Privacy Notice

Last update: 21/11/2024

1. Scope of application

This privacy notice (the "**Notice"**) describes how Innpact Fund Management S.A. (hereafter referred to as the "**Company**") treats the information collected or provided during the course of the Company's activities, how it is stored, processed, secured and what are the rights of the Data Subjects (as defined below) in relation to these Personal Data (as defined below in section 2).

Personal Data may be collected, recorded, stored in digital form or otherwise, adapted, transferred or otherwise processed and used in accordance with the Luxembourg law of 2 August 2002 on the protection of persons with regard to the processing of Personal Data (as amended), the European Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**") and any other European Union or national legislation which implements or supplements the foregoing.

This Notice is issued by the Company, identified as personal data controller within the meaning of the GDPR ("**Data Controller**"), and applies to individuals with whom the Company interacts, including but not limited to employees, consultants, clients, prospects, directors and other counterparties (hereafter referred to as the "**Data Subject(s)**").

This Notice applies to any Data Subject whose Personal Data is provided to the Company directly by the Data Subject or indirectly through another natural or legal person, public authority, agency or another body in connection with the Company's relationship with the Data Subject where the Company acts as Data Controller within the meaning of the GDPR.

This Notice may be amended from time to time to reflect changes in the Company's practice with respect to the processing of Personal Data, or changes in applicable law, and the Company will notify Data Subjects in writing of any changes it makes.

The Data Controller for the purposes of this Notice is the Company with the contact details provided in Section 10.

2. Types of Personal Data collected or provided to the Company and sources of Personal Data

The main categories of personal data processed by the Company (the "**Personal Data**") are (inter alia):

- Personal identification data, such as name, date and place of birth, address, email address, phone number, any other contact details, nationality, gender, social security number, copies of identity documents, drivers' license, CVs,
- Financial data, such as banking details, income details, tax information, source of wealth,
- IP addresses or other visitor origin profiles may be traceable from visiting our website or social media profiles,

- Profile pictures, pictures from events organised by the Company and videos.

For the avoidance of doubt, the Company does not process, and service providers of the Company are not authorized to process, any special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health related data (except medical certificates provided by any employee of the Company in case of sickness) or data related to sexual orientation.

The Company uses different sources to collect Personal Data including, but not limited to:

- Direct interactions: information provided verbally, electronically or in writing, including information provided during meetings, networking events or on questionnaires, websites and other forms provided by the Data Subject or the Data Subject's organization,
- Information generated by the Company: information created in the course of its relationship with Data Subjects,
- AML/ KYC obligations: information provided directly or indirectly by Data Subjects to comply with AML and KYC obligations,
- Third-parties or publicly available sources: information obtained from international sanctions lists, publicly available websites, financial market infrastructures and other public data,
- Service providers: information provided indirectly by the service providers of the Company.

The Company informs Data Subjects of the specific source of any indirectly collected Personal Data at the time it is processed, where applicable.

3. Purposes and legitimate basis of processing

Any Personal Data provided to the Company is processed based on the legal grounds enumerated in Art. 6, Par. 1 of the GDPR. The Company does not use Personal Data for marketing purposes without explicit consent of the relevant Data Subject.

Most of the Company's Personal Data processing arises from:

- Regulatory or contractual requirements (i.e. processing is necessary for compliance with a legal obligation to which the Data Controller is subject; processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract), without which the Company would not be able to provide the contracted services or comply with applicable laws.
- Legitimate interests (e.g. to ensure security of the Company's website or access to platforms the Company is using), except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data.
- Explicit consent: certain Personal Data, such as business cards and photographs that the Company may have of Data Subjects further to events, or IP address (for website users), may be processed based on consent or to pursue legitimate interests, such as internal communication and business administration.

Regarding website users, their Personal Data is processed for statistics purposes, to communicate with the user and to answer any request.

If the Company does rely on the Data Subject's consent, it will make this clear to the Data Subjects when asking for their consent. Data Subjects will have the right to withdraw their consent at any time and request that the Company stops processing and deletes such Personal Data.

In accordance with Art. 30 of the GDPR, each service provider of the Company which is processing Personal Data on behalf of the Company, shall maintain a record of its data processing, which shall be made available to the Data Controller for inspection upon request.

4. Recipients of Personal Data

The Company's data systems are maintained and backed-up by an external IT service provider which is also located in Luxembourg and is complying with GDPR requirements.

In order to fulfil the Company's obligations arising from contract or applicable laws, certain Personal Data may be transmitted to other service providers of the Company, such as investment advisors or portfolio managers, transfer agents, the Company's website service provider, HR support service providers, auditors, legal advisers, external valuers or tax and regulatory authorities.

Due diligence is performed on such third-party services providers to ensure that they are complying with the GDPR.

5. Storage of Personal Data

Any and all Personal Data will be held for a period of maximum ten (10) years after the termination of the relationship between the Data Subject and the Company, and will not be retained for longer than the duration required by applicable law or contractual obligations, taking into account any required retention period to meet any legal procedural requirements in case of any need to provide information with integrity to competent authorities.

