StriveTraining

SUPPORTED BY
MAYOR OF LONDON

European Union
European Social Fund

GDPR POLICY AND PROCEDURES DOCUMENT

VERSION 9

1 AUGUST 2024

StriveTraining

Contents

1) Introduction and Overview

The Data Protection Act 1998 (DPA) has regulated the processing of personal data in any format by the company, including both digital and hard copy personal data and all other formats. 'Personal data' is any information relating to a living individual, and 'processing' is any activity carried out involving personal data, including holding and storing it.

On 25th May 2018 the DPA was superseded in the UK by the General Data Protection Regulation (GDPR), which provides individuals with enhanced rights, and imposes

increased responsibilities on organisations processing personal data. This statement applies under both the DPA and GDPR.

This *Policy & Procedures Document* establishes **Strive Training (London) Limited** procedures governing the collection and release of personal data and is provided to all whose data is held and all who manage and administer this data.

The recent data protection legislation (GDPR Act and EU GDPR legislation) provide. greater clarity on the legitimate holding and viewing of personal information. The EU legislation harmonises data protection laws across the EU and a limited number of other countries.

GDPR Law does not only apply to EU companies, but to any company processing the personal data of individuals in the EU in relation to offering goods or services, or to monitoring their behaviour.

This document includes the company GDPR policy and procedures.

For the purposes of this document, "data" means personal, supplier and customer information held within the company; in particular HR, Student Enrolments, Marketing, and Accounts.

GDPR policy and procedure documents should be written in plain language and easy to read by those with no prior knowledge of the subject. GDPR documents should contain a minimum of specialist terminology.

What is Personal Data?

GDPR law applies to living individuals defined as "Natural Person"; Personal data is any information that allows the "Natural Person" to be identified

Personal data includes personally identifiable information in locations such as; CRM, MIS, HR Software, Newsletters, Filing systems, marketing lists.

Student personal data is collected and processed by Strive Training as it is necessary for the performance of the contract under which Strive Training provides services to students.

Some processing activities may also be carried out under a legal obligation (for example, disclosing personal data to external parties under statutory powers), where it is necessary to protect the vital interests of the student or another party (for example, disclosures to external parties to ensure the safety and wellbeing of individuals), where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority (for example, collecting or disclosing information in order to meet regulatory or statutory requirements), or where it is necessary for legitimate interests pursued by Strive Training or a third party (the legitimate interests will relate to the efficient, lawful and proportionate delivery of services and will not be to the detriment of the interests or rights of individuals).

Where any of these legal bases do not apply, the consent of an individual to process their personal data will be sought.

Privacy risk

Privacy risk is the risk of harm arising through an intrusion into privacy. This code is concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information. Some of the ways this risk can arise is through personal information being:

- Inaccurate, insufficient or out of date;
- Excessive or irrelevant;
- Kept for too long;
- Disclosed to those who the person it is about does not want to have it;
- Used in ways that are unacceptable to or unexpected by the person it is about; or
- Not kept securely.

Legislative requirements:

Organisations are required to provide employees, job applicants, customers, clients, suppliers and business partners with a privacy notice setting out certain information. Under the GDPR law, individuals whose data is held will need to be provided with more detailed information, such as:

- How long data will be stored for;
- If data will be transferred to other countries;
- Information on the right to make a subject access request; and
- Information on the right to have personal data deleted or rectified in certain instances.

Restrictions to consent

Data can only be stored by consent and individuals such as employees, job applicants, customers, students, freelancers, volunteers, clients, suppliers and business partners must be able to withdraw their consent at any time.

New breach notification requirement
GDPR law imposes a new mandatory breach reporting requirement. Where there has been a data breach (such as an accidental or unlawful loss, or disclosure of data), the company suffering the breach will have to notify and provide certain information to the data protection authority within 72 hours. Where the breach poses a high risk to the rights and freedoms of individuals, those individuals will also have to be notified.

2) Data Management Responsibility

An organisation holding and determining whether personal data will be held is known as the Data Controller. The Data Controller can be an individual. The Data Controller at Strive Training is Johnny Phillips.

The Data Controller
The Data Controller is responsible for developing a data breach response programme to ensure prompt notification. The Data Controller is the person instructing data to be held. The Data Controller is legally responsible.

The Data Controller will allocate responsibility to certain people to manage data protection.

Data Protection Officers
Companies involved in regular monitoring or large-scale processing of sensitive data will need to appoint a Data Protection Officer to:

- Advise on GDPR obligations;
- Monitor compliance;
- Liaise with the data protection authority (ICO).
- Investigate and contain any data breaches, log a data breach report
- Train employees to recognise and address data breaches, and
- Put appropriate policies and procedures in place.

Data Protection Officers manage data protection procedures but are not legally responsible.

