LATEST REVISION RECORD						
Revision	Issue	Date	By	Change Details	Approved by	Date

SCOPE

The scope of this procedure applies to how Assent Group handles personal data, with specific procedures that relate to the protection of data from employees, clients and service providers.

PURPOSE

Fundamentally data protection legalisation is about treating individuals' personal data with care, to ensure it is processed in a way that will not cause any harm, damage or distress to the individual. Personal data held by Assent Group from internal Assent Group employees and personal data supplied to Assent Group from clients, approved suppliers, approved contractors as 3rd party data, and any other form of personal data that may be received by Assent Group in the course of undertaking business activities, should be protected from accidental loss, and unauthorised access.

RESPONSIBILITIES

- CEO / Board of Directors
- HR Department
- Finance Department
- Employees

UK LEGISLATION

Data Protection Act 2018

UK GUIDANCE

N/A

ISO CLAUSES

Standard	Clause
ISO 9001	7.5

DEFINITIONS

Data	is information, which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this document include all living individuals about whom we hold personal data
DPRP	Data Protection Responsible Person – nominated Group officer responsible for primary Data Protection contact and control
Personal Data	means data relating to a living individual (data subject) who can be identified from that data (or from that data and other information in our possession). Personal Data can be factual (for example, a name, address, date of birth, identification number, location data, an online identifier) or one or more factors specific to that person, their actions, genetic material, mental health, economic status, cultural or social identity
Processing	is any activity that involves use of the data whether or not by automated means. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including: organising, amending, retrieving, using (adaption or alteration), disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties
Special Categories of Personal Data	includes, information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.
Data Portability	refers to the ability to move, copy or transfer data easily from one database, storage or IT environment to another. Portability describes the extent to which the data can easily be ported between different computers and operational environments

GDPR PROCEDURE

Collected, Held and Processed Personal Data

Our employment checks align with regional baseline security checks such as the UK Government Baseline Personnel Security Standard. We collect personal information about employees through the application and recruitment process, either directly from candidates or employment agencies. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

Personal data is collected at induction stage of employment during which stage consent is also obtained for further usage, storage and sharing with approved bodies.

Annual checks on data accuracy are also made, however employees can update their personnel files at any time via the HR Department. Where changes are identified, Assent Group external data handlers shall be informed.

The following table gives some examples of the type of personal data collected, held, and processed by Assent Group.

Business Function that Holds the Data	Categories of Personal Data	Personal Data Storage Location
Finance & HR	Income Tax and National Insurance details	Payroll
HR	Nationality (Immigration status and permission to work documents)	Recruitment/Personnel/Security
Facilities	CCTV footage	Security
HR	Health & Medical Records	Recruitment/Personnel
Training	Personnel and training files	Employee management
Finance	Retirement Benefits Schemes	Records of all notifiable events i.e. enrolments, adjustments or incapacity.
Operations	Clients	Access for site visits
Training (Incl. external clients)	Personal details including name, title, D.O.B, address, telephone number, personal email address, National Insurance number.	Training course requirements
Finance	Pensioners' records	Payroll
HR	Interviewee data	Recruitment/Personnel

Assent Group will only use personal information when the law allows it. Most commonly, we will use personal information in the following circumstances:

- Where we need to complete an employment contract
- Where we need to comply with a legal obligation
- Where it is necessary for legitimate interests pursued by us or a third party and interests and fundamental rights of an individual do not override those interests

We may also use personal information in the following situations, which are likely to be rare:

- Where we need to protect an individual’s interests (or someone else's interests)
- Where it is needed in the public interest

3rd party data held by Assent Group is required on a contractual basis as without such information we would be unable to perform site-based testing and inspections or deliver requested training. The following table gives some examples of the type of personal data supplied to Assent Group:

Business Function that Holds the Data	Categories of Personal Data	Personal Data Storage Location
Contracts	Name, Address, phone number and business email	DCC Electronic Project Files
Training	Name, Address, phone number and business email	Electronic Training Files

Data Security - Transferring Personal Data and Communications

Assent Group shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

i. All Assent Group emails are handled within the Microsoft 365 environment and are archived and access controlled in accordance with best practice security policies.
ii. Any Assent Group devices containing personal data must be encrypted using the platform's full disk encryption.
iii. Sending of personal data outside of the secured Assent Group domain must only be done in a secure fashion. Any non- Assent Group parties receiving that data must have an in-date data sharing agreement in place.
iv. Hard copy project files that are utilised on site must not be left unattended at any time.

