

## **Data Retention Policy**

### **How we operate.**

The Coaching Experience Limited is a boutique coaching and training company located in the UK with clients worldwide.

Clients typically contact us via our Contact option on our website, via email or phone.

Clients using the website leave a name and a contact number but this information is retained as a general enquiry email only.

Typically, that client's name and email address is stored on the general email software programme; and we have client names and phone numbers on a mobile phone.

We have clients that follow TCE Ltd on Facebook, LinkedIn and Twitter but we do not store any data on clients beyond the normal facility offered by these platforms.

Typically, we will engage in a series of emails currently via Gmail (Google). If a client is invoiced, we typically ask for the invoiceable name of the Company and their registered office. The invoice is typically generated in a password encrypted Excel workbook and that invoice will have the client's company name and address and information relating to the purchase.

The invoice is also raised in QuickBooks as a Company name only. QuickBooks is a cloud-based programme accessed via password.

A client will usually pay an invoice via direct deposit to our bank and show standard bank transaction details. Our bank account is accessed via the internet via a rigorous password procedure.

On very rare occasions we process payments via Square but the purchaser has the option to not save credit card details and our statements do not show credit card details. To date this has been minimal to say the least.

We keep business cards and client promotional literature for the life of that client relationship. We do not have a customer relations management system that stores client information.

When working with a client we record online sessions but the recording option is always a) declared to the client and b) handed to the client; so we do not actually save recordings to our computer.

With permission, we take client notes but these notes are scanned and saved and password encrypted and the raw notes are shredded; or handed back to the client at the end of a coaching assignment. Please note that we do not record sensitive information about our clients in these notes.

In short, any financial information about clients is limited to standard banking transaction records on our bank's closed platform. We do not store this data.

If we group email people, the contact details are always in the Blind Carbon Copy slot; and we only email people who have given permission to receive a group email i.e., a small group of course participants. We do not share email addresses with other course members.

## **Introduction**

This data retention policy sets out the obligations of The Coaching Experience Limited (“us/we/our”) and the basis upon which we shall retain, review and destroy data held by us, or within our custody or control. This policy applies to its director, and sub-contractors and sets out what the retention periods are and when any such data may be deleted.

## **Objectives**

It is necessary to retain and process certain information to enable our business to operate. We may store data in the following places:

- desktop
- any third-party servers – Google, QuickBooks;
- potential email accounts;
- potential backup storage; and/or
- 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. We are bound by various obligations under the law in relation to this and therefore, to comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully in respect of their 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 we aim to comply with the Regulation in so far as it is possible. In summary, the Regulation states that all personal data shall be:

- a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- b) 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;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- d) 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;

e) 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;

f) 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 and when it is no longer required, it shall be deleted and that the data should be adequate, relevant and limited for the purpose in which it is processed. With this in mind, this policy should be read in conjunction with our other policies, which are relevant such as our Privacy, Cookie and Terms and Conditions Policy.

### **Security and Storage**

All data and records are stored securely to avoid misuse or loss. We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. We employ encrypted hard drive backup 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 by them to comply with those procedures and policies, or if there are adequate measures in place.

Our data storage facilities are as follows:

- On an external hard drive stored separate to the desktop
- Standard data held by banking and QuickBooks

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

(a) Confidentiality means that only people who are authorised to use the data can access it.

(b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) 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 our central computer system instead of individual PCs.

### **Retention Policy**

Data retention is defined as the retention of data for a specific period of time and for back up purposes. We shall not keep any personal data longer than necessary, but acknowledge that this will be dependent on the different types of documents

and data that we have responsibility for. As such, our general data retention period shall be for a period, which is outlined in the table below. Our specific data retention periods are set out below:

**Type of Data:** Coaching Clients/Training clients

**Type of Data Collected:** First/Last name, Company name, Email address, web address, registered office address, Mobile/telephone number, Banking details – branch, account and sort code

**Type of Data:** Product purchasers

**Type of Data Collected:** First/Last name, credit card details

NB: We do not collate any data as it relates to web campaigns (opened, clicked, replied emails, answered phone calls, responded to text messages) that we have sent them. From time to time, it may be necessary to retain or access historic personal data under certain circumstances such as if we have contractually agreed to do so or if we have become involved in unforeseen events like litigation or business disaster recoveries.

#### **Destruction and Disposal**

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

Our Director and designated Data Protection Officer is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction if needed. The destruction of confidential, financial, and personnel-related records shall be securely destroyed electronically or by shredding if possible.

Non-confidential records may be destroyed by shredding and recycling.

Please contact Andrew Priestley at [info@andrewpriestley.com](mailto:info@andrewpriestley.com)