The Data Protection Officers for Strive Training (London) Limited are:

- John Stapleton (policies, data requests, data breaches & student data) - main contact
- Florina Todiras (Student data)
- Kim Franks (HR & Health & Safety)
- Jana Kucera (Financial, pensions and salary)
- Gersh Grosberg (IT systems and customer database)

Some personal data is processed on behalf of Strive Training, by our associated company Lyons Presentations Limited. The Data Protection Officers for Lyons Presentations Limited are Matt Bernstein (GDPR policy, data requests), Jana Kucera (salary and accounts) and Gersh Grosberg (IT and marketing).

Data Administrators
At department level, various individuals will be required to hold and process personal data in accordance with company policy and procedures. These people are known as Data Administrators. Data Administrators report to the Data Protection Officer.

Data Administrators should ensure that everyone in their workplace works in accordance with company GDPR procedures and ensure that risks of breaches are at a minimum.

Data Administrators should have:

- Copy of this GDPR Policy and Procedure document
- Record of retention period schedule for all data held in their department
- Schedule for sending Privacy Notices
- Privacy Notice Form
- Data Request Form / Data Deletion Form
- Shredder (cross)

If the Data Administrator has a breach reported to them or identifies are brief, the procedure detailed in **Section 6** should be followed. If an individual request for data to be returned to them, updated or deleted, the Data Administrator should follow the procedure detailed in **Section 7**, including sending the individual a *Data Request Form*.

Managing personal data
There are five parts of the GPDR legislation critical for managing individual and personal data. Personal data includes; employee, freelancer, student, job applicant customer, business partner, contractor and supplier data.

1. Consent: Businesses must ensure that individuals, whose personal data is being collected, understand how it's being used and get their affirmative, unambiguous consent to use it. No more pre-ticked boxes, bundled permissions and suchlike will be allowed. The company must ensure that it as easy to withdraw consent as it is to give it, so the permission will need to be earned and maintained.

2. Profiling: All individuals have the right to opt out of any form of automated profiling, which impacts everything from CRM and direct marketing to customised pricing. The company must be transparent about how data is being used and, critically, whether the value being created is balanced in the favour of the individual, whose personal data is being held.

3. The right to opt out of marketing: Once this is requested, all marketing must stop immediately.

4. The right to be forgotten: Once an individual has decided to leave, or cease business, they can request that all of their data is erased.

5. Data portability: Individuals must be able to ask for a copy of their personal data in a portable, unencrypted, easy to access, machine-readable format.

At all times, ask yourself what would the customer, student, business partner, contractor and supplier want? GDPR is complicated and there are still areas where the guidance is not clear. If you can keep the customer at the centre of your decision-making process then you will at least be compliant with the spirit of GDPR, even if not the letter.

3) Planning Procedure

Planning and communication:
Each Department Head and Data Administrators should be sent a copy of this document, Strive Privacy Statement, Data Deletion Form, Data Request Form. Business partners, freelancers and any other 3rd parties jointly holding personal data on behalf of the company should also be sent a copy of this document. A master version of this list will be held and provide definitive guidance on the storage and access to data.

Data audit overview
An audit of all identified personal data should be held on an annual basis, in

November of each year. Interim data audits should be held immediately if new categories of personal data are identified, or upon changes to any data storage, hosting or security measures.

Data Audit Procedure
Each year, the Data Protection Officer will send each Data Administrator a copy of the Data Audit Form for completion. All information provided by the Data Protection Officer must be easy to understand by those unfamiliar with data protection issues. Upon completion, this form is returned to the Data Protection Officer. Data Administrators should complete and send this form immediately if new categories of data are expected to be held, or if there are changes in security systems or data hosting.

Privacy Impact Assessment (PIA)
Upon receipt of completed data audit forms, the Data Protection Officer, will add new data to a Master Data Spreadsheet.

An additional assessment will be then conducted by the Data Protection Officer. This is called a Privacy Impact Assessment (PIA). The PIA is an audit/assessment within each data administrator Group (stakeholders). The outcome of a PIA should be a minimisation of privacy risk.

Within the PIA, the Data Protection Officer will assess the legal grounds for processing data. Where consent is currently relied on, check whether or not it meets GDPR requirements and remember that consent may be revoked at any time. Employers will generally need to rely on one of the other legal grounds to continue to process employee personal data.

Upon completion of the PIA, the Data Protection Officer will update the master data spreadsheet in compliance with GDPR law and other legislation impacting on data retention policy. The completed master spreadsheet will include a mandatory retention period and data risk level.

4) Privacy Notices

A Privacy Notice ensures all individuals are informed of what personal data we wish to hold. This notice also clarifies why and how we wish to hold and of the security systems and retention periods applied to their data.

A Privacy notice should be to tell people:

- Who you are;
- What you are going to do with their information;
- Who it will be shared with.

To cover all these elements, you will need to consider the following issues when planning a privacy notice:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?

Where you need consent from an individual in order to process their information you need to explain what you are asking them to agree to and why. This will often go hand in hand with providing privacy notices. Therefore, the code also includes information about obtaining consent.

It is important to make sure that where people do have a choice, they are given a genuine opportunity to exercise it. This means that it must be freely given, specific and fully informed. Consent must also be revocable (i.e. people must be able to withdraw their consent) and you should have procedures in place to action and record it when this happens.

