Privacy Policy

Background

Blackthorne International Transport Ltd ("we") are committed to protecting and respecting the privacy and rights of all our data subjects; the people whose personal data we collect and use. We value the personal information entrusted to us and we respect that trust, by complying with all relevant laws and adopting good practice. This policy sets out the basis on which any personal data will be processed by us, what we collect and why, what we do with the information, what we won't do with the information and what rights our data subjects have.

It also applies to all the websites we operate, our use of emails and social media for marketing purposes, paper-based communications and any other methods we use for collecting information.

Under the General Data Protection Regulation (GDPR), the data controller is Blackthorne International Transport Ltd.

Contents

1. The personal data we process

The definition of personal data under the GDPR is "*any information relating to an identifiable person who can be directly or indirectly identified*". This applies to data within both manual filing systems and data that is collected and processed electronically. Personal data items are therefore diverse and include names, email addresses, ID numbers, location data, online identifiers, employment details, photographs, voicemails, etc.

a) Personal data we collect

Information given to us by data subjects

Data subjects may give us information about themselves when they communicate to us via email or by corresponding with us by phone, in person or otherwise. This includes information provided when they use our website, subscribe to our service, etc. The information given to us at any stage of the shipment process may include, but is not limited to, a name, address, e-mail address and phone number, financial and credit card information and personal description.

Blackthorne International Transport Limited
Unit 9 Trident Industrial Estate
Blackthorne Road, Colnbrook
Berkshire SL3 0AX, UK

T +44 (0)1753 687 848
E info@blackthornetransport.co.uk
www.blackthornetransport.com

Information we collect automatically

We may automatically collect the following information each time an individual visits our website:

- technical information, including the Internet protocol (IP) address used to connect to the Internet, login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform;
- information about the visit, including the full Uniform Resource Locators (URL) clickstream to, through and from our site (including date and time); products viewed or searched for; page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page and any phone number used to call our customer service number.

Information we receive from other sources

We may receive information about individuals if they use any services we provide. (In this case we will have informed individuals when we collected the data that it may be shared internally and combined with data collected on our website.) We are also working closely with third parties (including, for example, business partners, sub-contractors in technical, payment and delivery services, advertising networks, analytics providers, search information providers, credit reference agencies) and may receive information about you from them.

b) Special category data

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. Sensitive personal data is data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership/activities, mental or physical health, sexual orientation, genetic and biometric data.
Information on criminal activity is also considered 'special category' data.

In the event that we process sensitive personal data, we must meet an extra condition for processing, as detailed in section 2.

c) Cookies

Our website uses cookies to distinguish individuals from other users of our website. This helps us to provide a good experience when browsing our website and also allows us to improve our site. For detailed information on the cookies we use and the purposes for which we use them, see our Cookie policy.

d) Categories of data subjects

Our data subjects typically fall under one of the following categories:

- Consultants
- Clients/Customers
- Employees
- Overseas Agents
- Regulatory Bodies
- Suppliers

2. Our lawful basis for processing personal data

Processing of personal data is only lawful if at least one of these legal conditions, as listed in Article 6 of the GDPR, is met:

- the processing is **necessary for a contract** with the data subject;
- the processing is **necessary for us to comply with a legal obligation**;
- the processing is necessary to protect someone's life (this is called "**vital interests**");
- the processing is necessary for us to perform a task in the **public interest**, and the task has a clear basis in law;
- the processing is **necessary for legitimate interests** pursued by Blackthorne or one of our business partners, unless these are overridden by the interests, rights and freedoms of the data subject.
- If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their clear **consent**.

Processing of 'special categories' of personal data is only lawful when, in addition to the conditions above, one of the extra conditions, as listed in Article 9 of the GDPR, is met. These conditions include where:

- the processing is necessary for carrying out our obligations under **employment** and **social security** and **social protection legislation**;
- the processing is necessary for **safeguarding the vital interests** (in emergency, life or death situations) **of an individual** and the data subject is incapable of giving consent;
- the processing is carried out **in the course of our legitimate activities** and only relates to our members or persons we are in regular contact with in connection with our purposes;
- the processing is necessary for **pursuing legal claims**;
- If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their **explicit consent**.

3. Our intended purposes for processing personal data

We use information held about our data subjects in the following ways:

Information given to us by data subjects

We will use this information to:

- meet our legal obligations as an employer under current employment legislation;
- meet our contractual obligations in facilitating training and development of our staff;
- identify and communicate with our clients, suppliers and other stakeholders;
- provide a personalised service to all our stakeholders;
- enable us to process our clients' requirements to the highest standards in liaison with our business partners;
- record any contact we have with people;
- prevent or detect fraud or abuses of our websites and enable third parties to carry out technical, logistical or other functions on our behalf;
- to carry out research on the demographics, interests and behaviour of our website users to help us gain a better understanding of them and to enable us to improve our service;
- where consent is obtained, or on a legitimate interest basis for existing customers, provide people with information that we think may be of interest to them.

Information we collect automatically

We will use this information to:

- administer our site and for internal operations, including troubleshooting, data analysis, testing, research and statistical purposes;
- improve our site to ensure that content is presented in the most effective manner for our website visitors;
- allow website visitors to participate in interactive features of our service, when they choose to do so;
- support our efforts to keep our site safe and secure;
- measure or understand the effectiveness of advertising we serve to website visitors, and to deliver relevant advertising;
- make suggestions and recommendations to users of our site about goods or services that may interest them.

