GDPR Compliance Policy

Rev 3.1

Dated 05 June 2022

ICO Number: Z2917146

Contents

1 What is the GDPR

The EU General Data Protection Regulation ("GDPR") came into force across the European Union on 25th May 2018 and brings with it the most significant changes to data protection law. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

The broader use of technology, new definitions of what constitutes personal data. The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

2 Who does this policy adhere to:

- All staff of SquareOne Training
- All contractors, suppliers and other people working on behalf of SquareOne Training

3 Data protection risks

This policy helps to protect SquareOne Training Ltd from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputation.**

4 SquareOne Training's Commitment

SquareOne Training are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR and Data Protection.

SquareOne are dedicated to safeguarding the personal information we hold and developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for regulations. To be compliant we have summarised in this statement and included the development and implementation of new data protection roles, policies, procedures, controls and measures that will ensure maximum and ongoing compliance.

We will consistently monitor all aspects of our business processes by doing the following:

Information Audit - carrying out a company information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if, and to whom it is disclosed.

Personal data of the individual

An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important that we establish whether the information requested falls within the definition of personal data.

We will update our Policies & Procedures - revising data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including:

- Data Protection – our main policy and procedure document for data protection has been reviewed to meet the standards and requirements of the GDPR and is constantly monitored.

- Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities.

- Data Retention & Erasure – we are constantly reviewing our retention policy and schedule to ensure that we meet the 'data minimisation' and 'storage limitation' principles and that personal information is stored, archived and destroyed compliantly and ethically.

- We have dedicated erasure procedures in place and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.

- Subject Access Request (SAR) – Individuals have the right to access information kept about them by SquareOne Training, including but not limited to: personnel files, sickness records, disciplinary, training records, appraisal or performance review notes, emails in which the employee is the focus of the email and documents that are about the individual. The GDPR does not specify how to make a valid request. Therefore, an individual can make a subject access request to us verbally/telephone or in writing. We also accept requests on Social Media. If the request is made verbally – then this should still be logged.

- We will have one month to respond to the request. This can be extended further by two months if the request is complex, or we have received a number of requests from the individual. SquareOne must let the individual know within one month of receiving their request and explain why the extension is necessary.

- There will be no charge fee to deal with this request if standard request, but may be a small admin fee may be applied if it is found to be manifestly unfounded or excessive.

- The GDPR information we provide will be concise, transparent, intelligible and easily accessible to read giving clear and plain language.

- Asking for ID: If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their request.

- Data referring to other people: Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual. The Data Protection Act says that you do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if: the other individual has consented to the disclosure; or it is reasonable to comply with the request without that individual's consent.

- In determining whether it is reasonable to disclose the information, SquareOne Training must take into account all of the relevant circumstances, including: the type of information that we would disclose; any duty of confidentiality we owe to the other individual; any steps we have taken to seek consent from the other individual; whether the other individual is capable of giving consent; and any express refusal of consent by the other individual.

- Data Breaches – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time in line with ICO guidance.

- Louise Papapavlou is responsible for dealing with data subject access requests – if not available then please contact the Managing Director.

5 Privacy Notice/Policy

SquareOne Training will comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.

6 Obtaining Consent

We have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing and agreeing to this. We must give clear, defined ways to consent to us processing their information. We have

developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, and an easy to see and access way to withdraw consent at any time.

Only people that have consented to our mailings, will be contacted. These are captured on our website, and post course feedback opt in processes.

Anyone wishing to be removed from lists or opt out – then this will be actioned immediately and any subsequent data stored will be destroyed.

7 Direct Marketing

An individual, even though opted in can ask us to stop processing their personal data for direct marketing at any time. This includes any profiling of data that is related to direct marketing. This is an absolute right and there are no exemptions or grounds for any staff at SquareOne Training to question or refuse.

If we hold data on a learner and they ask not to be contacted in the future – then we will unsubscribe them from all mailing lists - SquareOne will therefore stop processing the individual's data for this purpose.

