Khepri Privacy Policy

Khepri Limited, Khepri Services Limited, Khepri Advisers Limited and Khepri Fund Management Limited (collectively "Khepri" and "we", each individually, "Khepri Company") is committed to protecting your personal data and informing you of your rights in relation to that data. For the purposes of this Khepri Privacy Policy.

Khepri's Companies are each registered as a data controller in the United Kingdom under the Data Protection (Charges and Information) Regulations 2018 (the 2018 Regulations). Our registration details can be found via the Information Commissioner's Office Search Register link here.

One of our responsibilities as a data controller is to be transparent in our processing of your personal data and to tell you about the different ways in which we collect and use your personal data.

Khepri will process your personal data in accordance with the retained EU law version of the General Data Protection Regulation ("**UK GDPR**") and the Data Protection Act 2018 (UK) and this privacy notice is issued in accordance with the retained EU law version of the UK GDPR Articles 13 and 14.

We may update our privacy policy at any time. The current version of our privacy policy can be found below, and we encourage you to check here regularly to review any changes.

1. Identity and contact details of data controller

For the purposes of the UK GDPR and Applicable Local Laws, Khepri is the controller of your data. If you have any queries regarding this policy or complaints about our use of your data, please contact the Data Protection Officer, Mike Booth, at compliance@khepri.com or at the address below and we will do our best to deal with your complaint or query as soon as possible.

Khepri
95 Chancery Lane
London, WC2A 1DT
FAO: Mike Booth, Data Privacy Manager

2. Personal data and its processing

Personal data is defined in the UK GDPR as information relating to a live, identifiable individual. It can also include special categories of data, which is information about your racial or ethic origin, religious or other beliefs, physical or mental health, the processing of which is subject to strict requirements. Similarly information about criminal convictions and offences is also subject to strict requirements. "processing" means any operation which we carry out using your personal data, for example obtaining, storing, transferring or deleting.

We only process data for specified purposes and if it is justified in accordance with data protection law. Details of each processing purpose and its legal basis are given within each privacy notice listed below.

3. How long we keep your data for

Unless specific time periods are given in this privacy notice, your data will be kept in line with our data retention policies, please refer to the Terms and Conditions within your engagement letter or agreement for further information.

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 unauthorised 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 regulatory and legal requirements.

Where data is obtained for regulatory purposes, we may store this personal data for the time periods specified by the relevant regulators, which could be at least seven years.

4. Your rights as a data subject

You have the following rights in relation to your personal data processed by us:

4.1. Right to be informed

We will ensure you have sufficient information to ensure that you're happy about how and why we're handling your personal data, and that you know how to enforce your rights.

We will provide information in the form of privacy notices. You can read all our privacy notices online.

4.2. Right of access / right to data portability

In certain situations, you have a right to see all the information that we hold about you. Where data is held electronically in a structured form, such as in a database, you have a right to receive that data in a common electronic format that allows you to supply that data to a third party – this is called "data portability".

To make a request for your own information, please contact the Data Protection Officer.

4.3. Right of rectification

If we are holding data about you that is incorrect, you have the right to have it corrected.

Contact the Data Protection Officer for any related requests.

4.4. Right to erasure

You can ask that we delete your data and where this is appropriate we will take reasonable steps to do so.

Please contact the Data Protection Officer.

4.5. Right to restrict processing

If you think there is a problem with the accuracy of the data we hold about you, or you are of the opinion that we are using data about you unlawfully, you can request that any current processing is suspended until a resolution is agreed.

Please contact the Data Protection Officer.

4.6. Right to object

You have a right to opt out of direct marketing.

You have a right to object to how we use your data if we do so on the basis of "legitimate interests" or "in the performance of a task in the public interest" or "exercise of official authority" (a privacy notice will clearly state this to you if this is the case). Unless we can show a compelling case why our use of your data is justified, we have to stop using your data in the way that you've objected to.

Please contact the Data Protection Officer.

4.7. Rights related to automated decision making, including profiling

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making as we do not use automated decision-making.

5. Withdrawing consent

If we are relying on your consent to process your data, you may withdraw your consent at any time.

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the data processing team. Once we have received notification that you have withdrawn your consent, we consider your request and where applicable, will no longer process your personal data for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

6. Exercising your rights, queries and complaints

For more information on your rights, if you wish to exercise any right, for any queries you may have or if you wish to make a complaint, please contact our Data Protection Officer.

7. Complaint to the supervisory authority

You have a right to complain to the supervisory authority about the way in which we process your personal data.

You may lodge a complaint with any supervisory authority regarding our processing of your personal data. The relevant supervisory authorities are set out below:

United Kingdom – the Information Commissioner's Office whose contact details can be found on their website which can be viewed here – https://ico.org.uk/

8. Data Security

Your personal data is securely stored.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and securely.

