

Privacy notice

Introduction

In accordance with the UK General Data Protection Regulation (UK GDPR), Regency Shipping Ltd, Ferrari Express Ltd, Regency Freight Services Ltd, Pinehurst Financial Services Ltd, Fairleonline Ltd and TCTV Ltd (“the Organisation”) has implemented this privacy notice to inform website users, customers, and prospective customers how we collect, use, store, and protect personal data.

This notice explains:

- what personal data we collect
- why we process it
- the lawful bases we rely on
- how long we keep it
- your rights in relation to your data

Data Protection Principles

We process personal data in accordance with the UK GDPR principles. This means we ensure that personal data is:

- processed fairly, lawfully and transparently
- collected for specific, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date
- retained only for as long as necessary
- processed securely using appropriate technical and organisational measures
- handled in accordance with rules on international data transfers

Types of Data We Hold

Personal data is information that identifies an individual. We may collect, store and use the following categories of personal data about customers and prospective customers:

- names, job titles and company details
- business contact details (email address, telephone number, postal address)
- enquiry details, pricing requests and technical information
- purchase order and contract details
- billing and invoicing information
- correspondence and communications with us
- system usage records relating to our customer platforms (e.g. Boxtop)
- technical data relating to website use, such as IP address and browser information

We do not intentionally collect special category personal data from customers. Where such data is provided inadvertently, it will be handled in accordance with UK GDPR requirements and minimised wherever possible.

Communications and Call Recording

Telephone calls with the Organisation may be recorded to improve customer service and staff training, monitor service quality, investigate complaints or disputes and support security and fraud prevention. Recordings are accessed only where necessary and are retained in line with the Organisation’s Data Retention Policy.

CCTV and Security Monitoring

The Organisation operates CCTV and security monitoring systems at its premises and within certain company vehicles for safety, security, crime prevention and the protection of employees, visitors, customers, drivers and assets.

How We Collect Your Data

We collect personal data:

- directly from you when you make an enquiry, request a quotation, or place an order
- through ongoing communications during the provision of our services
- from publicly available sources (e.g. company websites or professional directories), where relevant

Personal data is stored within our business systems, including customer relationship, operational, and finance systems.

Website use

When you visit our website, we may collect limited information automatically, including your IP address, browser type, and basic usage data.

This information is used to ensure the security and proper functioning of our website, to respond to enquiries submitted through website forms, and to improve our services.

We do not use website data to make automated decisions about individuals.

Lawful Basis for Processing

We process personal data only where a lawful basis applies under the UK GDPR. The table below explains why we use your data and the legal basis we rely on.

Purpose of processing	Lawful basis
Responding to enquiries and providing quotations	Legitimate interests – to respond to business enquiries and assess service requirements
Providing shipping, logistics and related services	Performance of a contract
Processing purchase orders, invoicing and payments	Performance of a contract and compliance with legal obligations
Complying with customs, aviation, transport and other statutory requirements	Legal obligation
Managing customer relationships and service delivery	Legitimate interests: to manage, improve and maintain ongoing commercial relationships.
Dealing with legal claims, complaints or disputes	Legitimate interests: to establish, exercise or defend legal claims
Ensuring IT, operational and information security	

Purpose of processing	Lawful basis
Call recording and CCTV monitoring	Legitimate interests: to protect our systems, data and business continuity
Operation, security and performance of the Organisation's websites	Legitimate interests: to ensure service quality, site security, fraud prevention, regulatory compliance and effective complaint handling.
	Legitimate interests: to operate, secure and maintain our websites and online services. Where non-essential cookies are used, processing is carried out with user consent in accordance with our Cookie Policy.

Failure to Provide Data

If you do not provide personal data when requested, we may be unable to:

- provide quotations
- enter into contracts with you
- deliver services
- comply with legal or regulatory requirements

Who We Share Your Data With

We may share personal data with:

- employees who require access to perform their role
- service providers who support our operations (e.g. IT systems, finance systems)
- regulatory authorities, customs bodies, or law enforcement where required by law
- professional advisers (e.g. legal, auditors)

All third parties are required to protect personal data appropriately and, where applicable, are bound by data processing agreements.

International Data Transfers

We do not routinely transfer personal data outside the UK or EEA.

Where any processing involves third-party systems or service providers, appropriate safeguards are in place to ensure personal data is protected in accordance with UK GDPR.

Protecting Your Data

We have implemented technical and organisational measures to protect personal data against unauthorised access, loss, misuse or disclosure. Access to personal data is limited to those who need it for legitimate business purposes.

Retention Periods

The Organisation handles high-value goods within regulated aviation and logistics environments. For this reason, certain customer and shipment records must be retained for extended periods to:

- evidence chain of custody and provenance of goods;
- support investigation of theft, loss, fraud or security incidents;
- meet Civil Aviation Authority (CAA), customs and insurance requirements;
- comply with anti-money-laundering and sanctions obligations;
- establish, exercise or defend legal or insurance claims.

Extended retention is applied only to defined record categories and is subject to:

- documented legitimate interest assessments;

- periodic review;
- segregation of archived records from active systems;
- deletion or anonymisation where no continuing purpose exists.

We retain customer personal data only for as long as necessary. In most cases, this will be:

- for the duration of the customer relationship
- plus a retention period of Minimum 7 years from completion. Where required for aviation security, customs, insurance, fraud prevention or legal claims, records may be retained for extended periods in line with regulatory or risk-based requirements.

Call Recordings are retained for a standard period of 4 months, unless required for compliance, regulatory or legal purposes.

CCTV footage is retained for a standard period of 30 days, unless required for investigation, regulatory or legal purposes.

Further details are set out in our Data Retention Policy.

Automated Decision-Making

We do not make decisions about you that have legal or similarly significant effects based solely on automated decision-making.

Cookies

The organisation websites use cookies and similar technologies to ensure the websites function correctly and to support security and performance.

Cookies are small text files placed on your device when you visit a website. Some cookies are essential for the operation of our websites and do not require consent.

Where non-essential cookies are used, these will only be set with your consent, which you can manage through our cookie settings. Cookies may be set by the Group or by trusted third-party service providers supporting website functionality.

Further information about the cookies we use, including how to manage or withdraw consent, is available in our Cookie Policy, which applies across the Group:

<https://www.rslhr.co.uk/cookie-policy/>

AI Use

The Organisation may use approved Artificial Intelligence (AI) tools, including ChatGPT Team, to support internal analysis, contract review, due diligence, and drafting activities.

Only non-identifiable or publicly available information is processed using such tools. AI outputs are reviewed by a human and are not used to make automated decisions about individuals. Where AI tools are integrated within our approved business systems (e.g. Microsoft 365), processing remains within our controlled business environment.

Your Data Protection Rights

You have the right to:

- be informed about how your data is used
- access the personal data we hold about you
- request correction of inaccurate data
- request erasure of data in certain circumstances
- restrict processing
- object to processing
- request data portability

Further information on exercising these rights is available in our Subject Access Request Policy.

Making a Complaint

If you believe your data protection rights have been breached, you may raise a concern with us or complain to the Information Commissioner's Office (ICO):

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire SK9 5AF
Telephone: 0303 123 1113

Data Protection Compliance

The Organisation is the data controller under UK GDPR. Responsibility for data protection compliance rests with the Board of Directors, who ensure appropriate technical and organisational measures are in place. Operational tasks may be delegated to senior managers, but accountability remains with the Board.

For data protection queries, please contact: hr@rslhr.co.uk