You should always be honest with the public and not lead them to believe that they can exercise choice over the collection and use of their personal information when in reality they cannot.

There are some cases in which consent is not relevant, for example if individuals are required by law to provide their personal details. Giving people control and choice over how their personal data will be processed will not always be applicable in other situations, for example in an employer/employee relationship.

In all of these cases it is still important to be fair and transparent. Ensuring you have effective privacy notices can help you to achieve this.

Gaining consent

You need to consider how you will gain and record individuals' consent, if required. There is a fundamental difference between telling a person how you're going to use their personal information and getting their consent. Although in many cases it is enough to be transparent, and rely on a lawful basis other than consent, in others a positive indication of an individual's agreement will be needed.

When relying on consent, your method of obtaining it should:

- Be displayed clearly and prominently;
- Ask individuals to positively opt-in, in line with good practice; and
- Give them sufficient information to make a choice

If your consent mechanism consists solely of an “I agree” box with no supporting information then users are unlikely to be fully informed and the consent cannot be considered valid.

In addition if you are processing information for a range of purposes you should:

- Explain the different ways you will use their information; and
- Provide a clear and simple way for them to indicate they agree to different types of processing.

In other words, people should not be forced to agree to several types of processing simply because your privacy notice only includes an option to agree or disagree to all. People may wish to consent to their information being used for one purpose but not another.

Include list of rights to retrieve, correct or delete data.

All Data Administrators should use the authorised Privacy Notice shown. This notice should be sent to all individuals at the first instance point any data is expected to be recorded.

Individuals with data held prior to the introduction of GDPR law, should be provided with the Privacy Notice at the first point of contact after 25th May 2018 or within 6 months after this date. Returned and signed Privacy Notices should be forwarded to the Data Protection Officer, who will retain an up to date central record.

A maximum of 3 Privacy Notices can be sent to an individual. If after 3 attempts there has been no response, permission will be assumed to being refused and all personal data must be deleted.

Unless otherwise directed, personal data will be held for 3 years after permission is granted. Therefor Data Administrators should keep a record of when a fresh request for permission to hold data should be made.

Privacy Notice Form (Customers and Suppliers)
Here at Strive Training (London Limited) we take your privacy seriously and will only use your personal information to administer your account and to provide the products and services you have requested from us

For this purpose, your data will be securely stored, with access strictly limited to our sales, marketing, accounts, design and quality management departments.

Your data will be held for a period of up to 3 years beyond the last contact from you with us.

However, from time to time we would like to contact you with details about updates on new courses, training and products we provide. If you consent to us contacting you for this purpose, please tick to say how you would like us to contact you:

Post ☐

Email ☐

Telephone ☐

Text message ☐

Phone call ☐

You have the right withdraw consent and you can refuse to consent without detriment.

You have the right to request your data to be updated, corrected, and permanently deleted, or returned to you at any time. Requests of this nature should be made to John Stapleton (Data Protection Officer, email jstapleton@strivetraining.co.uk

If you consent to us retaining on your details for these purposes, please tick to confirm:

I agree ☐

Privacy Notice Form (employees and freelancers).
Here at Strive Training Ltd we take your privacy seriously and will only use your personal information for legal, personnel, administrative, management and other legitimate purposes and in particular to the processing of any sensitive personal data (as defined in the GDPR Act 2018) relating to you.

For this purpose, your data will be securely stored, with access strictly limited to our management and accounts departments.

Your data will be held for a period of up to 6 years beyond the last contact from you with us.

However, from time to time we would like to contact you with details of other freelance work if it becomes available. If you consent to us contacting you for this purpose, please tick to say how you would like us to contact you:

Post ☐

Email ☐

Telephone ☐

Text message ☐

Phone calls ☐

You have the right withdraw consent and you can refuse to consent without detriment.

You have the right to request your data to be updated, corrected, and permanently deleted. I or returned to you at any time. Requests of this nature should be made to Joel Marks (Data Protection Officer), email datacontroller@strivetraining.co.uk.

If you consent to us retaining on your details for these purposes, please tick to confirm:

I agree ☐

Privacy Notice Form (students).
The student Privacy Notice is included as part of the Student Learning Agreement form, which is completed by students prior to undertaking any learning. This form includes a weblink to the full Privacy Policy Terms and Conditions.

Privacy Notice:
Strive Training (London)Limited takes your privacy seriously and will only use your personal information to administer the services you have requested from us. For this purpose, your data will be securely stored, with access strictly limited to those within the business legitimately required to administer & manage your service and external parties in order to ensure the safety and wellbeing of individuals or in the public interest or to meet regulatory or statutory requirements.

Your data will be held for a period of up to 6 years beyond the last contact from you with us.

You have the right withdraw consent and you can refuse to consent without detriment.

You have the right to request your data to be updated, corrected, and permanently deleted, or returned to you at any time. Requests of this nature should be made via email to datacontroller@strivetraining.co.uk.

