

General Data Protection Policy

Introduction

Seaham Safety Services Ltd. (the company) needs to gather and use certain information about individuals, including clients, business contacts, employees and other people and organisations the company has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law. This data protection policy ensures Seaham Safety Services Ltd. complies with data protection law and follows good practice, additionally:

- It protects the rights of staff, customers, clients and partners
- Is open about how the company stores and processes individual's data
- It protects itself from the risks of a data breach

1.0 Scope

This policy applies to all personal data created or received during Seaham Safety Services Ltd. business in all formats, of any age. Personal data may be held or transmitted in paper, physical and electronic formats or communicated verbally in conversation or over the telephone.

2.0 Data subjects

These include, but are not confined to: prospective clients, clients, business contacts, contractors, professional contacts, training delegates, people attending meetings, employees and other people and organisations the company has a relationship with or may need to contact.

3.0 Users of personal data

The policy applies to anyone who obtains, records, can access, store or use personal data during their work for the company. Users of personal data include employees, training delegates, meeting attendees, contractors, suppliers, professional partners and visitors.

4.0 Lines of responsibility

4.1 Users of company information:

All users of company information are responsible for:

- Completing relevant awareness provided by the company to support compliance with this policy.
- Taking all necessary steps to ensure that no breaches of information security result from their actions.
- Reporting all suspected information security breaches or incidents promptly to the directors so that appropriate action can be taken to minimise harm.
- Informing the company of any changes to the information they have provided to the company in connection with their employment.

4.2 Individual responsibilities

4.2.1 The Managing Director, Mr. Gordon MacPherson Snr. has ultimate accountability for the company's compliance with data protection law.

4.2.2 Director, Mr. Gordon MacPherson Jnr. has senior management accountability for information governance as the Data Protection Officer.

4.0 Lines of responsibility (Continued)

4.3 Data Protection Officer (DPO)

The DPO is responsible for:

- Informing and advising company managers and all members of staff of their obligations under data protection law.
- Promoting a culture of data protection, e.g. through training and awareness.
- Reviewing and recommending policies, procedures, standards, and controls to maintain and demonstrate compliance with data protection law and embed privacy across the company.
- Advising on data protection impact assessment and monitoring its performance.
- Monitoring and reporting on compliance to the Managing Director.
- Maintaining records of activities.
- Providing a point of contact for data subjects regarding all issues related to their rights under data protection law.
- Investigating personal data breaches, recommending actions to reduce their impact and likelihood of recurrence.

The role may occasionally be filled by the Company Manager during the DPO's absence for oversight of these duties.

4.4 Right to be informed and privacy information

All individuals the company has a relationship with, or potential relationship, have the right to be informed about the collection and use of their personal data. This is a key transparency requirement of the Seaham Safety Services Ltd. (the company) policy under the GDPR.

The company will provide individuals with information including our purposes for processing their personal data, our retention periods for personal data and who it will be shared with. We will provide privacy information to individuals at the time we collect their personal data from them.

If we obtain personal data from other sources, we will provide individuals with privacy information within a reasonable period of obtaining the data. Circumstances when we will not provide people with privacy information includes when an individual already has the information or if it would involve a disproportionate effort to provide it to them by the company.

The information the company provides will be concise, transparent, intelligible, easily accessible, and use plain language. The company will regularly review, and where necessary, update our privacy information and bring any new uses of an individual's personal data to their attention before we start the processing. Individuals will be provided with the following privacy information:

- The name and contact details of our company.
- The contact details of our Data Protection Officer, when applicable.
- The purposes of the processing and the lawful basis for the processing.
- The legitimate interests for the processing.
- The categories of personal data obtained (where it is not obtained from the individual).
- The recipients or categories of recipients of the personal data (i.e. training awarding bodies).
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent, where applicable.
- The right to lodge a complaint.
- The source of the personal data (where it is not obtained from the individual).

