UK GDPR Compliance Certification Scheme for the Provision of Training and Qualifications Services Criteria

The APM Group Limited

And

The Trust Bridge

This document has been approved by the following

Role	Name	Version Details
CEO APMG	Richard Pharro	Version 1.0 June 2021
CEO TTB	Penny Heyes	
CEO APMG	Richard Pharro	Version 2.0 August 2021
CEO TTB	Penny Heyes	
CEO APMG	Richard Pharro	Version 3.0 October 2021
CEO TTB	Penny Heyes	
CEO APMG	Richard Pharro	Version 4.0 November 2021
CEO TTB	Penny Heyes	
CEO APMG	Richard Pharro	Version 5.0 March 2022
CEO TTB	Penny Heyes	
CEO APMG	Richard Pharro	Version 6.0 April 2022
CEO TTB	Penny Heyes	
CEO APMG	Richard Pharro	Version 6.1 May 2022
CEO TTB	Penny Heyes	
CEO APMG	Richard Pharro	Version 6.2 May 2022
CEO TTB	Penny Heyes	

Copyright & Disclaimer

The APM Group Limited
Sword House, Totteridge Road, High Wycombe, HP13 6DG, England
Email: help@apmg-international.com

Contents

Foreword

APMG certifies organizations to deliver training courses and consultancy services for a broad range of professional certification schemes.

Our long history of certifying organizations worldwide – combined with our rigorous assessment process means that APMG certified organizations are recognized for their commitment to delivering exceptional service.

We have a diverse portfolio of certification schemes including internationally renowned solutions for Project, Business, and Information & Technology (IT) Management, Cyber Security and Public-private partnerships.

Our portfolio of certification schemes – supported by our network of APMG certified organizations makes it easy to find a nearby training course or consultancy service.

APMG's certification schemes, exam and certification services support our goal of enabling organizations and professionals to maximise their effectiveness through use of the latest methodologies and core competencies. Successful candidates can also share their success with a digital badge - a dynamic representation of their certification for use on social media and online communications.

The Ethics and Standards Board is responsible for ensuring that The APM Group adheres to good governance standards and works ethically, representing the interests of all our stakeholders. If, as a stakeholder, you would like to contact the Chair of the Board, to raise a particular issue or concern, please send an email to them at chair-ethicsboard@apmgroupltd.com and the chair will respond to your enquiry as soon as possible. This email will be treated as confidential and will not be seen by internal APM Group staff.

The Trust Bridge™ offers organisations a unique combination of expertise and independently accredited training and education, designed to ensure that we deliver trusted, compliant services to our customers, in the light of UK GDPR, PECR, CCPA, e-privacy laws and global data protection regulations. Legal, technical, and practical management experience ensures we can offer a complete service to our clients.

We are a team of highly qualified specialists who guide organisations through a step-by-step alignment process to ensure personal data management is in line with this data privacy ecosystem within which we must all operate.

Introduction

This Certification Scheme has been drawn up with the objective of promoting confidence in training companies who process personal data. Certified training companies will be provided with a digital badge to show their processing activities, in relation to their training and qualifications services, are compliant with the certification scheme requirements, allowing data subjects to make an informed choice when they are selecting a training company and can be confident that their personal data will be processed in accordance with UK GDPR. This also helps training companies to differentiate themselves from other training companies offering similar courses. APMG as a Certification Body, in partnership with The Trust Bridge, will assess organisations on their compliance with UK GDPR for their personal data processing activities.

Training companies based in the UK or providing training and qualifications to individuals based in the UK, are required to process personal data in compliance with UK GDPR and the principles of lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. The general requirements with which these training companies are required to comply in order that their services are likely to seen as compliant with UK GDPR, by clients and the ICO, are harmonized in this Certification Standard.

This Standard covers the activities of training companies whose work can include providing the training and qualifications to individuals and the subsequent reporting of results of these activities, marketing to individuals, reporting to Certification Bodies and, when required, to authorities. The scheme applies to the entire lifecycle of the data i.e., all stages of processing of personal data relating to the delivery of training/qualifications. For example, from obtaining candidate details for registration to the retention of qualifications granted for future validation, until such time the candidate requests the deletion of the data, or the training company no longer has a lawful basis to retain the data, and it is securely deleted. Certification will be granted to training companies that properly reflect the requirements and principles concerning the protection of natural persons with regard to the processing of personal data laid down in UK GDPR by complying with this standard.

In this Standard, the following verbal forms are used:

- — “shall” indicates a requirement;
- — “should” indicates a recommendation;
- — “may” indicates a permission;
- — “can” indicates a possibility or a capability.

Background

This scheme was created by two organisations that have particular expertise, and by working together, can deliver this certification scheme to help training companies demonstrate their compliance with UK GDPR in their data processing activities when delivering training and qualifications services.

1. The Trust Bridge have an outstanding reputation in helping organisations understand and secure their information. Working with clients in the UK and America, they have numerous organisations gain accreditation to ISO27000 and also implement policies and procedures to meet the requirements of UK GDPR.
2. APMG has an international reputation as a Certification Body, providing certification to companies offering training for our certification schemes, and examinations. It is UKAS accredited (No 126) to run schemes in accordance with ISO17024 and ISO17065.

The scheme has a real business benefit to the data subject and the training companies, as the data controller: -

1. Both parties understand the training market so as well as having Subject Matter Expertise regarding certification and UK GDPR, we also have technical expertise on the way training companies operate.
2. APMG have a significant client base in the UK of in excess of 100 training companies, so there are strong existing commercial and professional relationships in place to enable the delivery of the certification scheme.
3. The personal data held by the training companies should be time bound so an end-to-end process should be completed within a matter of weeks or months to enable the organisation to demonstrate every aspect of their process and receive a badge to demonstrate their compliance with potential candidates. This will help differentiate them in the training market.
4. Candidates will have confidence, when choosing a training company, that their personal data will be processed in accordance with UK GDPR and the training company has implemented measures to help keep their data secure.

UK GDPR Compliance Certification Scheme Criteria

Conformity assessment — Requirements for training companies processing personal data when providing training and qualifications services to individuals

1.0 Scope

This standard contains requirements for training companies to establish, implement and maintain policies and procedures to process personal data in compliance with UK GDPR, for their processing activities relating to providing training and qualifications to individuals.

It applies to training companies, who are data controllers as defined in this standard, and it applies to all data processing in all stages of providing training and qualifications. The scheme applies to the entire lifecycle of the data i.e., all stages of processing of personal data relating to the delivery of training and qualifications. For example, from obtaining candidate details for registration to the retention of qualifications granted for future validation, until such time the candidate requests the deletion of the data, or the training company no longer has a lawful basis to retain the data, and it is securely deleted. These stages of processing should include, where necessary: -

- Direct marketing to potential candidates
- Obtaining candidate details for registration
- Processing of payment card details
- Delivery of the training
- Provision the examination
- Conducting the invigilation, where applicable
- Issue examination results
- Issuing digital badges and e-certificates
- Communication pre and post training course
- Reporting training and qualification information to Certification Bodies
- Reviewing performance of their trainers
- Retention policy of personal data to validate qualifications

The training companies will need to demonstrate compliance through evidence of their data processing, including data sharing and transfers to third parties, for the full end to end process of providing training and qualifications services. The training companies, as data controllers, are required to comply with all obligations under UK GDPR, with the exception of those listed as out of scope in section 1.3.

1.1 Territorial Scope

This standard applies to training companies established in the UK, regardless of whether the processing takes place in the UK, and to training companies not established in the UK but who are offering training and qualifications to candidates in the UK.

The training company must be a legal entity.

Note: - training companies that are not established in the UK shall appoint a UK representative in accordance with criteria 5.20

1.2 Material Scope

This standard applies to the personal data processing activities of a training company, acting as a data controller, in their provision of training and qualifications services to candidates, over the age of 16, only. This applies to all personal data processed, including third party data, when providing these services.

1.3 Sections of UK GDPR Out of Scope

The following articles of UK GDPR are excluded as they are not relevant for the processing of personal data for training and qualifications purposes: -

- **Article 8 Conditions applicable to child consent in relation to information society services:** this is not included as training companies provide training for professional qualifications that are not aimed at children.
- **Article 10 Processing of personal data relating to criminal convictions and offences** – this has not been included in the criteria as training companies do not need to process data relating to criminal convictions when providing training and qualifications to individuals.

1.4 Companies and Activities Out of Scope

A training company that is not acting as the data controller for the processing activities and is not based in the UK or is not offering training and qualification services to UK based candidates, is not eligible for this certification scheme. The following activities are also out of scope: -

- Processing of personal data for secondary purposes e.g., payroll or HR information.
- Processing of personal data when providing training to individuals under the age of 16.
- Processing of personal data when providing training to individuals in prisons or other institutions which would require the processing of criminal convictions and offence data.
- Processing of personal data when training companies provide both training and certification decisions for the same scheme, as this is a conflict of impartiality under ISO 17024.

