Blackthorn.

Data Protection Policy and Procedures

Background

- Blackthorn. ("the Company") in the normal course of business will collect and process information in order to carry on its business and meet the requirements of its clients.
- The Company is committed to ensuring its compliance with the requirements of the UK's retained law version of the General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("the Act") and other applicable data protection and related laws (all together, where applicable, the "DP Laws").
- We recognise the importance of personal data to our business and the importance of respecting the privacy rights of individuals.

Scope and Purpose

This Data Protection Policy (the Policy) sets out the principles which we will apply to our processing of personal data so that we ensure we safeguard and respect the data protection rights of individuals and process their personal data in accordance with the law. The aim of the Policy is to provide a consistent approach to the way the Company handles personal data and provides a clear set of guidelines on the processing of personal data.

Responsibilities

The Board of the Company is collectively responsible for maintaining this Policy and ensuring it continues to meet the requirements of the Company, its clients and any obligations prescribed by law or by a regulatory body. The Board is also responsible for establishing and communicating relevant procedures to the business. The Data Protection Manager will deal with any data protection issues that arise within the Company and will deal with subject access requests. Ensuring that this Policy is implemented, and that relevant documentation is maintained is the responsibility of the Company's managers. The Information Commissioner's Office is responsible for enforcing data protection in the UK, which includes breaches of the data protection principles set out in UK GDPR.

Definitions

The following definitions of terms used in this document are drawn from Article 4 of UK GDPR:

Personal data: data which relate to a living individual ("Data Subject") who can be identified from those data, or from those data and other information, which is in the possession of, or is likely to come into the possession of, the data controller.

Special categories of personal data: more sensitive personal data which needs greater protection. Special category data is similar to the concept of 'sensitive personal data' under Data Protection Act 1998 (now superseded by the Act) and includes one of the following types of data:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric data processed for the purpose of uniquely identifying an individual
- Health data

- Data concerning an individual's sex life or sexual orientation

Data Controller: The natural or legal person, public authority, agency, or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: A natural or legal person, public authority, agency, or any other body which processes personal data on behalf of a Data Controller.

Processing: An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of the data.

Anonymisation: Irreversibly amending personal data such that an individual cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The personal data processing principles do not apply to anonymized data as it is no longer personal data.

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymisation reduces, but does not completely eliminate, the ability to link personal data to a data subject. As pseudonymised data is still personal data, the processing of pseudonymised data should comply with the Personal Data Processing principles.

Key Considerations

Data protection principles

UK GDPR sets out six data protection principles and various safeguards to which the Company must adhere. All six principles must be met in order for the Company to comply with DP Laws.

(i) first data protection principle – processing must be lawful and fair
(ii) second data protection principle – purposes of processing must be specified, explicit and legitimate
(iii) third data protection principle – personal data must be adequate, relevant, and not excessive
(iv) fourth data protection principle – personal data must be accurate and kept up to date
(v) fifth data protection principle – personal data must be kept for no longer than is necessary
(vi) sixth data protection principle – personal data must be processed in a secure manner.

Rights of data subjects

The rights of data subjects are set out in Chapter 3 of UK GDPR and includes the following:

Key rights and obligations	Overview of requirements
Make information available to individuals	The controller is required to make available to the data subject a range of information, including: • The identity and contact details of the controller • The purpose for which their personal data is being processed • The existence of their right to exercise any of the below rights • The legal basis for the processing of their personal data • The retention period or criteria used to determine the retention period
Right of access	Confirmation from the controller whether or not a data subject's personal data is being processed and, if this personal data is being processed, access to that personal data.

Right to rectification	The controller must, if requested, rectify or complete inaccurate or incomplete personal data. A controller must notify the competent authority (if any) from which the inaccurate personal data originated, where this personal data has been rectified. A controller must notify the recipients of personal data, where personal data which been rectified, which has been disclosed by the controller. Similarly, the recipient must rectify the processing of the personal data in so far as they retain responsibility for it.
Right to erasure or restriction of processing	The controller is obliged, if conditions are met, to erase personal data or restrict its processing without delay. A controller must notify the recipients of personal data, where personal data which been erased or restricted which has been disclosed by the controller. Similarly, the recipient must erase or restrict the processing of the personal data in so far as they retain responsibility for it.
Right not to be subject to automated decision making	A controller cannot take a significant decision based solely on automated processing unless that decision is authorised by law.
Exercise of rights through the Commissioner	An individual has the option to exercise their rights through the Information Commissioner.