If an individual is happy for us to keep their data for analysis and support we can do this – without the need to erase the individual's personal learning plan, and in most cases it will be preferable to suppress their details if they haven't asked for them to be destroyed. Suppression involves retaining just enough information about them to ensure that their preference not to receive direct marketing is respected in future, unless they ask for their data to be erased.

8 Employees' Obligations Regarding Personal Information

Employees whom handle person data must ensure that:

- The information is accurate and up to date.
- The use of the information is necessary for a relevant purpose and that it is not kept longer than necessary.
- The information is secure.
- An employee must not take any personal information away from SquareOne Training premises without the prior consent of the Managing Director. Exceptional circumstances would be to hand deliver Government Funding Documents straight to the Liverpool City Region or Chester University for example. If these are to be delivered, then these are not to be taken to any other location beforehand.
- No Datasticks are used within the business.
- All data held is stored in a central SharePoint Team Site and not individual My Documents/OneDrive areas.
- Locks files in a secure cabinet.
- Passwords must contain a minimum of 8 characters and contain numbers and special characters, upper and lower combination. No family names or pets can be used. Refrain from using Dictionary words. Around 8-10 character length is acceptable.
- Use password-protected Spreadsheets/Documents. These must be different from your normal passwords.
- Use password-protected and encrypted software for the transmission and receipt of emails.
- Any paperwork must be disposed of by shredding.
- Any data to be destroyed must be permanently removed from the Network Server and SharePoint. All Inbox, Sent Items and Deleted Items must also be cleared.
- Where an individual is required to disclose personal data, they must ensure first that there are adequate safeguards for the protection of data - this includes all other countries outside of the UK.

If an employee is in any doubt about what about what they may or may not do with personal information, they should seek advice from Louise Papapavlou. More information can be found in the Government Guidelines.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

9 Working Online

Working via online tools (for example Adobe Connect, WebEx, Zoom or Teams) – no screen shots can be taken without the permission of the attendees for a photo capture. The only time we will capture the data is the names for proof of attendance.

Working via online tools (for example Adobe Connect, WebEx, Zoom or Teams) – No recording of training, meetings or events can be captured without the written permission of the attendees and the management of SquareOne.

Any agreed capture on this event must be held in a secure area for example our company Team Site and not stored in personal files such as OneDrive or My Documents. This data must then be deleted securely and only retained in accordance with the retention policies.

If it is agreed this is to be shared, this must be put in writing and all parties need to give consent and data shared must be sent via a secure portal which is password protected by all parties. Sharing must be done via an encrypted method for viewing and must be sent securely and locked for no forwarding of links.

No videos can be sent via normal email or saved onto a USB.

All Data Protection/Confidentially/Governance rights apply to online events.

10 Funding

When working with funded bodies such as Dfe, European Social Funding or British Computer Society (Exams). It may be necessary to collect information from the learners that is confidential and sensitive. Below are the terms set out by Liverpool City Region.

10.1 Funding/Exams

It may be necessary to obtain documents on individuals to carry out checks on Right to Work in the United Kingdom (UK) so that learners can be put forward onto a training programme(s). This applies also to learners that do our official British Computer Society Exams (BCS). Below is the guidelines that we must refer to as part of this process. This is an example of the Liverpool City Region Funding pot for Priority and Be More Training.

Liverpool City Region Combined Authority – Priority Training - Right to Live & Work in the UK Evidence

Q&A

Q1. Why do we need to obtain RTL&W evidence?

The European Social Fund National Eligibility Rules (point 5.12) states that '*To be eligible for support from the ESF an individual must be:*

- *legally resident in the UK*
- *able to take paid employment in a European Union member state'*

The European Social Fund – Data Evidence Guidance (point 2.2) states that *'Proof must be obtained to evidence that:*

- *The participant is legally able to reside in the UK (and work in the UK) during the period of ESF support'*

We have been advised by colleagues working on other ESF Programmes that ESF Auditors will ask us to provide evidence of RTL&W and if we are unable to provide this then we will not be eligible for ESF Support (i.e. we risk funding clawback).

