

Flight Logistics Group - Privacy Policy

This notice explains how Flight Logistics Group Ltd collects, uses, shares and protects personal information, and how you can exercise your rights. It applies to our website, enquiries, customers, shippers, recipients, business contacts, suppliers, visitors and job applicants, including services delivered under our ShipArt brand.

1. Who we are and how to contact us

Flight Logistics Group Ltd is the controller when we decide why and how your personal information is used. We comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and applicable Privacy and Electronic Communications Regulations (PECR), as amended.

Data privacy contact: Rob Crane, IT Manager

Email: rcrane@flightlg.com

Telephone: 01753 763500

Postal address: Global Logistics Centre, Horton Road, Colnbrook, SL3 0DL, United Kingdom.

Website: www.flightlg.com

For some fulfilment, mailing and logistics activities we process information on a client's instructions as a processor. The client's privacy notice then explains its use of your information. We help the client handle rights requests where appropriate. We may separately act as controller for our own legal, security and business administration purposes.

2. About this notice

Please read this notice alongside any service-specific privacy information and the cookie information available through our website. Our website and services are not directed at children. Where information about a child is necessary for a shipment or another service, it must be handled with appropriate safeguards.

We review this notice when our activities or legal requirements change. Its updated date identifies the latest revision. We will provide additional information about material changes where required.

3. Information we collect

The information we collect depends on your relationship with us and the service involved:

- **Identity and contact:** names, business roles, company details, postal and delivery addresses, telephone numbers and email addresses.
- **Service and shipment:** orders, booking details, collection and delivery instructions, shipment contents and values, customs documents, tracking information, signatures and proof of delivery.
- **Account and financial:** customer and supplier records, agreements, invoices, payment records, bank details and account access information where relevant.
- **Identification:** passport or identity-document details where necessary for customs clearance, identity verification or legally required screening.
- **Communications and marketing:** enquiries, correspondence, feedback, relevant business interests, marketing preferences, opt-outs and campaign interactions where collected lawfully.
- **Website and technical:** IP address, device and browser information, access logs, pages viewed, referral information and cookie preferences, where collected through the relevant technology.
- **Visitors and recruitment:** CCTV images, visitor details, CVs, applications, employment history, qualifications, references and right-to-work information.

We do not routinely need sensitive information for ordinary customer enquiries. Please avoid sending it unnecessarily. If special category information is needed, for example to support a recruitment adjustment, we must have both a lawful basis and a relevant additional legal condition. Criminal-offence information is handled only where legally permitted and with the required safeguards.

Anonymous statistics are outside data protection law only where people cannot be identified. Pseudonymised information and data that can be linked back to an individual remain personal information.

4. Where information comes from

We receive information directly from you through forms, orders, applications and correspondence; from customers or shippers arranging services for recipients; and from carriers, freight partners, payment providers and other service partners. Website logs and permitted analytics collect some information automatically.

For relevant business enquiries and prospecting we may use public business sources, company websites, professional networks and business-contact providers. We must check that their use is lawful. Where information comes from another source, we provide the required privacy information within the applicable period, normally within one month and no later than our first communication or disclosure, unless a lawful exemption applies.

5. Why we use information and our lawful bases

We identify the applicable basis for each activity. **Contract** applies where processing is necessary for a contract with you personally, or steps you request before entering it. For a company's employees, contacts and shipment recipients, we normally rely on **legitimate interests** for relevant service administration rather than a contract with that individual.

Our legitimate interests include providing and improving services, maintaining customer and supplier relationships, securing premises and systems, preventing fraud and carrying out relevant business development. We assess the impact on your rights before relying on this basis. You may ask for more information about that assessment.

