# Alert Training UK Ltd

# GDPR Statement

Contents



## 1. Introduction

Alert Training UK Ltd is registered as a Data Controller under the Data Protection Act 1998 and, from 25 May 2018, under the General Data Protection Regulation (GDPR). Registration is renewed annually.

Data Protection Register Registration Number: Z3334988

Data Controller: Alert Training UK Ltd

Address: 56 High Street, Salisbury, Wiltshire, SP12PF

Further details regarding the registration are available via www.ico.org.uk

Alert Training UK Ltd (The Company) needs to keep certain information about employees, learners and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully. To do this, we must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 and, from 25 May 2018, the General Data Protection Regulation (hereafter referred to as the GDPR).

## 2. The Types of Information Covered by Data Protection Legislation Personal Data

Data Protection legislation applies to personal information relating to a living person. It applies not only to computerised or automated personal data, but also to information held in manual filing systems. Included are such items of information as name, date of birth, contact details, title and gender, but also less obviously personal data such as IP addresses, online identifiers and pseudonyms. The legislation also applies to any records where an individual can be directly or indirectly identified from the information present, even where the name is not included. Sensitive Personal Data also known as Special Category Data, this is the subset of Personal Data where the data items are especially sensitive and need a greater level of protection. These include ethnic origin, health data, religion and sexual orientation.

## 3. Alert Training UK's Responsibilities

Under the Data Protection Act and the GDPR, the data protection principles set out the main responsibilities for the company. These require that data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

d) accurate and, where necessary, kept up to date

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 are processed

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing. Alert Training UK must have a lawful basis for processing any personal information and must make this clear in the privacy notice.

## 4. **The Data Controller and the Data Processors**

Alert Training UK Ltd is the Data Controller under the Act and the Managing Director is therefore ultimately responsible for compliance with the statutory legislative requirements.

The Managing Director takes this overall responsibility for compliance and delegates the overseeing of the implementation, giving advice and dealing with the subject access requests to the Compliance Manager. There are also designated Data Processors within the Company who deal with data on a day-to-day basis relating primarily to learner data and staff data matters. The majority of subject access requests will be dealt with through individual Data processors. The Managing Director is the Data Officer for all data issues relating to staff and is the Data Protection Officer.

## 5. The Rights of Individuals Whose Data is Processed by Alert Training UK Ltd

1. The right to be informed

Alert Training UK is obliged to provide fair processing information and does so through its privacy notices at enrolment.

2. The right of access

Individuals have the right to access their personal data, and this access will be provided as quickly as possible – we are legally bound to provide the data within one calendar month. This data will usually be provided free of charge.

3. The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

4. The right to erasure

An individual is entitled to request the deletion or removal of personal data where there is no compelling reason for its continued processing. It should be noted that Alert Training UK is legally obliged to process and retain much of the personal information it holds.

5. The right to restrict processing
Individuals have the right to restrict Alert Training UK from processing certain aspects of their personal data if one of the following circumstances applies:
- The accuracy of the data is contested
- The individual objects to the processing of the data in principle
- The Company's processing of the data is unlawful
- The Company wishes to delete the data, but the individual has need of the data for legal purposes

6. The right to data portability
Individuals may request an electronic copy of their personal data to use for their own purposes. Alert Training UK will make every effort to provide the data in a form that is useable and acceptable to the individual, and this will be done without charge.

7. The right to object
Individuals have the right to object to:
- Direct marketing – Alert Training UK Ltd will stop processing for this purpose on receipt of an objection.
- Data processing for research or statistics – Alert Training UK Ltd will engage with the individual to come to an agreement within the law.
- Data processing in the Company's legitimate interests – Alert Training UK Ltd will engage with the individual to come to an agreement within the law.

8. Rights in relation to automated decision making and profiling
Individuals who have any concerns about automated or computerised decision making should refer them to the Data Controller.

**Responsibilities of Staff**
- To ensure that any information that they provide to the Company in connection with their employment is accurate and up to date.
- To inform the Company of any change to information which they have provided.
- To check the information that the Company will send out from time to time, giving details of information kept and processed about staff, and change any information that is incorrect or incomplete.
- To comply with the guidelines for data collection and processing when, as part of their responsibilities, they collect information about other people, (for example learners' course work, opinions about ability, references to other academic institutions, or details of personal circumstances).