2.0 Target of Evaluation

The training company shall specify the processing activities that are subject to certification (Target of Evaluation), taking into account the processing activities involved with providing training and qualifications services from end to end (the lifecycle). Training Companies can refer to section 1.0 as an example of the lifecycle of data processing for training and qualification purposes. They shall provide a data map identifying all systems and software used; hosting; processors; all recipients of data transfers; methods of transfer; and retention period of personal data to be assessed against. It is important that the training company documents their data map to ensure they fully understand and can demonstrate the data types, systems and processes used when processing candidate personal data.

This data map should show the data types, formats, systems and processes used in the training companies' processing activities and highlight any processing activities that are likely to result in a high-risk processing, which is defined in 4.13. Processing that is likely to result in high-risk (based on the Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)) often involves: -

- Innovative technology
- Denial of service
- Large-scale profiling
- Biometric data
- Genetic data
- Data matching
- Invisible processing
- Tracking
- Targeting of children/other vulnerable individuals for marketing, profiling for auto decision making or the offer of online services
- Risk of physical harm

A explanation of each can be found on the Data Protection Impact Assessment (DPIAs) pages of the ICO site.

The training company shall also identify any data processing activities that include the processing of special category data, defined as: -

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

These processing activities require addition considerations and safeguards, which can be seen at section 5.7

This data map will form the basis of the training companies' Records of Processing Activities outlined in section 5.22

The training company shall identify where processing candidate personal data starts and where it ends, including a detailed explanation to justify any exclusions to the Target of Evaluation.

The Target of Evaluation shall be included on any certificates awarded by APMG.

3.0 Normative references

The certification criteria contained within this document have been approved by the Information Commissioner's Office in accordance with the Commissioner's tasks and powers under Articles 57(1)(n) and 58(3)(f) pursuant to Article 42(5) of the UK General Data Protection Regulation.

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- European Data Protection Board Guidelines on certification and identifying criteria in accordance with Articles 42 and 43 of the Regulation and the addendum Guidance on certification criteria assessment (not directly relevant for UK context but organisations may still find the guidelines useful)
- Privacy and Electronic Communications Regulations (EC Directive) 2003 (PECR) https://www.legislation.gov.uk/uksi/2003/2426
- ISO/IEC 17065:2012 Conformity assessment – Requirements for bodies certifying products, process and services
- ISO/IEC 17024:2012 Conformity assessment – Requirements for bodies operating certification of persons
- ISO 9001 Quality Management Systems
- ICO Guide to the UK GDPR https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- ICO Accountability Framework https://ico.org.uk/for-organisations/accountability-framework/

3.1 Supporting Documents

- UK GDPR Compliance Certification Scheme for the Provisions of Training and Qualifications Services Product Scheme Brochure
- Certification Scheme Application Form
- Assessment Form with guidance

4.0 Terms and definitions

For the purposes of this document, the terms and definitions given, the following apply.

4.1 **Certification**
The provision by an independent body of written assurance (a certificate) that a product, process, or service in question meets specific requirements.

4.2 **Policy**
Is a statement of intent and is implemented as a procedure.

4.3 **Procedure**
An established or official way of doing something.

4.4 **Process**
A series of actions or steps taken in order to achieve a particular end.

4.5 **Service**
A piece of work done for a client or customer that does not involve manufacturing goods.

4.6 **Certification Body**
Organisation that issues a certificate based on an assessment around a chosen standard, in this instance ISO/IEC 17065:2012

4.7 **Training Companies**
Training companies are defined as companies providing professional training and qualification services that are based in the UK or are providing these services to UK based individuals, over the age of 16. These can be private companies or further/higher education bodies if they provide training in accordance with ISO 17024.

4.8 **Candidate**
The client of the training company for training and qualifications services and the data subject for this scheme

4.9 **Data Subject**
An identifiable living person who can be identified, directly or indirectly from personal data. In this instance the Data Subject is the candidate.

4.10 **Information Commissioner's Office** (**ICO)**
The ICO is the UK's independent body set up to uphold information rights.

4.11 **Processing**
Any operation(s), 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, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure, or destruction.

4.12 **Qualification**
A pass of an examination or an official completion of a course, conferring a person's status as a recognised practitioner of a profession or professional activity.

4.13 **High-risk processing**
Risk in this context is about the potential for any significant physical, material or non-material harm to individuals and implies a more than remote chance of some harm. 'High-risk' implies a higher threshold, either because the harm is more likely, or because the potential harm is more severe, or a combination of the two. Any processing activities that are likely to result in a high-risk to the rights and freedoms of the candidates is considered to be high-risk processing.

4.14 **Shall, Should, May and Can**

For the intent and purpose of this document, “Shall” indicates requirements that must be complied with. “Should” indicates requirement which are expected to be complied with, unless specific and justifiable reasons exist for not doing so. The use of “May” indicates permission and “Can” as a possibility or capability.

5.0 Certification Scheme Criteria

General Requirements

5.1 General requirements

Certification Scheme Requirements

5.1.1 The training company shall register with the ICO for their data processing activities and pay the relevant data protection fee.

5.1.2 The training company shall declare if they are subject to any action by the ICO.

5.1.3 The training company shall declare if they have suffered any personal data breaches and, if so, the remedial actions taken.

Leadership and oversight

5.1.4 The board and senior management of the training company shall have responsibility and oversight of data protection, and shall have overall responsibility for data protection, compliance and accountability to UK GDPR and the Data Protection Act 2018.

5.1.5 The board and senior management shall also maintain a transparent approach to data processing and ensure compliance with transparency obligations, in accordance with criteria 5.8, 5.9 and 5.10.

5.1.6 The training company shall have board and senior management level support and direction for data protection compliance, including support for information security in accordance with business needs and relevant regulations.

5.1.7 The training company shall allocate information security responsibilities to ensure proper implementation and review of security policies and procedures and the supporting processes.

5.1.8 The training company shall ensure they have sufficient staff and resources, trained at an appropriate level under criteria 5.1.25 below to discharge their obligations under UK GDPR, and to meet the criteria within this standard.

5.1.9 The training company shall have an internal reporting structure for data processing governance, with responsibilities and accountabilities clearly defined in job descriptions.

5.1.10 The training company shall review and update job descriptions at least annually to ensure they remain fit for purpose.

5.1.11 The training company shall establish a defined data protection/information governance forum to provide oversight and direction for data processing activities. This forum should: -

1. consist of the DPO, if applicable, or the data protection lead, and representation from across the business including, but not limited to, IT Security and operational roles to support practical implementation of data protection compliance
2. have clear terms of reference to set out the aims of the forum
3. meet regularly to review compliance with UK GDPR and the Data Protections Act 2018.

4. maintain documented evidence of discussions and decisions
5. review any changes in regulations that need to be implemented by the business
6. report any risks in data processing activities, or compliance against UK GDPR to senior management.

Data Protection Officer

5.1.12 The training company shall appoint a Data Protection Officer (DPO), if: -

1. the core activities require regular and systematic monitoring of data subjects on a large scale e.g., tracking behaviour of customers on their website to target advertisements for training courses; or
2. the core activities consist of large-scale processing of special categories of candidate data e.g., processing health data of candidates attending training courses.

Note 1: - Article 37 1(a) is out of scope for this certification scheme as the training companies are not public authorities.
Note 2: - When determining if processing is large scale, the following factors need to be taken into consideration; the numbers of candidates concerned, the volume of candidate personal data processed, the range of different data items being processed; the geographical extent of the activity; and the duration or permanence of the processing activity.
Note 3: - If a training company does not meet the criteria for appointing a DPO, they can still do so on a voluntary basis. The person appointed is required to meet all requirements of being a DPO, regardless of whether their appointment is mandated or voluntary/
Note 4: If a training company appoints other data protection specialists they must not be referred to as the DPO.
Note 5:- the ICO has an online questionnaire to help determine if a company needs to appoint a DPO

5.1.13 If a DPO is not appointed, the training company shall document their reasoning and appoint someone, with appropriate seniority, as the data protection lead to ensure effective leadership and oversight of data protection.

5.1.14 If a DPO is appointed, the training company shall appoint them on the basis of their professional qualities and expert knowledge of data protection law and practices and their ability to fulfil the tasks in accordance with 5.1.16 below. The training company may appoint: -

1. an outsourced DPO
2. a single DPO to act for a group of companies, as long as they can perform their tasks effectively, taking into account the structure and size of the organisations
3. an existing employee, as long as there is no conflict of interest between their tasks or duties

5.1.15 The training company shall register any appointed DPO with the ICO, and provide the following information: -

1. The registration number of the organisation.
2. Whether they are required to appoint a DPO, or if they are doing so voluntarily;
3. The name, address, phone number and/or email address of the DPO if they are an employee, and whether or not they want the ICO to publish their name; or
4. The name, address, phone number and/or email address of the external organisation that will be carrying out the DPO duties on their behalf.

5.1.16 The DPO shall carry out the following tasks on behalf of the training company: -

1. inform and advise the training company, and its employees processing candidate data, of their obligations under UK GDPR and those set out in this standard.
2. Monitor compliance against UK GDPR and other data protection laws, and with the documented policies and procedures of the training company;
3. Managing internal data protection activities.
4. Awareness-raising of data protection and training of staff involved in the processing of candidate data and conducting internal audits.