Q2. How do we obtain RTL&W evidence?

The preferred evidence is one document from the Employer's Right to Work Checklist. This can either be obtained directly from the employer (who have a legal responsibility to undertake these checks and retain copies of these documents) OR you can request that the participants bring their documents with them to the training where you will take a copy.

Q3. What if we do not have access to a photocopier?

"Where there is no access to a photocopier then you can use your mobile phone to take a picture and then delete the picture once it has been uploaded and stored to your internal filing system. "

The above is guidance is from the funding – however SquareOne must only use this method if an emergency. The phone that takes the picture must be an authorised SquareOne phone that is locked with face recognition/password encrypted as documented and listed in the Cyber Security Policy.

Alternatively, you can request that the employer or participant sends you a picture of this evidence.

Q4. Why is it the responsibility of the Training Provider to gather this evidence?

The ESF Data Evidence Guidance (point 2.3) states that this evidence should be obtained as part of the enrolment process – this approach is recommended as best practice by the ESF Managing Authority. As the Training provider, you are contracted by the Liverpool City Region Combined Authority to undertake participant enrolment procedures and are therefore responsible for gathering RTL&W evidence as part of the participant eligibility checks.

You do not need to retain a copy of this evidence once you have submitted it to LCRCA.

Q5. What if we are delivering online only training?

For providers delivering online only courses, you will need to ask either the employer or the participant to email you a picture/copy of their RTL&W evidence.

Q6. What happens if a participant is unable to provide suitable evidence?

If a participant is unable to provide suitable evidence or a reason to apply an exception, this means that no ESF support is payable.

RTL&W evidence must be obtained before a participant engages in training to prevent Providers delivering training that cannot be claimed for.

If a participant does not have any of the documents listed in the preferred evidence, please contact the Compliance Team for further advice.

Q7. What about participants who are Self Employed?

The same evidence criteria applies only this will need to be provided directly by the Self-Employed participant.

Q8. Will there be GDPR implications to this?

Collecting the RTL&W evidence does have GDPR implications as the information is the personal data of the participants. This additional processing is permitted, however, as it is necessary in order for the programme to be delivered.

All processing is covered under 'Public Task' condition on the basis that we are a public authority performing a specific task in the public interest. Further information about this can be found at The Information Commissioner's Office.

Q9. What should we do about RTL&W evidence for training that was delivered prior to this change coming into effect on 27th May 2022?

For claims that you have not yet submitted for payment we request that you contact the employers/participants to retrospectively obtain this information from them. You can provide them with this Q&A document which explains why it is necessary.

For claims that have been submitted but not yet paid, we will need you to gather this evidence retrospectively and submit to us as soon as possible. We have been advised we cannot pay any claims until we receive this.

For claims that have already been submitted and paid, the compliance team will undertake a remediation task to obtain the necessary evidence.

Summary of the evidence format and SquareOne's Responsibility

For funding where evidence is required on the check for Right to Work – we can take the following forms of evidence:

- Full passport (not EU Member State)
- Passport either endorsed indefinite leave to remain – proceed (settled status) or includes work or residency permits or visa stamps (unexpired) and all related conditions met
- Some non-EEA nationals have an Identity Card issued by the Home Office in pace of a visa, confirming the individual's right to stay, work or study in the UK – these cards are acceptable
- Letter from the UK Immigration and Nationality Directorate granting indefinite leave to remain (settled status)
- Birth / adoption certificate (EU Member State)
- Residency permits for foreign nationals - usually in a passport
- Biometric residency permits

This information is to be kept in a secure location at all times and transfer of this data must be sent via a secure site such as Egress.

When asking for the information to be sent from the learner it is imperative that this data is sent in a secure way. SquareOne to send a document showing how to password protect this data before transfer from the learner. This must be password protected using 8 characters.

