CITRUS GROUP

DATA PROTECTION POLICY

VERSION 7
MAY 2023

CITRUS TRAINING | ALTITUDE SAFETY | BBE TRAINING | bookmycourse.co.uk

Data Protection Policy (Compliant with the GDPR)

This policy outlines the Data Protection Policy for Citrus Group and has been updated to meet the requirements of the General Data Protection Regulations (GDPR) and The Data Protection Bill. It is a requirement for all staff working within Citrus Group to comply with this policy.

Key individuals involved in developing the process and policy

Name	Job Title
Nadine Searle	HR Business Partner

Circulated to the following individuals for comments and approval

Name	Job Title
Wayne Taylor	Managing Director
Charlotte Walker	Director
Geoff Walden	Head of Group Operations & Services

Draft and Issue Information

Subject/Topic	Comments
Date of Draft	14/12/17
Date sent for review and approval	14/12/17
Date approved	09/05/18
Approved by	WT, CW, GW
Date of Issue	May 2018
Date for Review	May 2024
Where documents available and stored	Z:\GDPR\Policies and Privacy Notices\Data Protection Policy (GDPR).docx
Scope of Policy	All staff
Feedback on implementation and content to	Nadine Searle, Group HRBP

Version Control and Summary of Changes

Version Number	Date	Comments (description of change and/or amendments)
1.0	4 January 2017	Original Data Protection Policy as per The Data Protection Act 1988
2.0	1 May 2018	Reviewed and updated to meet the requirements of the GDPR (effective 25/5/18) and The Data Protection Bill
3.0	3 May 2019	Reviewed – no updates required
4.0	4 May 2020	Reviewed – no updates required
5.0	3rd May 2021	Reviewed – no updates required
6.0	2nd March 2022	Data classification added
7.0	20th May 2022	Reviewed – no updates required

8.0	19 May 2023	Reviewed – No Updates

CONTENTS

1.0: Introduction

1.1 The General Data Protection Regulation (2016/679 EU) (GDPR) came into force on 25 May 2018 and has been supplemented by The Data Protection Bill in the UK. This new legislation repeals and replaces The Data Protection Act 1988 and this policy supersedes any previous Data Protection Policy issued by any of the companies within Citrus Group.

1.2 Citrus Group is committed to being transparent about how it collects and uses personal data and to meeting its data protection obligations. This policy sets out the Company's commitment to data protection, and individual rights and obligations in relation to personal data.

1.3 This policy applies to all the personal data collected and processed by the Company, including the personal data of customers, clients, delegates, suppliers, job applicants, employees, workers, contractors, volunteers, interns, apprentices, and former employees.

1.4 The Company has appointed the IT & Facilities Manager as the person with responsibility for data protection compliance within the Company. He/she can be contacted at GDPR.compliance@citrustraining.co.uk. Questions about this policy, or requests for further information, should be directed to him/her.

2.0: Definitions that Apply to this Policy

The Company (Citrus Group)	This refers to all companies that make up the Citrus Group of companies, namely Altitude Safety Ltd, BBE Ltd, BookMyCourse Ltd, HR Training & Development Ltd and Citrus Training Ltd.
Data Subject	This refers to an individual who is the subject of personal data.
Data Controller	This refers to a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Processor	This refers to any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Recipient	This refers to any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller.
Third Party	This refers to any person other than, the data subject, the data controller, or any data processor or other person authorised to process data for the data controller or processor.
Personal data	This means any information relating to an identified or identifiable natural person ('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.
Processing	This is any use that is made of personal data, including collecting, storing, amending, disclosing or destroying it.
Special categories of personal data	This means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, and biometric data.
Criminal records data	This means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

3.0: Data Protection Principles

3.1 The Company processes personal data in accordance with the following data protection principles:

- The Company processes personal data lawfully, fairly and in a transparent manner.
- The Company collects personal data only for specified, explicit and legitimate purposes.
- The Company processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The Company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The Company keeps personal data only for the period necessary for processing.
- The Company adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.
- The Company tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.
- Where the Company processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.
- The Company will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.
- The Company keeps a record of its processing activities in respect of personal data in accordance with the requirements of the GDPR.

4.0: Individual Rights

4.1 As a data subject, individuals have a number of rights in relation to their personal data.

4.2 *Subject access requests*

4.2.1 Individuals have the right to make a subject access request. If an individual makes a subject access request, the Company will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored and how that period is decided;
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the Company has failed to comply with his/her data protection rights; and
- whether or not the Company carries out automated decision-making and the logic involved in any such decision-making.

4.2.2 The Company will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

4.2.3 If the individual wants additional copies, the Company will charge a fee, which will be based on the administrative cost to the Company of providing the additional copies.

4.2.4 To make a subject access request, the individual should send the request to GDPR.compliance@citrustraining.co.uk. In some cases, the Company may need to ask for proof of identification before the request can be processed. The Company will inform the individual if it needs to verify his/her identity and the documents it requires.

4.2.5 The Company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Company processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Company will write to the individual within one month of receiving the original request to tell him/her if this is the case.

4.2.6 If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, the Company can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Company has already responded. If an individual submits a request that is unfounded or excessive, the Company will notify him/her that this is the case and whether or not it will respond to it.

4.3 *Other rights*

4.3.1 Individuals have a number of other rights in relation to their personal data. They can require the Company to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the Company's legitimate grounds for processing data (where the Company relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Company's legitimate grounds for processing data.

4.3.2 To ask the Company to take any of these steps, the individual should send the request to GDPR.compliance@citrustraining.co.uk.

5.0: Data Security

5.1 The Company takes the security of personal data seriously. The Company has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

5.2 Where the Company engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

6.0: Privacy Impact Assessments

6.1 Some of the processing that the Company carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the Company will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

7.0: Data Breaches

7.1 If the Company discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery.

7.2 The Company will record all data breaches regardless of their effect. A copy of the breach notification process is available at Z:\GDPR\Breach Notification Process.xlsx

7.3 If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

8.0: International Data Transfers

8.1 The Company will not transfer personal data to countries outside the EEA.

9.0: Individual Responsibilities

9.1 Individuals are responsible for helping the Company keep their personal data up to date. Individuals should let the Company know if data provided to the Company changes, for example if an individual moves to a new house or changes his/her bank details.

9.2 Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the Company relies on individuals to help meet its data protection obligations to staff and to customers and clients.

9.3 Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

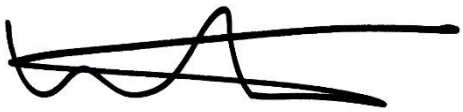
9.4 Further details about the Company's security procedures can be found in the IT & Security policy, which is available in section 8 of the Employee Handbook.

9.5 Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure, as detailed in the Employee Handbook. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

10.0: Training

10.1 The Company will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

10.2 Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Signed: 

Wayne Taylor
(Managing Director)