- **Quotes, bookings, fulfilment, storage, shipping and customer support:** contract, or legitimate interests in providing the service and managing business relationships.
- **Invoicing, payments and account administration:** contract or legitimate interests; legal obligation for required accounting and tax records.
- **Customs, import/export and applicable sanctions checks:** legal obligation where a duty applies; otherwise contract or legitimate interests for lawful shipment administration and risk management.
- **Security, fraud prevention, CCTV and access control:** legitimate interests in protecting people, premises, stock and systems; legal obligation where applicable.
- **Recruitment:** steps before entering a contract at your request, legitimate interests in assessing applications, and legal obligation for checks such as right to work. Additional conditions apply to sensitive information.
- **Website operation and enquiry handling:** legitimate interests in running a secure website and responding to requests, or contract for requested pre-contract steps. Cookie-related consent is addressed in section 7.
- **Relevant marketing:** consent where required, or legitimate interests where permitted, subject to PECR and your right to object. See section 8.
- **Regulatory and operational notices:** contract or legitimate interests in communicating service requirements; legal obligation only where a specific duty requires the communication.

If essential information is not provided, we may be unable to deliver the service or meet a legal requirement. We will explain this where appropriate. We use information for a new purpose only where legally permitted and provide further notice where required.

6. Logistics, security and communications

Shipment checks and exceptions. Shipments may be checked to verify contents, identify prohibited items, meet security requirements or resolve an undeliverable shipment, in accordance with applicable law and service terms.

Sanctions and denied-party screening. Where required or appropriate, we or our service partners check relevant details against applicable sanctions or restricted-party lists. A possible match does not itself establish wrongdoing. Further information may be requested to verify a match. Necessary records are retained only for the relevant purpose and applicable legal requirements.

Customs clearance. Customs authorities may require identification and shipment information. We share only the information needed for the clearance process. Identification records are protected and are not retained simply because they might be useful for a future shipment.

Calls and digital messages. We process correspondence to deal with services, enquiries and feedback. If a call is recorded, we will tell you and explain the purpose. Third-party messaging and social platforms also process information under their own privacy notices; you can instead contact us by telephone or email.

CCTV. CCTV supports security, access control, incident investigation and the safety of people and property at our premises. Notices identify monitored areas. Access to footage is restricted and disclosure is limited to authorised purposes.

7. Website, forms, cookies and analytics

Our website uses WordPress and Formidable Forms Pro to receive enquiries. Submitted information is used to respond, prepare quotations and maintain relevant customer or prospect records. It may be handled through our email and CRM systems, including HubSpot.

Cookie preferences are managed through CookieYes. Strictly necessary cookies support essential website functions. We seek your consent before using optional analytics, advertising or tracking technologies where required. You can accept, reject or change optional-cookie choices through the website's cookie controls; withdrawing consent does not affect earlier lawful use.

Where enabled with the appropriate permissions, Google Analytics 4 helps us understand website traffic, page use and referral sources. Cookie details and durations should be read in the website's cookie information. Declining optional cookies should not prevent you from contacting us.

Third-party links, embedded content and social platforms may involve their own data collection. Their privacy notices apply to that processing.

8. Marketing and Regulatory notices

We may use relevant business-contact information to communicate about our services and maintain prospect and customer relationships. We use consent where required, and legitimate interests for relevant business marketing where lawful.

Unsolicited email marketing to corporate subscribers, such as limited companies and LLPs, may be sent without PECR consent, but we still comply with data protection law for personal information. For individual subscribers, including sole traders and certain partnerships, we obtain consent unless the applicable soft opt-in conditions are met. Those conditions include obtaining details directly during a sale or negotiations for a sale of our own similar services, and offering an opt-out when details are collected and in every message.

Marketing messages identify Flight and provide a straightforward way to opt out. You can also contact our data privacy contact. We stop using your personal information for direct marketing when you object and may retain a minimal suppression record to respect that choice. We obtain your express consent before sharing your details with other organisations for their own marketing.

Regulatory notices and operational messages concern matters such as customs requirements, shipment administration and changes affecting a service. A marketing opt-out does not prevent necessary service communications. Calling a message “Regulatory” does not exempt promotional content from marketing rules.

