

# hi Global Privacy Notice

**Last Update: January 2026**

Welcome to the hi Global Privacy Notice (“Privacy Notice”). Please spend a few minutes reading it carefully before you provide us with any information about you or any other person.

## 1. Introduction

We respect your privacy and are committed to protecting your personal data. This Privacy Notice applies to the processing of personal data by hi group entities, including hi Financial Limited, a company incorporated and registered in the British Virgin Islands with company number 2044320 and its registered office at Intershore Chambers, Road Town, Tortola, British Virgin Islands, VG1110(business address) and its affiliates (“hi”, “hi.com”, “the Company”, “we”, “us”, “our”), in connection with:

- Use of any of our products, services, or applications (collectively, the “Services” or the “Platform”);
- Visiting or using our websites hi.com (“Site”), or mobile application (“App”).

hi Financial Limited, a company incorporated and registered in the British Virgin Islands with company number 2044320 and its registered office at Intershore Chambers, Road Town, Tortola, British Virgin Islands, VG1110 acts primarily as a data processor, providing services on behalf of other hi group entities or clients, except where it processes data for its own internal operations.

**Please note that our Services, Site, and Apps are not intended for individuals under the age of 18, and we do not knowingly collect data relating to minors.**

## 2. Purpose

This Privacy Notice aims to give you information on why and how we collect and process your personal data. This Privacy Notice informs you about your privacy rights and how the data protection principles set out in the EU General Data Protection Regulation (“GDPR”) and the post-Brexit privacy law publicly known as the UK GDPR protect you.

It is important that you read this Privacy Notice together with any other notice or policy we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of why and how we are using your data. This Privacy Notice supplements other notices and policies and is not intended to override them.

## 3. Who we are

### **Independent Regulated Service Provider (EEA)**

Noemon Tech Limited is a private limited company incorporated and registered in the Republic of Cyprus with registration number HE 427232. Noemon Tech Limited is duly registered as a Crypto-Asset Service Provider (CASP) and is regulated and supervised by the Cyprus Securities and Exchange Commission (CySEC) under Registration Number 014/24.

Noemon Tech Limited is not part of the hi group and provides regulated crypto-asset services to hi group entities as an independent third-party service provider, including under a Regulated-as-a-Service (RAAS) model.

---

## Role as Data Controller (EEA)

For individuals located in the European Economic Area (EEA), **Noemon Tech Limited** acts as an independent data controller within the meaning of the EU General Data Protection Regulation (“GDPR”) where it processes personal data in connection with the provision of regulated crypto-asset services.

In particular, Noemon Tech Limited acts as a data controller in respect of personal data processed for the purposes of:

- customer onboarding and identity verification (KYC);
- anti-money laundering (“AML”) and counter-terrorism financing (“CTF”) compliance;
- sanctions screening and transaction monitoring;
- custody-related regulatory obligations;
- regulatory reporting and record-keeping under applicable EU and Cypriot law.

As data controller, Noemon Tech Limited determines the purposes and means of processing such personal data and processes personal data in accordance with its obligations under the GDPR, Regulation (EU) 2023/1114 on Markets in Crypto-Assets (“MiCA”), and other applicable regulatory frameworks.

---

## hi Group Entities and Application Layer

The **hi mobile application (“hi app”)** is operated by entities within the **hi group** and functions solely as a **user interface** through which users may access services. The hi app does not itself provide regulated crypto-asset services within the European Economic Area.

For users located **within the European Economic Area (EEA)**, all regulated crypto-asset services — including **custody, customer onboarding and identity verification (KYC), anti-money laundering and counter-terrorism financing checks (AML/CTF), transaction monitoring, and regulatory reporting** — are provided **exclusively by Noemon Tech Limited**, acting as an independent Crypto-Asset Service Provider (CASP) and data controller.

For users located **outside the EEA**, regulated or unregulated services may be provided directly by the relevant **hi group entities**, which act as data controllers or processors as applicable under local law.

