Regency Shipping

Ferrari Express

Regency Freight Services

General Data Protection Regulations (GDPR) 2018

Manual and Policies

Contents

Definitions:

GDPR	General Data Processing Regulations
RSL	Regency Shipping Ltd
FEL	Ferrari Express Ltd
RFS	Regency Freight Services
Companies	Regency Shipping, Ferrari Express & Regency Freight
ICO	Information Commissioners Office

1. Introduction

The General Data Protection Regulations (GDPR) build upon the data privacy and security principles that the Company are already abiding by and enhance the concepts and requirements of the Data Protection Act (1998)

A key change is that the GDPR introduces the principle of accountability, requiring organisations to actively show how they comply with the data protection principles. The companies hold personal data in relation to our Employees, Customers and Suppliers and it is our responsibility under the GDPR as data controllers and data processors that we actively demonstrate that we are taking the protection of this data and the welfare of our Employees, Customers and Suppliers seriously.

The purpose of the Compliance Manual and Policies is to provide a framework by which we are able to develop and implement policies and procedures to ensure a proportionate and reasonable level of compliance with the GDPR in relation to the data that we hold

A key requirement of GDPR compliance is the documentation of both procedures that are implemented and of the thought process and judgements that are made in respect of data protection.

It is a fundamental right of individuals to expect respect of their privacy and at the companies we take this right very seriously. Through the implementation of a thorough review of data held, policies with regards to security, retention and access to data, the training of our staff and the assessment of any impact from our systems, we will ensure that the approach to the GDPR is appropriate to our business, employees, customers, contacts and suppliers.

We will endeavour to ensure that in all aspects, data is secure, relevant and appropriate to the roles we carry out in our business.

Regency Shipping, Ferrari Express & Regency Freight Services

October 2023

2. Overall Purpose of GDPR plan

GDPR applies to both data controller and data processors and in our operation of the business we both control and process data.

Our business operates in such a way that our employees, customers and suppliers provide us with data and we process that data under the terms of our contracts to our employees, customers and suppliers but more importantly for employees to HMRC and Pension Providers.

The purpose of any GDPR compliance plan needs to consider a range of factors such as:

- On what legal basis do we hold and process data
- What data is relevant to the business and is it lawfully held
- What Policies do we have for the holding and treatment of data
- What procedures do we have for ensuring the individual rights of those we are holding data in respect of
- How do we assess the impact on data security when changes in systems or technology occur
- Who is ultimately responsible for data protection within our business

3. The Basis for which we hold data

There are essentially two types of data that we hold:

1 Customer & Supplier Data – Contact data from Customers, Suppliers and Contacts in relation to our Products, Services and Applications

2 Company Data – Personal data we hold in relation to the management of employees and of our business affairs generally

The GDPR applies to “personal data”. This covers an array of information including any piece of information that identifies, or potentially identifies, an individual.

The GDPR also identifies special categories of data, including racial/ethnic, political, religious or philosophical information, or genetic or biometric data or information relating to sexual activity or orientation. These special categories of data are not relevant to our business and therefore if such data is found to be held from our review of data, it will be destroyed.

The GDPR applies to both automated personal data, which we have in our Accounting Software, HR Bamboo Software and manual & electronic filing systems which we also use to retain both Customer, Supplier and Employee data.

Our responsibility in relation to this data are as follows:

- That we process the data lawfully, fairly and in a transparent manner
- That data is collected for a specific purpose and that we do not process the data in a manner incompatible with those processes
- That the data is adequate, relevant and is limited to what is necessary
- That the data is accurate and kept up to date
- That the data is securely stored
- That the data is kept in a form which permits identification of data subjects for no longer than is necessary for the purpose of processing
- That the data is processed in a manner that ensures appropriate security of the data.

The starting point in ensuring that the basis for which we hold data is understood, is establishing the lawful basis for which we hold the data. Under GDPR there are six legal basis;

- Consent of the data subject
- Processing of the data is necessary for the performance of a contract
- Processing of the data is necessary for compliance of a legal obligation
- Processing of the data is necessary to protect the vital interests of the data subject or another person
- Processing of the data is necessary for the performance of a task out in the public interest
- Processing of the data is necessary for the purposes of the legitimate interests pursued by the controller except where those interests are overridden by those of the data subject.

In the majority of cases, the lawful basis of holding and processing data will be that of processing the data as necessary for the performance of a contract, eg: a Purchase Order. There may be other cases, particularly to do with marketing, where consent is the lawful basis used. However, in the majority of these other cases we rely upon legitimate interests as the lawful basis. In certain cases with employees we are required by law to hold data.