Evidence to only be sent to the Funding body via a secure means for example Egress when making a claim for the training.

Once training is completed and the paperwork approved from the funding body, any documents such as passport evidence must be deleted in a secure manner immediately. For the funding paperwork apart from the right to work evidence must be retained in accordance to the funding retention policies.

The Company will review employees' personnel files on a regular basis to ensure they do not contain a backlog of out-of-date or irrelevant information and to check there is a sound business reason requiring information to continue to be held.

Accurate and, where necessary, kept up to date. If your personal information changes, for example you change address or you get married and change your surname, you must inform your line manager as soon as practicable so that the Company's records can be updated. The Company cannot be responsible for any such errors unless the employee has notified the Company of the relevant change.

10.2 Not kept for longer than is necessary

SquareOne will keep personnel files for no longer than six years after an employee has left the Company's employment.

Different categories of data will be retained for different periods of time, depending on legal, operational and financial requirements. Any data which the Company decides it does not need to hold for a particular period of time will be destroyed. Data relating to unsuccessful job applicants will only be retained for a period of one year.

Processed in accordance with the rights of employees under the Act.

Secure. Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, data. Personnel files are confidential and are stored as such in locked filing cabinets. Only authorised employees have access to these files. For a list of authorised employees, please contact Lisa Johnson. Files will not be removed from their normal place of storage without good reason. Data stored on memory sticks, discs or other removable storage media is kept in locked filing cabinets. Data held on computer is also stored confidentially by means of password protection, encryption, or coding and again only the above

employees have access to that data. The Company has network back-up procedures to ensure that data on computer cannot be accidentally lost or destroyed.

Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection relation to the processing of personal data.

11 Working Remotely

Any employee working remotely must ensure that they do not leave their laptop, other device or any hard copies of records unattended. All laptops should be secured with a password and locked when unattended. They must also take care when observing the information on-screen or printouts, so such information is not viewed by anyone who is not legitimately privy to that information.

12 Processor Agreements

Where we use any third-party to process personal information on our behalf (i.e. Payroll, Web Hosting), every care has been taken to ensure all parties are compliant with the GDPR and are aligned to SquareOne Training's ongoing commitment.

13 Correction of data

SquareOne Training has a system in place that enables employees to check their personal information on a regular basis so that they can correct, delete or update any data. If an individual becomes aware that SquareOne Training holds any inaccurate, irrelevant or out-of-date information about them, they must notify Louise Papapavlou immediately and provide any necessary corrections and/or updates to the information.

14 Monitoring

SquareOne Training may monitor employees and associates by various means including, checking emails, checking evaluations, talking to our customers and monitoring telephone conversations. If this is the case, SquareOne Training will inform the employee/consultant that monitoring is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used. The employee/consultant will usually be entitled to be given any data that has been collected about them. SquareOne Training will not retain such data for any longer than is necessary.

15 Loss of Data

SquareOne Training takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including:

- Restricted access to files and folders, with a view of all personal data is accessed on a 'need to know' basis.
- Encryption software for sending personal data/special personal data.
- Explicit guidance regarding the security marking of such previously mentioned data.
- An appointed CISO (Chief Information Security Officer) to review SquareOne Training compliance and best practice surrounding all aspects of cyber security which is Louise Papapavlou.
- Accountable for reporting any breaches shall be directed to Louise Papapavlou. However, should there be any incident occur where there is loss or potential loss of personal or special personal data, it should be reported to the SquareOne Training Management immediately.

16 Non Compliance

What should we do if we refuse to comply with a request? SquareOne Training must inform the individual without undue delay and within one month of receipt of the request. SquareOne Training should inform the individual about: the reasons you are not taking action; their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce this right through a judicial remedy.

17 Consequences of Non-Compliance

All employees are under an obligation to ensure that they comply with the data protection principles when accessing, using or disposing of personal information. Failure to observe the data protection principles within this document may result in an employee facing disciplinary action and also incurring personal criminal liability.