**

**Seabrook Group of Companies**

(Seabrook Holdings Ltd &/or Subsidiary Companies)

**GDPR & DATA PROTECTION**

 **Policy Document**

version 1 / date 19th July 2018

 **Seabrook Group of Companies**

**GDPR & Data Protection Policy**

**Data Processing**

As part of its day-to-day operation, and in order to carry out its duties as a provider of Warehousing & Logistical Services and, as an employer, Seabrook Group (hereafter known as SGL) collects and processes a wide range of personal information, or data, about certain individuals. These include the following:

- past, present and future employees

- past, present and future customers

- past, present and future service providers

SGL, shall take all reasonable steps to collect and process data in accordance with this Policy.

Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data. In this Policy any reference to ‘customers’ includes current, past or prospective customers. Any reference to ‘staff’ also includes current, past or prospective staff. Any reference to service providers also includes current, past or prospective service providers.

This personal information may be held by SGL on paper or in electronic format in its capacity as “Data Controller”. SGL needs to collect and process data in order to fulfil its legal rights, duties and obligations, including those required to form contracts with customers, staff and service providers.

SGL is committed to being transparent about how it handles personal information, to protecting the privacy and security of personal information and to meeting its data protection obligations under the General Data Protection Regulation (“GDPR”) and the Data Protection Act 2018 (“DPA 2018”).

**General Data Protection Regulation (GDPR)**

From 25 May 2018 the General Data Protection Regulation (GDPR) replaced the previous Data Protection Act (DPA). The UK’s decision to leave the EU will not affect the GDPR.

The GDPR applies to ‘controllers’ and ‘processors’. The ‘controller’ says how and why personal data is processed and the ‘processor’ acts on the controller’s behalf. Both are required to maintain records of personal data and processing activities.

Under the GDPR, SGL has an increased responsibility to ensure that all information, regardless of the form in which it’s kept, is managed in the right way to comply with new regulations.

**Data Controller**

The Group IT Director, Mr Stuart Seabrook , is the Data Controller for SGL and ensures that all data is processed in compliance with this Policy and with the requirements of the General Data Protection Regulation.

The Group IT Director oversees:

• Ensuring that personal data is kept safe and secure.

• Responding to complaints and Subject Access requests.

• Cooperating with the supervising authority (ICO).

• Not using or processing personal data other than for the intended use.

• Ensuring that personal data is collected for legitimate use.

• Ensuring that personal data is kept up to date and not kept for longer than is necessary.

• Paying, or appealing against, any fines.

**Monitoring the collection of personal data**

SGL has appointed a Compliance Officer, Mr Mike Isbell, to oversee compliance with the GDPR.

The Compliance Officer is responsible for:

* Overseeing the day-to-day use of personal data
* Advising, training and informing staff about the GDPR.
* Ensuring that we are compliant with the GDPR.
* Ensuring that data is processed legally and fairly.
* Documenting all systems used to process personal data.
* Recording any breaches of data privacy.

**The Information Commissioner’s Office**

The Information Commissioner’s Office (ICO) is the UK’s independent body set up to uphold information rights. The ICO’s role is to uphold information rights in the public interest. It is a legal requirement that every organisation that processes personal information is registered with the ICO. The ICO monitors registered bodies’ storage and handling of personal data.

**Data protection principles**

Under the GDPR, there are eight data protection principles that SGL must comply with. These provide that the personal information we hold must be:

1.Processed lawfully, fairly and in a transparent manner. 2. Collected only for legitimate purposes that have been clearly explained and, not further processed in a way that is incompatible with those purposes. 3. Adequate, relevant and limited to what is necessary in relation to those purposes. 4. Accurate and, where necessary, kept up to date. 5. Retained in a form that permits identification for no longer than is necessary for those purposes. 6. Processed in accordance with a data subject’s rights. 7. Processed in a way that ensures appropriate security of the data. 8. Kept in the UK and not transferred abroad.

 SGL is responsible for, and must be able to demonstrate compliance with, these principles.

**Processing of Personal Data**

The GDPR requires that personal data shall be:

* processed lawfully, fairly and in a transparent manner in relation to individuals
* collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, historical research purposes shall not be considered to be incompatible with the initial purpose.
* adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.
* accurate and, where necessary kept up to date, every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purpose for which they are processed, are either erased or rectified without delay.
* kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, historical research or statistical purpose subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the freedoms and rights of individual.
* processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

**Purpose for collecting and storing personal information**

SGL will only use personal information when the law allows us to. These are known as the ‘legal basis for processing. We will use personal information in one or more of the following circumstances:

* where we need to do so to take steps to enter into a contract
* where we need to comply with a legal obligation (HMRC)
* where it is necessary for our legitimate interest (or those of a third party)

The purpose for which we are processing, or will process personal information include (but are not limited to);

Customers;