5. Provide advice where requested with regards to Data Protection Impact Assessments (DPIA) following the ICO's guidelines and monitor performance against them.
6. Cooperate with the ICO.
7. To act as a point of contact for the ICO and candidates, for data protection related queries.

5.1.17 The DPO shall perform their tasks having due regard to the risks associated with the processing operations, taking into account the nature, scope, context and purposes of processing.

5.1.18 The training company shall ensure that; -

1. The DPO is involved properly and in a timely manner on all issues relating to data protection.
2. The DPO is able to act independently
3. They have adequate resources
4. They report directly to the highest management level
5. They shall not to be penalised for performing their duties compliantly

Note: The Article 29 Working Party Guidelines on Data Protection Officers (as endorsed by the EDPB) contain further information.

Policies and Procedures

5.1.19 The training company shall have documented policies in place for all data processing activities. These should include: -

1. a data protection policy of the training company's' approach to data protection
2. a data privacy policy that meets the requirements of 5.9 and 5.10
3. an information security management system that supports security measures in accordance with 5.24, and includes the policies in 5.1.20 below
4. a data protection by design and default approach across the business in accordance with 5.2.

5.1.20 The training company shall have documented policies and procedures for the implementation of information security, these shall include:-

1. Access Control
2. Transfer of Data
3. Acceptable Use
4. Password Management
5. Incident Management
6. Breach Notification
7. Email Usage
8. Clear Desk and Clear Screen
9. Removable Media
10. Business Continuity Plan
11. Documents and Records Control
12. Remote Working
13. Data Protection by Design and Default
14. Legitimate Interest Procedure

Note: For further information on records management and security can be found on the ICO site.

5.1.21 The training company shall ensure the following in relation to the policies and procedures at 5.1.19 and 5.1.20 above:-

5.1.21.1 They follow a standard format and style;
5.1.21.2 There are processes in place to support the implementation;
5.1.21.3 They are easily accessible by all staff;
5.1.21.4 They clearly outline the roles and responsibilities;
5.1.21.5 If there are any changes required e.g., operational or regulation change, the documents are updated in accordance with 5.1.22 below

5.1.22 The training company shall have a change control policy and procedure in place to manage the documents at 5.1.19 and 5.1.20, this shall include: -

1. Frequent, but no less than annual, review and update of the policies and procedures
2. Quality review of any changes
3. Change approval process to formally sign off any changes at senior management level
4. The documents show the document control information, including version number, document owner, review date and change history.
5. How changes are communicated to the business.
6. Any training requirements for staff, following the changes.
7. documented evidence that staff have read, understood, and will comply with policies and procedures.

5.1.23 The training company shall implement technical and organisational processes in support of the policies in 5.1.19 and 5.1.20.

5.1.24 The training company shall have documented policies and procedures, with supporting processes, in place to respond to candidates' requests, in accordance with criteria 5.11-5.18,

Note: Certifications such as ISO 9001 is one way to demonstrate the training company has suitable procedures in place to manage and maintain documentation in a Quality Management System.

Training and Awareness

5.1.25 The training company shall establish a data protection training and awareness programme for all staff, including senior management, this programme shall: -

1. be appropriate for the roles and responsibilities and include key areas such as, handling requests, data sharing, information security, personal data breaches and records management.
2. identify any additional/specialised training required for individuals based on their roles and responsibilities
3. include induction training, overseen by the DPO or the data protection lead, prior to staff being given access to personal data
4. include training plans to meet training needs within agreed timescales
5. the training materials should be reviewed and updated frequently, but no less than annually, or when there is a change in legislation, to ensure it remains suitable for the target audience, is current and relevant.
6. include annual refresher training, appropriate for the roles and responsibilities, for all staff, including senior management
7. include an assessment of knowledge gained from the training, with a minimum pass mark
8. monitor the training and awareness of staff by:-
    a. maintaining copies of training received
    b. maintaining records of who received the training and who completed the training and passed the assessments
    c. following up with staff who have not completed the training within agreed timescales.
    d. Following up with staff who failed the assessments for additional training and to resit the assessment.
9. Include evidence of the methods used to raise staff awareness of data protection and information governance e.g., internal document management systems, emails, meetings, notice boards etc
10. Easy access to staff of relevant material and contact details if they have any queries relating to data protection and governance

Audit and Complaints Handling

5.1.26 The training company shall have a documented procedure to handle complaints about data protection and for data subjects to be made aware of their right to complain. This shall include information on their right to complain to the ICO, with contact details.

5.1.27 The training company shall maintain a log of all complaints, including responses and resolutions.

5.1.28 The training company shall undertake regular data protection compliance and information governance audits to assess their compliance with UK GDPR and the criteria set out in this standard. These should include: -

1. annual internal audits by the DPO or the data protection lead
2. an internal audit plan that sets out what will be covered in the audit and who will be audited
3. completion of the ICO Accountability Framework self-assessment
4. external verification through an audit or compliance check

5.1.29 Based on the findings at 5.1.28, the training company shall implement any corrective actions required to ensure compliance with UK GDPR.

Note: The ICO publishes an Accountability Framework together with a self-assessment and Accountability Tracker to help organisations demonstrate compliance with UK GPDR. Training Companies can use the Accountability Tracker to provide the board with an oversight of what data protection has been implemented and what areas require improvement.

Data protection by design and by default

5.2 Article 25 Data protection by design and by default

5.2.1 The training company shall consult their DPO to provide input into 5.2.2-5.2.6. If the training company does not have a DPO, they shall consult the data protection lead.

5.2.2 The training company shall undertake an information risk assessment to assess the risks posed to the candidate when developing/procuring any new system, or when considering a new purpose or new processing activity, prior to implementation.

5.2.3 The training company shall determine, as part of the information risk assessment at 5.2.2, what the 'timely manner' to restore access to systems and data should be, to include in the Business Continuity Plan, based on: -

1. the systems used to process data, and
2. the risk to the candidate if accessibility to personal data is compromised

5.2.4 If any of the information risk assessments, conducted under 5.2.2, indicate a high level risk to the rights and freedoms of the candidate, the training shall conduct a Data Privacy Impact Assessment in accordance with section 5.3.

5.2.5 The training company shall document and maintain the information risk assessment(s) of processing candidate data and shall review and update them frequently, but no less than annually, or if the processing activity changes, or the risks to the candidate changes.

5.2.6 The training company shall maintain a data protection/information risk register, which feeds into to their corporate risk register and manage the risks in accordance with their risk management process.

5.2.7 The training company shall have a defined and documented risk assessment methodology in place.

Note: - The training company can use their own internal risk management approach, or other recognised approach such ISO 31000, to conduct the risk assessments and manage the risk register.

5.2.8 Based on the assessments at 5.2.2 the training company shall identify technical and organisational measures to ensure processing complies with the data protection principles and candidates' rights are protected. When determining what measures to put in place, the training company shall consider the following: -

1. the state of the art (technology)
2. the cost of implementation
3. the nature, scope, context and purpose of processing and,
4. the severity and likelihood of the risk to the rights and freedoms of the candidate

5.2.9 The training company shall ensure that any technical and organisational measures identified at 5.2.8 are implemented to ensure data protection is embedded into the design of any systems, services, products and business practices.

5.2.10 The training company shall implement technical and organisation measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing is processed. This applies to the data collected, the extent of the processing, the period of storage and accessibility to the personal data.

5.2.11 Prior to any processing, the training company shall: -

1. adopt a privacy first approach with any default settings of systems and applications used in the provision of the training and qualifications services
2. ensure they do not mislead candidate's regarding choice when it comes to the processing of their data in the provision of the training and qualifications services
3. not process candidate data for purposes beyond the purpose it was originally collected for, without prior consent, unless they have a lawful purpose to do so.
4. provide the candidate with sufficient control and options to exercise their rights.

5.2.12 The training company shall frequently, but no less than annually, review and update the technical and organisational measures implemented, in relation to data protection, to ensure they remain effective.

5.2.13 The training company, when reviewing the technical and organisational measures under 5.2.12, shall also take into account any changes to the information risks, reviewed under 5.2.5 and 5.2.6.

Data Protection Impact Assessment

5.3 Article 35 Data Protection Impact Assessment

5.3.1 The training company shall, prior to processing, conduct a Data Protect Impact Assessment (DPIA) if an information risk assessment under 5.2.2 determines a high level of risk to the rights and freedoms of the candidates.

5.3.2 The training company shall determine when a DPIA is required. In addition to 5.3.1, a DPIA is required in the following instances: -

1. When using systematic and extensive profiling based on automated processing with significant effects on candidates;
2. When processing special category or criminal offence data on a large scale; or
3. Systematically monitoring publicly accessible places on a large scale.
4. When using innovative technology (in combination with any of the criteria from the European guidelines);
5. When using profiling or special category data to decide on access to services;
6. When profiling individuals on a large scale;

7. When processing biometric data (in combination with any of the criteria from the European guidelines);
8. When processing genetic data (in combination with any of the criteria from the European guidelines);
9. When matching data or combining datasets from different sources;
10. When collecting personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
11. When tracking individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
12. When profiling children or targeting marketing or online services at them; or
13. When processing data that might endanger the individual's physical health or safety in the event of a security breach.

