PERSONAL DATA PROTECTION POLICY

February 2023

1 Introduction

1.1 Ortus Secured Finance Limited, along with its subsidiaries (hereinafter collectively referred to as "**Ortus**" or the "**Company**"), is a **Data Controller**, in the meaning of the Data Protection Act and the General Data Protection Regulation (hereinafter collectively referred to as the "**GDPR**") and is as such responsible for ensuring that the processing of personal data is in accordance with the GDPR. Ortus has entered into an outsourcing agreement with its parent company, Kvika banki hf., Company number 540502-2930, with registered address at Katrinartun 2, 105 Reykjavik, Iceland ("**Kvika**" or the "**Data Processor**"), under which Kvika processes personal data on behalf of Ortus in accordance with the agreement. In the Personal Data Protection Policy (hereafter the "**Policy**") when referred to Ortus or the Company it shall be considered also to cover the tasks of Kvika as the Data Processor.

1.2 This Policy provides information on what personal data Ortus collects on its customers; how the Company processes personal data and for what purpose; how long this data can be expected to be stored; where and to whom it may be communicated; and how its security is assured in the Company's operations. Information is also provided on customer's rights regarding the processing of personal data by the Company. The policy has been adopted with the aim of ensuring fair and transparent processing of personal data in compliance with GDPR.

1.3 The term "**personal data**" includes all information that can be linked to a specific person directly or indirectly, e.g. through reference to his/her personal identification, such as a name, Id. No., username, loan no., etc. This policy applies to the Company's former, current and future customers, parties connected to the customer (e.g. family members), guarantors and other relevant parties, such as the beneficial owner of funds, a customer's agent, authorised signatories and parties related to the customer in the case of a legal entity. The policy also includes, as the case may be, individuals other than the customer, e.g. employees of the Company's contractors and persons visiting the Company's offices or website, www.ortussecuredfinance.co.uk, as further described in this policy. References to the "**customer**" in this policy apply to all of the above parties.

2 Types and Sources of Personal Data

2.1 When a customer applies to establish a business relationship with Ortus, the Company will request information, both from the customer and other parties. The collection of such information is necessary to fulfil the Company's statutory obligations, in particular in relation to money laundering prevention and MiFID client classification. The following is a list of the main categories of personal data that Ortus may process and a description of its purpose in processing this data:

- **Contact information**: Name, address and other contact information such as e-mail address, telephone number and job title to enable the Company to communicate with the customer.
- **IDs:** Identification numbers and information on nationality, e.g. passport, driver's licence and electronic ID, to enable the Company to identify the customer.

- **Financial data**: E.g. business history, turnover, account movements and account balances, account numbers, credit card information, interest terms, income, financial obligations, defaults, credit ratings, credit score etc. for the purpose, among other things, of making decisions on creditworthiness and solvency and prevent customer over-indebtedness.
- **Information on contracts:** Details concerning agreements that the customer has concluded with the Company and information on the products and services that the Company provides to the customer so that the provisions of the agreements can be implemented.
- **Information on the communications:** Information that the Company receives from the customer in letters and e-mails that the customer sends to the Company to enable the Company to provide the customer with services, improve them and respond to messages and suggestions.
- **Publicly available information:** E.g. information from public registers, as well as information that can be accessed from a financial information provider or information that has been made public on the Internet. This information is used for various purposes in connection with the Company's operations.
- **Information for customer due diligence:** Information to enable the Company to carry out due diligence in relation to anti money laundering, and to ensure compliance with international sanctions, including determining that the purpose and nature of a business relationship accords with law and whether the client is a politically exposed person.
- **Electronic surveillance:** The Company's offices are monitored using surveillance cameras for security and asset protection purposes.
- **Recording of telephone conversations**: The customer's telephone calls to the Company may be recorded. This processing takes place, e.g. in order to be able to prove whether a transaction has taken place and for security purposes.
- **Consent:** Any approval or authorisation given by the customer to the Company. This includes information on how the customer wishes to be contacted, e.g. whether he/she declines to receive mailings from the Company or communication based on cookies.
- **Cookies**: Cookies are small computer files that are sent to the customer's computer or smart device when the customer visits a website. They are stored in the customer's device and are sent back when he/she revisits the website. The cookies contain information about the customer's visits to websites, e.g. so that he/she need not enter a username or password on each visit, or to analyse website traffic, see further Ortus' terms for the use of cookies on Ortus' website.
- **Information on eligibility:** The Company assesses the client's eligibility to conclude transactions and for this purpose processes information on the client's education and experience, financial situation and risk appetite in order to classify the client as a retail client or professional client.
- **Information about behaviour and usage:** Information on how the customer uses the Company's products and services to enable the Company to make improvements to them, and also to monitor whether everything is in order, both in terms of security and usage.