Building data protection in business activities

In order to demonstrate compliance with relevant legal and regulatory requirements including the data protection principles, the Company has put in place comprehensive and proportionate governance measures which ensure and demonstrate compliance with data protection requirements which include:

- This Data Protection Policy and Procedures
- Informing and training all staff in the Company on how to implement this Policy
- Responsibility on senior management for monitoring this implementation, assessing, and demonstrating to external stakeholders and supervisory authorities the quality of the implementation
- Fair Processing Guidelines which are set out in Section 3 of this Policy

Subject access request

A Subject Access Request (“SAR”, or as it is often also known, a "DSAR") is any request made by an individual or his/her representative for personal data held by the Company in respect of that individual as well as certain other supplementary information (see below). When a SAR is received, a record must be kept of that request. The Company will not make a charge for responding to a SAR and will only request proof of identity where there are doubts about the identity of the person making the request. Where the Company uses third party suppliers who also hold personal data for the Company, then when complying with a SAR, copies of personal data held by such suppliers will also be requested and supplied within the time limits prescribed below.

What is an individual entitled to?

An individual has the right to obtain a copy of the personal data held relating to that individual, and other supplementary information set out below but not to personal data relating to other people, nor to any other information.

Supplementary information

When providing a copy of personal data, the Company must also provide individuals with the following information:

- The purposes of processing
- Categories of personal data concerned
- Recipients or categories of recipients to whom that personal data is disclosed
- Either the retention period for storing that personal data or (if that is not possible) the criteria used to determine for how long that personal data should be stored
- His/her right to rectification, erasure, or restriction or to object to processing of personal data
- If the information was obtained from a third party, the identity of that third party
- The right to make a complaint to the Information Commissioner's Office
- If appropriate the existence of automated decision making such as profiling
- Safeguards for protecting personal data in the event it is transferred outside the UK

The supplementary information is contained in the Company's privacy notice and a copy of this should be supplied when responding to a SAR.

Time for responding to a SAR

The Company will respond to a SAR without undue delay and no later than one month from the date the request is received (whether the date is a working day or not). If the date for responding falls on a weekend or public holiday then the Company can provide the information on the next working day. Where the Company cannot meet the deadline, then, exceptionally, it may take up to a further two months but in this event the individual must be notified within a month of receiving his/her request why an extension is necessary and when the Company expects to provide the information requested.

Reporting a personal data breach

In the event of a breach of these procedures leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data, then on the Company becoming aware of the personal data breach the Data Protection Manager will immediately assess the impact of the personal data breach to establish the likelihood and severity of the risk of damage to a person's rights and freedoms. If it is established there is a risk of such damage the personal data breach is reportable to the Information Commissioner's Office, the Data Protection Manager shall notify the Information Commissioner's Office within 72 hours of the Company becoming aware of the personal data breach, giving the following information:

- A description of the nature of the personal data breach including where possible the categories and approximate number of individuals and personal data concerned
- The name and contact details of the Data Protection Manager
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including where appropriate the measures taken to mitigate any possible effects.

If notification of a personal data breach is made to the Information Commissioner's Office, then the Company will also send a copy of the notice to:

- Insurers; and
- Where applicable, notification may need to be given to the Financial Conduct Authority.

All personal data breaches must be logged in the Data Protection Breach Register. If a decision is made that a personal data breach is not reportable to the ICO a full and detailed explanation as to why the personal data breach is deemed not reportable should be recorded in the register.

If the Company determines in the 72 hours of becoming aware of the personal data breach that it is likely to result in a high risk to the rights and freedoms of any individual, then the Company must communicate the personal data breach to the individual without delay and in clear and plain language.

Fair Processing Guidelines

The Company will adhere to these guidelines when processing personal data to ensure that when processing personal data, it is fair, lawful, and transparent.

The Company will:

- Only process data where the Company has a valid lawful basis in order to process personal data
- Ensure when collecting personal data directly from individuals that individuals are aware of this collection
- The Company's identity and of anyone else who collects personal data on behalf of the Company
- The purposes for which the Company intends to process the personal data
- Any other information needed to ensure fairness to individuals, taking into account the specific circumstances of the processing. This will include informing individuals of any disclosure of information about them to third parties, including disclosure to companies within the same group
- Be open and direct when dealing with individuals and explain how their information will be used. Individuals must be made aware that information is being collected and must always be informed of the purpose for which their information will be used, the source of the information obtained and to whom it may be disclosed. This is done by issuing a Privacy Notice in the form annexed to schedule 1, which is given to individuals prior to collecting any personal information and/or included in client agreements, terms of business or other client documentation. Consent clauses, if required, should also be present in telephone scripts
- Obtain, where required, consents from data subject before processing any personal data
- Respect the rights of data subjects and ensure that it has procedures in place including ensuring that personal data is processed in a way that complies with the Company's Privacy Notice and this Policy.