Note: Even if there is no legal requirement to do so, it is good practice to do a DPIA for any major new project involving the processing of personal data.

5.3.3 The training company shall consult their DPO, if they have one, or the data protection lead when a DPIA is required.

5.3.4 The training company shall document all decisions on whether to conduct a DPIA or not to demonstrate compliance with UK GDPR.

5.3.5 If a DPIA is required, the training company shall, prior to processing, carry out an assessment on the impact of the processing activities on the protection of personal data, and the impact on the rights and freedoms of the candidates.

5.3.6 The training company shall include the following in the assessment: -

1. a systematic description of the processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the training company and the intended outcome for the candidates;
2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
3. consideration of whether to consult and document views of the individuals;
4. an assessment of the risks to the rights and freedoms of the candidate, taking into account the nature, scope, context, and purpose of processing;
5. the measures envisaged to address each of the risks identified, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with UK GDPR, taking into account the rights and legitimate interests of the candidates and other persons concerned.

5.3.7 Following the assessment at 5.3.6, the training company shall either continue with the processing activities, if processing is deemed low risk, or consult with the ICO, in accordance with 5.27, if the processing is deemed high-risk.

5.3.8 The training company should, where possible, publish their DPIA's to demonstrate compliance with UK GDPR and to garner trust and confidence, but shall remove any sensitive details before publishing.

5.3.9 The training company shall carry out frequent, but no less than annually, reviews to assess if processing is performed in accordance with the DPIA, or when there is a change in the risks presented by the processing activity.

5.3.10 The training company shall document the review under 5.3.9 and any findings, to demonstrate compliance with 5.3.6

5.3.11 The training company shall maintain a register of DPIA's conducted and any updates in relation to 5.3.6, to demonstrate compliance with 5.3.1 to 5.3.10 above. This register should be maintained alongside the information risk register at 5.2.6

Note: The ICO has published detailed guidance for conducting a DPIA together with template documentation.

Principles relating to the processing of personal data

5.4 Article 5 Principles relating to the processing of personal data

Lawfulness, fairness and transparency

5.4.1 The training company shall process personal data of the candidate in a way that is lawful, and transparent and in accordance with scheme criteria 5.5, 5.8, 5.9 and 5.10.

5.4.2 The training company shall process personal data of the candidate in a way that is fair by ensuring that: -

5.4.2.1 the candidate is not deceived or misled when providing their personal data

5.4.2.2 the processing of their personal data is carried out in a way the candidate could reasonably expect.

5.4.2.3 the processing of their personal data does not have an unjustifiable negative affect on the candidate

Purpose Limitation

5.4.3 The training company shall ensure that personal data is only processed for the purposes in which it was collected in accordance with the following:-

5.4.3.1 The training company shall record the purpose of processing in accordance with 5.22 and make it clear to the candidate, at the point of collection, why the personal data is being collected and the intended uses, in accordance with 5.9.1

5.4.3.2 The training company shall not process the candidate's personal data for any new purposes' incompatible with the original purpose for which it was collected, without the candidate's prior consent

5.4.3.3 If the training company has a clear legal obligation or processing is in the public interest, for a new processing purpose, they shall notify the candidate prior to the further processing taking place.

5.4.3.4 The training company shall maintain records of notification and/or consent for any further processing activities

Note 1: 5.4.3.2 does not apply if the training company has a clear legal obligation or function to process the personal data
Note 2: Guidance on what is considered a compatible purpose can be seen on the ICO site.

Storage Limitation

5.4.4 The training company shall ensure that personal data is not retained for longer than is required, and shall: -

5.4.4.1 maintain a record of retention periods (a Retention Schedule) in accordance with 5.22 and document any reasons for retaining personal data beyond the retention period

5.4.4.2 frequently, but no less than annually, review the personal data held and securely destroy or anonymise it when it is no longer required

5.4.4.3 document the methods of secure destruction to demonstrate compliance, in accordance with 5.24.17.

5.4.4.4 retain records of certificates of destruction, where necessary

5.4.4.5 process any 'right to erasure' requests received from the candidates in accordance with 5.13.

Data Minimisation

5.4.5 The training company shall ensure that personal data is adequate, relevant and limited to only what is necessary for each specific purpose of the processing:

5.4.5.1 The training company shall only collect the minimum candidate data that is necessary for the processing purposes.

5.4.5.2 The training company shall have procedures in place to ensure the quality of the data and to minimise incomplete or incorrect personal data.

5.4.5.3 The training company shall process any 'right to rectification' requests received from the candidate in accordance with 5.12.

5.4.5.4 The training company shall review the candidate data processed frequently, but no less than annually, to ensure it is still adequate and relevant for the purpose for which it is being processed.

Accuracy

5.4.6 The training company shall ensure that personal data is accurate and kept up to date, where necessary, having regard to the purpose for which it was processed. Inaccurate data shall be erased or rectified within one month, of a request from a candidate, in accordance with criteria 5.10.

5.4.6.1 The training company shall ensure the source of the candidate data is clear, in the recording of processing activities (5.22) and in any privacy notices (5.9 and 5.10) and, where possible, obtained directly from the candidate to minimise errors.

5.4.6.2 The training company shall have a procedure to ensure the accuracy of candidate data, regardless of the source.

5.4.6.3 The training company shall action any challenges about the accuracy of the data received from the candidate in accordance with 5.12.

5.4.6.4 The training company shall have a documented procedure to review whether it is necessary to update candidate data or if a historical record is required e.g., the candidate email address may be required for registration but if the candidate changes their email address the original may need to be retained for verification purposes.

5.4.6.5 The training company shall ensure that any candidate data of historical records or records of opinion are marked as such.

Integrity and Confidentiality

5.4.7 The training company shall have documented policies and procedures in place, together with the supporting processes, to ensure the confidentiality and integrity of candidate data is maintained during processing, in particular, to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage, in accordance with criteria 5.24.

Accountability

5.4.8 The training company shall be accountable for all data processing activities and be able to demonstrate compliance with the UK GDPR principles in article 5 and the scheme criteria 5.4.1–5.4.7

5.4.9 The training company shall maintain records of processing activities, in accordance with 5.22, to demonstrate compliance with 5.4.8

Lawfulness of processing

5.5 Article 6 Lawfulness of processing

5.5.1 The training company shall ensure that the processing activities within the Target of Evaluation meet at least one of the following lawful bases for processing personal data, and the lawful basis was identified prior to processing activities taking place: -

1. the candidate has given consent to the processing of his or her personal data for one or more specific purpose, in accordance with criteria 5.5.4
2. processing is necessary for the performance of a contract to which the candidate is party or in order to take steps, at the request of the candidate, prior to entering into a contract, in accordance with 5.5.5.
3. processing is necessary for compliance with a legal obligation to which the controller is subject, in accordance with 5.5.6
4. processing is necessary in order to protect the vital interests of the candidate or of another living person, in accordance with 5.5.7
5. processing is necessary for the purposes of the legitimate interests pursued by the training company or by a third party and is in accordance with criteria 5.5.9 and 5.5.10.

Note 1: - Article 6 1 (e) is excluded as "public task" is not relevant to training companies' processing activities.
Note 2: The training company may rely on different lawful bases for processing types of personal data for different purposes, in this case the training company shall document each lawful basis e.g. the candidate email address may be processed under 5.5.1 (2) in order to provide the service to them and also under 5.5.1 (1) to send the candidate marketing emails.
Note 3: The ICO has published a lawful basis interactive guidance tool and guidance to help organisations determine their lawful basis for processing.

5.5.2 The training company shall record the lawful basis for processing personal data in accordance with criteria 5.22.

5.5.3 The training company shall have documented evidence that the processing of personal data is necessary, and the lawful basis applies, as they cannot reasonably achieve the purpose by some other less intrusive means, or by processing less personal data.

Consent

5.5.4 The training company shall ensure that all candidate data processing activities, relying on the basis of consent, are carried out in compliance with 5.6.

Contract

5.5.5 The training company shall, when relying on 5.5.1(2) as the lawful basis for processing, ensure that one of the following applies: -

- they have a contract with the candidate for the provision of training and qualifications and the processing is required to comply with the obligation under the contract.
- they have a contract with the candidate and need to process the personal data to comply with the candidate's specific obligations under the contract, e.g., if the candidate is required to pay for the training and qualification service directly, the processing of payment details will be required.
- They do not have as contract with the candidate, but processing was in the context of a potential contract with the candidate, when requested to do so by the candidate.

Note: 5.5.1 (2) does not apply if the training company is taking pre-contractual steps on their own initiative, to meet other obligations, or at the request of a third party.

Legal Obligation

5.5.6 The training company shall, when relying on 5.5.1(3) as the lawful basis for processing, ensure that: -

1. The legal obligation is laid down by UK common law or statute
2. They can identify the obligation by reference to the specific legal provision or by pointing to a source of advice or guidance that sets it out clearly

Note: - Processing candidate health data, to ensure fairness and equality when providing training and qualification services to the candidates, under the Equality Act 2010, would be a legal obligation.

