

Privacy Policy

Introduction

Your privacy is important to the HCT group of companies (“**HCT**”, “**we**”, “**us**” and “**our**”) and we want you to feel comfortable with how we use and share your personal information. HCT together with the various parties it works with to provide you with its products and services are committed to protecting and respecting your privacy. This policy explains when and why your data is collected, how it is used and disclosed and how it is kept secure.

The products and services referred to in this policy relate to those offered by HCT Concierge and HCT Finance.

Please read the following carefully to understand our views and practices regarding your personal data and how it will be treated.

We will act as a data controller of your personal data which: -

1. You provide to us (see ‘When you apply for a HCT Concierge Membership account’ below) and;
2. Which we may automatically collect about you – for example, details of your browser and operating system, the website from which you visit our site, the pages that you visit on our site, the date of your visit, and, for security reasons such as to identify attacks on our site, the Internet protocol (IP) address assigned to you by your internet service. We may use Google Analytics to collect tracking information about you.

This means that we are responsible for deciding how we hold and use personal data about you, and we are required to notify you about what data we collect and its usage in this policy.

Queries

If you have any queries, you can contact us using the details provided at the end of this policy in the “Contacting Us” section.

About HCT Concierge

HCT Concierge offers a bespoke suite of VIP to clients. For more information please visit <https://www.hctconcierge.com/>.

This policy together with the HCT Concierge Membership Terms and Conditions <https://claireh9.sg-host.com/hct-concierge-terms-and-conditions/> and any other documents referred to in them, set out the basis on which any personal data which we will collect from you, or collected about you, on <https://www.hctconcierge.com/> (“**Website**”), on [HCT FINANCE] (“**App**”) or when you communicate with us by email, telephone or post will be processed.

Information we collect about you and how it will be used

When you apply for a HCT Concierge Membership account

When you apply for a HCT Concierge Membership account (“**Concierge Membership**”) on the Website or App, we will need to collect (and in some cases store) some or all of the following details about you:

- Name
- Residential addresses (current)
- Date of birth
- Gender
- Email address
- Telephone numbers
- ID document numbers such as passport, driving licence or ID card.
- Image or photo of you

We will use this information for the purposes of processing your Concierge Membership application and, if your application is successful, creating and managing your Concierge Membership, and providing any products or services you request to you. If you have consented, we will also send our newsletter to you by email.

You will not be able to apply to apply for Concierge Membership or order products and services from us without providing this information.

For clarity, HCT will be the data controller of this personal data information.

Ensuring the lawful use of your personal data

Your personal data will only be used where we or the parties we work with to provide you products and services have a lawful basis to do so. The purposes for which we will use your personal data include:

- Where it is necessary for the **performance of the contract** with you or to take steps to enter into it. For example, when we need to verify your identity, to provide you with HCT Concierge products and services under the Membership agreement, communicating with you, to provide you with updates on the status of your membership, complaints handling dealing and notifying you of any changes to this statement).
- It is necessary for our **legitimate interests** or that of a third party. This includes:
 - to enhance and personalise your client or visitor experience;
 - to identify you when you contact us and to correspond and communicate with you;
 - for market research in order to continually improve the products and services that we offer and deliver to you;
 - to verify the accuracy of data that we hold about you and create a better understanding of you as a client or visitor;
 - creating a profile of you, which enables us to identify and personalise what products and services to offer to you for marketing purposes;
 - to administer our site, for website analysis and for internal operations, including troubleshooting, testing, statistical purposes;
 - for network and information security in order for us to take steps to protect your information against loss or damage, theft or unauthorised access;
 - for the prevention of fraud and other criminal activities;
 - to protect our contractual or other legal rights;
 - for general administration including managing your queries and to send service messages to you;
- It is necessary for compliance with a **legal obligation**. This includes, but not limited to, when you exercise your legal rights under data protection law, to verify your identity, for the establishment and defence of our legal rights and for compliance with our legal and regulatory responsibilities.

- You have given us your **consent** to use your personal data in certain ways, including when you request that we disclose it to a third party and for direct marketing communications (by us and the third parties named when we asked for your consent).
- In order to process your Concierge Membership we may need to perform **Fraud and money laundering checks** before and whilst we continue to provide services or supply goods to you. This may involve sharing your personal data with fraud prevention agencies who will also process your personal data, but only on the basis that we have a legitimate interest in preventing fraud and money laundering, and to verify identity, in order to protect our business and to comply with laws that apply to us. We, and fraud prevention agencies, may also enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime.

You have the right at any time to ask us, or the third parties we work with, to stop contacting you or passing your details to others for marketing purposes. Please contact us for further information.

Automated decisions

As part of the processing of your personal data, decisions may be made by automated means. This means we may automatically decide that you pose a fraud or money laundering risk if:

- our processing reveals your behaviour to be consistent with that of known fraudsters or money launderers; or is inconsistent with your previous submissions; or
- you appear to have deliberately hidden your true identity.

You have rights in relation to automated decision making: if you want to know more, please contact us using the details below.

Consequences of processing

If we, or a fraud prevention agency, determine that you pose a fraud or money laundering risk, we may refuse to provide the services you have requested, or we may stop providing existing services to you.