Data Protection Privacy Notice

This data protection notice contains important information on who we are, how and why we collect, store, use and share personal data, your rights in relation to personal data and on how to contact us and supervisory authorities in the event you have a complaint.

Who we are

Blackthorn. is the trading name of CHC Insurance Services Limited ("the Company") provides professional services to the Lloyd's, London, and international insurance markets. The Company collects, uses and is responsible for certain personal information about you. When we do so we are regulated under the United Kingdom's version of the General Data Protection Regulation, and is responsible as 'controller' of that personal data.

The personal data that we collect and use

Information collected by us

In the course of providing our services, we collect a variety of personal information by phone, email, and postal correspondence, through the use of our website, and during our dealings with clients, regulators and others. Personal information we might collect includes the following:

Type of Personal Information	Example
Individual details	• Name and title • Home address, personal email address, telephone numbers • Date and place of birth • Nationality • Sex • Marital status • Employer, job title, employment history, work address, work email address and telephone numbers

Official identification details	• National Insurance number • Passport • Driving license
Financial information	• Credit history and credit score • Source of income and amount • Details of assets
Risk details	• Criminal convictions or fraudulent activity • Directors' disqualification orders and undertakings
Anti-fraud information	• Information obtained through sanctions checks • Information received from various antifraud databases
Other	• Information obtained through general correspondence • IP address and domain name, location data and other information collected if you visit our website • Information obtained by other electronic means if you visit our offices, such as door access cards and CCTV security footage

Type of Personal Information	Example
	• Dietary information if you attend one of our events

Information collected from other sources

We might also obtain personal data from other sources as follows:

- As part of a recruitment process, eg from your employer or recruitment agencies.
- In the normal course of onboarding checks, eg from credit or background reference agencies, regulators, antifraud or sanctions databases or court judgements.
- From brokers and other insurance market participants as part of trading activities, or from participants in a claims process, such as witnesses, loss adjusters or advisers.
- In the normal course of business from other third parties eg. Commercial Business to Business data bases.

How we use your personal information

We use your personal data:

- To provide services to our clients
- To monitor our compliance within the laws and regulations that affect us
- For business-to-business emails regarding information about our business, and invitations to events we hold
- For our own internal analysis

We will share personal information with regulators including the Financial Conduct Authority, law enforcement or other authorities if required by applicable law. Subject to 4.7 below, we will not share your personal information with any other third party.

How long your personal information will be kept

We will hold personal information we collect for the period we are required to retain this information by applicable legal and regulatory provisions which will be currently 7 years from the termination of our arrangements, or such other period specified in our Data Retention Policy.

Reasons we can collect and use your personal information:

Under the GDPR, we must always have your consent or another lawful basis for using personal data. This may be because the data is necessary for our performance of a contract with you, or because it is in our legitimate business interests to use it (legal basis). If we rely on your consent, you may withdraw your consent to such processing at any time.

Transfer of your information out of the EEA

We may need to transfer your data to third parties including insurance market participants or their affiliates or sub- contractors which are located outside of the European Economic Area (EEA). Those transfers would always be made in compliance with the GDPR. If you would like further details of how your personal data would be protected if transferred outside the EEA, please contact the Data Manager at Blackthorn. (see 'How to contact us' below).

Your rights

Under the DP Law, you have a number of important rights which may exercise free of charge. In summary, those include rights to:

- Access to your personal information and to certain other supplementary information that this Privacy Notice is already designed to address
- Require us to correct any mistakes in your information which we hold
- Require the erasure of personal information concerning you in certain situations
- Receive the personal information concerning you which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to a third party in certain situations
- Object at any time to processing of personal information concerning you for direct marketing
- Object to decisions being taken by automated means which produce legal effects concerning you or similarly significantly affect you
- Object in certain other situations to our continued processing of your personal information
- Otherwise restrict our processing of your personal information in certain circumstances

For further information on each of those rights, including the circumstances in which they apply, see the Guidance from the UK Information Commissioner's Office (ICO) on individuals' rights under the UK GDPR.

Keeping your personal information secure

We have appropriate security measures in place to prevent personal information from being accidentally lost or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

How to complain

We hope that we can resolve any query or concern you raise about our use of your information.

If we are unable to resolve your concern or compliant about our processing of personal data, you may contact the Information Commissioner's Office at https://ico.org.uk/concerns/.

Changes to this privacy notice

We may change this privacy notice from time to time.

How to contact us

If you have any questions about this privacy notice or the information, we hold about you then you can contact us:

Blackthorn.
64-72 Leadenhall Market, London EC3V 1LT
info@blackthornrisk.com

If you would like this notice in another format (for example: audio, large print, braille) please contact us.