Vital Interests

5.5.7 If the training company conducts physical onsite training, and in the event of a medical emergency the training company is required to disclose personal information to the emergency services, they shall only do so under 5.5.1(4) if the candidate is incapable of giving consent.

5.5.8 If the training company is processing health information in relation to 5.5.1(4), they shall ensure the personal data is processed in accordance with criteria 5.7.

Note: The training company should not rely on vital interests for potential medical emergencies planned in advance e.g., collecting medical information, or next of kin details in advance of a physical training course in the event that something may happen during the course. In these cases, consent is a more appropriate basis, or explicit consent in the case of medical data.

Legitimate Interests

5.5.9 The training company shall conduct a Legitimate Interest Assessment (LIA) before processing personal data, if relying on 5.5.1(5) as the lawful basis for processing. This assessment shall consider the following: -

1. Purpose test: is the training company pursuing a legitimate interest?
2. Necessity test: is the processing necessary for that purpose?
3. Balancing test: is the legitimate interest overridden by the candidate's interests, rights or freedoms?

Note: For further information, the ICO has published detailed guidance on LIA's and a template LIA that organisations can use.

5.5.10 The training company shall document the outcome of the LIA and shall not proceed with processing if the legitimate interests of the training company are outweighed by the interests, rights or freedoms of the candidate. If this is the case, the training company must either find another lawful basis for processing or not proceed with the processing activity.

5.5.11 The training company shall maintain all records of LIA's conducted and shall keep them under review and updated if there are any changes in the purpose, nature or context of the processing.

5.5.12 The training company shall make the candidate aware of the risks, rules, safeguards, and their rights in relation to the processing of their personal data and how to exercise their rights in relation to such processing, at the point of data collection, in accordance with scheme criteria 5.8, 5.9 and 5.10.

Conditions of Consent

5.6 Article 7 Conditions of Consent

5.6.1 The training company shall, if applicable, ensure that when a candidate gives consent for the processing activities that it is freely given, specific, informed, and unambiguous. This means:

1. it shall be clear opt-in consent for each separate data processing activity. This opt-in shall be a clear affirmative action and shall **not** include pre-ticked boxes or inaction as consent.
2. It shall be separate from any other terms and conditions of the training and qualification services
3. the candidate shall be able to withdraw consent at any time and they shall be informed of this at the time of providing consent.
4. It shall be as easy for the candidate to withdraw consent as it was for them to give consent.

Note: Training companies should avoid making consent a requirement for providing the training and qualification services, as this does not provide candidates with a real choice, however it can be relied upon for other processing, such as direct marketing.

5.6.2 The training company shall make the candidate aware, when they are providing consent for processing, of the following, in accordance with criteria 5.8, 5.9 and 5.10:-

1. the name of the training company
2. the name of any third-party controllers who will rely on the consent
3. why the personal data is required
4. how the personal data will be processed
5. that the candidates can withdraw consent at any time and how they can do this
6. retention period of the data
7. Cookie consent management, to explain where and why non-essential cookies are set and how the individual can manage their preferences for providing consent or not, at the point of obtaining the consent.

Note: Training Companies using non-essential cookies, and other direct marketing, need to ensure they are processing this data in compliance with Privacy and Electronic Communications Regulations (EC Directive) 2003 (PECR) https://www.legislation.gov.uk/uksi/2003/2426 . The ICO site also has additional guidance on managing cookies and cookie consent.

5.6.3 The training company shall have a documented procedure in place to deal with any requests to withdraw consent.

5.6.4 The training company shall, if relying on consent for direct marketing, ensure clear, opt-in consent is obtained, and the candidate has the opportunity to opt-out of continuing to receive marketing with each communication sent, e.g., with a unsubscribe button on emails or details of how to withdraw consent on postal marketing. This opt-in shall be a clear affirmative action and shall **not** include pre-ticked boxes, silence, or inaction as consent.

5.6.5 The training company shall implement processes to ensure an effective audit trail of all records of consent, to demonstrate compliance. This audit trail shall show: -

1. what processing activity(ies) the individual consented to
2. who consented
3. when they consented
4. how they consented
5. and what information they were provided with at the time of consent

5.6.6 The training company shall proactively review consent provided to confirm and refresh these consents frequently, but no less than annually.

Processing of special categories of personal data

5.7 Article 9 Processing of special categories of personal data

5.7.1 The training company shall ensure that the processing of special category data meets the following criteria: -

1. a lawful basis for processing is identified under Article 6, in accordance with criteria 5.5; and
2. one of the following Article 9 special conditions are met: -
    - (a) Explicit consent
    - (b) Employment, social security and social protection (if authorised by law)
    - (c) Vital interests
    - (d) Not-for-profit bodies
    - (e) Made public by the data subject
    - (f) Legal claims or judicial acts
    - (g) Reasons of substantial public interest (with a basis in law)
    - (h) Health or social care (with a basis in law)
    - (i) Public health (with a basis in law)
    - (j) Archiving, research and statistics (with a basis in law)

Note 1: Special category data is defined as personal data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; or data concerning health; a person's sex life or sexual orientation.

5.7.2 If the training company is relying on conditions (b), (h), (i) or (j) above, it also needs to meet the associated condition in UK Law, set out in Part 1 of Schedule 1 of the Data Protection Act 2018.

5.7.3 If the training company is relying on conditions (g) above, it also needs to meet one of the 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the Data Protection Action 2018

5.7.4 The training company shall complete an Appropriate Policy Document (APD), where relying on a condition under criteria 5.7.3, when processing special category data for each processing activity.

5.7.5 The training company shall have safeguards in place when processing health data and shall only retain health data for as long as is required for the processing activity, in compliance with Part 4 of Schedule 1 of the Data Protection Action 2018.

5.7.6 The training company shall conduct a DPIA, in accordance with criteria 5.3 prior to processing special category data.

Note: The ICO has published detailed guidance on special category data, including a template APD.

Transparent information, communication and modalities for the exercise of the rights of the data subject

5.8 Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject

5.8.1 When communicating to individuals about personal data processing activities, the training company shall ensure any communications: -

1. Are concise, transparent, intelligible and in an easily accessible form.
2. use clear and plain language.

3. Are provided in writing and, where appropriate, by electronic means i.e., on websites and online portals, or via email.
4. if requested by the candidate, the information is provided orally, once their identity has been verified by appropriate means.

5.8.2 The bulleted criteria in 5.8.1 shall be applied by the training company to any communications sent to the candidate in relation to criteria 5.9, 5.10, 5.11, 5.12, 5.13, 5.14, 5.15, 5.16, 5.17, 5.18 and 5.26.

5.8.3 The training company shall facilitate any requests received from candidate, in relation to criteria 5.11, 5.12, 5.13, 5.14, 5.15, 5.16, 5.17, and 5.18, and have documented procedures in place to recognise and action these requests, bearing in mind such requests may be oral or in writing.

5.8.4 The training company shall have documented procedures in place to confirm the identity of a candidate, at the time of receiving the request and prior to actioning the request, in relation to 5.8.3. If the training company is unable to verify the identity of the candidate, the training company shall inform the candidate accordingly.

Note 1: The information requested to verify the candidate's identity must be reasonable and proportionate, the training company should not ask for more information if the candidate's identity is obvious to them. The training company should not ask for formal identification documents unless necessary. Further information regarding identity verification can be seen on the ICO site.
Note 2: If the candidate provides additional information to enable identification, the training company shall not refuse a request received in relation to 5.6.3 unless they can demonstrate they are unable to identify the candidate.

5.8.5 The training company shall have sufficient resources in place to handle such requests in relation to criteria 5.8.3, in accordance with criteria 5.8.6.

5.8.6 The training company shall respond to and action any request from a candidate within one month. This period can be extended by a further two months, depending on the complexity of the request, but this must be clearly documented and explained to the candidate.

5.8.7 The training company shall document response times to the candidate to ensure compliance with criteria 5.8.6.

Note: The ICO has published guidance on how to decide if a request is complex

5.8.8 The training company shall **not** charge a fee to the candidate, unless the request is manifestly unfounded or excessive, or the candidate requests further copies of their data following a request, in which case a reasonable administrative fee can be charged. This must be clearly documented and explained to the candidate.

Note 1: The ICO has published guidance on how to determine a reasonable administrative fee
Note 2: It is the responsibility of the training company to provide evidence that demonstrates a request is manifestly unfounded or excessive. Furter guidance on what can be considered manifestly unfounded and manifestly excessive can be seen on the ICO site.

5.8.9 If the training company is relying on an exemption to refuse a request, this should be clearly communicated to the candidate, within one month, with the following information: -
1. The reasons for not taking action
2. The candidate's right to make a complaint to the ICO
3. The candidate's ability to seek to enforce this right through a judicial remedy

Note: The exemptions to responding to a request received in relation to 5.8.3 are set out in the Data Protection Act 2018, Schedules 2, 3 and 4. Further guidance can be seen on the ICO site.

5.8.10 The training company shall respond to any request from the candidate in commonly used electronic format, if received electronically, unless the candidate makes a reasonable request for another commonly used format.