**hi Financial Limited**, a company incorporated and registered in the British Virgin Islands with company number **2044320** and its registered office at Intershore Chambers, Road Town, Tortola, British Virgin Islands, VG1110, acts **solely as a data processor** when providing technical or operational services on behalf of hi group entities or other third-party clients, unless it processes personal data for its own internal purposes (such as employment or internal compliance).

For the avoidance of doubt, **Noemon Tech Limited is not a hi group entity.**

## Our Role as Processor

hi Financial Limited, a company incorporated and registered in the British Virgin Islands with company number **2044320** and its registered office at Intershore Chambers, Road Town, Tortola, British Virgin Islands, VG1110, provides operational and technical services **as a data processor** and processes personal data solely on the documented instructions of the relevant data controller, **being either a hi group entity or another independent third-party client (excluding Noemon Tech Limited where it acts as a data controller)**.

hi Financial Limited does **not** determine the purposes or means of processing personal data when acting in a processor capacity.

---

## Data Protection Officer

We have appointed a **Data Protection Officer (“DPO”)** who is responsible for overseeing questions in relation to this Privacy Notice. If you have any questions or complaints related to this Privacy Notice or our privacy practices, or if you wish to exercise your data protection rights, please contact our DPO at **dataprivacy@hi.com**

### Complaints

You have the right to make a complaint about the way we process your personal data to a supervisory authority. If you reside in an EEA Member State, you have the right to make a complaint about the way we process your personal data to the supervisory authority in the EEA Member State of your habitual residence, place of work or place of the alleged infringement. Information about your supervisory authority could be found [here](#).

We would, however, appreciate the chance to deal with your concerns before you approach a data protection regulatory authority, so please feel free to contact us in the first instance.

### Our duties and your duties in case of changes

We keep our Privacy Notice under regular review. This version was last updated on the date above written. Please check from time to time for new versions of the Privacy Notice. We will also additionally inform you on material changes of this Privacy Notice in a manner which will effectively bring the changes to your attention. It is important that the personal data we hold about you is accurate and up-to-date. Please keep us informed if your personal data changes during your relationship with us.

## 4. What data we collect about you

### Personal data

Personal data, or personal information means any information that relates to an identified or identifiable living individual. This is a broad definition which includes the specific pieces of personal data which we have described below. It does not include data which cannot be used to identify an individual person, such as a company registration number.

A “data subject” is an individual who can be identified, directly or indirectly, by personal data. This is usually by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. It does not include data where the identity has been removed (anonymous data). More information could be found [here](#).

Depending on whether and how you use our Services, Site or App, we will collect, use, store and transfer different kinds of personal data about you which we have grouped in categories as follows:

<b>Category of Personal Data</b>	<b>Examples of specific pieces of personal data</b>
Identity Data	<ul style="list-style-type: none"><li>● first name,</li><li>● maiden name,</li><li>● last name,</li><li>● username or similar identifier,</li><li>● title,</li><li>● date of birth and gender,</li><li>● biometric information, including a visual image of your face,</li><li>● national identity cards,</li><li>● passports, driving licences or other forms of identification documents.</li></ul>
Social Identity Data	<ul style="list-style-type: none"><li>● your group/company data,</li><li>● information on referrals related to you,</li><li>● political background,</li><li>● close connections,</li><li>● behavioural data,</li><li>● risk assessment,</li><li>● compliance assessment.</li></ul>
Contact Data	<ul style="list-style-type: none"><li>● residence details,</li><li>● billing address,</li><li>● delivery address,</li><li>● home address,</li><li>● work address,</li><li>● email address and telephone numbers,</li><li>● proof of address documentation.</li></ul>
Financial Data	<ul style="list-style-type: none"><li>● bank account,</li><li>● payment card details,</li><li>● virtual currency accounts,</li><li>● stored value accounts,</li><li>● amounts associated with accounts,</li><li>● external account details,</li><li>● source of funds and related documentation.</li></ul>
Transactional Data	<ul style="list-style-type: none"><li>● details about payments to and from you,</li></ul>

