 |
| Superannuation Adjustments | Current plus 6 years | Legal | Pensions Act 1995 |
| Superannuation Reports | Current plus 6 years | Legal | Pensions Act 1995 |
| Minutes of meetings of trustees | Life of the scheme | Legal | |
| **SALARY AND WAGES** | | | |
| Tax Forms P6/P45/P46/P48/P11/P11D/P9D/P35/P60 | 6 years | Legal | Taxes Management Act 1970 |
| Payroll and Salary Records | 6 years from year end | Legal | Taxes Management Act 1970 |

| | | | |
|---|---|---|---|
| NI Contributions | 3 years after the end of the tax year to which they relate | Legal | 3 years after the end of the tax year to which they relate |
| Monthly Superannuation | 6 years +1 | Legal | Pensions Act 1995 |
| Annual Superannuation | 6 years +1 | Legal | Pensions Act 1996 |
| Annual Earnings Summary | 6 years +1 | Legal | |
| PAYE records | 3 years after the end of the tax year to which they relate | Legal | Income Tax (PAYE) Regulations 2003 (sI 2003/2682) - Regulation 97 |
| Maternity pay records and certificates required to be kept by employer under the Statutory Maternity Pay (General) Regulations 1986, reg 26. | 3 years after the end of the tax year in which the maternity pay period ends | Legal | The Maternity Allowance and Statutory Maternity Pay Regulations 1994 |
| **SALES RECORDS** | | | |
| Customer Orders | 6 years if VAT related | Commercial | VAT Act 1994 |
| Customer Complaints | 2 months after folder closure | Commercial | Data Protection Act 1998, Freedom of information Act, Environmental Information Regulations and Privacy and Electronic Communications Regulations |
| Nominal ledgers | 6 years | Legal | https://ico.org.uk/media/about-the-ico/policies-and-procedures/1904/ico-retention-schedule.pdf |
| Sales ledger | 10 years | Legal | Companies Act 2006, HMRC |
| Sales Invoices/Credit Notes | 6 years | Legal | Companies Act 2006 |
| Customer file | 6 years after last entry | Legal | HM Revenue and Customs (HMRC) |
| **MISCELLANEOUS** | | | |
| Customer deposits under escrow agreement | In accordance with the terms of the relevant escrow agreement | Legal | No statutory retention period |
| Requests to be removed from marketing lists and exception lists | Until person has been removed | Legal | Implied by Data Protection Act 1998 |

## Appendix 2 – Data Types

| Purpose | Data subjects | Data classes |
|---|---|---|
| 1. Staff administration of Appointments or removals, pay, discipline, superannuation, work management or other personnel matters in relation to the staff of the data controller. | Staff including volunteers, agents, temporary and casual works. Relatives, guardians and associates of the data subject | Personal details<br>Family, lifestyle and social circumstances<br>Education and training details<br>Employment details<br>Financial details |

| | | |
|---|---|---|
| | | Racial or ethnic origin<br>Religious or other beliefs of a similar nature<br>Trade union membership<br>Physical or mental health or condition |
| 2. Advertising, marketing & public relations<br>Advertising or marketing the business of the data controller, activity, goods or services and promoting public relations in connection with the business or activity, or those goods or services | Customers and clients.<br>Complainants, correspondents and enquirers<br>Advisers, consultants and other professional experts. | Personal details<br>Family, lifestyle and social circumstances<br>Goods or services provided |
| 3. Accounts & records<br>Keeping accounts related to any business or other activity carried on by the data controller, or deciding whether to accept any person as a customer or supplier, or keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by him or to him in respect of those transactions, or for the purpose of making financial or management forecasts to assist him in the conduct of any such business or activity. | Customers and clients<br>Suppliers.<br>Complainants, correspondents and enquirers. | Personal details<br>Financial details<br>Goods or services provided |

**Appendix 3 - EEA countries**

| | | |
|---|---|---|
| Austria | Greece | Norway |
| Belgium | Hungary | Poland |
| Bulgaria | Iceland | Portugal |
| Cyprus | Republic of Ireland | Romania |
| Croatia | Italy | Slovakia |
| Czech Republic | Latvia | Slovenia |
| Denmark | Liechtenstein | Spain |
| Estonia | Lithuania | Sweden |
| Finland | Luxembourg | UK |
| France | Malta | |
| Germany | The Netherlands | |

**Appendix 4 - Adequate' Data Protection jurisdictions**

The following jurisdictions are currently regarded by the European Commission as having an adequate level of protection for personal information:

| | | |
|---|---|---|
| Andorra | Guernsey | New Zealand |
| Argentina | Isle of Man | Switzerland |
| Canada | State of Israel | Eastern Republic of Uruguay |
| Faroe Islands | Jersey | |