Data Protection/General Data Protection Regulation (GDPR) Policy

1. Introduction

This policy is applicable to Dimensions Training Solutions Limited trading as QATSL.

We must protect personal and confidential data to both comply with the law and to prove to clients, stakeholders, and customers that we respect their information and/or their privacy. We are committed to all aspects of GDPR and aim to fulfil all our legal obligations, including under the GDPR regulation.

This Policy sets out how QATSL commits to dealing with personal data, including personal and personal sensitive data relating to employees (i.e., personnel files) and claimants.

This Policy will reflect the prevailing laws, regulations, and corporate policies. Up-to-date revisions of this Policy will be available on the company intranet.

1.1 Notification

Organisations who process personal data must register with the Information Commissioner's Office (ICO), the regulator for the DPA. Our notification tells the ICO, and data subjects, about the types of information we process, giving descriptions and reasons for the processing. Our registration reference is ZA275784 (Dimensions Training Solutions Ltd) and is renewed annually.

QATSL may not always be the Data Controller in relation to the processing of personal data and may be a Data Processor on behalf of another organisation. In these circumstances, QATSL will process personal data in line with the wishes of the Data Controller and will at all times aim to comply with the GDPR and otherwise in line with this Policy.

1.2 Data Protection Principles under GDPR

The GDPR outlines the following principles to follow to ensure compliance with the regulation. Personal data must be:

Lawfulness, fairness, and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be 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
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

These principles apply equally to personal data stored physically (for example, in paper files) and electronically.

1.3 Other relevant privacy legislation

- Human Rights Act 1998
- Privacy & Electronic Communications Regulations 2003
- Freedom of Information Act 2000

2. Scope

This Policy applies to all employees and representatives of QATSL, including all contractors, temporary workers, partner organisations and volunteers.

2.1 Supporting Documents

This Policy is supported by more detailed policies, process / procedures, guidelines, schedules and supporting documents. These include but are not limited to those documents listed in Information Security Framework.

3. Responsibilities

Directors	All Directors have a duty to ensure that their directorates comply with legislation affecting the handling of personal data and the supporting regulations and codes.
Data Protection Officer	The Data Protection Officer directly reports to the senior management. The Data Protection Officer is responsible for the implementation and maintenance of this Policy and compliance with it. Employees should direct any questions about data protection in general, this Policy or their obligations under it, to the Data Protection Officer – Data.Protection@dimensionstrainingsolutions.co.uk
All Employees	All employees are accountable to their managers for compliance with this Policy and related policies, procedures, standards, and guidance. All employees have a responsibility to handle personal data in accordance with the principles of the GDPR. Inappropriate processing of personal data may lead to or result in disciplinary action against individual employees.

4. Policy

This Policy requires the appropriate handling of Personal and Sensitive Personal Data in line with the GDPR regulation. This section outlines how we will comply with the data protection Principles outlined in Section 1.2 of this Policy.

4.1 Fair, Lawful and Transparency

QATSL will only process personal or sensitive personal data where specific conditions set out in the GDPR are met. Usually, the data subject's consent to process their personal data is sufficient. Explicit consent is required in order to process sensitive personal data – i.e., informed consent may not be adequate. Where consent is not held another processing condition may apply, however, the Data Protection Officer should be consulted in all cases to ensure compliance with the DPA.

We will tell data subjects what we do with the information we hold or access about them. We will do this by including information in relevant privacy policies, fair processing notices, etc. for example, the following:

- Who the Data Controller is?
- The purpose or purposes for which the data are processed.
- Any other information to make the processing fair, e.g., include details of third parties to whom the data may be disclosed.

For example, we tell users of the QATSL website(s) what we will do with their personal data on our website(s) Privacy Policy. The QATSL employee contract sets out how we will process employees' personal and sensitive personal data.

4.2 Specific Purpose

We will only use personal data for the purposes we have stated in our notification to the ICO and/or in line with any commitment given to a Data Controller (in our role as Data Processor) or the Data Subject directly (e.g., in line with a fair processing notice, privacy Policy, etc.).

If we have access to and use information for one purpose, we must not automatically use this information for another, potentially incompatible, purpose.

Employees who plan to use personal data for a new purpose must contact the Data Protection Officer to discuss whether this processing complies with the GDPR.

4.3 Data Minimisation; Accuracy; & Storage limitation

We will only collect, use, and disclose the minimum amount of information needed in order to carry out any particular task or processing activity.

We will endeavour to keep records about data subjects which we hold or access accurate and up to date.

We will only keep information as long as necessary either to comply with legislation, contractual requirement, industry good practice or our own business requirements. Our Data Retention and Disposal Policy incorporates more details of data retention and secure disposal requirements.

