光大新鴻基
EVERBRIGHT SUN HUNG KAI

Everbright Sun Hung Kai Privacy Policy

1. INTRODUCTION

In its everyday business operations, Sun Hung Kai Financial (UK) Limited, trading as Everbright Sun Hung Kai, "we"), as a data controller makes use of a variety of data about identifiable individuals, including data about:

(a) Current, past and prospective employees;
(b) Counterparties;
(c) Users of its services; and
(d) Other stakeholders.

In collecting and using this data, we are subject to a variety of legislation governing our processing of people's data and the safeguards that we must put in place to protect it. This policy sets out the relevant legislation and describes the steps we take to ensure that we comply with it.

This control applies to all systems, people and processes that constitute our information systems, including board members, directors, employees, suppliers and other third parties who have access to our systems. This includes contractors and agency employees.

2. THE GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (EU) 2016/679 (GDPR) is one of the most significant pieces of legislation affecting the way that we carry out our information processing activities. The principal aim of GDPR is to protect the personal data of residents of EU countries. Significant fines can apply if there is a breach under the GDPR. It is our policy to ensure that our compliance with the GDPR and other relevant legislation is clear and demonstrable at all times.

3. STATUS OF THE POLICY

The Data Protection Officer is responsible for ensuring compliance with the GDPR and with this policy. Any questions or concerns about the operation of this policy should be referred in the first instance to the Compliance Officer (the "Data Protection Officer") at pegan@ebshk.co.uk.

4. DEFINITIONS

The key definitions with respect to this policy are:

4.1. "**Personal data**" means any information relating to an identified or identifiable natural person ("**data subject**"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an 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 person.

4.2. "**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. These operations include collection, recording, organisation, structuring, storage, adaptation or alteration, or destruction of data.

4.3. "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

4.4. "**Processor**" means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of a data controller.

4.5. "**Profiling**" means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. Operations performed may include collection, recording, organisation,

structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4.6. "**Consent**" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

4.7. "**Binding corporate rules (BCR's)**" means agreements governing transfers of personal data to countries outside the European Union ("Third Countries") where such transfers are made between organisations within a corporate group.

4.8. "**Special categories of data**" means personal data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership. This also includes data concerning health or sex life and sexual orientation, genetic data (such as DNA samples) and biometric data (such as facial images).

5. PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

This policy is governed by the following guiding principles, we must adhere to under the GDPR.

5.1. **Lawfulness, Fairness and Transparency**
We must process personal data lawfully, fairly and in a transparent manner in relation to the data subject. This means we must justify the processing of personal data by one of the lawful bases set out in Section 6 (Lawful Basis), the processing must match the description given to the data subject (fairness), and we must tell the data subject what processing will occur (transparency).

5.2. **Purpose Limitation**
Personal data must be collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes. This means that we must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

5.3. **Data Minimisation**
Any personal data we hold must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This means we must not store any personal data beyond what is strictly required.

5.4. **Accuracy**
Personal data must be accurate and kept up to date. This means we must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.

5.5. **Storage Limitation**
We must keep personal data in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. We maintain retention policies and procedures to ensure that we delete data after a reasonable time for the purpose for which we held it, unless the law requires us to keep such data for a minimum period. Additionally, this means that wherever possible, we must store personal data in a way that limits or prevents identification of the data subject.

5.6. **Integrity & Confidentiality**
We must process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. We must use appropriate technical and organisational measures to ensure we maintain the integrity and confidentiality of personal data at all times. We must ensure that it complies with the above principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

6. LAWFUL BASIS

Personal data must only be collected and processed under the following circumstances:

(a) Where the data subject has given adequate consent (see below) for their personal data to be collected or processed;
(b) Where processing is necessary for us or a third party to pursue a legitimate interest (see below), and that interest does not conflict with the data subject's fundamental rights and freedoms;
(c) Where processing is necessary for the performance of a contract to which the data subject is a party;
(d) Where processing is necessary in order to comply with a legal obligation;
(e) Where processing is necessary in order to protect the vital interests of the data subject or of another person; or
(f) Where processing is necessary for the performance of a task carried out in the public interest. Where we rely on "legitimate interest" as the lawful basis for data processing, we must take into account the reasonable expectations of data subjects based on their relationship with us. We must consider whether the data subject could reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.

6.1 **Special categories of data**
In addition to establishing a lawful basis for processing, we must ensure that certain conditions apply when processing special categories of data, such as ethnic origin, health information or trade union membership. The conditions most relevant are set out below:

(a) The data subject has given explicit consent, in other words made a written statement of consent in relation to the processing;
(b) The processing is necessary for carrying out obligations in the field of employment, social security of social protection law;
(c) The processing is necessary to protect the vital interests of the data subject;
(d) The processing relates to personal data which are manifestly made public by the data subject;
(e) The processing is necessary as it relates to legal claims; and
(f) The processing is necessary as it relates to preventative or occupational medicine.

7. CONSENT

GDPR allows data to be collected and processed without consent in certain limited circumstances (see above). In all other cases, we must obtain the consent of the data subject to collect and process their data.