4.4 Right to be informed and privacy information (Continued)

We provide individuals with privacy information at the time we collect their personal data and if we obtain personal data from a source other than the individual, we provide them with privacy information:

- Within a reasonable of period of obtaining the personal data and no later than one month;
- If we plan to communicate with the individual, at the latest, when the first communication takes place; or
- If we plan to disclose the data to someone else, at the latest, when the data is disclosed.

We provide the information in a manner that is concise, transparent, intelligible, easily accessible and uses clear, plain language.

We regularly review and, where necessary, update our privacy information and if we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing. When providing our privacy information, we may use a combination of techniques, including a layered approach, dashboards, just-in-time notices, icons and mobile and smart device functionalities.

Information we need to provide	Personal data collected from individuals	Personal data obtained from other sources
Name and contact details of the company	✓	✓
Name and contact details of our Data Protection Officer, when applicable	✓	✓
The purposes of the processing and the lawful basis for the processing	✓	✓
The categories of personal data obtained	✓	✓
The legitimate interests for the processing	✓	✓
The recipients or categories of recipients of the personal data	✓	✓
The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint	✓	✓
The source of the personal data	✓	✓

4.4 Right to be informed and privacy information (Continued)

We actively provide privacy information to individuals and meet this requirement by putting the information on our website and by making individuals aware of it and giving them easy access to it. When collecting personal data from individuals, we will not provide them with information they already have. When obtaining personal data from other sources, we will not provide individuals with privacy information if:

- The individual already has the information.
- Providing the information to the individual would be impossible.
- Providing the information to the individual would involve a disproportionate effort.
- Providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing.
- We are required by law to obtain or disclose the personal data.
- We are subject to a legal obligation of professional secrecy that covers the personal data.

4.5 Lawful basis for processing personal data

The company's lawful basis for processing personal data under GDPR includes:

- **Consent:** An individual has given the company clear consent to process their personal data for a specific purpose.
- **Contractual:** Processing an individual's personal data required to fulfil a contract between the company and them.
- **Legal Obligation:** The company needs to process personal data to comply with the law.
- **Legitimate Interests:** It is in the company's and the person's legitimate interests to keep or use their personal data.

Seaham Safety Services Ltd. will use the following measures to demonstrate compliance with the law:

- Implementation of internal policies to demonstrate our compliance, including internal audits and reviews of HR policies.
- Maintenance of comprehensive documents, where appropriate, of processing activities to ensure all relevant data is appropriately processed and carefully documented.
- Appointment of a Data Protection Officer (DPO).
- Implementing measures such as data minimisation to ensure no more documentation than is required is collected and held.

The information we will collect and process includes: records of consent from data subjects, records of processing activities under our control and documented processes for protecting personal data, i.e. an information security policy.

4.5 Lawful basis for processing personal data (Continued)

An individual's right to be informed requires the company to include information about our lawful basis for processing their data. This takes the form of a privacy notice in all places where an individual can provide their personal data to the company, for example:

- On our company website when any individual signs up for our newsletter, bulletin or when someone makes an enquiry about our training and/or safety services.
- On the telephone or in person when someone books a training course or other service.

The information we will provide includes:

- Our intended purposes for processing the personal data.
- The lawful basis for processing the data.

4.6 Consent

Consent must be freely given, and the company will provide people with genuine ongoing choices and control over how we use their data. Consent will cover the controller's name, the purposes of the processing and the types of processing activity. Consent requests will be concise, easy to understand and user-friendly, and require a positive action to opt in. They will be explicit and not bound up with other terms and conditions. There is no set time limit for consent, how long it lasts will be dependent on the context of the information. The company will review and refresh consent as appropriate. The GDPR documents will include:

- A procedure for conducting a privacy audit.
- Templates for creating clear and accurate privacy notices.
- Data breach notification process and procedures.
- Subject access request templates and procedures.
- Consent form templates.
- Data protection impact assessment templates and procedures.
- Important information security policies and procedures to keep your information secure.