Information we receive from other sources

We may combine this information with information given to us and information we collect automatically. We may us this information and the combined information for the purposes set out above (depending on the types of information we receive).

4. Who we share personal data with

We may share personal information with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

We may share your information with selected third parties if:

- we are legally required to do so, e.g. by a law enforcement agency legitimately exercising a power or if compelled by an order of the Court;

- we believe it is necessary to protect or defend our rights, property or the personal safety of our people or visitors to our premises or websites;
- we are working with a carefully-selected partner that is carrying out work on our behalf;
- analytics and search engine providers that assist us in the improvement and optimisation of our site ;
- credit reference agencies for the purpose of assessing a credit risk where this is a condition of us entering into a contract with someone.

We may disclose personal information to third parties:
- in the event that we sell or buy any business or assets, in which case we may disclose personal data to the prospective seller or buyer of such business or assets;
- if Blackthorne or substantially all of its assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets;
- if we are under a duty to disclose or share personal data in order to comply with any legal obligation, or in order to enforce or apply our terms of use or terms and conditions of supply and other agreements; or to protect the rights, property, or safety of Blackthorne, our clients or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

We never sell or share personal information to other organisations to use for their own purposes.

5. How we protect personal data

We will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage.

We will implement security measures which provide a level of security which is appropriate to the risks involved in the processing.

Measures will include technical and organisational security measures. In assessing what measures are the most appropriate we will take into account the following, and anything else that is relevant:
- the quality of the security measure;
- the costs of implementation;
- the nature, scope, context and purpose of processing;
- the risk (of varying likelihood and severity) to the rights and freedoms of data subjects;
- the risk which could result from a data breach.

Measures may include:
- technical systems security;
- measures to restrict or minimise access to data;
- measures to ensure our systems and data remain available, or can be easily restored in the case of an incident;
- physical security of information and of our premises;
- organisational measures, including policies, procedures, training and audits;
- regular testing and evaluating of the effectiveness of security measures.

If stored electronically, information is stored by us on computers located in the UK and on reputable cloud-based storage systems. We may transfer the information to other offices and to other reputable third-party organisations for the purposes of back-up and mobile working. They may be situated inside or outside the European Economic Area.

Where we have provided (or where individuals have chosen) a password which enables access certain parts of our site, individuals are responsible for keeping this password confidential. We advise that passwords should not be shared with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect personal data, we cannot guarantee the security of data transmitted to our site; any transmission is

at individuals' own risk. Once we have received information, we will use strict procedures and security features to try to prevent unauthorised access.

We may also store information in non-electronic forms, for which we have security procedures in place to protect it in line with current data protection legislation.

Our **Information Security Policy** contains further details on the measures we have in place to protect personal data and prevent a data breach.

6. How we erase data upon expiry of retention period

We will not keep personal data longer than necessary for the purposes for which it was collected. We will comply with official guidance on retention periods for specific records. Further information can be found in our Data Retention Schedule.

Personal data stored electronically will be deleted from the individual systems so it is no longer accessible by regular users of the system. Devices containing personal data that are due for destruction will have the data overwritten then the device destroyed in line with BS EN15713:2009 standards.

Documentation containing personal data stored or archived in physical files will be shredded upon expiry of the retention period in line with BS EN15713:2009 standards. We can provide data destruction certificates for both data and devices to our clients if required.

7. Data subject rights

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 bring new legal rights for individuals whose personal data is processed; we will process personal data in line with individuals' rights to:

- **be informed** that their personal information is being collected - at the point of collection - and the purposes for which it is being processed, retention periods and who it will be shared with;
- **access** personal data held and processed by us;
- **rectification** of any personal data that is inaccurate or incomplete;
- **erasure**, or to 'be forgotten' if their data is no longer necessary for the purpose for which it was collected, unless it is being processed under the basis of *'legal obligation'* or to perform a task in the *'public interest'*;
- request that processing is **restricted** although we may still store their personal data; this is an alternative to requesting erasure of their data and the restriction is likely to be for a fixed period;
- **data portability**, which allows individuals to copy or transfer their personal data easily from one IT environment to another if the processing is carried out by automated means on the basis of *'consent'* or to fulfil a *'contract'*;
- **object** to processing in certain circumstances, including preventing the use of their data for direct marketing.

If we receive any request from a data subject that relates or could relate to their data protection rights, this will be forwarded to Gary O'Grady, MD, immediately, who will follow the relevant procedures accordingly.

We will act on all valid requests as soon as possible, and at the latest within **one calendar month**, unless we have reason to, and can lawfully extend the timescale. This can be extended by up to two months in some circumstances. Any information provided to data subjects will be concise and transparent, using clear and plain language.

8. Social media sites & links to third party websites

Our site may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

We operate social media pages on various platforms, as detailed on our website. Although this policy covers how we will use any data collected from those pages it does not cover how the providers of social media websites will use personal information. The privacy policy of the social media website should be read before sharing data and use made of the privacy settings and reporting mechanisms to control how personal data is used. Before providing

anyone else's data (e.g. tagging photos, etc.) please ensure they have given consent to do so and under no circumstances must another person's home address, email address, or phone number be made public.

9. Contact

Questions, comments and requests regarding this privacy policy are welcomed and should be addressed to our Data Compliance Officer via email to info@blackthorneit.com, or phone or write to us on the contact details at the foot of the first page of this policy.