- **Technical data:** E.g. information about the equipment with which the customer connects to the Company and derivative data from that connection, such as IP addresses, versions of operating systems and actions performed. The purpose is to improve service and for debugging.
- **Information on job applicants:** Information provided by applicants seeking to work for the Company included in their CVs, such as name, Id. No., address, telephone number, e-mail address, education and qualifications, work experience etc.
- **Sensitive personal information:** Some personal information is classified as sensitive under GDPR. This includes information relating to race or ethnic origin, political views, religion or philosophical convictions, trade union membership, genetic data, biometric data and health information. Ortus neither collects nor processes this personal information without the customer's consent except with special legal authorisation. In individual instances, processing may prove necessary for the Company with reference to the public interest or in order to establish, bring or defend legal claims.

2.2 The above list is not exhaustive and the Company may process other information about the customer, as necessary at any given time, depending on the nature of the business relationship or the customer's communication with the Company.

2.3 It should be noted that the customer can always choose whether to provide personal information. Failure to provide information may, however, affect Ortus' ability to provide services to the customer.

3 Use of Personal Data and Processing Basis

3.1 The authorisation for processing personal data depends upon the nature of the customer's contractual relationship with Ortus and the purpose of processing. Ortus uses the customer's personal information in particular to contact the customer, to identify him/her and ensure the security and reliability of business transactions, to execute orders and provide financial services, to develop the Company's products and services offered, to respond to legal requests and to ensure network and information security. Ortus' authorisations for processing personal data are in most cases based on the following:

a. To fulfil the Company's contractual obligations

Personal data is processed to provide services in accordance with an agreement concluded with the Company's customer. The purpose of the processing varies depending on the services provided.

b. To fulfil statutory obligations

Ortus' processing of personal data is based to a large extent on GDPR that requires Ortus to process certain personal data for a specific purpose.

c. To safeguard legitimate interests of the Company or third parties

In cases where processing is necessary due to the legitimate interests of Ortus, a third party or the customer, the Company may process personal data of the customer beyond what is necessary to fulfil and enforce the Company's contractual obligations, unless the customer's interests take precedence. Ortus' processing of personal data on this basis is connected, in particular, with the Company's asset and security, e.g. in connection with:

- enforcing claims of the Company or third parties;
- risk management;
- prevention of fraud and organised crime;
- the Company's information security;
- surveillance of the Company's offices and access controls;
- general customer management and communication;
- marketing, unless the customer has objected; and
- auditing and optimisation of services.

d. On the basis of consent

If the customer has given consent for the Company's processing of personal data for a specific purpose, such consent is the basis for this processing. The customer can always withdraw this consent. Withdrawal of consent does not, however, affect the legality of the processing of personal data that took place prior to revocation.

4 Communication of Personal Data

4.1 Insofar as this is necessary to enforce the Company's contractual obligations to the customer, Ortus' employees have access to personal data. In addition, Ortus' service providers, who process personal data on the Company's behalf, have access to personal data. These are companies that provide e.g. payment services, financial services, hosting and IT services, postal services, printing, telecommunications, debt collection, consulting, auditing and sales and marketing services. Ortus deals only with service providers who offer adequate protection for personal data in accordance with data protection legislation.