4.4 The rights of Data Subjects

We ensure Data Subjects rights under the GDPR are protected by ensuring a data subject can request:

	The right to be informed encompasses our obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how we use personal data of individuals.
The right to be informed	The information we supply about the processing of personal data must be: • concise, transparent, intelligible, and easily accessible. • written in clear and plain language, particularly if addressed to a child; and • free of charge.
	Individuals have the right to access their personal data and supplementary information. This is known as a Subject Access Request (SAR). The right of access allows individuals to be aware of and verify the lawfulness of the processing. Under the GDPR, individuals will have the right to obtain: • confirmation that their data is being processed; • access to their personal data; and • their supplementary information – this largely corresponds to the information that should be provided in a privacy notice.
The right of access	We must provide a copy of the information free of charge. However, we can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. Information must be provided without delay and at the latest within one month of receipt. We will be able to extend the period of compliance by a further two months where requests are complex or numerous. Certain data may not be disclosed where a relevant exemption applies. We will provide an explanation and a right of appeal in these circumstances. Where we are not the Data Controller, we will forward the request to the Data Controller and otherwise assist in answering the request, where appropriate. For example, where we are a Data Processor, we will provide information we hold on behalf of the Data Controller to the Data

	Controller within a reasonable amount of time to allow them to respond to the request within the statutory time limits. For more information about SAR process, please refer to QATSL Subject Access Request process.
The right to rectification	The GDPR gives individuals the right to have personal data rectified. Personal data can be rectified if it is inaccurate or incomplete. We must respond within one month. This can be extended by two months where the request for rectification is complex. If we cannot take any action in response to a request for rectification, we must explain why to the individual, informing them of their right to complain to the supervisory authority (ICO) and to a judicial remedy.
The right to erasure	QATSL employees may check their own personal information held in the HR Portal so that they can correct, update, or delete any data. If an employee becomes aware that QATSL holds any inaccurate, irrelevant, or out-of-date information about them, they must update this information themselves if they are able to. If they are unable to, they must notify their line manager or the HR department immediately and provide any necessary corrections or updates to the information. The right to erasure is also known as "the right to be forgotten". The broad principle behind this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have a right to have personal data erased and to prevent processing in specific circumstances: • Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed; • When the individual withdraws consent; • When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing; • The personal data was unlawfully processed (i.e., otherwise in breach of the GDPR). • The personal data has to be erased in order to comply with a legal obligation. We can refuse to comply with a request for erasure where the personal data is processed for the following reasons: • to exercise the right of freedom of expression and information; • to comply with a legal obligation for the performance of a public interest task or exercise of official authority; • for public health purposes in the public interest;

- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

Individuals have a right to "block" or suppress processing of personal data.

When processing is restricted, we are permitted to store the personal data to comply with legal or contractual obligations, but not further process it.

We can retain just enough information about the individual to ensure that the restriction is respected in future.

We will be required to restrict the processing of personal data in the following circumstances:

The right to restrict processing

- Where an individual contests the accuracy of the personal data, we should restrict the processing until we have verified the accuracy of the personal data;
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our organisation's legitimate grounds override those of the individual;
- When processing is unlawful, and the individual opposes erasure and requests restriction instead.
- If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

We must inform individuals when we decide to lift a restriction on processing.

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

The right to data portability

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means;

We must provide the personal data in a structured, commonly used, and machine-readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to

use the data.

We must respond without undue delay, and within one month. This can be extended by two months where the request is complex, or we receive a number of requests. We must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

The information must be provided free of charge.

If a data subject believes that the processing of personal information about them is causing, or is likely to cause, substantial and unwarranted damage or distress to them or another person, they may notify the organisation in writing to request QATSL to put a stop to the processing of that information.

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling).
- direct marketing (including profiling); and
- processing for purposes of scientific/ historical research and statistics.

The right to object

We must stop processing the personal data unless:

- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual; or
- the processing is for the establishment, exercise, or defence of legal claims.

We must inform individuals of their right to object "at the point of first communication" and in our privacy notice. This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

The GDPR applies to all automated individual decision-making and profiling. This may be not applicable to QATSL if we are not using any automated means to process personal data.

Rights in relation to automated decision making and profiling

Automated individual decision-making (making a decision solely by automated means without any human involvement)

Profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

We can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.

4.5 Security of personal data

QATSL must take appropriate measures to maintain the security of personal data. We will do this in two ways.

4.5.1 Technical measures

We will maintain an appropriate level of security in our systems when collecting, storing, exchanging, and disposing of data. Our Information Security Policies and Procedures will provide more detail on how exactly this will be achieved.

4.5.2 Organisational measures

We will take specific organisational measures including the following:

4.5.2.1 Data Protection Training & Guidance

QATSL employees are legally and contractually obliged to protect personal data.

