# Optimal Risk Training

# Data Protection Policy (Personal Information)

| | |
|---|---|
| Created by: | Compliance Lead |
| Document owner: | Managing Director |
| Approved by: | Center Manager |
| Confidentiality level: | Uncontrolled – may be disclosed externally, in full |

## Change history

| Date | Version | Created by | Description of change |
|---|---|---|---|
| Jan 25 | 0.1 | Compliance Lead | Rewrite and Renewal of ORT QMS |
| | | | |

# Table of contents

# 1. Introduction

Optimal Risk Training Limited, part of the Optimal Risk Group may have to collect and use information about people with whom we provide our services. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the UK General Data Protection Regulation (GDPR) and Data Protection Law.

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our service delivery functions (delivering training services to learners). It also covers our response to data breach and other rights under the GDPR from a client or client related individual.

This policy applies to the personal data of learners, clients, client employees, clients of clients or any person who may feel affected by our operational delivery of training services. These people are referred to in this policy as relevant individuals.

## 1.1. Definitions

Definitions are taken directly from the UK GDPR or Data Protection Act 2018.

“Personal data” is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person’s name, identification number, location, online identifier. It can also include pseudonymised data.

“Special categories of personal data” is data which relates to an individual’s health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for identification purposes).

“Criminal offence data” is data which relates to an individual’s criminal convictions and offences.

“Data processing” is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

‘Personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

## 1.2. Data Protection Principles

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

- processing will be fair, lawful and transparent
- data be collected for specific, explicit, and legitimate purposes
- data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
- data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
- data is not kept for longer than is necessary for its given purpose
- data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- we will comply with the relevant GDPR procedures for international transferring of personal data

To ensure we demonstrate compliance with the data protection principles, we will maintain documented records sufficient to demonstrate that we complied with our obligations.

## 1.3. Types Of Personal Data Held

We keep several categories of personal data relating to our clients so that we may carry out effective and efficient operational processes to deliver our contractual obligations and fulfil our legal obligations.

Specifically, we may hold the following types of data:

- contact details such as name, address, phone numbers
- information gathered during the negotiation and onboarding process such as that published online by the client or public registers (companies house, ICO etc)
- emergency contact information, such as medical or health information
- course specific and or learning information, such as additional requirements
- banking details so we may exchange payments via banking systems

## 1.4. Lawful Bases Of Processing

We acknowledge that processing may only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity. See separate Records of Data Processing Activities.

- Contract - All personal data, where relevant, is necessary either to determine if we may enter into a contract, or in the performance of a contract with the client.
- Legal Obligation - Information regarding who we have financial arrangements with and what services we have delivered, including any health and safety considerations is necessary for compliance with our legal obligations.

- Vital Interests - Information concerning emergency contact information is necessary protect the vital interests of the data subject or others.
- Consent - Where no other lawful basis applies, we may seek to rely on the individual's consent in order to process data. Consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Individual's will be given clear information concerning the desired processing activity, informed of the consequences of their consent being withheld and of their clear right to withdraw consent at any time.

## 2. Responsibilities

To protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies relating to data protection.

We have also appointed employees with responsibility for reviewing and auditing our data protection systems.

### 2.1. Data Protection Compliance Lead

Our appointed Data Protection Compliance Lead is responsible for compliance in respect of our data protection activities:

Stuart Crighton

Stuart.crighton@optimalrisk.com

## 3. Data Subject Rights

Relevant individuals have the following rights in relation to their personal data that we hold:

- the right to be informed about the data we hold on them and what we do with it;
- the right of access to the data we hold on them. More information on this can be found in the section headed "Access to Data" below;
- the right for any inaccuracies in the data we hold on them, however they come to light, to be corrected. This is also known as 'rectification';
- the right to have data deleted in certain circumstances. This is also known as 'erasure';
- the right to restrict the processing of the data;
- the right to transfer the data we hold on them to another party. This is also known as 'portability';
- the right to object to the inclusion of any information;
- the right to regulate any automated decision-making and profiling of personal data.

## 4. Access To Data

As stated above, Data Subject Rights individuals have a right to access the personal data that we hold on them. To exercise this right, individuals may make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide

that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made by us to fulfil a request unless the request is manifestly unfounded or excessive, or unless a request is made for duplicate copies to be provided to the individual making the request or to a third party acting on the individual's behalf. In these circumstances, a reasonable charge may be applied.

## 5. Data Disclosures

The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- learners undergoing regulated course – to satisfy the awarding body that the learner has completed the requested learning objectives
- disabled individuals - whether any reasonable adjustments are required;
- individuals' health data - to comply with health and safety or occupational health obligations;
- to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.

## 6. Data Security

All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so they are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up (we use Egnyte, Bright HR, Bright SAFE, O635 and Xero for this purpose). If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary.

- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
- ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

## 7. Third Party Processing

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Company's commitment to protecting data.

Senior Leaders, Employees and or Contractors, must not engage a service provider that will process our personal data without awareness of the Data Protection Compliance Lead.

### 7.1. International Data Transfers

The Company does not routinely transfer personal data to any recipients outside of the EEA.

## 8. Requirement To Notify Breaches

All personal data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required and or deemed appropriate by us, we will inform the individual whose data was subject to breach.

## 9. Training

New employees must read and confirm understanding of our policies on data protection as part of their induction.

We utilise a suite of GDPR and Data Protection online tutorials that we require all staff to complete at least annually. Role dependant, staff conduct more additional training commensurate with their levels of exposure to personal data or potential to receive Subject Access Requests.

All employees receive training covering information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data protection lead for the Company are trained appropriately in their roles under the GDPR.

All employees who need to use the computer systems are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

## 10.Records

The Company keeps records of its processing activities including the purpose for the processing and retention periods. These records will be kept up to date so that they reflect current processing activities. See separate Records of Data Processing Activities.