GENERAL DATA PROTECTION POLICY

Version:	Rev 04	
Date of version:	13/04/2026	
Created by:	Ian Inman (Moore Kingston Smith)	
Approved by:	 Karolina Zickyte | QA Manager	 Tony Cassidy | Commercial Director
Confidentiality level:	Everyone	
Review date:	April 2028	

INTRODUCTION

This policy sets out the approach taken by Essex Services Group (ESG) when it collects, stores, uses, or otherwise handles personal data.

Under the principle of accountability, ESG is responsible for demonstrating compliance with the requirements of the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018). This policy, and the wider policy framework, form a core part of demonstrating compliance with that principle.

Scope

This policy applies to employees, board members, contractors, volunteers, nonexecutive directors and anyone who processes personal data on behalf of ESG. This policy applies to all processing of personal data undertaken by ESG.

ROLES & RESPONSIBILITIES

ESG is the Data Controller.

The board of directors are accountable for ensuring that ESG complies with its obligations under data protection law, as well as promoting and fostering a positive culture and proactive approach to data protection compliance.

Senior Management are responsible for ensuring that any personal data processed as part of the functions they have ownership and responsibility for is processed in compliance with the requirements of data protection law and the requirements of this policy.

Board of Directors are responsible for providing senior level oversight of data protection risks, as well as providing direction on how those risks are to be managed. This includes agreeing mitigation and remediation plans and overseeing their implementation. In addition, they will report to the **board of directors** on data protection risks and performance.

Data Protection Officer is responsible for providing advice, guidance, and support to ESG relating to compliance with applicable data protection legislation, as well as risk assessing and supporting with the management and investigation of personal data breaches.

All Staff are responsible for ensuring that they have read and understood this policy, that they have completed any mandatory data protection training and that they handle personal data in compliance with the requirements of data protection law and this policy.

DATA PROTECTION PRINCIPLES

This section sets out the measures ESG will put in place to comply with the data protection principles. The principles are set out in Appendix 1.

Lawful & Transparent Processing: To comply with this principle, ESG will ensure that it has the following measures in place:

- **Privacy Notices:** ESG will ensure that it has a comprehensive privacy notice published on its website (www.esglimited.com/policies-accreditations) which contains all information required under data protection

law. Where necessary all data capture points will contain short form privacy statements containing information about particularly intrusive activities such as direct marketing, data sharing or surveillance and a link to the full privacy notice.

- **Lawful Processing:** ESG will ensure that all personal data will be handled in accordance with common and statute law. It will ensure that it has an appropriate lawful basis for handling personal data as set out under data protection law. The lawful basis will be documented as part of the Privacy Policy.

- **Purpose Limitation:** ESG shall ensure that personal data shall not be collected, stored, and used unless there is a legitimate reason to do. The purposes for collecting, storing, and using personal data shall be documented in the Privacy Notice.

- **Data minimisation:** Data collection channels will be kept under review to ensure that only personal data which is strictly necessary is collected.

- **Data accuracy:** ESG will implement technical and organisational measures to ensure that all personal data it handles will be kept accurate and up to date.

- **Storage Limitation:** ESG will ensure that personal data is not retained for longer than it is required. Records shall be documented as part of a retention and disposal schedule along with defined retention periods. Retention periods must be based off either a legal requirement to retain the personal data or a legitimate business need to retain it. If both apply, then the personal data shall be kept for the longest period of the two.

- **Data Security:** ESG shall adopt measures which afford an appropriate level of security for the personal data. In particular ESG shall:

- Document the technical and organisational security measures it has in place to protect the personal data.

- Conduct a risk assessment of the personal data it collects and uses as part of determining what an appropriate level of security should be. These assessments should factor in the measures available and the costs of implementing those measures against any risks to individuals that may arise if the personal data is lost, stolen, or otherwise compromised.

- **Accountability:** ESG shall adopt a framework of policies, including this Data Protection Policy, covering key aspects of data protection compliance. These policies shall include as a minimum personal data breach management, handling individuals' rights, records retention and disposal and information security.

- In addition, ESG shall ensure that all staff undertake data protection training which shall be refreshed annually. Staff who require training in specific aspects of data protection, such as handling individuals' rights, shall be identified and appropriate training shall be provided and periodically refreshed.

DATA SUBJECTS' RIGHTS

ESG shall ensure that it handles requests made by individuals exercising their data protection rights in compliance with data protection law. A summary of the rights is set out in Appendix 1.

In particular, ESG shall adopt policies and procedures setting out how individuals rights are to be handled and by whom and it shall ensure that those who are responsible for handling requests are properly trained.

DISCLOSURE OF DATA

ESG will implement a data sharing policy setting out its approach to the disclosure of personal data. In any event, it will ensure that personal data will only be disclosed if:

- Any request clearly sets out the personal data being requested or required for disclosure.
- The disclosure is being made for a legitimate and lawful purpose.
- The request was made in writing.

DATA TRANSFER

A data transfer occurs whenever personal data is either stored at rest outside of the UK or it is made accessible to third parties (including members of the same corporate group) who are based outside of the UK. This includes where a supplier does this on our behalf.

ESG shall not transfer personal data outside of the UK unless:

- The country to which the personal data is being transferred is subject to a finding of adequacy by the UK Government. A full list of those countries is available on the ICO website here.

- If there is no finding of adequacy, an International Data Transfer Agreement (IDTA), or the Standard Contractual Clauses, including the UK Addendum, must be put in place.

DISCIPLINARY ACTION

All staff are to adhere to this policy and its intent. Failure to do so may result in disciplinary action being taken. Such action might include written or verbal warnings or instant dismissal in circumstances that amount to gross misconduct.

ESG reserves the right to take appropriate disciplinary action against contractors and self-employed service providers who fail to comply with this policy. Such actions include, but are not limited to, the termination of any contract with ESG.

Any breaches may also need to be reported to the Information Commissioner's Office (ICO).

APPENDIX 1 – PRINCIPLES & RIGHTS

Data Protection Principles

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Personal data shall be collected (whether from the data subject or otherwise) for specified, explicit and legitimate purposes and not further processed, by or on behalf of the Controller, in a manner that is incompatible with those purposes.

Personal data shall be adequate relevant and limited to what is necessary in relation to the purposes for which they are processed.

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Personal data shall be kept in a form which permits identification of data subject for no longer than is necessary for the purposes for which they are processed.

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organisational measures.

Individuals' Rights

Individuals have the following rights under the UK GDPR:

- **Right to be informed:** Individuals have the right to be provided with certain information relating to the processing of their personal data. This includes who is collecting and using it, what it will be used for, who it will be shared with and how long it will be retained for.
- **Right of access:** Individuals are entitled to request access to their personal data which we hold. This includes being entitled to a copy of that personal data.
- **Rectification & Erasure:** Individuals are entitled to have inaccurate personal data about them rectified. They are also entitled, in certain circumstances, to have their personal data erased.
- **Right to restriction of processing:** Individuals have the right to request that we restrict or limit what we do with their personal data.
- **Right to data portability:** Individuals have the right, in certain circumstances, to require us to transfer personal data we hold about them to another organisation.
- **Right to object to direct marketing:** Individuals have the right to object to us using their personal data for direct marketing activities including profiling.
- **Right to object to specific processing:** Individuals have the right to object to specific uses of their personal data, including profiling.