A record of any fraud or money laundering risk will be retained by the fraud prevention agencies, and may result in others refusing to provide services, financing or employment to you. If you have any questions about this, please contact us on the details below.

Other than the automated processing set out above, we shall not carry out solely automated decision-making using your personal data.

When you contact us

When you contact us, we will need to collect personal data about you to verify your identity before we disclose any information to you for data security purposes. We will be unable to deal with your query unless you provide the information we request. We may also collect any other personal data you choose to provide to us when communicating with us. We will only use that personal data for the purposes of dealing with your enquiry.

The information we receive from other sources

We are also working closely with third parties (including, for example identity verification agencies, marketing agencies and fraud prevention agencies) and we may receive information about you from them for the purposes of identity verification, marketing and fraud prevention.

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will usually notify you and we will explain the legal basis which allows us to do so.

Disclosures of your information

We may disclose your information to:

- Law enforcement and fraud prevention agencies, identity verification services and other organisations for the purposes of preventing fraud and money laundering;
- Our group companies, for the purposes of processing transactions and providing services relating to your Concierge Membership;
- Courts in the United Kingdom or abroad as necessary to comply with a legal requirement, for the administration of justice, to protect vital interests and to protect the security or integrity of our business operations;
- Third parties acting on our behalf, such as service providers, agents, subcontractors and other organisations for the purposes of providing services to us or directly to you on our behalf. These parties may include back-up and server hosting providers, IT software and maintenance providers, third parties that provide income verification services and affordability checks, claims management companies, communication fulfilment services, marketing research organisations and Google Analytics;
- Other third parties, with your consent, who may contact you by email to provide you with information about their products and services which may be of interest to you;
- In the event that we sell or buy any business or assets, to the prospective seller or buyer of such business or assets;
- A third party if we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply our Terms and Conditions and other agreements; or to protect the rights, property, or safety of HCT, our clients or others.

Protecting your information

Your data is secured by encryption, firewalls and Secure Socket Layer (SSL) technology. This is industry standard encryption technology which manages the security of messages transmitted across the internet. When we receive your data, we store it on secure encrypted servers with access controls applied to all data.

Storing your data within and outside the EEA

Our third-party data host provider uses servers located in the UK to store personal data. As a result, when you use the Website or App to make transactions or update your account

information, your personal data may be transferred to the UK which is located outside of the European Economic Area and so is not governed by European data protection laws.

Whenever fraud prevention agencies transfer your personal data outside of the European Economic Area, they impose the EU standard contractual clauses adopted by the European Commission on the recipients of that data in order to safeguard personal data when it is accessed from outside of the European Economic Area. They may also require the recipient to subscribe to 'international frameworks' intended to enable secure data sharing.

More information about the EU Standard Contractual Clauses is available here <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32010D0087>.

Use of Cookies

What are Cookies?

Cookies are small text files that are placed on your device (e.g. computer, mobile device) when you visit a website and give permission for that site to recognise your device. Cookies stores information about a user's visit, which may include the content viewed, language preference, time and duration of each visit to the website.

Why do some websites use Cookies?

Cookies are widely used in order to make websites work more efficiently, such as letting you navigate between pages efficiently, remembering your preferences, as well as providing information to the website owner.

Does HCT use Cookies?

No, we do not use cookies on our websites, and this is the reason why we do not ask for your express consent to place cookies onto your device, unlike other websites which use them and are legally obliged to get your consent before placing them on your device.

Should our decision to use cookies change in the future, we will firstly seek your express consent before placing them on your device.

Future changes

Any changes we make to our policy will be put on our Website and App and, where appropriate, notified to you by e-mail. Please check for updates from time to time.

Retention of your Data

We will retain your personal data for as long as you continue to use our services. Thereafter, we may retain your information for an additional period as is permitted or required under applicable laws. For example:

- If you hold a Concierge Membership with us, your personal data will be retained for six years after the closure of your account to comply with our obligations under anti-money laundering regulations;
- If you make a complaint, your personal data relating to that complaint will be retained for five years from the resolution of that complaint to defend against legal claims; and

- If you make any transactions, your personal data relating to that transaction will be retained for seven years from the date of the transaction to comply with taxation and accountancy legislation.

Your rights

Data protection laws provide you with the following rights to:

- request access to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it;
- request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected;
- request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below);
- request the restriction of processing of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it;
- request a copy of your personal data which you have provided to us, in a structured, commonly used and machine-readable format and the right to transfer it, or to require us to transfer it directly, to another controller.
- object to the processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights above). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

If you are unhappy about how your personal data has been used, please refer to our complaints procedure which is available by contacting us. You also have a right to complain to the supervisory authority, which in the United Kingdom is the Information Commissioner's Office <https://ico.org.uk/> who regulates the processing of personal data.

Contacting us

If you have any questions about this policy, you can contact us by using the ‘Contact us’ facility on the Website or App or in the following ways:

By post at:

Data Protection Officer
Unit F, Bromley Business Centre,
127 Hastings Road,
Bromley
BR2 8NA

By email at: info@eic.ltd

This policy was last updated on 16.01.2023