* undertake Due Diligence / Compliance investigations in order to meet HMRC ‘FITTED’ criteria
* maintain ongoing customer relationships and communication related to business requirements
* assist SGL to undertake financial reconciliation’s related to transactions
* provide references for historic/potential customers

Staff;

* manage the recruitment process of staff and assess suitability for employment or engagement through the collection of cv’s, references and referrals
* administer the contract we have entered into with individuals
* utilise biometric data for the purpose of recording attendance in the workplace
* maintain and update records of employment and engagement terms
* comply with statutory and/or regulatory requirement and obligations, e.g. checking your right to work in the UK.
* ensure compliance with your statutory employment rights
* ensure effective HR personnel management and business administration
* plan for career development and succession
* ensure compliance with Income Tax & NI requirements
* enable us to establish, exercise or defend legal claims

Service Providers & General

* maintain ongoing supplier relationships and communication related to business requirements
* provide references for historic/potential suppliers
* undertake Due Diligence investigations in order to ensure that they meet the criteria to supply goods and service either directly to us or to our customers
* for security purposes, including the collection of images on CCTV in accordance with SGL security policy
* assist in the reasonable forecasting and statistical analysis as required for effective management planning
* enable legitimate outside bodies such as HMRC to monitor performance, legality of transactions and assist with incidents as appropriate
* where appropriate, to obtain legal or professional advice

We may share personal information with third parties where it is necessary to take steps to request to enter into a contract, where we need to comply with a legal obligation, or where it is necessary for our legitimate interests (or those of the third party).

 **What types of personal information does SGL collect?**

Personal information is any information about an individual from which that person can be directly or indirectly identified.

SGL collects, uses and processes a range of personal information. This includes (as applicable);

* contact details, including names, addresses, telephone number, e-mail addresses, photographic id’s etc.
* personal information about a prospective or future member of staff as included in a cv, Application Form, covering letter or interview notes.
* references from past/current employers.
* information about a staff members right to work in the UK driving licences/passport/ID Cards
* copies of qualifications and other relevant certifications
* bank details and other relevant financial information for staff payroll
* information about staff members salary level, including benefits and pension entitlements

The GDPR refers to sensitive personal data as “special categories of personal data”. SGL may also collect, use and process the following special categories of personal information including (as appropriate)

* whether or not there is a disability for which the company needs to make reasonable adjustments
* detailed information about and individuals health
* details of an individuals next of kin
* information about criminal convictions and offences

**How do we collect personal information?**

SGL collects personal information either directly from the data subject, or from a third-party such as an employment agency. We may also collect personal information from other external third parties such as former employers to obtain references.

SGL , as is the nature of the business may acquire information related to potential ‘new business’ through various networking and other corporate activity where personal data is shared and regarded as ‘legitimate business’ within the GDPR framework.

**Where and how we store personal information?**

Personal information may be stored in different places, including on an ‘application record’, in the Groups HR Management system (Croner) and, on other IT systems used in the undertaking of normal business practice. All information is kept safe and secure either through locked filing cabinets in secure areas or through password-protected (and restricted) access to database servers.

**SGL stores data as follows;**

**Manual filing systems**

Each customer has a secure file within a locked filing cabinet located in the Compliance Department at SGL, in which documentation is held for transactional reference and, in order to meet the compliance requirements of HMRC.

Hard copies of certain data-gathering official forms, such as company formation, VAT registration and other general information.

Each staff member has a secure file within a locked filing cabinet located in the HR Department office in which documentation is held for possible future reference. Hard copies of certain data-gathering official forms such as employment contract, salary details, original employment forms, medical records/absence & attendance are kept together along with other general information

**Electronic Databases**

Each customer will have personal information stored electronically on one or more of SGL’s secure databases –

Vision – Warehouse Management System. HMRC and use for stock control and movement

BoxTop – Freight Forwarding and logistics system

Sun Accounts – Financial Management System

Bensoft – Freight Forwarding System

Each Staff member will have personal information stored electronically on SGL’s secure HR Management System – Croner Simplify

**Cloud Based Storage**

Some Customer files are stored in cloud-based folders utilising the DropBox service.

In this instance, this provider has assured us that the personal data is kept securely and is password protected.

**Personal Storage**

Some personal data is stored on portable devices namely, Directors Laptops. In all cases, the devices are password protected and the personal data is stored on databases that are also protected by passwords.

**How does SGL protect Personal Information?**

SGL has put in place measures to protect the security of personal information. It has internal policies, procedures and controls in place to try and prevent personal information from being accidently lost or destroyed, altered, disclosed or used or, accessed in any unauthorised way.

In addition, we limit access to personal information to those employees, workers, agents, contractors and other third-parties who have a legitimate business need to know, in order to perform their duties and responsibilities.