5.8.11 The training company shall ensure that, regardless of the format of any communication, information is provided to the candidate securely.

5.8.12 Where possible, the training company shall provide the candidate with direct access to their data through a secure online system and, where applicable, enable them to update personal data, manage their permissions and allow for a downloadable copy of their data.

5.8.13 The training company shall maintain a record of all requests received in relation to 5.8.3 to track the handling of each request and demonstrate compliance with criteria 5.8.1-5.8.12 above.

Information to be provided where personal data are collected from the data subject

5.9 Article 13 Information to be provided where personal data are collected from the data subject

5.9.1 The training company shall include the following information in the Privacy Policy: -

1. the identity and contact details of the data controller and, where applicable, of the controller's representative
2. the contact details of the DPO, where applicable
3. the purpose of the processing for which the personal data are intended as well as the legal basis for processing
4. details of the legitimate interests pursued by the controller or third parties, where processing is based on the legitimate interests pursued by the controller or third party
5. the recipient or categories of recipients of the personal data, if any
6. provide details of any transfer, where the training company intends to transfer personal data to a third country and what additional safeguards are in place.
7. the period for which the personal data will be stored, or the criteria used to determine this period
8. the process for the candidate to request access to and rectification or erasure of personal data or to restrict or object to processing, as well as data portability.
9. the process for the candidate to withdraw consent
10. the right for the candidate to lodge a complaint with the ICO.
11. Whether the provision of personal data is a statutory or contractual requirement or a requirement necessary to enter into a contact, as well as whether the candidate is obliged to provide the personal data and the possible consequences of the failure to do so.
12. The existence of automated decision-making, including profiling and information about how decisions are made, the significance and the consequences, and where artificial intelligence/algorithms are used in the processing.

5.9.2 The training company shall provide the information covered in criteria 5.9.1 in accordance with criteria 5.8.1.

5.9.3 The training company shall provide the candidate with the Privacy Policy at the point of collection of the personal data from the candidate and shall maintain records of how and when the Privacy Policy was provided.

5.9.4 The training company shall update the Privacy Policy in line with any new processing activities in relation to criteria 5.4.3.2 and 5.4.3.3.

5.9.5 The training company shall establish a process to frequently, but no less than annually, review the Privacy Policy provided to candidates and make sure it is accurate and up to date.

5.9.6 The training company shall maintain records of all versions of the Privacy Policy as an audit trail of information provided to candidates, at the point they received the training and qualification services, to demonstrate compliance with criteria 5.9.

Information to be provided where personal data have not been obtained from the data subject

5.10 Article 14 Information to be provided where personal data have not been collected from the data subject

5.10.1 Where information has been provided by someone other than the candidate, for example when an employer has booked training on behalf of the candidate, the training company shall provide the privacy information to the candidate either when it first communicates with the candidate, or prior to sharing their data with a third party, but no later than 1 month from obtaining the candidate's personal data.

5.10.2 The training company shall, in addition to all information required in criteria 5.9.1, provide the candidate with the following: -

1. The categories of the personal data obtained
2. The source of the data and whether it came from publicly accessible sources

5.10.3 The training company shall provide the privacy information in accordance with 5.8.1.

Right of access by the data subject

5.11 Article 15 Right of access by the data subject

5.11.1 The training company shall enable the candidate the right to obtain confirmation as to whether or not their personal data is being processed and, where that is the case, access to the personal data and the information described in 5.9.1 above.

5.11.2 The training company shall provide the candidate with a copy of their personal data in accordance with 5.8.10, 5.8.11 and 5.8.12.

5.11.3 The training company shall process all requests received under 5.11.1 in accordance with the criteria in 5.8.

Note 1: Article 23 Restrictions – the training company shall refer to the Data Protection Act, Schedule 2, Part 3 (16) when processing a subject access request so that personal data of another individual is not disclosed, unless the conditions set out are met.
Note 2: Article 23 Restrictions – If the training company receives a Subject Access request for exam papers or exam results, the following exemptions apply, in accordance with the Data Protection Act 2018, Schedule 2, Part 4 (25).

(1) The listed GDPR provisions do not apply to personal data consisting of information recorded by candidates during an exam.

(2) Where personal data consists of marks or other information processed by a controller—
(a)for the purposes of determining the results of an exam, or
(b)in consequence of the determination of the results of an exam,
the duty in Article 12(3) or (4) of the GDPR for the controller to provide information requested by the data subject within a certain time period, as it applies to Article 15 of the GDPR (confirmation of processing, access to data and safeguards for third country transfers), is modified as set out in sub-paragraph (3).

(3) Where a question arises as to whether the controller is obliged by Article 15 of the GDPR to disclose personal data, and the question arises before the day on which the exam results are announced, the controller must provide the information mentioned in Article 12(3) or (4)—
(a)before the end of the period of 5 months beginning when the question arises, or

(b)if earlier, before the end of the period of 40 days beginning with the announcement of the results.

Right to rectification

5.12 Article 16 Right to rectification

5.12.1 The training company shall enable the candidate with the right to obtain the rectification of inaccurate personal data or, depending on the purpose of processing, the right to have incomplete personal data completed, including by means of a supplementary statement.

5.12.2 While the training company investigates any requests from the candidate, challenging the accuracy or completeness of the personal data, a note should be added to the system advising of this.

5.12.3 The training company shall have technical and organisational measures in place to ensure they can comply with such requests, including being able to intervene in the processing to make corrections to the data.

5.12.4 Where personal data has been amended or updated, the training company shall comply with the requirements in criteria 5.15, where applicable.

5.12.5 The training company shall handle all requests in relation to 5.12.1 accordance with criteria 5.8.

Right to erasure

5.13 Article 17 Right to erasure

5.13.1 The training company shall enable the candidate with the right to erasure of their personal data and the training company shall erase the personal data where one of the following applies: -

1. The personal data are no longer necessary in relation to the purpose for which they were collected or otherwise processed
2. The candidate withdraws consent on which the processing was based, and where there is no other legal ground for processing
3. The candidate objects to processing and there are no overriding legitimate grounds for processing
4. The personal data is being unlawfully processed
5. The personal data have to be erased for compliance with a legal obligation in UK law.

5.13.2 The training company shall handle all requests received in relation to 5.13.1 in accordance with criteria 5.8.

5.13.3 The training company shall have technological and organisational measures in place to ensure they can comply with such requests, including being able to intervene in the processing to delete data.

5.13.4 Where personal data has been erased, the training company shall comply with the requirements in criteria 5.15, where applicable.

5.13.5 The training company shall notify the candidate if there will be a delay in the erasure of the data and the reason for the delay e.g., the data being available in backups until the next backup date

Right to restriction of processing

5.14 Article 18 Right to restriction of processing

5.14.1 The training company shall enable the candidate with the right to restriction of processing of their personal data and the training company shall restrict the personal data where one of the following applies: -

1. The accuracy of the personal data is contested by the candidate, for a period enabling the training company to verify the accuracy of the personal data; or
2. The processing is unlawful and the candidate requests restriction of the use of their personal data instead of erasure; or
3. The training company no longer needs the personal data for the purposes of the processing, but they are required by the candidate for the establishment, exercise, or defence of legal claims; or
4. The candidate objects to processing and there are no overriding legitimate grounds for processing.

5.14.2 The training company shall automatically restrict processing of candidate personal data when a candidate contests the accuracy of the data under 5.12 or objects to processing under 5.17, while the training company investigates the request.

5.14.3 The training company shall have technological and organisational measures in place to ensure they can comply with such requests, including being able to intervene in the processing to restrict processing of data.

5.14.4 The training company shall add a note to the system advising of any restriction of processing personal data, and the reasons why.

5.14.5 Where the processing of personal data has been restricted, the training company shall comply with the requirements in criteria 5.15, where applicable.

5.14.6 The training company shall handle all requests received in relation to 5.14.1 in accordance with criteria 5.8.

Notification obligation regarding rectification or erasure of personal data or restriction of processing

5.15 Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing

5.15.1 The training company shall advise any third parties, they have transferred the personal data to, of any rectification under 5.12, erasure under 5.13 or restriction of processing under 5.14, of that personal data.

5.15.2 The training company shall also inform the candidate about any recipients of their personal data when processing their request under 5.15.1.

Right to data portability

5.16 Article 20 Right to data portability

5.16.1 The training company shall provide the candidate with any personal data which they have provided in a structured, commonly used and machine-readable format or transmit the data to another controller where: -

1. The processing is based on consent or contract, and
2. The processing is carried out by automated means.

Note: this shall not affect the candidates right under article 17.

5.16.2 The training company shall handle all requests received in relation to 5.16.1 in accordance with criteria 5.8.

Right to object

5.17 Article 21 Right to object

5.17.1 The training company shall provide the candidate with the right to object to their personal data being processed, under legitimate interests, and shall no longer process their data, if they exercise that right, unless: -

1. their legitimate grounds override the interests, rights and freedoms of the candidate; or
2. The processing is for the establishment, exercise or defence of legal claims

5.17.2 The training company shall provide the candidate with the right to object to their personal data being processed, for direct marketing including profiling for that purpose, and shall no longer process their data, if they exercise that right.