It is our policy that consent will be the lawful basis of the last resort and that the performance of a contract will be the primary lawful basis for holding data in relation to customers, suppliers and employees. This is because there is a business rationale for holding the data. In certain aspects of marketing, the lawful basis would be that of legitimate interest as we would only market our products and services to those that we believed would genuinely benefit from our advice.

4. Assessment of Data held

In order for the GDPR principles to be complied with, it is essential that we understand the types of data that we hold. In order to do that a “data audit” has been undertaken whereby the different types of data we hold have been assessed. This has been carried out through both a review of the software used, paper files and functions we carry out.

A description of the categories of data subjects and categories of personal data are contained in Appendix 4 together with a summary of the business functions and software.

5. Assessment of Relevant Data

Relevant data is the data that is regarded as necessary to perform the terms of the contracts we have with our Customers, Suppliers and Employees and that data which we have legitimate interest in holding.

In order to assess the relevancy of the data we hold, we have applied our data retention policies to the data held on the system so that only ongoing data is held.

Annual reviews of data are conducted to ensure that the data on our systems is only held in accordance with those policies and remains relevant at all times.

Data is also consistently reviewed for accuracy. Our procedures to ensure this adhere to the following aspects:

- If data is required to be changed through notification from a data subject, details of the amendment are notified to the Administration Team using the Data Amendment Sheet (see Appendix 5) noting the necessary change to the data, the source of the change and the date we were notified. The system is consequently updated to reflect that change

- If data change is identified internally through an error or omission, the system is updated immediately

- If a data change becomes apparent from a third party, the data subject is contacted and the procedures set out above are followed.

Together with the assessment of the data, it is also a prudent and protective exercise to consider and assess the software and systems that we use. The Software has been detailed in Appendix 4 and is mainstream and widely used. The assessment of each has concluded that it poses no risk to the security of personal data, especially given that the software works within the environment of a secure server.

6. Policy statements regarding the holding and treatment of data

The processing of data is subject to the company's internal procedures, which document all of the areas of the business and the procedures and policies in place.

e-mail is the most common method of breaching the requirement of the GDPR, especially when e-mailing attachments, internal e-mails are not encrypted but some external e-mails maybe.

The GDPR imposes restrictions on the transfer of personal data outside of the European Union, in the course of operating global business, it can occur on occasion and therefore procedures are in place:

- All data holders. Such as software providers and IT providers provide us with a statement of compliance with the GDPR where we consider there to be, or have become aware of, such a geographical risk
- If data does need to be transferred outside of the EU, prior to that data being transferred, confirmation is obtained from the recipient of adequate protection levels with regards to the security of the data.

As a business we have developed and are maintaining a suitable and proportionate data security programme.

The policies and procedures that are set out in the company's procedures are the minimum levels expected and which if followed will ensure compliance with the necessary levels of security. All staff are expected to comply with these and are aware of the necessity to do so. Furthermore the Company's Employee Handbook reinforces these expectations and staff are aware that they are required to keep up to date with any changes.

Security

The IT systems are password protected and access is only granted to appropriately authorised employees.

The Company's premises are secured with an electronic door entry system and protected by an intruder alarm system linked to a monitoring station.

All employees are Aviation Security Trained in security of the building.

HR files are electronically stored on the company's shared network and only accessible by appropriately authorised employees. Paper HR files are kept in a locked cabinet in the Operations Managers office.

HR Management System, is structured with security access per employee and overall access by appropriately authorised employees.

Back up / Server Security

Back-ups are taken daily by the IT provider and the system access is restricted through ID and password security.

Mobile Devices

Data held on mobile devices is protected through the use of access codes and passwords, in particular if the mobile device is lost or stolen, then staff are required to immediately inform the company so that the device can be disabled and reset by the company's IT provider.

Internal Policies can be accessed on the Company's Network under the ISO and AEO folders held securely on a server.

7. Privacy Notice

It is a requirement of the GDPR that the policies for the provision of information to individuals for who we control or process personal information are communicated to the data subjects. This privacy information should be communicated in a concise, clear and understandable way.

It is a consequence of the individual's right to be informed and as such should be actively provided.

We have considered the most appropriate way to do this and it will be communicated in two ways:

- On the company's website, www.rsllhr.co.uk

This has been implemented for the companies

- By individual statement that will be highlighted to the customer not only as a provision of the necessary information but as an addendum to the contract until the contract is updated to include full companies terms and conditions.