Please note that the right to the erasure of personal data will only apply where there is no legitimate reason for Strive Training to continue to process the personal data. There will usually be a requirement for Strive Training to keep a basic student record indefinitely for legal compliance.

The full terms and conditions of our Privacy Statement can be viewed here: Link

Tick box to agree. I agree ☐

5) Data Breaches

When the security of personal data is compromised, this is called a data breach. Data breaches are when personal information becomes available to anyone who does not have the individual's permission to view or hold it.

Data Breaches include:

- Emails containing personal information sent in error to 3rd parties
- Personal information stored without security measures preventing unauthorised access.
- Personal information accessed as a result of a cyber-attack or virus
- Personal information being stored on servers or hosted in countries not in compliance with GDPR law
- Personal information held on devices not under company ownership or security management
- Personal information lost or stolen from laptops, briefcases, etc.

- Unauthorised access to data by service providers, such IT support, CRM providers

6) Data Breach Management Procedure

All employees, freelance workers and service providers must report data breaches immediately. Data breaches should be reported to the Data Administrator or the Data Protection Offer.

Anyone suspecting a breach should:

- Prevent further risk of breach
- Record the nature and possible cause of the breach
- Identify who is affected by the breach and who may have gained access to data.

Data Administrators must report breaches to the Data Protection Officer **immediately** and without any delay.

The Data Protection Officer will:

- Make all attempts to reduce the impact of the breach
- Ensure contact is made with those affected by the breach
- Record all breach details to the Data Protection Breach Log
- Contact Information Commissioners Office to formally report the breach

All data breach processes must be completed within 72 hours of initial notification.

The Data Protection Officer's contact details will be known on Privacy Statements and company web site, in order for individuals to report suspected breaches without delay.

7) Data Deletion Procedure

Data will be deleted in accordance with the mandatory retention periods

Data Administrators should be aware of the retention period for the data they hold.

Data should be deleted on ½ yearly schedule, ahead of the next mandatory retention date.

There may be business circumstances when it is beneficial to both the individual and the company to hold data for a further period. In these cases, a fresh Privacy Notice must be sent to the individual ahead of the retention period ending.

Printed data should be shredded, using a cross shedder. If large quantities are needed to be shred, data should be deleted on site.

Computer files should be deleted, using the Secure Trash option if available

Back up versions, include those held remotely or disk, must also be deleted.

Archive versions should be deleted.

Data deletions should be recorded.

Individuals have the right to have their personal data deleted; this is called the Right to Erasure or Right to be forgotten. Requests to have data deleted by individuals should be made to the Data Protection Officer.

Individual requests must verify formally using the Data Request Form. Requests for deletion by individuals must be completed within 30 days.

Please note that the right to the erasure of personal data will only apply where there is no legitimate reason for Strive Training to continue to process the personal data. There will usually be a requirement for Strive Training to keep a basic student record indefinitely for legal compliance.

8) Data Return and Correction Procedure

Individuals have the right to have their data returned to them or for it to be updated and corrected.

Individual requests to have data returned or corrected by should be made to the data Protection Officer.

Individual requests must verify formally using the Data Request Form.

Requests for deletion by individuals must be completed within 30 days.

9) Data Retention Periods

In the simplest terms, non-sensitive employee, freelancer and customer data can normally be retained up to 3 years beyond the individual authorising data to be held.

Accounts data, including transaction documents must be retained for 7 years, to comply with Tax regulations.

Student data includes financial data and must be retained for 7 years. Some funding conduits, for example the Education Skills Funding Agency (ESFA) and Greater London Authority (GLA), contractually require a longer period of student data retention.

Bank account details give rise to a serious data risk. As such, bank account details for employees and freelancers should be deleted 3 months after they have stopped working for the company.

There is however other legislation in place which overrides GDPR law, where statutory (UK Law) retention periods apply. These periods are detailed below.

A) Statutory Retention Periods

Accident books, accident records/reports

Statutory retention period: 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 authority: The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances (see below).

Accounting records:

Statutory retention period: 3 years for private companies, 6 years for public limited companies.

Statutory authority: Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006.

Income tax and NI returns, income tax records and correspondence with HMRC

Statutory retention period: not less than 3 years after the end of the financial year to which they relate.
Statutory authority: The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631).

Medical records (general): 12 years.

Medical records (specific):

Medical records and details of biological tests under the Control of Lead at Work Regulations

Statutory retention period: *40 years from the date of the last entry.*
Statutory authority: *The Control of Lead at Work Regulations 1998 (SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676).*

Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)

Statutory retention period: *40 years from the date of the last entry.*
Statutory authority: *The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).*

Medical records under the Control of Asbestos at Work Regulations: medical records containing details of employees exposed to asbestos and medical examination certificates

Statutory retention period: *(medical records) 40 years from the date of the last entry; (medical examination certificates) 4 years from the date of issue.*
Statutory authority: *The Control of Asbestos at Work Regulations 2002 (SI 2002/ 2675). Also see the Control of Asbestos Regulations 2006 (SI 2006/2739) and the Control of Asbestos Regulations 2012 (SI 2012/632)*

Medical records under the Ionising Radiations Regulations 1999

Statutory retention period: *until the person reaches 75 years of age, but in any event for at least 50 years.*
Statutory authority: *The Ionising Radiations Regulations 1999 (SI 1999/3232).*

National minimum wage records

Statutory retention period: 3 years after the end of the pay reference period following the one that the records cover.
Statutory authority: National Minimum Wage Act 1998.

Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)

Statutory retention period: 5 years from the date on which the tests were carried out.

Statutory authority: The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).

Records relating to children and young adults

Statutory retention period: until the child/young adult reaches the age of 21.
Statutory authority: Limitation Act 1980.

Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity

Statutory retention period: 6 years from the end of the scheme year in which the event took place.
Statutory authority: The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)

Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence

Statutory retention period: 3 years after the end of the tax year in which the maternity period ends.
Statutory authority: The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended.

Wage/salary records (also overtime, bonuses, expenses)

Statutory retention period: 6 years.
Statutory authority: Taxes Management Act 1970.

Working time records

Statutory retention period: 2 years from date on which they were made.
Statutory authority: The Working Time Regulations 1998 (SI 1998/1833).

B) Non-statutory Retention Periods

For many types of HR records, there is no statutory retention period. However, retention periods must be legally justifiable and not be excessive.

The UK Limitation Act 1980 contains a 6-year time limit for starting many legal proceedings. So, where documents may be relevant to a contractual claim, it's recommended that these are kept for at least a corresponding 6-year period.

Actuarial valuation reports
Recommended retention period: permanently.

Application forms and interview notes (for unsuccessful candidates)
Recommended retention period: 6 months to a year. (Because of the time limits in the various discrimination Acts, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months. A year may be more advisable as the time limits for bringing claims can be extended. Successful job applicant's documents will be transferred to the personnel file in any event.

Assessments under health and safety regulations and records of consultations with safety representatives and committees
Recommended retention period: permanently.

Inland Revenue/HMRC approvals
Recommended retention period: permanently.

Money purchase details
Recommended retention period: 6 years after transfer or value taken.

Parental leave
Recommended retention period: 18 years from the birth of the child.

Pension scheme investment policies
Recommended retention period: 12 years from the ending of any benefit payable under the policy.

Pensioners' records
Recommended retention period: 12 years after benefit ceases.

Personnel files and training records (including disciplinary records and working time records)
Recommended retention period: 6 years after employment ceases.

Redundancy details, calculations of payments, refunds, notification to the Secretary of State
Recommended retention period: 6 years from the date of redundancy

Senior executives' records (that is, those on a senior management team or their equivalents)
Recommended retention period: permanently for historical purposes.

Statutory Sick Pay records, calculations, certificates, self-certificates
Recommended retention period: The Statutory Sick Pay (Maintenance of Records) (Revocation) Regulations 2014 (SI 2014/55) abolished the former obligation on employers to keep these records. Although there is no longer a specific statutory retention period, employers still must keep sickness records to best suit their business needs. It is advisable to keep records for at least 3 months after the end of the period of sick leave in case of a disability discrimination claim. However if there were to be a contractual claim for breach of an employment contract it may be safer to keep records for 6 years after the employment ceases.

Time cards
Recommended retention period: 2 years after audit.

Trade union agreements
Recommended retention period: 10 years after ceasing to be effective.

Trust deeds and rules
Recommended retention period: permanently.

Trustees' minute books
Recommended retention period: permanently.

Works council minutes
Recommended retention period: permanently.

C. All other data retention periods

Some specific types of data is retained may be retained on either a periodic or rare basis. A summary of specific data retention periods is detailed in the table below.

Type Of Document	Statutory Minimum Retention Period	Recommended Period Of Retention
Incorporation Documents		
Certificate of Incorporation and Certificates on Change of Name	N/A	Permanently
Certificate to commence business (Public Company)	N/A	Permanently
Memorandum and Articles of Association (original and updated copies)	Permanently	Permanently

Printed copies of resolutions submitted to Companies House	Permanently	Permanently

Statutory Returns, Records and Registers	**Statutory Minimum Retention Period**	**Recommended Period Of Retention**
Annual Return (copy)	N/A	Permanently
Return of Allotments (copy)	N/A	Permanently
Directors' Service Contracts	6 years after cessation	6 years after cessation
Register of Directors and Secretaries (original)	Permanently	Permanently
Register of Directors' interests in Shares and Debentures	Permanently	Permanently
Register of interests in voting shares	Permanently	Permanently
Register of Charges	Permanently	Permanently
Register of Documents sealed (if applicable)	N/A	Permanently
Unpaid dividend records	N/A	12 years after dividend declared
Dividend and interest mandate forms ceased to be valid	N/A	3 years from when the instruction
Notification of address change by member	N/A	2 years after notification