9. Who receives information

We share information only where necessary and lawful, with:

- Authorised employees and relevant group entities involved in the service or business administration.
- Carriers, couriers, freight and customs partners, warehouse and fulfilment partners, and payment providers needed to provide the service.
- Providers of website hosting, IT support, email, CRM, analytics and other approved business systems.
- Professional advisers, insurers, auditors, tax authorities, regulators, law enforcement and other authorities where legally required or justified.
- Prospective or new business owners and their advisers where necessary for a business transaction, subject to appropriate confidentiality and safeguards.

Processors acting on our behalf must follow our instructions under appropriate contracts. Some recipients, including certain carriers, banks and authorities, act as independent controllers and are responsible for their own processing. We do not describe all recipients as processors or joint controllers automatically.

10. International transfers

International shipments and some service providers may involve transferring information outside the UK. Where UK GDPR restricted-transfer rules apply, we use a lawful transfer mechanism.

This may be UK adequacy regulations, including the UK Extension to the EU-US Data Privacy Framework for eligible certified recipients; or appropriate safeguards such as the UK International Data Transfer Agreement or UK Addendum to the EU Standard Contractual Clauses, together with the required data protection test or transfer risk assessment. A specific statutory exception may be used only where its conditions are met.

Where EU GDPR also applies, we meet its transfer requirements separately. You can ask our data privacy contact about the safeguards relevant to your information and how to obtain a copy, subject to necessary redactions.

11. Security and retention

We use appropriate technical and organisational measures to protect personal information, limit access to those who need it and manage service-provider risks. We assess suspected personal-data breaches and notify affected people and the relevant regulator where required.

We keep information only as long as needed for its purpose, taking account of legal duties, contractual requirements, complaints, disputes and limitation periods. We then securely delete or anonymise it.

- **Customer, shipment, customs and financial records:** for service administration and the applicable tax, customs, accounting and claims periods.
- **Enquiries and prospect records:** while relevant to the enquiry or business relationship, with periodic review of inactive records.
- **Marketing preferences and suppression records:** while needed to document choices and prevent unwanted contact.
- **Recruitment records:** for the recruitment process and an appropriate period for queries or claims; longer talent-pool storage requires separate justification and information.
- **CCTV, call recordings, technical logs and identification documents:** for their specific security, operational or verification purpose, with restricted longer retention for an incident or legal duty.

Contact us for the applicable retention period for a particular record. Cookie durations are described in the website's cookie information.

12. Your rights

Subject to the conditions and exceptions in the law, you may:

- Request access to your personal information and information about how it is used.
- Ask us to correct inaccurate or incomplete information.
- Ask us to erase information or restrict its use where the relevant conditions apply.
- Object to processing based on legitimate interests. We must stop unless we demonstrate overriding grounds or need the information for legal claims.
- Object to direct marketing at any time. This includes profiling related to that marketing; we must stop that use.
- Withdraw consent at any time where processing relies on it, without affecting the lawfulness of processing before withdrawal.
- Receive information you provided in a portable, machine-readable format where processing is automated and based on consent or contract.

We do not currently make decisions about you based solely on automated processing that have legal or similarly significant effects. If that changes, we will provide the required information and safeguards, including the ability to seek human intervention and challenge a significant automated decision.

Contact our data privacy contact to exercise your rights. We request identity information only where reasonably necessary and proportionate. Requests are normally free; a fee or refusal is possible only where legally permitted, for example for a manifestly unfounded or excessive request.

We respond without undue delay, normally within one month. Where legally permitted, we may extend this by up to two further months for complex or multiple requests and explain the extension within the initial period. Applicable rules may allow the response clock to pause while necessary identity information or clarification is obtained.

13. Complaints

You can complain about our use of your information by emailing rcrane@flightlg.com, telephoning 01753 763500 or writing to the address in section 1. Please explain your concern and how we can contact you. We acknowledge data protection complaints within 30 days, investigate and respond without undue delay.

You also have the right to complain to the Information Commissioner's Office (ICO). You do not have to complain to us first.

Website: ico.org.uk/make-a-complaint/

Telephone: 0303 123 1113.