	<ul style="list-style-type: none"> <li>● other details of any transactions you enter into using the Services, Site or App.</li> </ul>
Investment Data	<ul style="list-style-type: none"> <li>● information about your: <ul style="list-style-type: none"> <li>○ investment objectives,</li> <li>○ investment experience,</li> <li>○ prior investments.</li> </ul> </li> </ul>
Technical Data	<ul style="list-style-type: none"> <li>● internet connectivity data,</li> <li>● internet protocol (IP) address,</li> <li>● operator and carrier data,</li> <li>● login data,</li> <li>● browser type and version,</li> <li>● device type, category and model,</li> <li>● time zone setting and location data,</li> <li>● language data,</li> <li>● application version and SDK version,</li> <li>● browser plug-in types and versions,</li> <li>● operating system and platform,</li> <li>● diagnostics data such as crash logs and any other data we collect for the purposes of measuring technical diagnostics, and</li> <li>● other information stored on or available regarding the devices you allow us access to when you visit the Site, or use the Services or the App.</li> </ul>
Profile Data	<ul style="list-style-type: none"> <li>● your username and password,</li> <li>● your identification number as our user,</li> <li>● information on whether you have hi.com App account and the email associated with your accounts,</li> <li>● requests by you for products or services,</li> <li>● your interests, preferences and feedback</li> <li>● other information generated by you when you communicate with us, for example when you address a request to our customer support.</li> </ul>
Usage Data	<ul style="list-style-type: none"> <li>● information about how you use the Site, the Services, mobile applications and other offerings made available by us, including: <ul style="list-style-type: none"> <li>○ device download time,</li> <li>○ install time,</li> <li>○ interaction type and time,</li> <li>○ event time, name and source.</li> </ul> </li> </ul>
Marketing and Communications Data	<ul style="list-style-type: none"> <li>● your preferences in receiving marketing from us or third parties, <ul style="list-style-type: none"> <li>○ your communication preferences,</li> <li>○ your survey responses.</li> </ul> </li> </ul>

As explained above under Identity Data, we will also collect a visual image of your face which we will use, in conjunction with our sub-contractors, to check your identity for onboarding purposes. This data falls within the scope of special categories of data.

### **If you refuse to provide personal data**

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you refuse to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you – for example, to provide you Services. In this case, we may have to cancel a product or service you have with us, but we will notify you if this is the case at the time.

## **5. How we collect your data**

We use different methods to collect information from and about you, including through:

**Direct interactions.** You may give us your Identity Data, Social Identity Data, Contact Data, Financial Data, Profile Data and Marketing and Communications Data by directly interacting with us, including by filling in forms, providing a visual image of yourself via the Service, by email or otherwise. This includes personal data you provide when you:

- visit our Site, Web App or App;
- apply for our Services;
- create an account;
- make use of any of our Services;
- request marketing to be sent to you, for example by subscribing to our newsletters;
- enter a competition, promotion or survey, including through social media channels;
- give us feedback or contact us.

**Automated technologies or interactions.** As you interact with us via our Site or App, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. We will also collect Transactional Data, Investment Data and Usage Data . We may also receive Technical Data and Marketing and Communications Data about you if you visit other websites employing our cookies.

**Third parties or publicly available sources.** We also obtain information about you, including Social Identity Data, from third parties or publicly available sources. These sources may include:

- fraud and crime prevention agencies,
- a customer referring you,
- public blockchain,
- publicly available information on the Internet (websites, articles etc.)

## **6. How we use your data**

### **Lawful basis**

We will only use your personal data when the applicable legislation allows us to. In other words, we have to ensure that we have a lawful basis for such use.

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- **performance of a contract:** means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract; we use this basis for provision of our Services;
- **legitimate interests:** means our interests (or those of a third party), where we make sure we use this basis as far as your interests and individual rights do not override those interests;
- **compliance with a legal obligation:** means processing your personal data where we need to comply with a legal obligation we are subject to;
- **consent:** means freely given, specific, informed and unambiguous indication of your wishes by which you, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to you; under specific circumstances this consent should be explicit – if this is the case, we will ask for it properly.

### Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please [contact us](#) if you need details about the specific legal ground, we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose and/or activity	Categories of personal data	Lawful basis for processing
To register you as a new customer	<ul style="list-style-type: none"> <li>● Identity Data</li> <li>● Social Identity Data</li> <li>● Contact Data</li> <li>● Financial Data</li> </ul>	<ul style="list-style-type: none"> <li>● Performance of a contract</li> </ul>
To carry out and comply with anti-money laundering requirements	<ul style="list-style-type: none"> <li>● Identity Data</li> <li>● Social Identity Data</li> <li>● Contact Data</li> <li>● Financial Data</li> </ul>	<ul style="list-style-type: none"> <li>● Compliance with a legal obligation</li> </ul>
To process and deliver our Services and any App features to you, including to execute, manage and process any instructions or orders you make	<ul style="list-style-type: none"> <li>● Identity Data</li> <li>● Contact Data</li> <li>● Financial Data</li> <li>● Transactional Data</li> <li>● Technical Data</li> <li>● Marketing and Communications Data</li> </ul>	<ul style="list-style-type: none"> <li>● Performance of a contract</li> </ul>

<p>To prevent abuse of our Services and promotions</p>	<ul style="list-style-type: none"> <li>● Identity Data</li> <li>● Contact Data</li> <li>● Financial Data</li> <li>● Transactional Data</li> <li>● Technical Data</li> <li>● Marketing and Communications Data</li> </ul>	<ul style="list-style-type: none"> <li>● Legitimate interests</li> </ul>
<p>To manage our relationship with you which will include asking you to leave a review, take a survey or keeping you informed of our company's business and product development</p>	<ul style="list-style-type: none"> <li>● Identity Data</li> <li>● Contact Data</li> <li>● Profile Data</li> <li>● Transactional Data</li> <li>● Marketing and Communications Data</li> </ul>	<ul style="list-style-type: none"> <li>● Performance of a contract</li> <li>● Consent, if required</li> </ul>
<p>To keep our records updated and to study how customers use our products/services</p>	<ul style="list-style-type: none"> <li>● Identity Data</li> <li>● Contact Data</li> <li>● Profile Data</li> <li>● Transactional Data</li> <li>● Marketing and Communications Data</li> </ul>	<ul style="list-style-type: none"> <li>● Legitimate interests</li> <li>● Consent, if required</li> </ul>
<p>To manage, process, collect and transfer payments, fees and charges, and to collect and recover payments owed to us</p>	<ul style="list-style-type: none"> <li>● Identity Data</li> <li>● Contact Data</li> <li>● Financial Data</li> </ul>	<ul style="list-style-type: none"> <li>● Performance of a contract</li> </ul>
<p>To ensure good management of our payments, fees and charges and collection and recovery of payments owed to us</p>	<ul style="list-style-type: none"> <li>● Identity Data</li> <li>● Contact Data</li> <li>● Financial Data</li> </ul>	<ul style="list-style-type: none"> <li>● Legitimate interests</li> </ul>