StriveTraining

Share Registration Documents	Statutory Minimum Retention Period	Recommended Period Of Retention
Register of Members	Permanently	Permanently
Register of Debentures and Loan Stock holders	N/A	Permanently / 7 years after redemption of stock
Letters and forms applying for Shares, Debentures etc.	N/A	12 years from issue, with a permanent microfilmed record
Renounceable Letter of Allotment and Acceptances	N/A	Originals for 12 years from renunciation, with a permanent microfilmed record
Renounced Share Certificates	N/A	Originals for 12 years from renunciation, with a permanent microfilmed record
Contracts for purchase of own shares by Company	N/A	
Share & Stock Transfer forms and Letter of Request with permanent microfilmed record	N/A	
Requests for designating or redesign ting accounts with permanent microfilmed record	N/A	
Cancelled share/stock Certificate	N/A	
Stop Notice and other Court Orders	N/A	
Letters of indemnity for lost Certificates	N/A	
Powers of Attorney	N/A	
Dividend and interest payment lists	N/A	

Paid dividend and interest warrants	N/A	
Bank Records		
Cheques, bills of exchange and other negotiable instruments	N/A	
Paying-in counterfoils	N/A	
Statements from and instructions to the bank	N/A	
Public Company	6 years	10 years
Limited Company	3 years	10 years
Annual report and accounts (signed)	N/A	Permanently
Annual report and accounts (unsigned)	N/A	Permanently (keep sufficient copies to meet requests)
Interim report and accounts	N/A	Permanently (keep sufficient copies to meet requests)
Budgets, forecasts and periodic internal financial reports	N/A	5 years
Taxation records and tax returns	Inspection possible up to 6 years after tax/accounting period	Permanently
VAT records and Customs & Excise returns	Inspection may be conducted up to 6 years after tax/accounting period	Permanently
Expense accounts	N/A	7 years
Charity Donation Documents	**Statutory Minimum Retention Period**	**Recommended Period Of Retention**
Deeds of Covenant	6 years after last payment	12 years after last payment

Documents supporting entries in accounts for donations	3 or 6 years	6 years

Contracts	**Statutory Minimum Retention Period**	**Recommended Period Of Retention**
Contracts executed under seal	N/A	12 years after expiry
Contracts with customers, suppliers, agents or others	N/A	6 years after expiry or contract completion
Rental and hire purchase agreements	N/A	6 years after expiry
Licensing agreements	N/A	6 years after expiry
Trust deeds and rules (pension schemes)	N/A	Permanently

Insurance	**Statutory Minimum Retention Period**	**Recommended Period Of Retention**
Public liability policies	N/A	Permanently
Product liability policies	N/A	Permanently
Employers' liability policies	40 years	Permanently
Sundry insurance policies and insurance schedules	N/A	Until claims under policy are barred or 3 years after policy lapses, whichever is longer
Group health policies	N/A	12 years after final cessation of benefit
Group personal accident policies Claims correspondence N/A 3 years after settlement	N/A	12 years after final cessation of benefit

Health & Safety	**Statutory Minimum Retention Period**	**Recommended Period Of Retention**
Record of consultations with safety representative and committees	N/A	Permanently

Health & Safety policy documents (old and revised copies)	Implied permanently by Health & Safety at Work Act (1974 S2(3)	Permanently
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 (Management of Health & Safety at Work Regulations 1992 S1 1992/2051)	Permanently (old and current copies)
Accident report book and relevant records/ correspondence	3 years from date of entry (Health & Safety at Work Act 1974 S7)	Permanently
Medical records – general	N/A	12 years

Employees Records	**Statutory Minimum Retention Period**	**Recommended Period Of Retention**
Personnel records	N/A	7 years after employment ceases, with permanent microfilmed record
Senior executive records	N/A	Permanently
Training records	N/A	6 years after employment ceases
Employment agreements	N/A	Permanently
Payroll and wage records (including details of overtime, bonuses and expenses)	6 years	12 years
Salary records	N/A	5 years
Time cards and piecework records	N/A	2 years
Details of benefits in kind	6 years	12 years
Income tax records (P45/P60/P58/P48 etc.)	6 years	12 years
Annual return of taxable pay and tax paid	6 years	12 years
Labour agreements	N/A	10 years after ceasing to be effective

Works council minutes	N/A	Permanently
Employee records fro closed units	Some 6 years	12 years

Material With Copyright Protection	**Statutory Minimum Retention Period**	**Recommended Period Of Retention**
Literary, dramatic and musical works	N/A	Life plus 50 years
Artistic works, recordings, films, photos and broadcasts.	N/A	50 years

Pension Scheme Documents(unapproved schemes)	**Statutory Minimum Retention Period**	**Recommended Period Of Retention**
Trust deeds and scheme rules	N/A	Permanently
Trustees' minute books	N/A	Permanently
Record of pensioners	N/A	12 years after cessation of benefit
Money purchase details	N/A	6 years after transfer or value taken
Pension scheme investment policies	N/A	12 years after transfer or value taken