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, altered, disclosed, used or accessed without authorisation. In addition, we restrict access to personal data to those employees, agents, contractors, consultants and other third parties who have a business need to access the personal data. They will only process personal data on our instructions and they are also subject to a duty of confidentiality.

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

9. How do we collect your personal data?

We collect your personal data through the following channels ("**Collection Channels**"):

a) when you subscribe to our newsletters or events ("**Marketing**");
b) when you complete one of our surveys ("**Survey**");
c) by you otherwise interacting with us a prospective, current or former client or customer ("**Business Development**");
d) by you or your employer providing us with details to assist us in fulfilling a contract for services with you ("**Khepri Services**");
e) by you providing your details to us, or your employer providing your details to us, in connection with a service you or your employer provides to Khepri ("**Supplier**"); and/or
f) by you contacting us or otherwise providing your personal data to us, directly or indirectly ("**Other**").

10. What data to we collect

Across all of the above Collection Channels, we collect the following personal information:

a) name;

b) business postal address;
c) residential address;
d) business email address;
e) telephone number;
f) date of birth;
g) nationality;
h) job title;
i) mobile telephone number;
j) copy of your passport or other form of photographic ID;
k) corporate and personal Bank Details;
l) source of wealth and source of funds;
m) FCA/CSSF/GFSC registration number (if applicable);
n) list of directorships;
o) employment history;
p) criminal convictions;
q) credit reports/ratings;
r) whether you are a politically exposed person(s);
s) whether you are on a sanctioned or watch list; and
t) other information about you which you may provide to us in the course of us providing the agreed services.

In certain circumstances, the information we hold about you may include special category data (as defined in the UK GDPR), including data which reveals your ethnicity, your political opinions, your health or your criminal convictions.

11. What we use your data for

We use your data for the following purposes:

a) in order to provide services pursuant to our contract with you;
b) in order to comply with our legal obligation such as to carry out anti-money laundering checks on our clients;
c) in order to provide marketing communications to you (but only where we have obtained your consent to do so);
d) for our legitimate business interests such as for internal record keeping purposes or to manage our client relationship with you;
e) Any special category data we hold about you will only be processed so far as necessary in order to comply with our legal requirements.

12. Who we share your data with

Please note that we may on occasion be required to share your information with the following categories of recipients:

a) Third parties who provide services on our behalf; and
b) Regulators or other agencies where there is a legal basis to do so.

We have taken steps to ensure that all such third-party providers keep your data confidential and secure and only use it for the purposes that we have specified and have informed you of. Our service providers are subject to data processing agreements which have been, or are in the process of being, updated to become,

compliant with the requirements set out in the UK GDPR and/or Applicable Local Laws.

In relation to any other third parties, we will only disclose your information where you have given your consent or where we are required to do so by law or enforceable request by a regulatory body or where it is necessary for compliance with a legal obligation.

13. Article 28 – Where Khepri is a Data Processor

Where, in relation to any personal data, Khepri is the data processor under the terms of an agreement with our clients, for the purposes of Article 28.3 of the UK GDPR, the personal data used in the processing will be based on the agreement between Khepri and the controller and we will:

a) process the personal data only in accordance with the data controllers instructions, including where relevant for transfers of personal data to a third country or an international organisation, unless required to do so by domestic law; in such a case, Khepri shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
b) ensure that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
c) take all measures required pursuant to Article 32 of the UK GDPR;
d) appoint sub-processors only in accordance with Article 28.2 and Article 28.4 of the UK GDPR;
e) taking into account the nature of the processing, assist the data controller by taking appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the data controllers obligation to respond to requests for exercising a data subject's rights laid down in Chapter III of the UK GDPR;

    i. keep personal data secure (Article 32 UK GDPR);
    ii. notify personal data breaches to the supervisory authority (Article 33 UK GDPR);
    iii. advise data subjects when there has been a personal data breach (Article 34 UK GDPR);
    iv. carry out data protection impact assessments (Article 35 UK GDPR); and
    v. consult with the supervisory authority where a data protection impact assessment indicates that there is an unmitigated high risk to the processing (Article 36 UK GDPR);

f) taking into account the nature of the processing and the information available to Khepri, assist the data controller in ensuring compliance with the data controller's obligations;
g) upon the data controller's request, delete or return all personal data to the data controller upon termination of the agreement, save to the extent that European Union or EU member state law requires retention of the personal data;

h) make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in these terms and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controllers;
i) co-operate on request, with the Information Commissioner's Office (or any successor body thereto or any relevant supervisory authority) in the performance of its tasks; and
j) notify the data controller without undue delay after becoming aware of a personal data breach.

We shall be liable in respect of any breach of our obligations under the agreement and/or data protection legislation with respect to the processing of personal data other than where such breach is caused by or results from an act or omission by the data controller. We shall fully and effectively indemnify the data controller for any claim brought by a data subject and/or any competent authority or body arising from any action or omission by us with respect to the processing of their personal data other than to the extent that such action or omission resulted from compliance with the data controller's instructions.