DATA RETENTION POLICY

Introduction

This Data Retention Policy sets out the obligations of STM Group (UK) Ltd**,** together with the basis upon which the Company shall retain, review and destroy held data, or data within STM custody or control.

This policy applies to the entire STM organization, including all employees, and aims to set out related retention periods, and at what point in time data may be deleted.

Objectives

It is necessary to retain and process certain information in order to enable the STM business to operate in compliance with prevailing legislation, and Company Registrations ISO 9001, ISO 18001 and ISO 14001. STM may store data in the following places:

- Company servers
- any third-party servers
- email accounts
- desktops, laptops, tablets, telephones and other electronic devices
- employee-owned devices
- potential backup storage
- STM paper files.

This policy applies equally to paper, electronic media and any other method used to store personal data. The period of retention only commences when the record is closed.

STM is bound by various obligations (under the Law) in relation to data storage and therefore, to comply with the Law, information must be collected and used fairly, stored safely and not unlawfully disclosed to any other person in respect of personal data under the General Data Protection Regulation ("the Regulation").

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the procedures that are to be followed when dealing with personal data and how STM aims to comply with the Regulation in so far as it is possible. In summary, the Regulation states that all personal data shall be:

- processed lawfully, fairly, and in a transparent manner in relation to the data subject
- collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject

to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Fourth and Fifth Data Protection Principles require that any data should not be kept longer than necessary for the purpose for which it is processed; when it is no longer required, it shall be deleted; and that the data should be adequate, relevant, and limited to the purpose for which it is processed.

Taking this into consideration, the Policy should be read in conjunction with other relevant STM policies including, but not limited to, the Data Protection Policy and IT Security Policy.

Security and Storage

All data and records are stored securely, in order to avoid misuse or loss. STM will process all personal data in its possession in accordance with the STM IT Security Policy, whilst taking appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

STM will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if there is agreement, from them, to comply with those procedures and policies, or if there are alternative adequate measures in place.

STM will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** - means that access to data is restricted to authorised personnel.
- **Integrity** - means personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** - means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the STM Group (UK) Ltd central computer system (as opposed to individual personal computers).

Retention Policy

Data retention is defined as the retention of data for a specific period of time, and for back-up purposes.

STM will not keep any personal data longer than necessary, but acknowledge that this will be dependent on the different types of documents and data for which it has responsibility. The STM specific data retention periods are set out below:

Purpose of processing Employee Personal Data	Categories of personal data -what we record (Paper and/or electronic records)	Typical Categories of recipients	Agreed Retention Period
Payroll Records	Contact and personal details (Name, title, address, tel numbers, email address, gender, date of birth, marital status, start date, role, job title, location of employment, employment ID numbers), bank account details, salary, pension details, tax status information inc National Insurance Number, Benefits Information, authority to deduct	HMRC, Centralis, Pension Provider, Attachment of Earning Orders, Benefit Providers - SSP, Maternity and Paternity, Childcare Vouchers, Court Orders, HSF, Accountants Ashley Richmond, Finance Auditors GB&CO and HSBC	6 years post-employment
HR Personnel File-	Contact details (Name, title, address, tel numbers, email address and details of Next of Kin details, emergency contact details, title, location of employment, employee ID numbers)	STM Operations, STM HSE, Clients, Trades Union, BTP, Chaplaincy Services, External Trainers, HSE, Auditors -NSI, FORS, RISQS, External Audit Consultants,	7 years post-employment
	Personal data -date of birth, gender, ethnicity, marital status, dependants, NI number, start date, education, Professional memberships, work history, criminal Convictions, cautions and offences, TUPE data if applicable, credit check,	Centralis, HMRC, Pension Provider, Clients, Trades Union	7 years post-employment
	Uniform sizes, measurements, other details	STM Operations, Uniform Suppliers	3 months
	Annual leave details	STM Operations, STM Finance Dept , Cobia	1 year
	Sick leave details, Sick notes, Return to work interviews	STM Operations, STM Finance Dept, STM HSE	7 years post-employment
	Bradford Factor absence monitoring -automated decision making	STM Operations	1 year
	Performance details inc Disciplinary record, Grievance records, Appraisals and Probationary Reviews	Clients, STM Operations, Employment Law Advisors, Trades Union	7 years post-employment
	Right to Work details inc photo ID, Identification numbers, passports, visas, birth certificate, work permits, proof of address, all screening and vetting data to 7858	Clients, Home Office, auditors NSI and external audit consultants	7 years post-employment
	DBS	N/A	3 years
	Medical History and information and conditions, D&A tests and other medical information such as welfare interviews	Clients, STM HSE Dept, STM Operations, Express Medicals, Doctors, RISQS	7 years post-employment
	Training Records including exam results, achievement certificates, feedback documents, pass/fail dates recorded on Logosoft	Clients, External Trainers, Auditors - NSI, external audit consultants, RISQS, unions, Logosoft platforms	Period of employment or 7 years