**Responsibilities of Learners**
- To ensure that all personal data provided to Alert Training UK Ltd is accurate and up to date.
- To ensure that changes of address, next of kin etc. are notified to Alert Training UK Ltd.
- To ensure that they keep their passwords to e-portfolios and online systems secret and secure.
- To report to Alert Training UK Ltd if they suspect their account security has been breached.

**Data Security**
In order to ensure the security of personal information, Alert Training UK Ltd will:
- Maintain security guarding the Company's network and systems.
- Prevent users from storing data on local drives of non-portable IT hardware
- Ensure staff maintain safety of their passwords
- Wipe hard drives and memory of all equipment before disposal in order to ensure the security of personal information, staff are required to:
- Lock their IT device when leaving their PC/Laptop unattended
- Avoid opening emails on a projected screen – private information may be displayed to anyone else in the room or even outside via the window

• When emailing personal data, password protect in an attachment and phone the password through to a trusted number
• Refer all requests for disclosure of personal data from external sources to be dealt with via the central register
• Contact the Director if in doubt about any data security matter
• Only use Company approved cloud-based repositories (OneDrive for Business and SharePoint Online & dropbox for business, accessed via their work email address)
• Check the email addresses of intended recipients before sending any email, as email programs often incorrectly predict email addresses you are typing in
• Consider using BCC to restrict visibility of other recipients' addresses when emailing to a group of recipients (especially where there are large numbers of recipients or some external addresses). Where the Company process data on behalf of other organisations, e.g. conducting external DBS checks, it will comply to ICO requirements.

Loss or Theft of Personal Information All incidences of loss or theft of personal information must be reported immediately to the Company's Data Controller (the Managing Director). A data or IT security incident relating to breaches of security and/or confidentiality could range from computer users sharing passwords, to the loss or theft of personal information either inside or outside the Company. A security incident is any event that has resulted or could result in:
• The disclosure of personal/sensitive/confidential information to any unauthorised person.
• The integrity of the system or data being put at risk.
• Threat to personal safety or privacy.
• Legal obligation or penalty. All incidents must be reported to the Data Controller in the first instance, as soon as possible after the event. In the case of a potential breach, the Data Controller will instigate an investigation into the incident and will decide whether it needs to be reported to any regulatory bodies, in particular the Information Commissioner's Office (ICO). If a breach has occurred, the ICO will be informed within 72 hours of the incident, and if appropriate all data subjects concerned will also be contacted and informed. If possible, the offending paperwork, data or communication will be retrieved as soon as possible. The Data Controller will retain a central register of all such incidents occurring within the Company, whether or not they resulted in a breach. The following is a list of examples of breaches of security and breaches of confidentiality. It is neither exclusive nor exhaustive and should be used as a guide only. If there is any doubt as to what constitutes an incident, you should consult the Data Controller who will decide what action should be taken.
Examples of a breach of confidentiality:
• Finding confidential/personal information either in hard copy or on a portable media device outside company premises.
• Finding any records about a staff member, student, or applicant in any location outside the Company premises.
• Passing information to unauthorised people either verbally, in writing or electronically. Subject Consent In many cases, the Company can only process personal data with the consent of the Individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the Company processing some specified classes of personal data is a condition of acceptance of a learner onto any course, and a condition of employment for staff. This includes information about previous unspent criminal convictions (all convictions in the case of staff). Therefore, all prospective staff and learners will be asked to sign a Consent to Process form, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

**Conclusion**
Compliance with the 1998 Data Protection Act, and from 25th May 2018 the GDPR, is the responsibility of all members of Alert Training UK Ltd. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken or even a criminal prosecution. Any questions or concerns about the interpretation or operation of the policy should be taken up with the Managing Director.

If you require any further information on the Data Protection Act 1998, the superseding General Data Protection Regulation, or how any aspect of either is implemented at Alert Training UK Ltd, please make contact with: Damon Saddler: damon.saddler@alerttraining.co.uk, 01722332212

Useful Links:
Information Commissioner: www.ico.gov.uk
ICO GDPR Resources: https://ico.org.uk/for-organisations/guide-to-the-general-dataprotection-regulation-gdpr/
JISC GDPR Resources: https://www.jisc.ac.uk/gdpr