<p>To manage risk and crime prevention including performing anti-money laundering, counter terrorism, sanction screening, fraud and other background checks, detect, investigate, report and prevent financial crime in broad sense, obey laws and regulations which apply to us and response to complaints and resolving them</p>	<ul style="list-style-type: none"> <li>● Identity Data</li> <li>● Social Identity Data</li> <li>● Contact Data</li> <li>● Financial Data</li> <li>● Technical Data</li> <li>● Transactional Data</li> <li>● Investment Data</li> <li>● Sensitive Data (a.k.a. Special Categories Data) data that you give us directly or that we receive from third parties and/or publicly available sources: - data which might be revealed by KYC or other background checks (for example, because it has been reported in the press or is available in public registers); - data that is incidentally revealed by photographic ID although we do not intentionally process this personal data</li> </ul>	<ul style="list-style-type: none"> <li>● Compliance with a legal obligation</li> <li>● We may also process such data in connection with these purposes if it is necessary for the performance of our contract with you</li> <li>● In addition to our legal obligations, we may process this personal data based on our legitimate interest in ensuring that we are not involved in dealing with the proceeds of criminal activities and do not assist in any other unlawful or fraudulent activities, as well as to develop and improve our internal systems for dealing with financial crime and to ensure effective dealing with complaints</li> <li>● For Special Categories Data, it is necessary for reasons of substantial public interest under EU Anti-Money Laundering Directives and the relevant EU Member States' laws implementing them, as well as under the anti-money laundering legislation of the UK</li> </ul>
<p>To enable you to partake in a prize draw, competition or complete a survey</p>	<ul style="list-style-type: none"> <li>● Identity Data</li> <li>● Contact Data</li> <li>● Profile Data</li> <li>● Usage Data</li> <li>● Marketing and</li> <li>● Communications Data</li> </ul>	<ul style="list-style-type: none"> <li>● Performance of a contract</li> <li>● Consent, if required</li> </ul>
<p>To gather market data for studying customers' behavior including their preference, interest and how they use our products/services,</p>	<ul style="list-style-type: none"> <li>● Identity Data</li> <li>● Contact Data</li> <li>● Profile Data</li> <li>● Usage Data</li> </ul>	<ul style="list-style-type: none"> <li>● Legitimate interests: understanding our customers and improving our products and services</li> </ul>

determining our marketing campaigns and growing our business	<ul style="list-style-type: none"> <li>• Marketing and Communications Data</li> </ul>	
To administer and protect our business, our Site, App(s) and social media channels including bans, troubleshooting, data analysis, testing, system maintenance, support, reporting, hosting of data	<ul style="list-style-type: none"> <li>• Identity Data</li> <li>• Contact Data</li> <li>• Financial Data</li> <li>• Technical Data</li> <li>• Transactional Data</li> <li>• Investment Data</li> </ul>	<ul style="list-style-type: none"> <li>• Legitimate interests: to run our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganization or group restructuring exercise</li> </ul>
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	<ul style="list-style-type: none"> <li>• Identity Data</li> <li>• Contact Data</li> <li>• Profile Data</li> <li>• Usage Data</li> <li>• Technical Data</li> <li>• Marketing and Communications Data</li> </ul>	<ul style="list-style-type: none"> <li>• Legitimate interests: to study how customers use our products/services, to develop them, to grow our business and to form our marketing strategy</li> <li>• Consent, if required</li> </ul>
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	<ul style="list-style-type: none"> <li>• Technical Data</li> <li>• Usage Data</li> </ul>	<ul style="list-style-type: none"> <li>• Legitimate interests: to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to form our marketing strategy</li> <li>• Consent, if required</li> </ul>
To make suggestions and recommendations to you about goods or services that may be of interest to you	<ul style="list-style-type: none"> <li>• Identity Data</li> <li>• Contact Data</li> <li>• Technical Data</li> <li>• Usage Data</li> <li>• Profile Data</li> <li>• Investment Data</li> <li>• Marketing and Communications Data</li> </ul>	<ul style="list-style-type: none"> <li>• Legitimate interests: to develop our products/services and grow our business</li> <li>• Consent, if required</li> </ul>
To use the services of social media platforms or advertising platforms some of which will use the personal data they receive for their own purposes,	<ul style="list-style-type: none"> <li>• Technical Data</li> <li>• Usage Data</li> </ul>	<ul style="list-style-type: none"> <li>• Consent</li> </ul>