An example of such a privacy statement is contained in Appendix 10

In addition, a letter/e-mail to employees explaining the fair processing of their data is also in included in Appendix 8

8. Staff Training Procedures

All employees are informed of the requirements and importance regarding the protection of customer, supplier and employee data and the requirements of GDPR. The memo/email sent to employees is included in Appendix 8

All employees will be trained on the requirements concerning accountability and governance, as well as practical implications.

Staff will be expected to confirm in writing that they have completed the training.

9. Procedures in relation to data breaches and access requests

The GDPR introduces a duty on us to report certain types of data breach to the relevant supervisory authority and in some cases to the individuals concerned. This should be done within 72 hours of the breach being identified.

As a company we have an internal breach reporting procedure in place, where the initial step is for the breach to be recorded and the person responsible for data protection informed in writing, normally by e-mail, immediately to info@rsllhr.co.uk

If an incident occurs we have procedures in place to contain and correct the issue. Procedures in place need to cover employees, managers and the IT providers and so the company has put in place adequate procedures and responsibilities between the company and its IT providers to be able to carry out suitable investigations of the weakness and rectify it to prevent future incidents. This involves reporting of the breach in accordance with the above procedure and liaison between the person responsible for data processing and the Company's IT providers to determine what action needs to be taken. The Companies has cyber insurance in place.

10. Procedures regarding Impact Assessments

All new systems and procedures that are implemented within the company are assessed for their adequacy and compliance with the GDPR. In all cases of new technology, software or other medium where data will be stored, kept, processed or transmitted, appropriate assessments of risks associated with the confidentiality of personal information will be made.

The outlining process will be:

- To identify the type of data that will be used or affected by the system change
- Assess what risks are associated with the new process

- Identify any mitigations that are available to adopt
- Make an assessment of the impact of our data protection responsibilities
- Conclude as to the adequacy of the system and either accept or reject the proposed change.

11. Allocation of Responsibilities

All employees within the Company have a responsibility to ensure that the policies and procedures designed for compliance with GDPR are maintained and upheld and complied with. However the GDPR requires that someone assumes overall responsibility

Whilst the Company does not require a formal Data Protection Officer, the responsibility for Data Protection lies with the Managing Director, assisted by the General Manager and IT Manager.

The GDR policies adopted by the Company have been assessed and compared with the ICO check list of GDPR compliance

12. Marketing Activities

The companies do not carry out direct marketing activities with data held.

We do not share information. We do not sell personal information to any third party. We only collect personal information that is necessary for prospective customers to access and use our Services and the Website or to provide information that has been requested.

The Web Site: www.rsllhr.co.uk has a “contact us” section whereby enquires can be received for product and technical information.

Data held in respect of individuals unconnected with the running of the business requires consent. Without this consent we are unable to market to them, for these data subjects we should hold:

a Name, Job title, Company and e-mail address

b The source of the data (Business Card, Web Enquiry)

c The data record pf when the person opted in

d The legal status of the prospect

e Telephone number and address

Data of “soft” opt-ins such as business cards and verbal consents should be recorded, in these cases no explicit opt-in has been received but it can be assumed as sufficient if:

- The contact has initiated a sales enquiry AND
- We are only marketing our own products and services AND
- We include the ability for the contact to opt-out

Note that for business cards received, this is an implied consent to contact once when positive opt-in can be obtained.

For existing lists of contacts and prospects, evidence of consent may still be required and an e-mail campaign may be run to obtain these.

The marketing data needs to have restricted access to only those who will use the data, the Boxtop system is password protected.

Assessment of marketing data

a. Identifying a legitimate interest	
1.What is purpose of the processing of data	To keep Customers, contractors, suppliers, prospective customers & suppliers updated with the company Products and Services.
2. Is Processing necessary to meet one or more specific operational objectives	To provide timely advice and information on company Products and Services
3.Does the GDPR or other legislation specifically identify the processing activity as being a legitimate activity	Marketing is a legitimate interest under GDPR regulations
b. The necessity test	
1.Why is the processing activity important to the business	Providing information and marketing information to those identified in a.1 above helps ensure the best quality of service and offer a wider range of services
c. The balancing test	
1. Would the individual expect the processing activity to take place?	Any of those in a.1 would expect added value and proactive services from a professional company on their Products and Services

Appendix 1 - GDPR Policy for Employees

From May 2018 new Legislation requires the companies to provide a notice to our staff on why and how we will use and store personal data

Upon appointment of a new employee, data is obtained in order for us to consider suitability for the appointment and then to comply with appropriate Employment Legislation.

