PRIVACY NOTICE

Last update: October 2026

1. Scope of application

This privacy notice (the "**Notice**") describes how Innpact S.A. and Innpact Fund Management S.A. (hereafter referred to as "**Innpact**" or "**we**" or "**us**") treats the information collected or provided during the course of Innpact'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 1 August 2018 on the organisation of the National Commission for Data Protection and implementing the GDPR (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 jointly by Innpact Fund Management S.A. and Innpact S.A. Depending on the relevant processing activity, the Data Controller within the meaning of the GDPR ("**Data Controller**"), is Innpact Fund Management S.A. and/or Innpact S.A. as applicable. The Notice applies to individuals with whom Innpact interacts, including but not limited to employees, consultants, clients, prospects, directors and other counterparties (hereafter referred to as the "**Data Subject(s)**" or "**you**").

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

This Notice may be amended from time to time to reflect changes in our practice with respect to the processing of Personal Data, or changes in applicable law, and we will notify you of any material changes in writing.

The Data Controller for the purposes of this Notice is Innpact with the contact details provided in section 11.

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

The main categories of personal data processed by Innpact (the "**Personal Data**") include, as applicable:

- Personal identification and contact information, such as name, date and place of birth, address, email address, phone number, nationality, gender, social security number, copies of identification documents, driver's license, CVs,
- Professional and corporate information, such as job title, employer, professional experience, corporate and directorship mandates;

- Financial and tax information, such as banking details, income information, tax information, source of wealth, payroll-related information;
- Employment and HR information, such as leave and absence records, performance evaluations, training records and, where applicable, medical certificates of employees;
- Technical and electronic information, such as IP addresses, browser information, website usage data, cookies and other online identifiers that may be collected through visits to our website or social media profiles,
- Meeting and communication information, including professional correspondence and, where meetings are recorded, voice recordings, video recordings, transcripts and related metadata;
- Images and audiovisual content, including profile pictures and photographs or videos taken at events organised by Innpact.

For the avoidance of doubt, Innpact does not process, and service providers of Innpact are not authorised 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 Innpact in case of sickness) or data related to sexual orientation.

We use different sources to collect your 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 you or your organization,
- Information that is generated by Innpact in the course of its business with you,
- 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 Innpact.

Innpact 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 us is processed based on the legal grounds enumerated in Art. 6, Par. 1 of the GDPR. Innpact does not use Personal Data for marketing purposes without consent of the relevant Data Subject.

Most of our Personal Data processing arises from:

- Regulatory or contractual requirements: Processing is necessary for compliance with a legal obligation (e.g. AML/KYC obligations) or for the performance of a contract to which the Data Subject is party. Without this processing, we would not be able to provide the contracted services or comply with applicable laws.

- Legitimate interests (e.g. to ensure security of Innpact's website or access to platforms Innpact 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.
- Consent: Some Personal Data, such as pictures collected at events, may be processed based on consent.

Regarding website users, their Personal Data is processed for statistical purposes, to communicate with users, and to respond to requests.
If we rely on your consent, we will make this clear at the time we request it. You have the right to withdraw consent at any time and may request that we stop processing and delete such Personal Data.

In accordance with Art. 30 of the GDPR, each service provider processing Personal Data on behalf of Innpact must maintain a record of its data processing activities. In accordance with Art. 28(3)(h) of the GDPR, relevant information regarding processing activities must be made available to the Data Controller for inspection upon request.

4. Recipients of Personal Data

Innpact'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 conduct its business activities and fulfil contractual, legal or regulatory obligations, Innpact may disclose Personal Data, where appropriate and on a need-to-know basis to external recipients including Innpact's IT & software service providers, HR support service providers, auditors, legal advisers, or regulatory authorities.

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

5. Storage of Personal Data

Personal Data is retained only for as long as necessary for the purposes for which it was collected, and in any event no longer than required by applicable law or contractual obligations. The retention period for each category of Personal Data is determined by reference to: (i) the purpose of the processing and the duration of the relationship with the Data Subject; (ii) any retention period imposed by applicable law, including anti-money-laundering and counter-terrorist-financing legislation; and (iii) the period during which a claim or legal or regulatory procedure may arise, so that we are able to provide accurate information to competent authorities where required.

Where no specific legal or contractual retention period applies, Personal Data is retained for a maximum of ten (10) years following the termination of the relationship between the Data Subject and Innpact, after which it is deleted or anonymised.

6. Transfer of Personal Data

In order to fulfil Innpact's obligations arising from contract or applicable law, certain Personal Data may be transferred to service providers located outside the European Economic Area (the "**EEA**").