including marketing purposes		
To use the services of financial institutions, crime and fraud prevention companies, risk measuring companies, which will use the personal data they receive for their own purposes in their capacity of independent controllers	<ul style="list-style-type: none"> <li>● Identity Data</li> <li>● Social Identity Data</li> <li>● Contact Data</li> <li>● Financial Data</li> <li>● Transactional Data</li> <li>● Investment Data</li> <li>● Technical Data</li> <li>● Usage Data</li> </ul>	<ul style="list-style-type: none"> <li>● Legitimate interests: to conduct our business activities on the market of financial services, to participate actively in the prevention of crime and fraud</li> </ul>
To record voice calls for compliance, quality assurance and training purposes	<ul style="list-style-type: none"> <li>● Identity Data</li> <li>● Social Identity Data</li> <li>● Contact Data</li> <li>● Financial Data</li> <li>● Transactional Data</li> </ul>	<ul style="list-style-type: none"> <li>● Legitimate interests: to comply with the industry standards and requirements in payments services, to ensure quality of our service, including by proper training of our personnel</li> </ul>

## Marketing

We may use your Identity Data, Contact Data, Technical Data, Transactional Data, Investment Data, Usage Data and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us and consented to receive marketing communications, or if you have purchased from us and you have not opted out of receiving such communications. We will use your Marketing and Communications Data for our respective activities.

## Opting out

You can ask us to stop sending you marketing messages at any time by following the “unsubscribe” links on any marketing message sent to you.

Further, you can let us know directly that you prefer not to receive any marketing messages by emailing [dataprivacy@hi.com](mailto:dataprivacy@hi.com).

Where you opt out of receiving marketing messages, this will not apply to service messages which are directly related to the use of our Services (e.g. maintenance, change in the terms and conditions and so forth).

## Cookies

We use cookies to monitor and observe your use of our websites, compile aggregate data about that use, and provide you with a more effective service (which may include customizing parts of our websites based on your preferences and past activities on those websites). "Cookies" are small text files created and stored on your hard drive by your internet browser software, in order to hold relevant information about the web

page you are currently viewing. Most internet browsers have a facility that will allow you to disable cookies altogether – please refer to your browser’s help menu to find out how to do this. While you will still be able to browse our websites with cookies disabled on your internet browser, some website functionality may not be available or may not function correctly.

## Google Analytics

Our website uses Google Analytics, a web analytics service provided by Google, Inc. (“Google”). Google Analytics uses cookies to help the website analyze how users use our website.

The information generated by the cookie about your use of our website (including your IP address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity for website operators and providing other services relating to website activity and internet usage. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google’s behalf. Google will not associate your IP address with any other data held by Google.

You may refuse the use of cookies by selecting the appropriate settings on your browser, however please note that if you do this you may not be able to use the full functionality of our website. By using our website, you consent to the processing of data about you by Google in the manner and for the purposes set out above.

## 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 you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please [contact us](#).

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

## 7. Disclosures of your data

We share your personal data with our third-party service providers, agents, subcontractors and other associated organizations, our group companies, and affiliates (as described below) in order to complete tasks and provide the Services and use of the hi.com App to you on our behalf. When using third party service providers, they are required to respect the security of your personal data and to treat it in accordance with the law.

We may pass your personal data to the following entities:

- companies and organizations that assist us in processing, verifying or refunding transactions/orders you make and in providing any of the Services that you have requested;
- identity verification agencies to undertake required verification checks;
- fraud or crime prevention agencies to help fight against crimes including fraud, money-laundering and terrorist financing;
- anyone to whom we lawfully transfer or may transfer our rights and duties under the relevant terms and conditions governing the use of any of the Services;
- any third party because of any restructure, sale or acquisition of our group or any affiliates, provided that any recipient uses your information for the same purposes as it was originally supplied to us and/or used by us; and

- regulatory and law enforcement authorities, whether they are outside or inside of the EEA, where the law allows or requires us to do so.

## 8. International transfers

We share your personal data within our group. This will involve transferring your personal data outside the European Economic Area (EEA) or the UK.

Many of our external third parties are based outside the EEA so their processing of your personal data will involve a transfer of data outside the EEA.

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- the country to which we transfer your personal data has been deemed to provide an [adequate level of protection](#) for personal data by the European Commission;
- a specific contract approved by the European Commission which gives safeguards to the processing of personal data, the so called Standard Contractual Clauses.