Data held on computer is protected by user/share level security, personal key identifier passwords, virus protection, back-up systems, dedicated servers and robust internal control procedures via an administrator. Filing cabinets are locked when not in use and the Administration Offices are covered by both security access fobs and, intruder alarms that are armed overnight.

Where personal information is shared with third-parties, we require all third parties to take appropriate technical and organisational security measures to protect personal information and to treat it subject to a duty of confidentiality and in accordance with data protection law.

We only allow them to process information for specified purposes and in accordance with our instructions. We do not allow them to use personal information for their own purposes.

Third party providers are responsible for:

* Only acting on the documented instruction of the Data Controller.
* Only using the personal data for the agreed purpose
* Returning or deleting personal data when the service or contract ends
* Making available all information necessary to demonstrate compliance with the contract and, allowing for audits .
* Assisting with compliance and security provisions

Any information that falls under the definition of personal data, and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with the consent of the appropriate individual or under the terms of this Policy.

**Rights in connection with personal information**

Data subjects have a number of statutory rights. Subject to certain conditions, and in certain circumstances they have the right to:

* request access to personal information- this is usually known as making a ‘data subject access request’ and it enables them to receive a copy of the personal information we hold about them at to check that we are lawfully processing it.
* request error amendments to personal information – this enables them to have any inaccuracies corrected
* request for the erasing of personal information – this enable them to ask us to delete or remove personal information where there’s no compelling reason for its continued processing.
* object to the processing of their personal information - this enables them to ask us to stop processing their personal information where we are relying on the legitimate interests of the business as our legal basis for processing.
* restrict the processing of personal information – this enables them to ask us to suspend the processing of their personal information , eg if they contest its accuracy and want us to verify prior to continued processing.

To exercise any of these rights, a data subject should contact our Compliance Officer. We may need to request specific information in order to verify the data subject’s identity and check their right to access the personal information.

This is a security measure to ensure that their personal information is not disclosed to any person that has no right to receive it.

**Data Accuracy and Security**

SGL aims to ensure that all personal data held in relation to an individual is as up-to-date and as accurate as possible. Individuals must notify the Compliance Officer of any significant changes to important information held for both customers and staff.

An individual has the right to request that any out-of-date, irrelevant or inaccurate information ahem is erased or corrected (subject to certain exemptions and limitations under Data Protection Law)

SGL will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around the use of technology and other administrative systems. All staff have been made aware of this policy and their duties under Data Protection Law and have received relevant training.

**Personal Data Breaches**

Data breaches may include:

* Loss/theft of data (or equipment on which stored)
* Equipment failure
* Malicious or accidental deletion of data
* Hacking attack
* ‘Blagging’ cons
* ‘Phishing’ cons
* Given away willingly or mistakenly
* Inappropriate viewing – over the shoulder
* Data sharing – too many copies made

The GDPR requires mandatory breach notification to the Information Commissioner’s Office within 72 hours and, in some cases to affected individuals. The Compliance Officer shall monitor and record any data breaches and liaises with the ICO.

**Minimising the Risk of Data Breaches**

Staff have been trained about the GDPR and how to minimise data breaches. Such measures may include:

* Updated internet and anti-virus security
* Using secure storage (Vision / BoxTop / Bensoft/
* Encryption
* Keeping backups of important data (securely)
* Being aware of the importance of personal data
* Knowing where the data they are using is

In addition, staff have been advised to:

* Make sure we use data safely and securely
* Only use what is needed
* Be aware of who is around us when looking at data
* Keep a policy of ‘Clear Screen, Clear Desk’
* Make sure we store data securely
* Electronic data ‘password-protected’ at all times
* Paper-based data locked away
* Noticeboards, shelves, desks etc clear of data

Change passwords as instructed and keep them secure for:

* Desktop logins
* Laptop logins
* Wifi passwords
* Company Smartphones

 Eliminate random pen drives

* Use company systems to transfer files/documents

Do not give out other people’s personal data

* Event Invitations

Do not use personal devices

* Only use SGL devices to store data

Consider and plan for data loss

* Equipment failure
* Fire, theft, loss
* Hacking/blagging attacks

 Look at warehouse/offices

* Clear anything sensitive that should be locked away
* Do not leave anything on view for others to see
* Check noticeboards etc for sensitive data

**Access to Data**

*Rights of Access*

Individuals have a right of access to personal information held by SGL. Any individual wishing to access their personal data should contact the Compliance Officer.

SGL will endeavour to respond to any such requests as soon as is reasonably practicable and, as far as possible within 30 days.

**Changes to this Policy**

SGL reserves the right to update or amend this policy at any time. We will issue a new policy via e-mail when we make significant updates or amendments. We may also notify you about the processing of personal information in other ways.

**Contact**

Any questions about this policy or how we handle personal information should be directed to the Compliance Officer , through the email mike.isbell@seabrookgroup.com or by telephone on 0208 596 7500 ext 1005.