We collect and use your personal information so that we are able to fulfil the terms of our employment contract with you and for the purposes of legislative compliance. We therefore process your data for the performance of a contract to which you are a party

We have a duty to ensure that your data is secure and confidential at all times and we will only collect the data that is necessary. We will use the data for no other purpose.

We will retain the information provided to us for the duration of your employment contract, and for 6 months following the cessation of that contract unless there is a specific reason, legislative or otherwise, to retain the data for a longer period. Information once no longer required will be disposed of securely.(see Data Retention Policy)

Under GDPR you have rights as an individual which you can exercise in relation to the data we hold about you

- The right to be informed – this is a right to be informed about the collection and use of personal data, retention periods and is the purpose of this notice

- The right of access – this is the right to access your personal data and be aware of the lawfulness of the processing

- The right to rectification – this is the right to have inaccurate data corrected

- The right to erase – this is the right to have personal data permanently deleted, although this is not an absolute right and only applies in certain circumstances.

- The right to restrict processing – this is the right to request a restriction or suppression of the processing of your data and again, this only applies in certain circumstances

- The right to data portability – this is the right to have your personal data provided in a format that is easily transferrable to other data processors.

- The right to object – this is the right to object to processing and will depend upon the legal basis for processing your data.

The companies endeavour to meet the highest standards when collecting and using personal information For this reason, we take any complaints we receive about this seriously. We encourage individuals to bring to our attention any circumstances whereby they believe that our collection or

use of their data is unfair, misleading or inaccurate. We also welcome suggestions for improvements to our procedures.

If you feel that the companies has not complied with your data protection rights, you can complain directly to info@rsllhr.co.uk or to the Information Commissioners Office (ICO)

Appendix 2 - GDPR Policy for Suppliers and Contractors

From May 2018 new Legislation requires the companies to provide a notice to our Contractors on why and how we will use and store personal data

We collect and use your personal information so that we are able to fulfil the terms of our contract with you and for the purposes of legislative compliance. We therefore process your data for the performance of a contract to which you are a party

We have a duty to ensure that your data is secure and confidential at all times and we will only collect the data that is necessary. We will use the data for no other purpose.

Details of Suppliers are obtained initially when their services are required. This data includes appropriate vetting information, data that is required under legislation of professional standards.

We collect Data of person(s) who are certified to handle our goods under the Aviation Security Regulations, this consists of:

- Name
- Aviation Security Training Certificate number, training date and expiry date
- Photograph for identification of certified person

We collect data from our Contractors, ie proof that personnel are qualified to carry out work at our site as required by ISO1 9001-2015 4001-2015 45001-2018 Standards, this consists of:

- Name
- Certificate of Competence, Training date and expiry date

The data will be reviewed on an annual basis to ensure we have up to date information.

We will retain the information provided to us for the duration the Contract and for 6 months following the cessation of that contract unless there is a specific reason, legislative or otherwise, to retain the data for a longer period. Information once no longer required will be disposed of securely.

If you feel that the companies has not complied with your data protection rights, you can complain directly to Info@rsllhr.co.uk or to the Information Commissioners Office (ICO).

Appendix 3 -GDPR Policy for Customers & Prospects

From May 2018 new Legislation requires the companies to provide a notice to our Contractors on why and how we will use and store personal data.

Customers:

On receiving of a customer enquiry for Pricing Quotations or Technical Information relevant to our Shipping & Logistics, data is obtained to enable the companies to determine the best product for the customer's requirement and application. The data is held in our Boxtop system.

Where the enquiry results in a Purchase Order from Customers, these are processed according to our Finance & Accounting Policies.

Customer details are kept solely for the purpose of their specific requirement and applications, to comply with customs and other statutory legislation.