## 9. Data security

While there is an inherent risk in any data being shared over the internet, we have put in place appropriate security measures to prevent your personal data from being accidentally lost, used, damaged, or accessed in an unauthorized or unlawful way, altered, or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a legitimate business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

Depending on the nature of the risks presented by the proposed processing of your personal data, we will have in place the following appropriate security measures:

- **organisational measures** (including but not limited to staff training and policy development);
- **technical measures** (including but not limited to physical protection of data, pseudonymization and encryption); and
- **securing ongoing availability, integrity, and accessibility** (including but not limited to ensuring appropriate back-ups of personal data are held).

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

## 10. Data retention

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

Here are some exemplary factors which we usually consider when determining how long we need to retain your personal data:

- in the event of a complaint;
- if we reasonably believe there is a prospect of litigation in respect to our relationship with you or if we consider that we need to keep information to defend possible future legal claims (e.g. email addresses and content, chats, letters will be kept up to 10 years following the end of our relationship, depending on the limitation period applicable in your country);
- to comply with any applicable legal and/or regulatory requirements with respect to certain types of personal data:
  - under the EU Anti-Money Laundering legislation (Anti-Money Laundering Directives) we are obliged to retain your personal data for a period of 5 years after the end of the relationship between us as a company and you as a customer; this period may be further extended in certain cases if so provided by and in accordance with the applicable legislation;
  - if information is needed for audit purposes and so forth;
- in accordance with relevant industry standards or guidelines;
- in accordance with our legitimate business need to prevent abuse of the promotions that we launch. We will retain a customer's personal data for the time of the promotion and for a certain period after its end to prevent the appearance of abusive behavior.

Please note that under certain condition(s), you can ask us to delete your data: see your legal rights below for further information. We will honor your deletion request ONLY if the condition(s) is met.

## 11. Your legal rights

You have rights we need to make you aware of. The rights available to you depend on our reason for processing your personal data. If you need more detailed information or wish to exercise any of the rights set out below, please [contact us](#).

You may:

- request **access to your personal data**, which enables you to obtain confirmation of whether we are processing your personal data, to receive a copy of the personal data we hold about you and information regarding how your personal data is being used by us;
- request **rectification of your personal data** by asking us to rectify information you think is inaccurate and to complete information you think is incomplete, though we may need to verify the accuracy of the new data you provide to us;
- request **erasure of your personal data** by asking us to delete or remove personal data we hold about you; note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you;
- **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 as you feel it impacts on your fundamental rights and freedoms; in some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms; you also have the right to object where we are processing your personal data for direct marketing purposes;
- **require that decisions be reconsidered if they are made solely by automated means**, without human involvement; we use automated tools to make sure that you are eligible to be our customer taking into account our interests and legal obligations; if these automated tools indicate that you do not meet our acceptance criteria, we will not onboard you as our customer;
- **request restriction of processing your personal data**, which enables you to ask us to suspend the processing of your personal data, if you want us to establish the data accuracy; where our use of the data is unlawful, but you do not want us to erase it; where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims, or if you have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it;

- **request the transfer of your personal data** to you or to a third party, and we will provide to you, or a third party you have chosen (where technically feasible), your personal data in a structured, commonly used, machine-readable format; note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you;
- **withdraw consent at any time** where we are relying on consent to process your personal data; however, this will not affect the lawfulness of any processing carried out before you withdraw your consent; if you withdraw your consent, we may not be able to provide certain products or services to you, but we will advise you if this is the case at the time you withdraw your consent;
- complain to the IDPC, ICO, DPC or any relevant authority about any perceived violation.

### **No fee usually required**

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

### **Period for replying to a legitimate request**

The statutory period under GDPR for us to reply to a legitimate request is one month. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

Please note that we may request that you provide some details necessary to verify your identity when you request to exercise a legal right regarding your personal data.

### **Contact details**

If you want any further information from us on privacy matters, please contact our privacy compliance team at [dataprivacy@hi.com](mailto:dataprivacy@hi.com).