Data Security - Storage

Assent Group shall ensure that the following measures are taken with respect to the storage of personal data:
i. All electronic devices (company mobile phone, mobile tablets and desk top computer) must be secured using passwords set by the individual user. The password must adhere to Assent Group password protocol In place at the time.
ii. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely.
iii. All personal data stored electronically is backed up in line with Assent Group internal procedures as stated in Section C – Records and Data Control.
iv. Personal data utilised for the purposes of site contacts must only be stored on mobile devices (laptops, tablets, and smartphones), which are encrypted, and password protected.
v. No personal data should be transferred to any device personally belonging to an employee or an external party, unless approved by a member of the senior leadership team. Monitoring of this is relatively impossible and relies on both the training and integrity of the member of staff controlling that data.

Data Security – Use of Personal Data

Assent Group shall ensure that the following measures are taken with respect to the use of personal data:

i. No personal data may be shared informally and if an employee, ex-employee, agent, sub-contractor, or other party working on behalf of Assent Group requires access to any personal data that they do not already have access to, such access should be formally requested from the DPRP.
ii. No personal data may be transferred to any employees, ex-employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of DPRP.
iii. All service providers who are required to hold personal employee data must complete a GDPR Data Sharing Agreement
iv. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, ex-employees, agents, sub-contractors, or other parties at any time.
v. If a computer is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.
vi. Where personal data held by Assent Group is used for marketing purposes, it shall be the responsibility of DPRP to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

Data Security – IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

i. All passwords used to protect personal data should be in line with Assent Group password protocols. Checks on mobile tablet passwords may be conducted during technical audits. Checks on office-based PC's may be conducted during internal audits.
ii. Under no circumstances should any passwords be written down or shared between any employees, ex-employees, agents, contractors, or other parties working on behalf of Assent Group, irrespective of seniority or department. If a password is forgotten, it must be reset via IT support channels.
iii. All software shall be kept up-to-date. Assent Group's IT Service Provider shall be responsible for installing all major security-related updates, however standard software updates are the responsibility of the individual issued with IT equipment.
iv. No software may be installed on any company-owned computer or device without the prior approval of the Assent Group IT team.

Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

i. All employees, critical suppliers, contractors, or other parties working on behalf of Assent Group shall be made fully aware of both their individual responsibilities and the company's responsibilities under the GDPR.
ii. Only employees, critical suppliers, contractors, or other parties working on behalf of Assent Group that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data.
iii. All employees, critical suppliers, contractors, or other parties working on behalf of Assent Group handling personal data will be appropriately trained to do so.

Transferring Personal Data to a Country Outside the EEA

Currently Assent Group are not required, through current working conditions / contracts to transfer personal data to countries outside of the EEA. Should this element change in the future, amendments will be made to this procedure.

Data Breach Notification

i. All personal data breaches must be reported immediately to the DPRP.
ii. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the DPRP must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
iii. Data breach notifications shall include the following information irrespective of any requirement to notify ICO:
    a. The categories and approximate number of data subjects concerned;
    b. The categories and approximate number of personal data records concerned;
    c. The name and contact details of Assent Group's DPRP
    d. The likely consequences of the breach;
    e. Details of the measures taken, or proposed to be taken, by Assent Group to address the breach including, where appropriate, measures to mitigate its possible adverse effects.
    f. Recording of decision and reasoning for ICO notification (or not).