The information and data is retained in accordance with our Data Retention Policy (See Appendix 6)

If you feel that the companies has not complied with your data protection rights, you can complain directly to Info@rsllhr.co.uk or to the Information Commissioners Office (ICO)

Appendix 4 - Categories of Data

Data Subject	Category of Data
Customer Data	Contact Details, GPS for locating
Former Customer Data	Contact Details
Employees	Contact Details
	Date of Birth
	NI Number
	Tax Reference
	Bank Account Details
	Pension Details
	Next of Kin/Contact Details
	Pay Details
	Annual Leave Details
	Sick Leave Details
	Performance Details
	Training Competence (qualifications)
	Photograph for company ID and Aviation Security
	Driving Licnece
	Passport ID
	Work Permit or Visa if applicable
	DBS Check for Aviation Security
	Medical Information to carry out our Duty of Care
Suppliers (including former)	Contact Details

Business Function	Software Applications
Boxtop management services	Fairlea online Ltd
HR Management	Pinehurst
Payroll	Pinehurst Financial services

Appendix 5 - Data Request / Amendment / Breach form

Name:		Date:	
Reference:			

Purpose of Data notifications

Information request		Processing Restrictions request:	
Access request		Data Movement Request:	
Rectification request		Processing Objection Request:	
Erasure request		Data Breach Notification:	

Outline of request:

Proposed Action:

Actioned by:		**Completed by:**	

Appendix 6 – Retention of company Records & Policies

	RECORDS/DOCUMENTS	LOCATION	RESPONSIBILITY	MINIMUM PERIOD RETAINED	COMMENTS
1	Quality Management System	Server 25	General Manager		Amended and re-issued as required.
2	Quality Management Team Review Minutes	Server 25	General Manager	3 years	
3	Customer Order Processing (Jobs): - Client orders - Worksheets	Job File under RE/RI/FE/FI Reference	I.T Team	3 years	
4	Customer Order Processing (Contracts): - Client orders - Worksheets	Electronic	I.T Team	3 years	
5	Faxed/Email Quotations	Imports/ Exports	I.T Team	3 years	
6	Emailed Quotations/Quote Analysis Forms	Digital Job Files	I.T Team	3 years	
7	Contract Service Agreements	Q.M Office / Servers	Director	6 years	
8	Customer Service Files:- - Collection Notes - Delivery Notes - Certification	Unit 12 P.O.D is kept also digital by job number	Warehouse & I.T Team	7 years	

9	Approved Supplier/Sub-Contractors List	Server 25	General Manager/ QM Team	3 years	Reviewed and updated as required
10	Purchasing:- - Purchase order/delivery notes - Purchase invoices	Q M office / Accounts	Accounts Manager / I.T. Team	7 Years	

13	Accounts:- - Invoices - Aged debtors lists/credit control faxes/emails/letters	Finance Manager Office/ Devon	Finance Manager	7 years	
14	Staff Training Plans/Records	Server 25	Department Manager's	Duration of employment	Reviewed and updated annually.
15	Calibration Records	Operations Manager Office	Transport Manager	3 years	Reviewed and updated at scheduled intervals
16	Data Storage and Protection:- - Back-up tapes	IT Department Office/ Off-site Internally	IT		Daily tape held in back-up drive of computer server in Comms. Cabinet

17	**Document Control:-** **- Master forms file** **- Withdrawn/superseded** **Documentation**	**Operations Manager** **Office**	**General Manager**	**3 years**	**Updated as required**
18	**Non-conformance/customer complaints**	**Operations Manager** **Office**	**Department Manager's**	**3 years**	
19	**Internal Quality Audit Forms**	**Operations Manager** **Office**	**General Manager**	**3 years**	
20	**Regulations/Standards/** **Legislative documents/Health & Safety/Environment Standards**	**Operation Manager** **Office**	**QM Team**		**Purchased/** **updated** **as required**

Appendix 7 – Nature of relevant data

Data Subject	Relevance of data
Customer Data	Data is required to perform our contractual obligations to the customer. This will involve compliance with legislation as well as current and historical data to provide accurate services to our customers. GPS data is removed from company vehicles & mobile phones at the end of the working week. GPS data is used in conjunction with a customer's address to minimise travel time and confirm address for security purposes.
Former Customer Data	It is within our legitimate interests to retain data in respect of past customers.
Employees	We are required by law to hold data on current employees as part of a contractual basis of employment. Details regarding potential employees who were not successful are destroyed.
Former Employees	Data regarding former employees is held for legitimate interests' purposes in case of retrospective complaints or information requests. All data except an y relevant legal compromise or settlement agreements, will be destroyed after six months following an employee leaving the company. Any documents retained for legal purposes will be destroyed after 7 years or earlier upon review.
Suppliers	Data is held for the purposes of contractual adherence.
Potential customers and suppliers	Data is held for legitimate purposes so that future revenue streams may be developed. Only minimal data is held and consent will be obtained where necessary.

