Data Retention Policy

Policy statement

In the course of business, Timico Limited collects and stores a broad range of information. This policy explains why we need to retain and delete information and the processes involved. It is followed by an Information Retention and Deletion Schedule, setting out the retention periods for Timico information.

Purpose

The purpose of this policy is to formulate an internal schedule for the retention and eventual destruction of data records.

We have duties under legislation and/or regulations to retain information for certain periods of time, for example under anti-money laundering regulations or health and safety legislation. We also have other retention obligations to our insurers, regulators, accreditation bodies and customers. Balanced against this, the General Data Protection Regulation ('**GDPR**') only permits us to retain personal data for as long as is necessary for the purpose for which it was collected.

The accidental or intentional destruction of these records during their specified retention periods, or the retention of personal data for longer than those periods, could result in serious consequences for Timico and/or its employees, including criminal charges or significant fines (up to the greater of €20m or 4% of annual global turnover in the case of personal data). Failure to follow this policy could lead to disciplinary action.

Definitions

- **Information:** Can include both hard copy documents and electronic information. It may be stored at work premises, on electronic devices or stored online or in the cloud. It includes information belonging to or controlled by Timico which is stored by third parties such as suppliers, consultants or IT service providers. Some examples of where information may be located are:

    - Electronic files
    - Emails
    - Voicemails
    - Letters and other correspondence
    - Handwritten notes
    - Appointment books and calendars
    - Audio and video recordings
    - Contracts
    - Invoices
    - Memory in mobile phones and other devices
    - Websites such as Facebook, Twitter, Instagram
    - Instant messenger conversations such as Skype, WhatsApp
    - Performance reviews
    - Computer programs

- **Confidential Information:** Could be business sensitive information relating to company finances, commercial agreements or product specifications, or it could be data about individuals. We may also hold third party information which is confidential.

- **Personal data:** Some information which we store will be personal data. Storage of personal data is regulated by the GDPR. It includes any information which identifies an individual or

relates to an identifiable individual. It can include identifying someone by reference to an identifier such as a name, address, email address, ID number, location or an online identifier such as an IP address. Information relating to an identifiable individual's physical, psychological, economic, cultural or social identity is also personal data. All personal data shall be treated as also being confidential information.

- **Special Category Personal Data:** Some types of personal data are especially sensitive. These special categories of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health, sexual orientation or sex life. Genetic or biometric data (such as fingerprint or retinal scan data) is also special category personal data. Criminal convictions and offences data is not special category data but its processing is restricted and it is similarly sensitive in nature. Due to the potential sensitivity of this data there are increased risks involved should it be lost or retained for longer than required.

Scope

This policy defines Timico's established protocol regarding the retention and subsequent deletion of data.

Responsibilities

Managers within the relevant departments that are responsible for data must ensure compliance with the Data Retention Schedule. They must ensure that retained data is appropriately protected from unauthorised access, as detailed in the Access Control Policy available on the Intranet or on Sharepoint.

Individuals responsible for the retention of data are additionally responsible for its destruction following the retention period.

The Chief Operating Officer ('**COO**') is responsible for ensuring compliance with Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the COO at compliance@timico.co.uk.

The COO is the owner of this document and is responsible for ensuring that it is reviewed. An annual review will be performed to determine whether retention of data is adequate and appropriate. Subsequent disposal will not take place until a review has taken place. The relevant managers must ensure disposal is appropriate to the media involved.

Information Retention

Legal, regulatory requirements or agreed industry practices are captured in the Data Retention Schedule, which provides a more granular view of the policy.

Information must only 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 ongoing/anticipated litigation or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record or if you believe information should be retained for longer than the period stated in the Schedule, contact the COO.

Retention of data will be in accordance with the Information Security Policy.

Information Deletion

Deleting information which is no longer required is of benefit to Timico and is also required by legislation. One of the principles of the GDPR is data minimisation– only collecting and processing the personal data necessary for the purpose for that collection and processing. Personal data should only be kept for as long as is necessary for the purpose for which it was collected. Minimising the amount of information we retain reduces the amount of information which can be lost in a cyberattack. Individuals also have the right to access the personal data we hold about them. The more personal data we store unnecessarily, the more burdensome it is to respond to these requests.

Deletion of data will comply with the following relevant documents:

- Data Protection and Privacy Policy
- Acceptable Use Policy
- Secure Disposal or Re-Use of Equipment Policy

Information Destruction

The destruction of hard copy personal data and confidential, financial, and personnel-related records must be conducted by shredding.