We will maintain a system to:

(a) Determine what information must be provided to the data subject in order to obtain valid, informed consent where this is relied on as a lawful basis;
(b) Ensure that the request for consent is presented in clear and plain language in an easily accessible form;
(c) Ensure that the consent is given freely;
(d) Document the date, method and content of the consent obtained;
(e) Provide a simple method for a data subject to withdraw their consent at any time.

8. ADEQUATE CONSENT

(a) Where consent forms the lawful basis for processing personal data, we must be able to show that consent was given freely;
(b) Consent must also specific. This means that our name, the purposes of the processing and the types of processing activity must have been made clear to the data subject before obtaining consent to such processing.
(c) Consent to process personal data must not be requested as a condition for the performance of a contract except where the data is necessary for the contract's performance.

9. WRITTEN DECLARATIONS OF CONSENT

Requests for consent must be communicated to the data subject in a written declaration. The declaration must:

(a) Contain a separate request for each processing activity;

(b) Contain the purpose for data processing;
(c) Communicate this purpose to the data subject in an intelligible and easily accessible form, using clear and plain language;
(d) Be free from unfair terms, in other words avoiding making consent a condition for accessing goods or services, except where strictly necessary;
(e) Include all necessary disclosures;
(f) Give the data subject a genuine choice to refuse or withdraw consent without detriment; and
(g) Be recorded and documented.

10. WITHDRAWAL OF CONSENT

The data subject retains the right to withdraw their consent at any time, without prejudice. The method of withdrawing consent must be as easy as the method of giving it.

11. RIGHTS OF THE INDIVIDUAL

Data subjects have certain rights under GDPR. These consist of:

(a) The right to be informed – about the fact that their data is processed, the purposes of that processing and the identification of us as a controller, among other things;
(b) The right to request access to their data;
(c) The right to request rectification – where data is inaccurate or out of date;
(d) The right to request erasure of data;
(e) The right to request that processing be restricted;
(f) The right to data portability – in other words to request that their data be available for reuse by another provider;
(g) The right to object to processing – where 'legitimate interests' or 'public interest' are used as the lawful basis.

These rights and the exercise of them are subject to the provisions of the GDPR and the guidance provided by the Information Commissioners Office.

We have appropriate procedures to allow the requested action to be taken within the timescales stated in GDPR. These timescales are shown in Table 1 below.

Table 1
Timescales for Data Subject Requests

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

12. PRIVACY NOTICES

We must provide transparent information to data subjects about our usage of their data at the time that we collect the data. We must also explain their rights with regard to their data, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge. This is normally communicated via our Privacy policy. The requirement for transparency/notification is not dependent exclusively on whether consent is involved in the processing.

If the personal data are not obtained directly from the data subject, then this information must be provided within a reasonable period after the data are obtained and definitely within one month.

13. PRIVACY BY DESIGN It is our policy to ensure that all new or significantly changed systems that collect or process personal data give due consideration to privacy issues. This includes the completion of data protection impact assessments (DPIAs). The privacy of individuals should be considered for all new projects and processes to ensure that no excessive data is collected.

The DPIA must:

(a) Consider how personal data will be processed and for what purposes;
(b) Assess whether the proposed processing of personal data is both necessary and proportionate to the purpose(s);
(c) Assess of the risks to individuals in processing the personal data; and
(d) Consider what controls are necessary to address the identified risks and demonstrate compliance with legislation.

14. SHARING OF PERSONAL DATA WITH THIRD PARTIES

We must take reasonable steps to ensure that personal data is only shared with third parties that have provided sufficient guarantees in respect of their data security measures.

In addition, we must require that all third party contractors who process personal data on behalf of us are GDPR compliant. Any existing contracts with third parties must be reviewed and updated on an ongoing basis. Where this is not possible, we must communicate with those third parties to alert them to their responsibilities under the GDPR.

15. TRANSFER OF PERSONAL DATA OUTSIDE THE EU

GDPR imposes restrictions on the transfer of personal data outside the European Union. These restrictions will depend, for example, on the level of data protection in the country to which the data is to be transferred. We must review the position before any proposed transfer takes place.

Intra-group international data transfers must be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

16. BREACH NOTIFICATION

If there is a breach of personal data which is likely to result in a risk to the rights and freedoms of individuals, we must notify the Information Commissioner within 72 hours.

17. COMPLIANCE WITH GDPR

In order to comply with the accountability principle under GDPR, the following processes will be put in place:

(a) The legal basis for processing personal data must be clear and unambiguous;
(b) The Data Protection Officer will have specific responsibility for data protection in the organisation;
(c) All staff involved in handling personal data must understand their responsibilities for following good data protection practice;
(d) Training in data protection will be provided to all relevant staff;
(e) Rules regarding consent will be followed;
(f) Individuals who wish to exercise their rights regarding personal data will be made aware of the relevant process and their enquiries must be handled effectively;
(g) Regular reviews of procedures involving personal data will be carried out;
(h) The following documentation of processing activities will be recorded:

i. Our name and relevant details as data controller
ii. Purposes of the personal data processing
iii. Categories of individuals and personal data processed
iv. Categories of personal data recipients
v. Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
vi. Personal data retention schedules
vii. Relevant technical and organisational controls in place

(i) These actions will be reviewed annually as part of the management review process of the information security management system.