General Data Protection & Privacy Policy

CONTENTS

Directors: D Carr PgD FIIRSM DipSM FaPS, GradIOSH, D Cooper CMIOSH MIIRSM CMaPS, V Carr
Registered in England No. 2131209
Registered Office: Yardley House, 11 Horsefair, Rugeley, Staffs WS15 2EJ

General Data Protection & Privacy Policy

1. Introduction

Callsafe Services Limited needs to gather and use information about individuals. These can include trainees, customers, suppliers, business contacts, employees and other people the organisation has or may need to contact.

This policy describes how this potential data must be collected, handled, stored and disposed of to meet The GDPR 2018 requirements, to comply with the Law.

2. Purpose

This policy ensures Callsafe Services Limited:

- ❒ Complies with the regulations and follows good practice
- ❒ Protects the rights of staff, clients and partners
- ❒ Is transparent about how it collects, stores and processes individual's data
- ❒ Protects itself from the risks of data breach

3. Data Protection Law

The General Data Protection Regulations (GDPR 2018) came into force on 25th May 2018. The regulations describe how a company must collect, handle, store and dispose of personal information.

The Regulations apply whether the data is stored electronically or as hard copy.

Data kept will be:

1. Collected fairly and legally
2. Individual will be made aware and must actively give permission
3. Data must be relevant
4. Data will be accurate and current
5. Not be held for longer than necessary
6. Be protected appropriately
7. Destroyed on request – right to be forgotten
8. Be supplied on request to the relevant individual FOC
9. Not shared with any other party without permission

4. Scope

This policy applies to:

- ❒ All Callsafe Services Limited offices
- ❒ All staff working from Callsafe Services Limited offices, client facilities and/or when working from home
- ❒ All associates performing training and/or consultancy on Callsafe Services behalf

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside GDPR 2018. This data will include:

- ❒ Names of individuals
- ❒ National Insurance Number (where required for identification purposes)
- ❒ Other individual identification numbers, e.g. employee number
- ❒ Company name and postal address
- ❒ Individual's postal address, for Callsafe Services Limited employees and associates, and where individual trainees do not have a company address
- ❒ E-mail addresses
- ❒ Telephone numbers – landline and mobile
- ❒ Any other information relating to individuals for employment or training record purposes

5. Risks

This policy helps to protect Callsafe Services Limited from security risks including:

- ❒ Breaches of confidentiality e.g. divulging information by mistake
- ❒ Failing to offer choice, e.g. preventing the individual giving permission on holding data, what is held and how it is stored
- ❒ Reputational damage, e.g. company servers being hacked and sensitive data being stolen
- ❒ Personal and organisational data being stolen from laptops

6. Responsibilities

All staff have some responsibility for ensuring that data is collected handled stored and disposed of appropriately, in line with the requirements of GDPR 2018.

Managing Director is responsible for ensuring the company meets its legal requirements under GDPR 2018, and is the Data Protection Officer (DPO), although the appointment of a DPO is not a specific requirement for Callsafe Services Limited. The key stake holders are:

The Managing Director (Data Protection Officer) is responsible for:

- ❒ Keeping the directors and managers updated
- ❒ Reviewing GDPR procedures
- ❒ Arranging GDPR briefings and training for people covered by this policy
- ❒ Handling data protection questions from staff and anyone else covered by the policy
- ❒ Dealing with requests from individuals who request to see data Callsafe Services Limited holds on them
- ❒ Ensure any third party conforms with Callsafe Services Limited's GDPR policy
- ❒ Ensuring marketing initiatives conform with GDPR
- ❒ Approving any data protection statements attached to letters and email
- ❒ Ensuring that all systems, security and equipment used for storing data meet acceptable security standards

- ❒ Perform regular checks and scans to ensure security hardware and software is functioning correctly
- ❒ Evaluate any third-party services the company is considering using to store or process data, e.g. cloud computing services

Staff and Associates are responsible for:

- ❒ The only staff and/or associates accessing data should need to do it for their work
- ❒ Data must not be shared informally
- ❒ Staff and associates should keep all data secure and take sensible reasonable precautions.
- ❒ Staff and associates should use strong passwords and change them regularly
- ❒ Personal data must not be disclosed to unauthorised people either internally or externally
- ❒ Where on review data is found to be no longer needed it should be disposed of appropriately, e.g. the deletion of electronic data or shredding of hard copy data
- ❒ Staff should request help from their manager or Data Protection Officer if they are unsure of any aspect of GDPR

7. Collection, Storage & Payments

- ❒ When data is collected it must be with the permission of the individual. Passive agreement is not agreement. The individual must be told we are keeping their data, what will be recorded and the fact it will be stored, and their agreement obtained
- ❒ Data will be stored in a secure place, either electronically or as hard copy
- ❒ Staff should ensure that they do not leave hard copy records where unauthorised people could see them
- ❒ Data should be disposed of securely, e.g. shredded when no longer required
- ❒ Where data is stored electronically it must be protected from unauthorised access, accidental deletion and malicious hacking attempts
- ❒ Data should be protected by strong passwords, changed regularly and never shared between staff, except to the Senior Office Administrator who keeps a record of company passwords within a password secured electronic document
- ❒ Data will only be stored on password protected designated desktop and laptop computers and approved cloud computing services
- ❒ The cloud computing services data is continuously backed-up. Data on desktops and laptops will be backed up frequently, at least weekly, with the backup password protected and stored separately to the desktop/laptop
- ❒ The cloud computing service is protected with security software and appropriate firewalls
- ❒ Access to the cloud computing service from a laptop is provided through a virtual private network (VPN)
- ❒ All desktops and laptops are installed with Carbon Black virus and malware protection software, which must be updates as required by the supplier, and never be disabled, unless permission has been obtained from the Data Protection Officer
- ❒ Payment for courses through our website or through the Virtual Card Reader option is controlled by our Merchant Bank (WorldPay), who will collect payment card details electronically, they use encryption by using Secure Site Certificate technology. It is strongly

recommended that persons do not to send full credit or debit card details in unencrypted electronic communications with us. Payment through the Virtual Card Reader shall have the individuals card details entered directly into the WorldPay secure server, without any written record made or retained. A record or the payment being received will be provided by WorldPay