Appendix 8 – Staff communication re GDPR

Email sent to all staff as shown below,

A new Read Task has been assigned to you for the document **Data Protection Training.** You must READ and SIGN the task online to confirm it has been read, you can see your tasks at SOP Documents Read - Sign and the document **Data Protection Training** at Data Protection Training

Appendix 9 – Policies in respect of individual rights

Individual Right	Policy in respect of Individual Right
The right to be informed	All data subjects will be provided with the necessary information as included in Appendix 1
The right of access	Any requests for access to personal data will be recorded in writing and provided to the individual responsible for the data protection within 24 hours. The request will be reviewed and if considered appropriate the information will be provided within a maximum of 15 working days from the date of the request. If not considered appropriate the data subject will be informed as to why access has not occurred and informed them of their right to complain.
The right to rectification	Any written request from a data subject to rectify inaccurate date will be provided in writing within 24 hours of the request to the individual responsible for data protection who will arrange for the data to be corrected immediately.
The right to erase	Any requests for access to personal data will be recorded in writing and provided to the individual responsible for the data protection within 24 hours. The request will be reviewed and if considered appropriate the information will be provided within a maximum of 15 working days from the date of the request. If not considered appropriate the data subject will be informed as to why access has not occurred and informed them of their right to complain.
The right to restrict processing	Any requests for access to personal data will be recorded in writing and provided to the individual responsible for the data protection within 24 hours. The request will be reviewed and if considered appropriate the information will be provided within a maximum of 15 working days from the date of the request. If not considered appropriate the data subject will be informed as to why access has not occurred and informed them of their right to complain.
The right to data portability	Any requests for access to personal data will be recorded in writing and provided to the individual responsible for the data protection within 24 hours. The request will be reviewed and if considered appropriate the information will be provided within a maximum of 15 working days from the date of the request.
The right to object	Any requests for access to personal data will be recorded in writing and provided to the individual responsible for the data protection within 24 hours. The request will be reviewed and if considered appropriate the processing of information will stop immediately.

Appendix 10 – Privacy Statement

What information does the company hold on behalf of customers?

The company will never hold personally identifying information that has not been directly collected by the company or is not relevant to its explicit business with the end customer.

What information does the company collect?

We may collect the following types of personal data:

- Name
- Job Title
- Organisation
- Business Address
- Business e-mail address
- Telephone number (predominantly business telephone number, but may include personal mobile numbers if preferred by the customer)
- Gender
- Photograph
- Bank details
- Dependants and next of kin (where applicable for specific business contexts)

How we collect this information

- Directly from you during Product or Technical inquiries, or when setting up a new customer account.
- From third-party intermediaries who may act as introducers in certain business contexts.

How we store this information

After obtaining your consent to retain personal data, we securely store this information in our Boxtop System, protected with two-factor authentication and other technical safeguards. Personal data may also be stored in personnel files or the company's HR and IT systems, depending on its use.

Why do we need this personal data?

We collect and process your data for:

- Customer communication for business purposes, including sales and technical support.
- Contractual obligations such as account setup, service delivery, and payment administration.
- Legitimate business interests, including fraud prevention, legal claims handling, and administrative purposes.

Who has access to this data?

- Internally: Authorized members of the Sales and Operations teams, and other employees as necessary for their duties.
- Externally: Third-party service providers (e.g., shipping, payroll, IT services) as required for specific business processes. We ensure third parties adhere to secure and lawful data handling practices.

Data transfers outside the EEA

From time to time, data may be processed outside the EU to support our global business operations. This is conducted in a secure and appropriate manner, ensuring compliance with GDPR requirements for international transfers.

How does the company protect data?

We have implemented internal policies and measures to safeguard your data from loss, misuse, unauthorized access, or disclosure. These measures include:

- Access control with two-factor authentication for systems like the Boxtop platform.
- Written agreements with third parties to ensure GDPR-compliant data processing.
- Regular audits and reviews of our data protection practices.

How long will the company retain data?

We retain customer account information for 7 years after an account becomes dormant. Contractor information is retained for a minimum of 6 years post-engagement. A data subject can withdraw consent at any time, and the company will comply with erasure requests where applicable.

Your rights as a data subject

You have the following rights regarding your personal data:

- **Right to be informed**: You have the right to know how your data is collected, used, and retained.
- **Right of access**: You can request access to the personal data we hold about you.
- **Right to rectification**: You can ask us to correct inaccurate or incomplete data.
- **Right to erasure**: You may request the deletion of your personal data where processing is no longer necessary or lawful.
- **Right to restrict processing**: You can request a restriction of processing while we verify or address your concerns about the data.
- **Right to data portability**: You may request that we provide your data in a format that can be transferred to another data controller.
- **Right to object**: You can object to processing based on legitimate interests or direct marketing purposes.
- **Rights related to automated decision-making and profiling**: You have the right not to be subject to automated decisions that significantly affect you.