Pension Scheme Documents(inland revenue approved and statutory pension schemes)	**Statutory Minimum Retention Period**	**Recommended Period Of Retention**
Pension fund accounts and supporting documents	6 years from date of accounts signed	Permanently
Actuarial valuation reports	6 years from date of report signed	Permanently
Inland revenue approvals	N/A	Permanently
Medical records – Radiation accident assessment	50 years	Permanently
Medical records – Radiation dosage summary	2 years from end of calendar year	Permanently

Under control of Lead at Work Regulations 1998 (replaced 1980 regulations)	2 years from date of last entry to be effective	Permanently
Under Control of Asbestos a Work Regulations 1987	40 years	Permanently
Under Control of Substances Hazardous to Health regulations 1994 9COSHH Regulations)	40 years	Permanently

Intellectual Property Records	**Statutory Minimum Retention Period**	**Recommended Period Of Retention**
Certificates of registration of trade/service marks (current and lapsed)	N/A	Permanently or 6 years after cessation of registration
Documents evidencing assignment of trade/service marks	N/A	6 years after cessation of registration
Intellectual property agreements and licences	N/A	6 years after expiry

Property Documents	**Statutory Minimum Retention Period**	**Recommended Period Of Retention**
Title deeds for property	N/A	Permanently or until sold or transferred
Leases	N/A	12 years after lease and liabilities under the lease have terminated

Other Records	
Diaries	3 Years

Board Meeting Reports	30 Years
Business Plans	20 Years
Commissioning Decisions	6 Years from date of appeal decision
Complaints Correspondence	10 Years
Health & Safety Documents	3 Years
Incident Forms	8 Years
Manuals	10 Years
Meetings & Minutes	30 Years
Minor Paperwork (reminders , advertising etc)	2 Years
Quality Assurance Records	12 Years
Reports	30 Years
Incident Files	30 Years
Time Sheets	3 Years
Annual Accounts	30 Years
Accounts – Minor Records (cash books etc)	2 Years
Financial Contracts	15 Years
Bacs Payments, Fraud Investigations, Invoices	6 Years
Personnel Records	6 Years

D. Greater London Authority (GLA) contractual requirements:

Strive Training is contractually required to retain all documents necessary to verify its Services provided to the GLA. Documents to support claims will be retained for a minimum of 3 years after the European Commission has made its final payment. This is expected to be until at least 31 December 2030.

Documents are stored in line with the *England European Social Fund Operational Programme 2014-20 Guidance: Guidance on document retention, including electronic data exchange, for 2014-20 ESF projects.*

Where learner data is used by the GLA as match on the Mayor's 2019-23 ESF Programme, GLA Supplementary Data, ILR data submitted to the ESFA, and supporting evidence, will be retained securely for at least 2 years after the final ESF claim has been paid by the EU Commission to the UK Managing Authority, which is expected to be until at least 31 December 2033.

The Data Controller is responsible for determining any further need to process the data, including its retention, prior to secure destruction.

10) Other GDPR Documents and Forms

An inventory is made of all personal data held by the company. This is called a Personal Data Record List. This document details:

- The nature of the data
- The record format
- The person/people who hold the data
- Where the data is held
- A description of security measures in place
- Who has access to this data
- The legal justification for holding the data
- The retention periods
- The risk level of this data

This can all be found in ST Personal Data Record V02

Data requests made by employees, former employees, students, former students, customers, suppliers and business partners must be made in writing. Written requests are made using the forms listed below:

ST Subject Access Request Form V01
ST Subject Erasure Request Form V01
ST Subject Correction Request Form V01

This document provides a specific breakdown of all data held, the reasons for holding it and of any mandatory retention periods or other legislation which may restrict the company's ability to erase data. This document also details the GDPR responsibilities or students.

Data breaches are recorded on to a data breach log. This is called: ST Data Breach Log 2018. This log records the breach (as originally reported), the investigation, date reported to ICO, remedy and recommended future actions.

If you have any queries about the policies which have been explained within this document, please do not hesitate to contact the Data Protection Officers at datacontroller@strivetraining.co.uk.

11. Training

The Data Protection Officers should have formal and up to date GDPR training.

The Data Protection Officers should provide GDPR training to all staff, as part of the induction process.

Refresher training should be provided to staff every 2 years or when there are changes to GDPR law.

12. Review

The Data Protection Officer will conduct an audit of GDPR processes annual in November. The audit shall:

- Review effectiveness and compliance of processes
- Review understanding of processes within the workforce
- Identify discrepancies in how process is conducted in comparison to the described policy and procedures.
- Review and update the list of personal data

13. Transfer of personal data to processors established in third countries

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, the data exporter and the data importer identified in any contractual signature pages (commonly known as a DPA Standard Contractual Clauses (SCC) document) pertaining to the transfer of said data will agree to the clauses outlined in this section. Each a 'party', together 'the parties', WILL HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Schedule 1.