QATSL provides training on data protection issues to all employees who handle personal information in the course of their duties at work to help employees to understand their responsibilities. The Information Security Policy sets out when the Information Security & Data Protection training needs to be completed and renewed.

Guidance will be issued regularly via bulletins, newsletters and via the intranet and targeted emails to advise relevant colleagues of specific issues that need to be addressed, useful hints and tips and developments in legislation and company policies.

4.5.2.2 Advice and Support

The Data Protection Officer is responsible for providing an appropriate advice and support service to all directorates. Where appropriate, the Group Chief Information Officer (CIO) and/or external legal experts will be consulted to ensure compliance with all relevant legislation and standards. The advice & support service will include appropriate contract and agreement review.

Any questions about data protection issues should be directed to your line manager in the first instance and escalated as appropriate to the Data Protection Officer – Data.Protection@dimensionstrainingsolutions.co.uk.

4.5.2.3 Privacy / Data Protection Impact Assessments

When we are planning something new, Privacy / Data Protection Impact Assessments (PDPIAs), previously known as Privacy Impact Assessments (PIAs), help us think about any privacy, confidentiality, and information security issues before we start. We should think about the impact new initiatives (e.g., a new project; new or changed Policy; or new information sharing activity) will have on the people whose information we plan to use.

PDPIAs allow us to identify potential risks at the start of a project and develop a plan to manage, mitigate and / or avoid them. This approach can save time and effort later if things do go wrong. PDPIAs help to ensure that we are compliant with the GDPR and other relevant Privacy legislation.

We will seek to conduct a PDPIA for initiatives involving:

- building new IT systems for storing or accessing personal data;
- sharing data with external organisations;
- asking external organisations to share data with us;
- using existing data for a new purpose.

If a project plan changes you should consult the Data Protection Officer to consider whether a new PDPIA may be required.

4.5.2.4 Privacy and Data Protection Forums

Privacy and Data Protection forums will operate in tandem with Information Security forums where appropriate.

4.6 Transfer of personal data outside the European Economic Area

QATSL will not transfer personal or sensitive personal data outside the EEA to countries other than those approved by the European Council unless personal / sensitive personal data is suitably protected. The Data Protection Officer should be consulted for any new initiative which may involve the transfer and / or storage of data outside the UK.

We will only transfer and / or store personal data outside the EEA where:

- we have permission (in cases where it relates to information for which we are the Data Processor).
- we are confident it is adequately protected, i.e., we have assessed and found any risk in transferring the personal data is mitigated; and/or
- we have otherwise made the third party contractually aware of their responsibilities, for example by using EU model clauses.

5. Monitoring

QATSL may monitor employees by various means including, but not limited to, checking emails and internet use. QATSL will retain such data in line with the **Document Retention Policy**.

QATSL reserves the right to use covert monitoring. This may be appropriate where there is, or could potentially be, damage caused to the organisation by the activity being monitored

and where the information cannot be obtained effectively by any non-intrusive means (for example, where an employee is suspected of stealing property belonging to the organisation). Covert monitoring will take place only with the approval of senior management and HR department.

6. Compliance

6.1 Policy Compliance

Breaches of this Policy and / or security incidents can be defined as events that have, or could have resulted in, loss or damage to QATSL assets, or an event that is in breach of QATSL information security policies and procedures.

All QATSL employees, partner agencies and contractors have a responsibility to report security incidents and breaches of this Policy as quickly as possible through the **Whistleblowing Procedures**. This obligation also extends to any external organisation contracted to support or access the Information Systems of QATSL.

Failure to observe the standards set out in this Policy may also be regarded as serious and any breach will be dealt with in line with **Disciplinary Policy**. Action taken against employees under **Disciplinary Procedure** may include dismissal. The **Disciplinary Procedure** is part of the Local Conditions of Employment.

Any user who does not understand the implications of this Policy or how it may apply to them, should seek advice from their immediate line manager or the Data Protection Officer.

Occasionally there may be situations where exceptions to this Policy are required, as full adherence may not be practical, could delay business critical initiatives or could increase costs. These will need to be risk assessed on a case-by-case basis. Where there are justifiable reasons why a particular Policy requirement cannot be implemented, a Policy exemption may be requested in line with the Policy Exemption Process.

6.2 Legal compliance

We have a procedure to ensure that staff know what to do in the event of a security incident, for example an inappropriate disclosure of information leading to a potential breach of the GDPR.

Advice is available to staff, who must report breaches in line with the **Whistleblowing Procedures** and **Information Security Policy** to ensure incidents are reported, managed, and assessed properly and consistently.

Breaches will be notified to the data subject and the Information Commissioner's Office (ICO) where required in line with ICO guidance. This will be determined by the Data Protection Officer.