8. Use

Data is at the highest risk of loss corruption or theft when it is being used:

- ❒ Staff and associates should ensure no data is visible on screens when they are unattended
- ❒ Personal data should not be shared informally, where possible it should not be sent by email which is not secure
- ❒ Staff should not save copies of personal data to their own computer, except for contact and training details required for business and/or training purposes

9. Accuracy

Callsafe Services Limited will take reasonable steps to ensure data is kept up to date and it is accurate and relevant. It is the responsibility of staff and associates to take reasonable steps to ensure data kept is accurate and up to date.

- ❒ Data will be held in as few places as possible. Unnecessary additional sets will not be created
- ❒ Staff should take the opportunity to update client personal data, e.g. by confirming client details when speaking to a client
- ❒ Data will be updated as inaccuracies are discovered, e.g. if the client can no longer be reached on a specific phone number it should be deleted from the contact details within Outlook

10. Subject Access Request

The person whose data is held is referred to under GDPR 2018 as the subject. The subjects of Callsafe Services Limited are entitled to:

- ❒ Ask what information is held on them
- ❒ Ask how to gain access to it
- ❒ Be informed how to keep it up to date
- ❒ Be informed how the company is meeting it legal obligations under GDPR 2018

Subject access requests should be made to the Data Controller formally in writing.

Information will be supplied free of charge within 1 month of the request.

The Data Protection Officer will always verify the identity of the person making the subject access request before handing over any information.

11. Disclosing Data for Other Reasons

We may disclose information relating to staff and associate training, qualifications and experience to Callsafe Services Limited's clients or third-party accreditation bodies for skills, knowledge and experience verification purposes.

We will disclose trainees' training and qualifications to the trainees' employer.

We may also pass on information relating to vocational qualifications to the relevant government bodies, e.g. police, HSE, etc. in accordance with our obligations to such bodies. We will not disclose other information to third parties for any other purposes. Under these circumstances the data controller will ensure the request is legitimate, seeking legal advice where necessary.

12. E-mails & the Use of Tablets and Smart Phones

All e-mails sent out by Callsafe Services Limited staff, and associates on Callsafe Services Limited behalf, shall have the following text included as part of the e-mail signature:

> This e-mail is confidential and may be read only by the intended recipient. If you are not the intended recipient, please do not forward, copy or take any action based on it and, in addition, please delete this e-mail and inform the sender. We cannot be sure that this e-mail or its attachments are free from viruses. In keeping with good computing practice, please ensure that you take adequate steps to check for any viruses. Before replying or sending any e-mail to us, please consider that the Internet is inherently insecure and is an inappropriate medium for certain kinds of information. We reserve the right to access and read all e-mails and attachments entering or leaving our system.

Access to e-mails within Microsoft Outlook from a desktop or laptop shall always be through the Virtual Private Network (VPN) installed on company desktops and laptops.

Access to e-mails within Microsoft Outlook from a tablet or smart phone shall only be where finger print log-in is enabled.

13. Training Personal Data

Callsafe Services Limited will retain personal details of trainees for training record and analysis purposes, as follows:

- ❒ Name of individual trainees
- ❒ National Insurance Number of trainee (Required for specific identification where trainees may have the same name. This is required by the Safety Pass Alliance)
- ❒ Other individual identification numbers, e.g. employee number if required by the trainee's employer
- ❒ The trainee's employer name and address, training organiser name, e-mail address and telephone numbers, and order and payment details
- ❒ Trainee feed-back forms
- ❒ Course assessments / examinations papers and results
- ❒ Course certificates
- ❒ Any other information relating to individual trainee's training

All of this data shall be stored electronically within the Callsafe Services Limited a secure cloud computing service, having scanned hard copies and shredded the hard copies.

All of the above data will be made available to the trainees' employers for their training and qualifications records.

This data will also be made available to third-party accreditation bodies for their training accreditation purposes and the production of certificates and cards. These bodies are:

- Safety Pass Alliance (SPA)
- Institution of Occupational Safety and Health (IOSH)
- Association for Project Safety (APS)
- UK Asbestos Training Association Limited (UKATA)
- McDonald's Restaurants (For training records and issue of McDonald's Passports)

The permission from trainees for Callsafe Services Limited to retain and pass onto authorised persons their personal data, described above, shall be obtained from them during course registration, as follows:

Non-Accredited Training

GDPR – By signing the Attendance Register you are agreeing to Callsafe Services Limited retaining your personal data for training record purposes only (Attendance register including your name and contact details, course results, certificates and course feed-backs). This data will only be provided to your employer.

Accredited Training

GDPR – By signing the Attendance Register you are agreeing to Callsafe Services Limited retaining your personal data and passing it onto *insert accreditation body, e.g. the Association for Project Safety* for training record purposes only (Attendance register including your name and contact details, course results, certificates and course feed-backs). This data will also be provided to your employer.

Some accreditation bodies, such as the Safety Pass Alliance (SPA) Limited have their own Privacy Notice, that requires similar authorisation by the individual trainees, which will used instead of the notice above.

14. Disciplinary Action

Violation of this policy by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.