Clause 1
Definitions
For the purposes of the Clauses:

(a)	*'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the

14. European Parliament and of the Council of 24 October 1995 on the protection of individuals with
regard to the processing of personal data and on the free movement of such data;

(b)	'*the data exporter'* means the controller who transfers the personal data;
(c)	*'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

	'the subprocessor' means any processor engaged by the data importer or by any other
(d)	

Subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e)	'*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of

Personal data applicable to a data controller in the Member State in which the data exporter is established;

(f)	*'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration,

Unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a)	that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law

(and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b)	that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses; that the data importer will provide sufficient guarantees in respect of the technical and
(c)	

organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) (f)	that it will ensure compliance with the security measures; that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC; to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension; to make available to the data subjects upon request a copy of the Clauses, with the exception of
(g)	
(h)	

Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i)	that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and that it will ensure compliance with Clause 4(a) to (i).
(j)	

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a)	to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees

To inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c)	that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred; that it will promptly notify the data exporter about:
(d)	

(i)	any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, any accidental or unauthorised access, and
(ii)	

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability
1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction
1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a)	to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority; to refer the dispute to the courts in the Member State in which the data exporter is established.
(b)	

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities
1. The data exporter agrees to deposit a copy of this contract with the supervisory authority

if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law
The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract
The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing
1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such thirdparty liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and / or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

StriveTraining

Appendix 2

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

In addition to the security measures set forth in Section 6 of the ActiveCampaign Data Processing Addendum, data importer will implement technical and organizational security measures intended to secure the processing of Client Personal Information and to preserve the security, availability, integrity and confidentiality of Personal Information ("**Security Measures**"), in accordance with its obligations under Applicable Law including, as applicable:

(a) the pseudonymization and encryption of Personal Information;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing Personal Information.

StriveTraining

Appendix 3

StriveTraining

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

Where the EU Controller-to-Processor Model Clauses ("Clauses") apply pursuant to Section 5B of this Addendum, then this Appendix 3 sets out the parties' interpretations of their respective obligations under specific provisions within the Clauses, as identified below. Where a party complies with the interpretations set out in this Appendix 3, that party shall be deemed by the other party to have complied with its commitments under the Clauses. When used below, the terms "data exporter" and "data importer" shall have the meaning given to them in the Clauses.

Nothing in the interpretations below is intended to vary or modify the Clauses or conflict with either party's rights or responsibilities under the Clauses and, in the event of any conflict between the interpretations below and the Clauses, the Clauses shall prevail to the extent of such conflict. Notwithstanding this, the parties expressly agree that any claims brought under the Clauses shall be exclusively governed by the limitations on liability set out in the Agreement. For the avoidance of any doubt, in no event shall any party limit its liability with respect to any data subject rights under the Clauses.

Clause 4(h): Obligations of the data exporter regarding non-disclosure requirements

Data exporter agrees that the terms of these Clauses, as executed, constitute data importer's confidential information and may not be disclosed by data exporter to any third party without data importer's prior agreement (other than to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8, with the exception of any confidential or commercial information as consistent with the parties' respective obligations in Sections 4(h) and 5(g), respectively)).

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data.
3. If the data exporter intends to suspend the transfer of personal data, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("Cure Period").
4. If after the Cure Period, the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(b): Supplementary Measures:

1. The parties acknowledge that it is the responsibility of the data exporter to verify whether the safeguards employed by data importer are sufficient to meet its obligations under Applicable Law, including with respect to the provision of adequate safeguards necessary to secure the transfer of personal data through these clauses.

2. Data importer has not, to its knowledge, received any requests for the personal data of EU residents processed within the provision of the Services, under Section 702 of the U.S. Foreign Intelligence Surveillance Act.
3. The parties acknowledge that personal data transmitted between data exporter and data importer within the course of the Services is encrypted in transit.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement in effect as of the date of execution of these Clauses or other written or electronic agreement for data exporter's use and purchase of data importer's products and services. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC" the data exporter may provide a general consent to onward subprocessing by the data importer.
2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out below, which collectively ensure that the onward subprocessor will provide adequate protection for the personal data that it processes:
    a. any onward subprocessor must agree in writing: (i) to only process personal data in the European Economic Area or another country that the European Commission has formally declared to have an "adequate" level of protection in accordance with the requirements of EU Data Protection Law; or (ii) to process personal data on terms equivalent to these Model Clauses, pursuant to a Binding Corporate Rules approval granted by competent European data protection authorities and whose scope extends to transfers of personal data from the territories in which the data exporter is established, or subject to a mechanism providing adequate safeguards for the transfer of personal data in accordance with applicable law, including Article 46 of the General Data Protection Regulation; and
    b. data importer must restrict the onward subprocessor's access to personal data only to what is strictly necessary to perform its subcontracted data processing services to data importer (which shall be consistent with the instructions issued to data importer by data exporter) and data importer will prohibit the onward subprocessor from processing the personal data for any other purpose.

Version	Description of changes	Date	Auth	Appr.
V9	Review document	01/08/24	Kim Franks/John Stapleton	Jonny Phillips