DATA RETENTION AND CONSENT

Assent Group shall ensure that upon employment, consent is obtained for the use and storage of personal data. The consent must include the use of third party service providers that carry out essential duties on behalf of the company, such as the company pension provider, medical insurance and vehicle insurance providers.

Where Assent Group obtain third party data, it is the responsibility of the data controller (client) to ensure consent has been obtained and received and that they inform Assent Group of all data changes as per the data sharing agreement.

SUBJECT ACCESS REQUESTS

Data subjects have the right to find out whether the company collects, holds, or processes personal data about them, the right to obtain a copy of any such data, and certain other supplementary information. The right of access is designed to help data subjects to understand how and why Assent Group use their data, and to check that we are doing so lawfully.

Upon receipt of a Subject Access Request, the HR Department and the complaints team will review the request. The requester is obliged to provide Assent Group with specific data parameters and any specific information being sort. The requester is reminded that data is only retained for the periods specified within the retention procedure and certain emails may not be supplied should they reference other personnel.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Ideally, a DPIA should be performed annuallyas part of the GDPR audit review, however new DPIAs should be conducted as part of the PQQ process for critical suppliers, for clients who supply personal information over and above contact details (name and company email) or where contractually specified.

1. Does the business need to carry out a DPIA for this project/process?
2. Describe how the data will be gathered/processed – in particular, consider the nature, scope, context and purposes of the processing.
3. Consider if external advice is needed to deal with the risk appropriately.
4. Assess the necessity and proportionality of gathering/processing the data, this includes any issues of legal compliance that these actions bring up.
5. Identify and assess risk of gathering/processing the data, especially if those risks affect individuals. To assess the level of risk, consider the likelihood and the severity of harm resulting from that risk. High risk events are not just those that cause serious harm but can be those which cause little harm individually and occur frequently.
6. Identify any required measures to mitigate the identified risk.
7. Sign off and record the outcomes of any decisions made.
8. Integrate these outcomes into the overall business plan/objectives.
9. Keep these outcomes under review so that they remain applicable.

When a new service provider is put forward via Assent Group PQQ Procedure, they will be required to complete a GDPR Data Sharing Agreement. Dependant on the information to which the supplier has access to, they may also be required to complete a Non Disclosure Agreement, but this will be determined via the Data Protection Impact Assessment.

NON DISCLOSURE AGREEMENT

A Non-Disclosure Agreement is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain defined purposes. The NDA is a high level confidentiality agreement in comparison to the Data Sharing Agreement as it covers a greater level of access, whereas the Data Sharing Agreements centre around certain specific types of data, normally associated with the service being delivered.

Typically, should a supplier need to have access to all of Assent Group policies, procedures, training, audit, test and inspection data, they will be required to sign a Non-Disclosure Agreement.

RECORDING

All GDPR completed documentation is held by the HR Department.

COMMUNICATION OF PROCEDURE

Communication of this Procedure is via the Integrated Management System.

MONITORING & REVIEWING

The GDPR Procedure will be reviewed by a responsible person in the following circumstances:

- If a data breach has occurred
- Because of legislation or regulatory change
- If requested by a Director
- If requested by an accreditation body, client or any other stakeholder
- Any other relevant requirement

RESPONSIBILITIES

CEO / Board of Directors	• Promote a positive approach to GDPR compliance throughout the company. • Implement the Company GDPR Procedures. • Ensure the Procedure is reviewed regularly with the GDPR Compliance team as necessary. • Make adequate financial provision for adhering the GDPR and general Cyber Security IT requirements.
HR Department	• The HR Department is responsible to obtaining and maintaining consent records. • The HR Department assisted by the Finance Department are responsible for ensuring all Assent Group employee details are kept up to date with third party service providers. • HR with the assistance of the Data Protection Responsible Person will undertake system audits on an annual basis to determine compliance.
Finance Department	• The Finance Department assisted by the HR Department are responsible for ensuring all Assent Group employee details are kept up to date with third party service providers.
Employees	• All employees are responsible for the security of their designated IT systems.