To the extent practicable, Innpact avoids transferring Personal Data to non-EEA countries. Should that occur, Innpact transfers Personal Data outside the EEA only where a valid transfer mechanism under Chapter V of the GDPR is in place. This means the transfer is made either (i) to a country in respect of which the European Commission has adopted an adequacy decision recognising an equivalent level of data protection, or (ii) on the basis of appropriate safeguards, in particular the European Commission's standard contractual clauses, or (iii) where permitted, on the basis of a derogation for specific situations.

Prior to any such transfer, Innpact assesses whether the level of protection afforded to the Personal Data is adequate and, where necessary, implements supplementary measures to ensure that it is transferred and stored securely.

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 section 9 below "**Handling of Data Requests**".

Please find below an outline of the most pertinent rights you have as Data Subjects in relation to your Personal Data processed by Innpact as Data Controller. The exhaustive list of your rights as Data Subject can be found in Art. 15-22 and Art. 77 of the GDPR.

- *Right to access (Art. 15 GDPR), rectification (Art. 16 GDPR), erasure (Art. 17+19 GDPR)*

You have the right to see what Personal Data we have of you in our files.

If you spot an error in your Personal Data in our files, or that it is no longer up to date, you have the right to request that it is rectified.

Any of your Personal Data we have in our files will be deleted upon request, unless Innpact 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)*

Innpact will limit the ways and purposes your Personal Data is processed upon request, unless there are overriding obligations arising out of contract or applicable laws.

- *Right to data portability (Art. 20 GDPR)*

Where the processing is based on your consent or on a contract and is carried out by automated means, you have the right to receive the Personal Data you have provided to us in a structured, commonly used and machine-readable format, and to request that it be transmitted to another controller where technically feasible.

- *Right to object (Art. 21+22 GDPR)*

You have the right to object to the processing of your Personal Data by Innpact and to request Innpact to stop processing your Personal Data. In such case Innpact will stop processing your Personal Data unless there are overriding obligations such as those arising from contract or applicable laws.

- *Right to withdraw your consent at any time (Art. 7)*

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 we stop processing and delete such Personal Data at any time.

Please note that Innpact does not send any newsletters and does not pass on your contact details to any third parties for their own marketing purposes without your explicit consent. You can unsubscribe from the Innpact newsletter or marketing messages at any time via the "unsubscribe" link at the bottom of the emails you receive or by contacting us.

- *Right to complain (Art. 77 GDPR)*

You have the right at all times to lodge a complaint regarding the processing of your Personal Data, whether to Innpact using the contact form on Innpact's website or the contact details in section 11. You also have the right to lodge a complaint directly to a supervisory authority, in particular in the Member State of your habitual residence, place of work or the place of the alleged infringement. In Luxembourg such authority is referred to as the *Commission Nationale de Protection des Données* ("**CNPD**").

8. Security of Personal Data

Innpact has implemented appropriate technical and organisational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data, in accordance with Art. 32 of the GDPR.

Access to Personal Data is restricted to those employees, service providers and other persons who require access in order to perform their functions, and such persons are bound by obligations of confidentiality. Personal Data is stored in controlled environments, and Innpact applies access controls, and organisational safeguards appropriate to the nature and sensitivity of the Personal Data concerned.

Where Innpact engages service providers to process Personal Data on its behalf, such providers are engaged under written agreements requiring them to implement appropriate security measures and to process Personal Data only in accordance with Innpact's instructions, in accordance with Art. 28 of the GDPR.

9. Handling of Data Requests

Data processors shall assist Innpact 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 Innpact, we shall be responsible for obtaining and coordinating the necessary information from the relevant service providers as well as responding to the relevant Data Subject.

10. Handling of Data breaches

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.

In its capacity as Data Controller, Innpact will notify the CNPD of a Personal Data Breach in accordance with Art. 33 of the GDPR, without undue delay and, where feasible, not later than 72 hours after becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the breach is likely to result in a high risk to the rights and freedoms of Data Subjects, Innpact will also notify the affected Data Subjects without undue delay.

Taking into account the processing and storage of Personal Data by service providers, a Personal Data Breach may first be detected by the relevant service provider, which will notify us without undue delay after becoming aware of it. The service provider experiencing the Personal Data Breach is the primary party responsible for assessing the nature of the breach and the likelihood of risk to the rights and freedoms of Data Subjects.

Innpact 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.

11. Contact information

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

Postal and visitor's address:

Innpact S.A. / Innpact Fund Management S.A.

5, rue Jean Bertels

L-1230 Luxembourg

Grand Duchy of Luxembourg

Phone number: +352 27 02 93 1

Email: info@innpact.com