6. Transfer of Personal Data

In order to fulfil the Company's obligations arising from contract or applicable laws, certain Personal Data may be transmitted to other service providers outside of the European Union ("**EU**").

To the extent practicable, the Company avoids transferring Personal Data to non-EU countries or to countries without EU equivalent data protection rules. In the event Personal Data is transferred outside of the EU, prior due diligence is performed to ensure that data processors or service providers only transfer data to their affiliates that are compliant with data protection rules equivalent to GDPR, that the IT cloud solutions chosen have implemented GDPR compliant security measures, and that the Personal Data is transferred in a secure way.

The data systems shall be maintained and backed-up by an external IT service provider located within the EU, in jurisdictions deemed to have an EU-equivalent level of protection, or which are otherwise bound contractually to comply with GDPR requirements, based on standard contractual clauses.

7. Rights of Data Subjects

Requests from Data Subjects related to the exercise of the rights described below shall in general be referred to as "Data Requests" and shall be handled in accordance with the section below "Handling of Data Requests".

The Company's Data Subjects have the following rights:

- Right to access (Art. 15 GDPR) and rectification (Art. 16 GDPR): Data Subjects have the right to see Personal Data the Company have in its files. If the Data Subject spots an error in his/her Personal Data in the Company's files, or if his/her Personal Data is no longer up to date, the Data Subject has the right to request that it is rectified.
- Right to withdraw consent (Art. 7 GDPR): For the processing of Personal Data that are based on Data Subjects' consent, Data Subjects have the right to withdraw their consent and request that the Company stops processing and deletes such Personal Data at any time.
- Right of erasure (Art. 17 and 19 GDPR): Any of the Personal Data that the Company has in its files will be deleted upon request of the Data Subject, unless the Company has an overriding obligation to maintain the Personal Data such as those arising from contract or applicable laws.
- Right to restriction of processing (Art. 18+19 GDPR): Upon request from the Data Subject, the Company will limit the ways and purposes Personal Data is processed, unless there are overriding obligations arising out of contract or applicable laws.
- Right to data portability (Art. 20 GDPR): The Data Subject has the right to request that his/her Personal Data is transferred from the Company to another recipient of his/her choosing.
- Right to object (Art. 21+22 GDPR): The Data Subject has the right to object to the processing of his/her Personal Data by the Company and to request the Company to stop processing his/her Personal Data. In such case the Company will stop processing Personal Data unless there are overriding obligations such as those arising from contract or applicable laws.
- Right to lodge complaints (Art. 77 GDPR): The Data Subject has the right at all times to lodge a complaint regarding the processing of his/her Personal Data, whether to the Company using the contact form on the Company's website or the contact details in section 12 below, or directly to a national data protection authority of a European Union Member State, such as the Luxembourg data protection authority, the Commission Nationale de Protection des Données ("CNPD").

8. Handling of Data Requests

Data processors shall assist the Company as Data Controller within the scope of its abilities and the information reasonably available to it, to respond to requests from Data Subjects regarding the Personal Data mentioned hereabove.

For data requests addressed to the Company, the Company shall be responsible for obtaining and coordinating the necessary information from the relevant service providers as well as responding to the relevant Data Subject.

9. Handling of Data Breaches

In the event of a data breach likely to result in harm to Data Subjects (a "**Personal Data Breach**"), the Company in its capacity as Data Controller has the responsibility to notify the CNPD in accordance with Art. 33 of the GDPR.

Taking into account the processing by service providers and storage of the Company's Personal Data, a Personal Data Breach requires detection by the relevant service provider, which will in turn immediately notify the Company (addressing the Data Protection Officer) without undue delay after becoming aware of such Personal Data Breach.

The service provider experiencing Personal Data Breach is the primary party responsible for performing assessment regarding the nature of the breach and the likelihood of risk to the rights and freedoms of Data Subjects.

The Company will determine the likelihood of risk to the rights and freedoms of Data Subjects (with the continuous information from the service provider) and whether there is a need to further notify the CNPD and the relevant Data Subjects (as required).

The above-mentioned notifications shall include the following information:

- Describe the nature of the Personal Data Breach;
- Communicate the name and contact details of the Data Protection Officer or contact point where more information can be obtained;
- Describe the likely consequences of the Personal Data Breach;
- Describe the measures taken or proposed to be taken by the Data Controller to address the Personal Data Breach.

10. Contact Information

In case of any questions about this Notice, Personal Data held by the Company or rights of the Data Subjects, please contact the Company by using the contact form on the Company's website or the contact details below:

Postal and visitor's address:

Innpact Fund Management S.A.

5, rue Jean Bertels

L-1230 Luxembourg

Grand Duchy of Luxembourg

Phone number: +352 27 02 93 1

Email: aifm@innpact.com