Non-confidential records may be destroyed by recycling.

The destruction of electronic records must be coordinated with the Technical Director.

Destruction of data will comply with the following relevant documents:

- Data Protection and Privacy Policy
- Acceptable Use Policy
- Secure Disposal or Re-Use of Equipment

Third Party Data

Information we hold which is controlled by third parties will be deleted in accordance with the agreement in place with that third party.

Information under our control which is held by third parties on our behalf must be destroyed in line with this policy unless the agreement in place with that third-party states they have the right to retain data. The contracts in place with third parties will include provisions requiring the deletion and destruction of information.

Deletion and destruction of data will comply with the following relevant documents:

- Data Protection and Privacy Policy
- Acceptable Use Policy
- Secure Disposal or Re-Use of Equipment

Reporting Policy Infringements

Timico is committed to enforcing this policy. The effectiveness of Timico's efforts, however, depends largely on employees. If you feel that you do not understand this policy or you or someone else may have infringed this policy, you should report the incident immediately to your supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the

supervisor has dealt with the matter properly, you should raise the matter with the COO. If employees do not report inappropriate conduct, Timico may not become aware of a possible infringement of this policy and may not be able to take appropriate remedial action.

Data Retention Schedule

Customer/Supplier Data

AREA AND OWNER	EXAMPLES INCLUDE	RETENTION POLICY
Core Information- Product Team/Commercial Team/Finance	• Account Information - Name / Address / Payment Terms & Type etc. • Sensitive Account Information - Account Access Answer / Customer Portal Password • Contact Information - Individuals and their contact details • Listing of all Services (Live and Historic) • Records of orders And any other records which relate to a customer	Retained for the life of an account and for 7 years after an accounts closure
Financial Information Finance	• Direct Debit Details • Invoices - Manual & Standard • Sales Ledger Transactions • Payment Status • Journal Entries • Record of Invoices and Services	
Customer Notes Client Operations Director	• Tickets / Notes / Tasks (including attachments) • Incidents (including attachments) • Sales & Marketing Activity	
Customer Usage Client Operations Director	• Broadband Usage Logs • Mobile Usage Logs • Fixed Line Usage Logs • Internet Telephony Usage Logs • Email Usage Logs • Internet Access Usage Logs And any other usage records	Retained for 2 years following date of usage
PCI Technical Director	PCI Logs	System, event and audit logs are retained for 30 days and are immediately available for analysis

CCTV Senior Data Centre Engineer	CCTV Logs	System, event and audit logs are retained for 30 days and are immediately available for analysis

Internal Data

AREA	DESCRIPTION	RETENTION POLICY
HR Records HR Director	Recruitment records: • 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.	12 months after the conclusion of the recruitment process
HR Records HR Director	Personnel records • qualifications/references; • consents for the processing of special categories of personal data; • annual leave records; • annual assessment reports; • disciplinary procedures; • grievance procedures; • death benefit nomination and revocation forms; and • resignation, termination and retirement. Contracts of employment, written particulars of employment and any alterations to the terms and conditions if applicable.	6 years from the date an employee leaves the employment of Timico

	Medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry
	Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	
	Medical records containing details of employees exposed to asbestos	
	Medical records under the Control of Asbestos at Work Regulations	
	Medical records under the Ionising Radiations Regulations 1999	Until the person reaches 75 years of age, but in any event for at least 50 years
	Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	12 years from the end of the scheme year in which the event took place
	Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	5 years from the date on which the tests were carried out
	Medical examination certificates	4 years from the date of issue
	Accident books, accident records/reports	3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21). (See below for accidents involving chemicals or asbestos)
	Statutory Maternity certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends
	Statutory Sick Pay certificates, self-certificates	3 years after the end of the tax year to which they relate
HR Records HR Director	Records relating to working time	2 years from date on which they were made
	Records relating to children and young adults	Until the child/young adult reaches the age of 21

Finance records Group Financial Controller	Wage/salary records (also overtime, bonuses, expenses)	6 years
	Accounting records	3 years for private companies, 6 years for public limited companies
	Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate
	Statutory Maternity Pay records, calculations	3 years after the end of the tax year in which the maternity period ends
	Statutory Sick Pay records, calculations	3 years after the end of the tax year to which they relate
	National minimum wage records	3 years after the end of the pay reference period following the priod that the records cover
Staff Usage	Internal Email and files	Retained for life of business