Note 1: the right to object to personal data being processes for direct marketing purposes, including profiling for that purpose, is an absolute right that must be afforded to the candidate.
Note 2: Article 21 (1) in relation to processing under 6 (1) (e) is out of scope for training companies processing personal data for the provision of training and qualifications.
Article 21 (5) and (6) are out of scope for training companies processing personal data for the provision of training and qualifications.

5.17.3 The training company shall handle all requests received in relation to 5.17.1 in accordance with criteria 5.8.

Automated decision-making, including profiling

5.18 Article 22 Automated decision-making, including profiling

5.18.1 The training company shall not base decisions solely on automated processing, including profiling, unless the processing is based on explicit consent from the candidate or is necessary for entering into, or for the performance of a contract with the candidate.

5.18.2 Where 5.18.1 applies, the training company shall provide the candidate with the following rights:-

1. To obtain human intervention;
2. To express their point of view; and
3. To obtain an explanation of the decision making to be able to challenge it.

Note:- Article 22 only applies if the profiling and automated decision making is carried out with no human involvement and there is a legal or similarly significant effect on the candidate. This is unlikely to apply to training companies, as they are not making automated decisions that would have a legal or similarly significant effect on the candidate.

5.18.3 The training company shall handle all requests in received in relation to 5.18.2 accordance with criteria **5.8.**

Joint Controllers

5.19 Article 26 Joint controllers

5.19.1 If the training company is a joint controller, for the processing of the candidate data, the training company shall have an agreement in place covering: -

1. The provision of privacy notices to their candidates in accordance with criteria 5.9 and 5.10;
2. A contact point for their candidates; and
3. The obligations in respect of the rights and freedoms of their candidates.

5.19.2 The training company shall make the candidate aware of the nature of the agreement, in accordance with 5.8.1.

5.19.3 Regardless of the terms of the agreement, the training company shall facilitate any requests received from candidates, in relation to criteria 5.11, 5.12, 5.13, 5.14, 5.15, 5.16, 5.17, and 5.18,

Representatives of controllers or processes not established in the United Kingdom

5.20 Article 27 Representatives of controllers or processes not established in the United Kingdom

5.20.1 Where the training company is not established in the UK but provides training and qualifications services to candidates based in the UK, the training company shall designate in writing a representative in the UK.

5.20.2 The training company shall mandate the representative be addressed in additional to or instead of the training company, in particular, by the ICO and candidates, on all issues relating to the processing for the purpose of ensuring compliance with UK GDPR.

Processor

5.21 Article 28 Processor

5.21.1 Prior to entering into an agreement with a processor, the training company shall conduct due diligence on the processor e.g. checking data security, audit reports, whether the processor has previously suffered a data breach and will require the processor to implement appropriate technical and organisational measures.

5.21.2 The training company shall document the findings of the due diligence, including if any issues where identified and rectified, and the decision on whether to proceed with the data processing agreement or not.

5.21.3 If the training company is using processors to carry out data processing of candidate data on their behalf, in accordance with 5.21.1 and 5.21.2, the training company shall have a signed contract with the processor, that documents details of the data processing activities, the duration, the nature and the purpose of the processing, the type of personal data of the candidates and the obligations and rights of the controller, and requires: -

1. the implementation of technical and organisation measures to ensure the security of any personal data they process.
2. the processor shall not engage another processor without the prior written consent of the training company and shall inform the training company of any intended changes concerning the addition or replacement of other processors, and provide them with an opportunity to object
3. the processor processes personal data of the candidate only on documented instructions of the training company, including transfers of candidate data to a third country or an international organisation, unless it is required to do so by UK law
4. persons authorised to process candidate data are bound by a duty of confidentiality.
5. the processor takes all measures required under criteria 5.24.
6. the processor shall assist the training company in their obligation to respond to candidate requests to exercise their rights under criteria 5.11, 5.12, 5.13, 5.14, 5.15, 5.16, 5.17, and 5.18

7. the processor shall report any data breaches to the training company, without delay, and will assist the training company in ensuring compliance with obligations under criteria 5.3, 5.24, 5.25, 5.26, and 5.27.
8. at the choice of the training company, they delete or return all candidate data to the training company at the completion of the provision of services.
9. the processor makes available to the training company all information necessary to demonstrate compliance with the obligations under these criteria and allow for and contribute to audits conducted by the training company or another auditor appointed by the training company.

5.21.4 Once the training company has entered into an agreement with a data processor, they will review and monitor the performance of the contract in accordance with criteria **Error! R eference source not found.**– 5.24.16.

Records of processing activities

5.22 **Article 30 Records of processing activities**

5.22.1 The training company shall maintain a record of all processing activities they are responsible for.

5.22.2 The Record of Processing Activities (ROPA) shall contain the following information: -

1. Contact details of the training company and, where applicable, the joint controller, the controller's representative (where outside the UK) and the DPO, if applicable, or the person responsible for data protection within the training company
2. Purposes of processing of the candidate personal data
3. Lawful basis for processing of the candidate personal data
4. Contact details of any joint controllers
5. Categories of personal data
6. Categories of data subjects (e.g. candidates)
7. Categories of recipients of the personal data, including recipients in third countries or international organisations
8. Details of international transfers to third countries, including the names of the country and organisation
9. Details of the safeguard(s) for the transfer of personal data to third countries
10. Retention schedule, in accordance with 5.4.4.1
11. Details of the security measures in place to protect personal data, with links to the training companies Information Security Management System.

Note: The ROPA can link to where other documents are held and maintained e.g. contracts, DPIAs, documented data breaches, LIA's, and security measures where they are documented in an ISMS, rather than duplicating the information in the ROPA.

5.22.3 The training company shall frequently, but no less than annually, review the data map and records of processing activities to ensure they are comprehensive and accurate.

Note: the ICO has published detailed guidance and template regarding documentation.

Cooperation with the supervisory authority

5.23 Article 31 Cooperation with the supervisory authority

5.23.1 The training company shall cooperate, on request, with the ICO in the performance of its tasks and shall make available its records of processing activities to the ICO.

Security of processing

5.24 Article 32 Security of processing

5.24.1 The training company shall determine the level of security required, based on the risk assessments conducted under 5.2, to prevent the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to candidate personal data transmitted, stored, or otherwise processed.

5.24.2 The training company shall implement the technical and organisation measures to ensure information security as documented in the policies and procedures at 5.1.20.

5.24.3 The training company shall document policies and procedures and establish the technological and organisational measures required to implement the following: -

1. secure storage of candidate personal data
2. secure disposal of candidate personal data in accordance with criteria 5.24.17.
3. secure configuration of network and devices
4. system password security
5. access control in accordance with 5.24.8
6. malware protection
7. backup and restoration of systems and candidate data
8. patch management
9. boundary firewalls
10. vulnerability testing
11. supplier management
12. data encryption at rest and in transit
13. Device security
14. Remote working security (if applicable)

Note 1: the NCSC site provides advice and guidance on the implementation of security requirements
Note 2: Note the ICO site provides guidance on the Accountability Framework and how to demonstrate compliance with security

5.24.4 The training company shall have documented policies and procedures in place to assess, identify and systematically manage risks to personal data to ensure: -

1. the ongoing confidentiality, integrity, availability, and resilience of processing systems and services
2. candidate data can only be accessed, altered, disclosed or deleted by those authorised to do so, and those people only act within the scope of the authority given to them
3. candidate data held continues to be accurate and complete over its lifecycle
4. candidate data remains accessible and usable and the availability and access to personal data can be restored, in a timely manner, in the event of a physical or technical incident.

Note: - 'Timely manner' depends on the systems the training company uses, and the risk posed to candidates if the data processed is unavailable for a period of time, which should be considered in the risk assessments, in accordance with criteria 5.2.3 and should be documented in the training company's Business Continuity Plan.

5.24.5 The training company shall implement technical and organisation measures to protect the candidate's personal data from cyber-attack and to reduce the impact in the event of one.

5.24.5.1 Where applicable, the training company should store personal data offline.

5.24.5.2 The training company shall use anonymisation, where possible, to reduce the amount of candidate personal data being processed.

5.24.5.3 Where applicable, the training company shall implement pseudonymisation (defined in note 2 below) as soon as possible when processing candidate data, to reduce the risks to the candidate, e.g., processing performance reports for their trainers. The candidate's

name can be replaced with a pseudonym, such as a reference number, so that the result can no longer be attributed to a candidate, without the use of additional information.

5.24.5.4 The training company shall have technical and organisational measures in place to ensure the additional information required to tie the pseudonym back to the candidate is stored separately.

5.24.5.5 Where possible, the training company shall implement encryption when processing candidate data or when data is at rest and, if used, shall have a documented policy and procedure in place with supporting processes to implement correctly.

5.24.5.6 The training company shall have security measures in place to protect data in transit when transferred to third parties e.g., use encrypted communication channels, encrypt data prior to transmission

5.24.5.7 The training company shall store candidate data in password protected systems with access control and setting minimum requirements to ensure passwords are secure.

5.24.5.8 The training company shall install firewalls to prevent unauthorised access and malware protection to prevent ransomware attacks.