4.2 Ortus also shares information with companies within the Company's group in connection with statutory risk management. Finally, Ortus is obliged to provide public parties, such as, tax authorities, regulators, police authorities, liquidators and courts, with access to personal data. With regard to disclosure of personal data to parties outside the Company, it should be noted that Ortus' employees are legally bound by obligations of confidentiality in all matters concerning the interests of the Company's clients and other matters of which they may become aware in the course of employment and should be kept confidential, unless obliged by law to provide this information or if the customer has given consent for such disclosure.

4.3 Examples of such disclosure of personal information are cases where, for example, when it is necessary to trace funds on suspicion of fraud or financial crime; for the collection of claims

in default; in connection with the handling of cases before complaints tribunals or courts; and where the law provides for the disclosure of information.

5 Disclosures beyond the UK

5.1 Ortus can only transfer personal data outside the UK after considering the protection available for that data in the country where the data will be sent and meeting certain conditions. Ortus may freely transfer data to entities in the European Economic Area (EEA), including to Kvika, without taking any special measures. This is because the UK has decided that EEA countries have an adequate level of protection in terms of holding and processing personal data.

5.2 In certain cases, data may be transferred out of the UK and outside the EEA, for example, to fulfil contractual obligations to the customer or obligations imposed on the Company by law. Ortus only transmits personal data to countries outside the UK or the EEA if this is necessary in order to carry out the customer's requests, such as payment requests or requests for transactions, if this is required by law, such as obligations to notify under tax legislation (CRS and FATCA), or if the customer has consented to such disclosure. When such transmission occurs, Ortus is responsible for ensuring that the recipient has appropriate protection measures in place to ensure adequate protection of personal data[1].

6 Preservation of Data

6.1 Personal data is preserved as long as the business relationship is in effect and the law prescribes or as Ortus' business interests require and there is valid reason for doing so. There is considered to be valid reason if processing of the data is still underway in accordance with the original purpose of its collection or due to the Company's commercial interests, e.g. to define, present and protect the Company's claims.

6.2 Ortus endeavours to avoid storing data in personally identifiable form for longer than necessary. Ortus bases its retention period in particular on GDPR. If data is considered to have historical value, it is made non-personally identifiable by erasing personal identification.

7 Customer Rights

7.1 In connection with the processing of his/her personal data, the customer is entitled to:

- request information on how Ortus processes the personal data and receive a copy of that data;
- request the correction of incorrect personal data processed by Ortus or request that incomplete personal data be completed;
- request that the personal data be deleted if the customer considers the information no longer necessary for the purpose of its collection. The same applies when the customer withdraws the consent on which the processing of personal data is based

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/

and there is no other legal basis for its processing or if the processing of the information is unlawful;

- request that Ortus limit its processing of personal data in certain cases, such as when processing has been objected to;
- request to receive the personal data in a systematic, common and computer-readable format and have it sent to another institution;
- revoke previously granted consent for the processing of personal data. Withdrawal of consent does not affect the legality of the processing based on consent that took place prior to revocation;
- object to processing for the purpose of direct marketing;
- object to the processing of personal data by Ortus on the basis of legitimate interests, such as processing that involves the creation of a personal profile (personal profiling);
- file a complaint with the Information Commissioner's Office if the customer considers that Ortus' processing of his/her personal data violates applicable law.

7.2 If the customer objects to the processing of personal data, Ortus will cease processing the personal data unless the Company can demonstrate a legal obligation or legitimate interests that take precedence over the customer's interests.

7.3 If you wish further information about your rights or how you can exercise them, you are advised to contact Ortus' Compliance Manager, who is registered as the Company's Data Protection Officer (the "**DPO**") with the Information Commissioner's Office (see contact details in Section 11).

8 Automated Decision-Making (ADM) and Personal Profiling

8.1 Automatic decision-making means that a decision is made on the basis of automatic data processing, without the involvement of Ortus' employees or other individuals, and such a decision has legal effect vis-à-vis the customer. At present, no business decisions are made automatically; however, if this changes, Ortus will provide the Company's customers with further information.