	SIA Licence number and photo card	Clients, Auditors-NSI, external audit consultants	3 years
	Driving license details and copy of license	Insurance company, Clients, Police, Masternaut, FORS auditors	Period of employment or 7 years
	Personal data on contract of employment	N/A	Period of employment or 7 years
Recruitment Records - successful applicants	CV and cover letter		1 month following employment
	Name and Contact details, completed application form with Employment History, references, education history, qualifications, job descriptions	Referee (character and work), Clients, STM Training Dept	7 years post-employment
	Qualifications	Clients, STM Training Dept	7 years post-employment
	Ethnicity	STM HR Dept	7 years post-employment
	Disability details	STM HR Dept	7 years post-employment
	Interview Notes and tests	STM HR Dept	1 year
Recruitment Records- unsuccessful applicants	CV	N/A	if consent given up to 1 yr, if not 1 month from job being fulfilled
	Name and Contact details, completed application form with Employment History, education history, qualifications	N/A	if consent given 1 year, if not 1 month from job being fulfilled
	Ethnicity	N/A	
	Disability details	N/A	
General Business Operations and Operational Contract Management	Email inc various categories of personal data	All Employees, Clients, Interested Parties	Up to 5 year
	Recorded Telephone calls	All Employees, Clients, Interested Parties	Up to 3 years in case of injury and accident and claim
	Swipe card records	N/A	Termination of employment
	CCTV footage	All Employees, Clients, Interested Parties	Up to 12 months
	Text Messages	All Employees, Clients, Interested Parties	Up to 12 months
	Communication via Apps	All Employees, Clients, Interested Parties	Up to 12 months
	Letters	All Employees, Clients, Interested Parties	Up to 36 months following closure
	Photographs	All Employees, Clients, Interested Parties	Pfile 7 yrs. Up to 3 years social media
	Site Documentation e.g. AIs	All Employees, Clients, Interested Parties, Auditors	Contract term plus 1 year

	Vehicle tracking	STM HR, STM Operations, Insurance companies, FORS, clients	Up to 12 months
	Master Forms completion e.g. expenses, vehicle and equipment handover, vehicle policies etc	STM Operations, STM HR, Auditors	Up to 6 years.
	Bearer Passes	Clients, Auditors	Only in employment until expiry date or termination of contract or employment
	ICP addresses	Freedom IT, Communication providers	Only in employment
	Internal documentation - meeting minutes, customer complaint forms, comms logs, asset databases	Clients, Auditors	3 years
	HSE incident reports and records	Clients, HSE, RIDDOR	3 years
	Password list	Freedom IT	Only in employment
	ID Cards	Clients	Only in employment
	SIA No, Staff name, Staff email*, SIA badge photo + any performance issues	Clients, Auditors, Jotform platform provider	3 years
	Staff names, client names and any staff performance issues/complaints	Clients, Auditors, Jotform platform provider	3 years where performance issues
	Staff telephone private telephone numbers	Logosoft platform provider	Until termination of employment and up to 3 months after to enable for contact for adjustments
	Staff identification details such as name, ID no, location, client name	Clients	1 year
	Name, employee ID, site location,	Clients, Auditors	3 years

From time to time, it may be necessary to retain or access historic personal data under certain circumstances, including where STM has contractually agreed to do so, or if the Company has become involved in unforeseen events such as litigation or business disaster recoveries.

Destruction and Disposal

Upon expiry of agreed retention periods, STM will delete confidential or sensitive records categorised as requiring high protection and very high protection, STM will either delete or anonymise less important documents.

The STM Head of HR is responsible for ongoing process of identifying records that have met their required retention period, including the supervision of their destruction. The destruction of confidential, financial, and personnel-related records shall, if possible, be securely undertaken either electronically or by shredding. Non-confidential records may be destroyed by recycling.

Paul Jacomb

Paul Jacomb
CEO
STM Group (UK) Ltd