To exercise these rights, please contact **Info@rsllhr.co.uk**.

Making a complaint

If you believe we have not handled your data in accordance with GDPR, you may contact the Information Commissioner's Office (ICO) in the UK.

Regency Shipping, Ferrari Express & Regency Freight Services

October 2019

Appendix 11 - GDPR Recruitment Policy

This document demonstrates our commitment to protect the privacy and security of your personal information. It contains information regarding how we collect and use personal data or personal information about you in advance of any employment relationship in accordance with the General Data Protection Regulation (GDPR) and all other data protection legislation currently in force.

Pursuant to that legislation, when processing data we will:

- process it fairly, lawfully and in a clear, transparent way
- collect your data only for reasons that we find proper for the course of your employment in ways that have been explained to you
- only use it in the way that we have told you about
- ensure it is correct and up to date
- keep your data for only as long as we need it
- process it in a way that ensures it will not be lost or destroyed or used for anything that you are not aware of or have consented to (as appropriate).

The companies is a “data controller”. This means that we are responsible for determining the purpose and means of processing personal data relating to you.

“Personal data”, or “personal information”, means any information relating to an identified, or identifiable individual in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

There are “special categories” of sensitive personal data, meaning data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health conditions, sex life or sexual orientation, genetic data, and biometric data which require a higher level of protection.

This statement is applicable to job applicants. It is not intended to, neither will it, form part of any contract of employment or contract of services. We reserve the right to make changes to this statement at any time, if you are affected by substantial changes we will make an alternative statement available to you.

Where you are successful in your application and are appointed to a position you will receive details of our data protection compliance statement (privacy notice).

DETAILS OF INFORMATION WE WILL HOLD ABOUT YOU

The list below identifies the kind of data that we will process about you during the application process:

- personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- date of birth
- your photograph
- marital status and dependents
- information included on your CV including references, education history and employment history
- documentation relating to your right to work in the UK
- national Insurance number
- copy of driving licence
- evidence of qualifications or professional memberships.

The following list identifies the kind of data that we will process and which falls within the scope of “special categories” of more sensitive personal information:

- information about your health, including any medical conditions and disabilities;
- information about criminal convictions and offences

HOW WE COLLECT YOUR PERSONAL INFORMATION

Your personal information is obtained through the application and recruitment process, this may be directly from candidates, via an employment agency or a third party who undertakes background checks. We may occasionally request further information from third parties including, but not limited to, previous employers, credit reference agencies or other background check agencies.

PROCESSING INFORMATION ABOUT YOU

We will only administer personal information in accordance with the lawful bases for processing. At least one of the following will apply when we process personal data:

- consent: You have given clear consent for us to process your personal data for a specific purpose.
- contract: The processing is necessary for a contract we have with you, or because we have asked you to take specific steps before entering into a contract.
- legal obligation: The processing is necessary for us to comply with the law (not including contractual obligations).

LAWFUL BASIS FOR PROCESSING YOUR PERSONAL INFORMATION

We consider that the basis for which we will process the data contained in the list above (see section above - **details of information we will hold about you**) is to enable us to consider whether we may wish to/prepare for entering into a contract or agreement with you and to enable us to comply with our legal obligations. Occasionally, we may process personal information about you to pursue legitimate interests of our own or those of third parties, provided there is no good reason to protect your interests and your fundamental rights do not override those interests.

The circumstances in which we will process your personal information are listed below:

- making a decision about your recruitment or appointment
- making decisions about terms and conditions, salary and other benefits
- checking you are legally entitled to work in the UK
- assessing qualifications for a particular job or task
- education, training and development requirements
- complying with health and safety obligations
- preventing fraud
- in order to fulfill equal opportunity monitoring or reporting obligations

There may be more than one reason to validate the reason for processing your personal information.

LAWFUL BASIS FOR PROCESSING "SPECIAL CATEGORIES" OF SENSITIVE DATA

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- consent: You have given clear consent for us to process your personal data for a specific purpose.
- contract: The processing is necessary for a contract we have with you, or because we have asked you to take specific steps before entering into a contract.
- legal obligation: The processing is necessary for us to comply with the law (not including contractual obligations) and meets the obligations under our data protection policy.
- vital interests: the processing is necessary to protect someone's life.
- public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law. and meets the obligations under our data

protection policy. (For example in the case of equal opportunities monitoring).

- legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect your personal data which overrides those legitimate interests (For example to assess your capacity to work on the grounds of ill health).

Occasionally, special categories of data may be processed where you are not capable of giving your consent, where you have already made the information public or in the course of legitimate business activities or legal obligations and in line with the appropriate safeguards.

Examples of the circumstances in which we will process special categories of your particularly sensitive personal information are listed below (this list is non-exhaustive):

- in order to protect your health and safety in the workplace
- to assess your physical or emotional fitness to work
- to determine if reasonable adjustments are needed or are in place
- in order to fulfill equal opportunity monitoring or reporting obligations

Where appropriate, we may seek your written authorisation to process special categories of data. Upon such an occasion we will endeavor to provide full and clear reasons at that time in order for you to make an informed decision. In any situation where consent is sought, please be advised that you are under no contractual obligation to comply with a request. Should you decline to consent you will not suffer a detriment.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We will only collect criminal convictions data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your engagement should you be successful.

We may process such information to protect yours, or someone else's, interests and you are not able to give your consent or we may process such information in cases where you have already made the information public. Where we process information regarding criminal convictions we will adhere to the guidelines currently in force regarding data security and data retention as determined by the appropriate governing body.

We anticipate that we will process information about criminal convictions.

SHARING DATA

Your data will be shared with individuals within the Companies where it is necessary for them to undertake their duties with regard to recruitment. This includes, for example, the HR department, those in the department where the vacancy is who are responsible for screening your application and interviewing you, the IT department.

It may be necessary for us to share your personal data with a third party or third party service provider (including, but not limited to, contractors, agents or other associated/group companies) within, or outside of, the European Union (EU). Data sharing may arise due to a legal obligation, as part of the performance of a contract or in situations where there is another legitimate interest (including a legitimate interest of a third party) to do so.

The list below identifies which activities are carried out by third parties on our behalf:

- payroll
- pension providers/administrators
- IT services
- legal advisors
- security
- insurance providers

- Health & Safety and HR providers

Data may be shared with 3rd parties in the following circumstances:

- in relation to the maintenance support and/or hosting of data
- to adhere with a legal obligation
- in the process of obtaining advice and help in order to adhere with legal obligations.

If data is shared, we expect third parties to adhere and comply with the GDPR and protect any data of yours that they process. We do not permit any third parties to process personal data for their own reasons. Where they process your data it is for a specific purpose according to our instructions.

DATA SECURITY

As part of our commitment to protecting the security of any data we process, we have put the appropriate measures in place.(See Page 7 of Manual & Policies)

In addition, we have put further security measures in place to avoid data from being accessed, damaged, interfered with, lost, damaged, stolen or compromised. In cases of a breach, or suspected breach, of data security you will be informed, as will any appropriate regulator, in accordance with our legal obligations.

Any data that is shared with third parties is restricted to those who have a business need, in accordance with our guidance and in accordance with the duty of confidentiality.

DATA RETENTION

We anticipate that we will retain your data as part of the recruitment process for no longer than is necessary for the purpose for which it was collected. We will keep your data for 6 months for unsuccessful candidates.

If your application is successful, your data will be kept and transferred to the systems we administer for employees. We have a separate data protection compliance statement (privacy notice) for employees, workers and contractors which will be provided to you when applicable. Refer to: Appendix 1 and Appendix 2

YOUR RIGHTS IN RELATION TO YOUR DATA

In the event that you enter into an employment contract with us, any information already collected may be processed further in accordance with our data protection policy, a copy of which will be provided to you.

If you wish to exercise any of the rights in Appendix 1 or Appendix 2 please contact:

The companies – General Manager

Consequences of your failure to provide personal information

If you neglect to provide certain information when requested, it may affect our ability to enter into an employment contract with you and it may prevent the company from complying with our legal obligations.

Change of purpose for processing data

We commit to only process your personal information for the purpose for which it was collected, except where we reasonably consider that the reason for processing changes to another reason, example if you become an employee. Should we need to process your personal information for another reason, we will inform you of this and advise you of the lawful basis upon which we will process.

Important note: We may process your personal information without your knowledge or consent, in compliance with the above rules (see section **Lawful Basis for Processing your Personal Information).**

In the event that you enter into an employment contract with the company, any information already collected may be processed in accordance with our data protection policy, a copy of which will be provided to you.