9 Security and Protection of Personal Data

9.1 Ortus takes appropriate measures to protect customers' personal data from misuse, compromise and damage, unauthorised access, alteration or disclosure. The measures that the Company relies on are, in particular:

- implementing technical and organisational measures designed to ensure the lasting confidentiality, continuity, availability and resilience of processing systems and services;
- controlling individuals' access to Ortus' offices and maintaining security surveillance;
- controlling access by employees and others to systems that contain personal data;

- ensuring that persons with access to the customer's personal data have taken appropriate protection measures to ensure the security of personal data; and
- when required by law, deleting, pseudonymising or encrypting the customer's personal data.

9.2 In all processing work involving information security, Ortus follows the ISO 27001 data security standard and has adopted a written policy on information security management.

9.3 In the event of a security breach in the processing of personal data, where it is confirmed or suspected that personal data has fallen into the hands of an unauthorised party, the Information Commissioner's Office and, as the case may be, the customer, are notified of the security breach, i.e. unless it involves no major risk to the customer's rights and freedom. Please refer to Appendix 1 for Ortus' Data Breach Escalation procedure.

10 Changes to the Personal Data Protection Policy

10.1 This policy will be updated regularly to accord with changing business practice and legal obligations. If Ortus and/or Kvika make significant changes to the manner in which personal data is processed, the policy will be updated to reflect those changes. Ortus encourages the customer to review this policy regularly in order to keep informed about how the Company uses and protects personal data.

11 Contact Information

11.1 Any questions concerning the processing of personal data or how you can exercise your data rights should be directed to the DPO by letter or e-mail.

Ortus Secured Finance Limited
Att. Steven Buchanan
Nations House, 103 Wigmore Street, London W1U 1QS
E-mail: steven.buchanan@kvika.co.uk

This document was approved by the Board of Directors of Ortus Secured Finance Limited on

21 February 2023

Appendix 1

Data Breach Escalation Procedure

Ortus is committed to ensuring that all personal data we process, including that of colleagues and customers, is managed appropriately and in compliance with the GDPR. All members of staff are expected to comply with this procedure in the event of a Personal Data Breach.

1) What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.
Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data

2) If we think a personal data breach has occurred, what do we do?

Immediately inform the DPO, Steven Buchanan. Do not rely on an email – if we are not around then call, Whatsapp or text to make sure you inform the DPO as quickly as possible.
The DPO will manage and coordinate the next stage:

a) Escalating the breach

The DPO will manage/coordinate the following escalation process

- Quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it.
- We will try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.
- Establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we must notify the ICO; if it's

unlikely then we don't have to report it. However, if we decide you don't need to report the breach, we need to be able to justify this decision, so we will document it with a file note. The DPO will hold conversations with the Head of Compliance, MD and CEO to agree on the next steps where a breach has occurred.

- In assessing risk to rights and freedoms, we will focus on the potential negative consequences for individuals.
- A breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. We will assess this case by case, looking at all relevant factors.

b) Immediate process and timescales

We must provide the ICO with;

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned;
- the name and contact details of the person handling the breach (DPO).
- a description of the likely consequences of the personal data breach; and
- 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 adverse effects.
- If we don't have all the required information available yet, we will prioritise the investigation, give it adequate resources, and expedite it urgently. We will also still notify the ICO of the breach when we become aware of it, and submit further information as soon as possible. If we know we won't be able to provide full details within 72 hours, we will explain the delay to the ICO and tell them when you expect to submit more information.

c) How do we notify a breach to the ICO?

To notify the ICO of a personal data breach, we will use the reporting link on the ICO website.

d) When do we need to tell individuals about a breach?

- If a breach is likely to result in a high risk to the rights and freedoms of individuals, we will inform those concerned directly as soon as possible.
- If we decide not to notify individuals, we will still need to notify the ICO unless we can demonstrate that the breach is unlikely to result in a risk to rights and freedoms.

e) What information must we provide to individuals when telling them about a breach?

We need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of our data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

3) Recording

We will ensure that we record all breaches, regardless of whether or not they need to be reported to the ICO.

Change Log				
Version number	**Originally approved**	**Changed**	**Change Owner**	**Changes**
1.0	27/10/2022			
1.1		21/02/2023	Steven Buchanan	Version control created Amended reference to "Data Protection Authority" to "Information Commissioner's Office" Added in Data Protection Officer and reference to Data Breach procedure