5.24.5.9 The training company shall be able to intervene and apply urgent patches to systems, outside of any scheduled patch applications.

Note 1: Further information can be found on the ICO site regarding security outcomes.
Note 2: Pseudonymisation refers to techniques that replace, remove or transform information that identifies an individual
Note 3: Pseudonymisation can help reduce the risk to the candidate concerned but it is still classed as personal data and the training company's obligations under UK GDPR and the Data Protection Act 2018 remain.

5.24.6 The training company shall implement technical and organisation measures to detect security events, and be able to intervene in the processing operations to carry out these measures, to include: -

1. Monitoring the status of systems processing personal data
2. Vulnerability scans to detect any security risks
3. Monitoring user access to personal data and any anomalous activity

5.24.7 The training company shall implement technical and organisational measures so any unexplained events detected under 5.24.6 can be acted on as soon as possible to prevent access to candidate personal data or to minimise the impact.

Note 1:- Guidance on the use and implementation of appropriate levels of encryption is available on the ICO site.

5.24.8 The training company shall limit access to personal data to authorised staff only and frequently, but no less than annually, review these access rights and;

5.24.8.1 Access controls should cover physical access to paper records and digital access to electronic records

5.24.8.2 Access rights shall be role based and based on the principle of least privilege i.e., only those users who need access to a particular area of your premises, or a certain system, should have such access.

5.24.9 The training company shall implement physical security such as: -

1. Locks on doors and security to premises such as alarms and CCTV
2. Access control to the premises and supervision of visitors
3. Secure disposal of paper and electronic waste; and
4. Access control and remote deletion of IT equipment and mobile devices

5.24.10 The training company shall manage and document data sharing decisions and shall establish data sharing agreements, including Standard Contractual Clauses, with third party controllers.

5.24.11 The training company shall ensure that persons acting under their authority, or any of their processors who access the personal data, do not process the personal data except on their instructions, unless they are required to do so under UK law.

5.24.12 The training company shall carry out due diligence checks to ensure that processors will implement technical and organisational measures to comply with UK GDPR requirements.

5.24.13 The training company shall undertake compliance audits on processors, the frequency of which should be based on a risk-based approach, determined by the results of the assessments under 5.24.14.

5.24.14 The training company shall determine the risk the processor poses for the processing activities based on: -

1. the nature, scope, context and purpose of processing and,
2. the severity and likelihood of the risk to the rights and freedoms of the candidate and
3. The location of the data processor i.e., does the processing involve a restricted transfer, in accordance with 5.28.1.

5.24.15 The training company shall record all decisions regarding the risk of a processor, determined under 5.24.14, and any audits undertaken under 5.24.13.

5.24.16 The training company shall, based on any audit findings, document any decisions regarding the contract with the processor and whether any remedial actions are required by the processor.

5.24.17 The training company shall have a documented procedure in place to cover methods of destruction of data when it is no longer required for processing, either because the retention period has expired, or the candidate has requested the erasure of their data. This procedure shall cover: -

1. Secure destruction of physical personal data
2. Secure destruction of electronic personal data
3. Secure destruction of redundant IT equipment used in the processing of personal data.

5.24.18 The training company shall ensure they have the technical and organisational processes in place to destroy the data in accordance with 5.24.17.

Note 2: Certificates such as Cyber Essentials, Cyber Essentials Plus and ISO27001 are one of the ways that can be used to demonstrate compliance with article 32.

Notification of a personal data breach to the supervisory authority

5.25 Article 33 Notification of a personal data breach to the supervisory authority

5.25.1 The training company shall establish procedures to detect, manage and record personal data incidents and breaches, categorised according to the following information security principles:-

1. Confidentiality breach – where this is an unauthorised or accidental disclosure of, or access to, candidate data
2. Integrity breach – where there is an unauthorised or accidental alteration of candidate data
3. Availability breach – where there is an accidental or unauthorised loss of access to, or destruction of, candidate data

5.25.2 In the event of a breach, the training company shall conduct a risk analysis and assessment to determine the risks to the rights and freedoms of the candidate and the potential adverse consequences, based on how serious or substantial these are, and how likely they are to happen.

5.25.3 The training company shall notify the ICO of any personal data breaches, without undue delay but no later than 72 hours after becoming aware of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the candidate.

Note 1: The ICO has published a self-assessment to help organisations determine if they need to report a breach.

5.25.4 The training company shall provide the ICO with the following information regarding any data breach at the time of reporting the issue, if possible. If it is not possible, the information can be provided in phases, without undue delay: -

1. describe the nature of the personal data breach including, where possible, the categories and approximate number of candidates concerned, and the categories and approximate number of personal data records concerned.
2. the name and contact details of the DPO, or other contact point, where more information can be obtained.
3. the likely consequences of the personal data breach
4. the measures taken, or proposed to be taken, by the training company to address the personal data breach, including, where required, measures to mitigate its possible adverse effects to the candidate to minimise the impact of the data breach.

5.25.5 The training company shall document any personal data breaches, including the facts relating to the data breach, its effects and remedial actions taken to mitigate future incidents.

Communication of a personal data breach to the data subject

5.26 Article 34 Communication of a personal data breach to the data subject

5.26.1 The training company shall notify the candidate, without undue delay, of any personal data breach that is likely to result in a high-risk to their rights and freedoms.

5.26.2 The training company shall provide the candidate with the following information in clear and plain language: -

1. The name and contact details of the DPO, or other contact point, where more information can be obtained.
2. The likely consequences of the personal data breach
3. The measures taken or proposed to be taken by the training company to address the personal data breach, including, where required, measures to mitigate its possible adverse effects to the candidate.
4. Advice about the steps they can take to protect themselves in the event of a breach, e.g., changing passwords to a strong unique password, looking out for phishing emails, checking for any fraudulent activity on accounts and signing up to a credit monitoring service.

Prior Consultation

5.27 Article 36 Prior Consultation

5.27.1 If a DPIA, conducted under 5.3, indicates the processing would result in a high-risk, and the training company cannot take measures to reduce that risk, the training company shall consult with the ICO prior to processing the data.

5.27.2 If prior consultation with the ICO is required, the training company shall send the following information to dpiaconsultation@ico.org.uk,:-

1. where applicable, the respective responsibilities of the training company and processors involved in the processing, in particular for processing within a group of undertakings
2. the purposes and means of the intended processing
3. the measures and safeguards provided to protect the rights and freedoms of the candidates
4. where applicable, the contact details of the Data Protection Officer.
5. the Data Protection Impact Assessment, in accordance with 5.3.6.
6. any other information requested by the ICO.

5.27.3 The training company shall **not** proceed with processing the candidate data, in accordance with 5.27.2, until the ICO has provided a written response advising whether the risks are acceptable, or whether further action is needed.

General principle for transfers

5.28 Article 44 General principle for transfers

5.28.1 The training company shall not transfer candidate personal data to a separate organisation located outside of the UK, i.e., a restricted transfer, unless they meet the requirements of criteria 5.28.4-5.28.7.

Note: If the candidate data being transferred is anonymised this section does not apply.

5.28.2 If the training company is making a restricted transfer, the training company shall assess whether they can achieve their aims without sending the candidate data, or anonymising the data before transfer.

5.28.3 If the candidate data cannot be anonymised and the restricted transfer must take place, the training company shall determine if the transfer is covered by the UK adequacy regulations.

Note: The UK adequacy regulations are explained in further detail on the ICO site

5.28.4 If the transfer of candidate data does not meet the criteria of 5.28.3 e.g. the country is not covered by adequacy regulations, the training company shall conduct a transfer impact assessment to determine if they may rely on additional safeguards outlined in Article 46 – transfers subject to safeguards, such as:-

1. binding corporate rules
2. standard data protection clauses adopted by the ICO
3. an approved code of conduct
4. an approved certification mechanism
5. contractual clauses authorised by the ICO

5.28.5 If the training company identifies a safeguard to make the restricted transfer under 5.28.4, it shall conduct a further assessment to determine if any laws or practices in the recipient third country may impinge on the effectiveness of the safeguard.

5.28.6 The training company shall document this due diligence and, if it is found that the additional safeguard will not afford an equivalent level of protection as the UK, the training company shall consider the supplementary measures that can be used to provide the equivalent level of protection as the UK.

5.28.7 If the transfer of candidate data does not meet any of the criteria in 5.28.4 or 5.28.5, the training company shall consider whether the restricted transfer is covered by one of the exceptions below:-

1. Has the candidate given their explicit consent to the restricted transfer?
2. Do they have a contract with the individual? Is the restricted transfer necessary for them to perform that contract?
3. They need to make the restricted transfer to establish if they have a legal claim, to make a legal claim or to defend a legal claim.
4. They are making a one-off restricted transfer and it is in their compelling legitimate interests.

Note: Each exception has certain conditions that must be met by the training company before relying on that exception, these are outlined on the ICO site.

5.28.8 The training company shall record and maintain a record of all candidate data transfers, in accordance with criteria 5.28 to demonstrate compliance with UK GDPR.

5.28.9 If the training company does not meet any of the conditions in criteria 5.28.2-5.28.7, the restricted transfer of candidate data cannot take place.