**PRIVATE CAPITAL BELGIUM ESG TEMPLATE**

**DISCLAIMER:**

**Private Capital Belgium would like to extend a heartfelt thank you to the team of Vendis Capital for generously sharing their ESG-related templates with Private Capital Belgium and her members.**

**It is understood that this ESG template is provided to Private capital Belgium members solely for informational and inspirational purposes.** **While every effort has been made to ensure the accuracy and completeness of the information contained herein, no guarantees can be made regarding its full completeness and accuracy. The author cannot be held responsible for any consequences arising from the implementation of any policy and/or procedure based on this template. Users are advised to seek professional advice and conduct their own due diligence before making any decisions based on the content of this document.**

**INSTRUCTION MANUAL**

* **There is a set of ESG templates for portfolio companies in a private equity context and a venture capital context. This set covers these for private equity portfolio companies.**
* **Each template covers a specific ESG topic indicated in the title of the template. The full set of templates includes the following documents:**
  + **Employee Code of Conduct**
  + **Suppliers Code of Conduct**
  + **Anti-corruption & anti-bribery policy**
  + **Anti-discrimination policy**
  + **Whistleblowing policy**
  + **Privacy policy**
  + **Health & safety policy**
  + **Environmental policy**
* **Fields marked in yellow are cross-references to templates with other topics in the BVA ESG template set.**
* **Fields marked in green require policy discretion from the portfolio company.**

**Data Privacy and Security Policy**

[*This document provides a framework for a Data Privacy & Security and should be tailored to the business and practices of each portfolio company*.]

[*Portfolio company*] (the **Company**) is committed to ensuring that privacy is protected, in particular personal data, and that applicable personal data laws and regulations are respected. Ensuring data privacy creates trust between people and organisations.

**Personal information obtained in the context of the Company’s operations must be adequately protected. Every member of staff dealing with Personal Data must be conscious about applicable rules and regulations.**

This Data Privacy & Security Policy (the **Policy**) sets out how the Company uses and protects any personal data that its staff comes across in the execution of their job.

The Company’s executive management is responsible for the effective implementation of the rules set out in this Policy.

|  |  |
| --- | --- |
| To which aspects of the Company’s business and for which persons within the Company is this Policy intended? | See section 1 (Scope) |
| What Personal Data is collected by the Company and how is it used? | See section 2 |
| In what manner does the Company collect Personal Data? | See section 3 |
| How does the Company secure Personal Data? | See section 4 |
| What transfers of Personal Data are permitted? | See section 5 |
| How long can Personal Data be kept? | See section 6 |
| For what reasons can the Company contact any person in respect of whom it has collected Personal Data? | See section 7 |
| What are the rights of the Data Subjects in relation to the Personal Data kept by the Company? | See section 8 |

1. **Scope**

This Policy applies to all Personal Data collected, processed, or stored by the Company in relation to its stakeholders (each, a **Data Subject**), such as:

* its suppliers
* its customers
* its service providers
* its job applicants
* its (website) visitors
* [*others?*]

The scope of this Policy extends to all Data Subjects about which the Company collects and stores data, with the exception of its employees, whose data are collected and stored in accordance with the provisions of the [*employment regulations or national equivalent*].

It covers all aspects of data privacy and protection within the Company’s operations.

1. **What Personal Data is collected and how is it used**

Personal Data is information which helps identify a person, or details that can be traced back to an individual.

The Company limits the collection and use of non-public personal information to the minimum that it believes is necessary to run its business. The categories of data collected (together, the **Personal Data**) include:

* [Name]
* [Email address]
* [IP address]
* [Financial information such as bank details]
* [*please complete with other Personal Data collected by the Company*].

The Company uses Data Subjects’ Personal Data for several purposes, including the following:

* [to ensure that a commercial transaction can proceed]
* [to respond to queries and to resolve complaints]
* [to comply with applicable laws and regulations]
* [to send marketing communications when the Company has permission]
* [*please complete with other purposes of data use*].

The Company will only use Personal Data where it has a legal ground to do so. The legal grounds are determined on the basis of the purposes for which the Personal Data have been collected and used. In every case, the legal ground will be one as specified by Art. 6 of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (the **GDPR**), i.e.:

1. *the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
2. *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;*
3. *processing is necessary for compliance with a legal obligation to which the controller is subject;*
4. *processing is necessary in order to protect the vital interests of the data subject or of another natural person;*
5. *processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
6. *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*
7. **How is Personal Data collected**

The Company collects Personal Data when:

* [*Describe data sources here, e.g. clients visit website, contact via email, etc.*]

1. **How is Personal Data secured**

The Company is committed to maintaining the confidentiality, integrity and security of Personal Data. The Company maintains appropriate technical and organisational measures to prevent Personal Data processed by or on behalf of the Company from accidental or unlawful destruction, loss, alteration, unauthorised disclosure. However, no electronic transmission or storage of information is 100% secure. Therefore, the Company cannot guarantee that loss, misuse, or alteration of Personal Data will never occur.

The Company has implemented the following measures and procedures related to the storage, processing and transfer of Personal Data:

* [*please complete with specific security measures taken by the Company, e.g. measures regarding information classification, encryption measures, protection of computers, backups, network security management, access control measures*]
* [*please describe the Company’s employee training programmes to raise awareness of data privacy and security best practices*]
* [*please describe the Company’s incident response procedures in case of data breaches or unauthorised access to personal information*]

The Company conducts regular reviews and audits to assess and improve the effectiveness of privacy measures.

The Company ensures that any third party agreements contain clear and adequate data protection provisions, as required by the GDPR. These agreements should include:

* the subject matter of the processing, its nature and duration;
* the purpose of the processing;
* the type of personal data and categories of data;
* the obligations and rights of the controller;
* technical and organisational measures that ensure data is processed in line with individual’s rights; and
* the data security measures required.

In case of a Personal Data breach or a security incident that has affected the confidentiality, integrity or availability of Personal Data, the Company’s employees are instructed to immediately inform the data protection officer (insofar appointed) and the executive management. When deemed necessary, the [*relevant supervisory authority*] will be informed within 72 hours of the breach.

1. **International data transfers**

Data may be transferred to, stored and processed in any country or territory where one or more of the Company’s group companies or service providers are based or have facilities.

Transfers of Personal Data may be made to countries located in or outside of the EEA. Certain countries in which recipients and data processors may be located and to which Personal Data may be transferred may not have the same level of protection of Personal Data as the one afforded in the EEA.

Personal Data transferred to countries outside of the EEA will be protected by appropriate safeguards such as standard contractual clauses approved by the European Commission. Data Subjects may obtain a copy of such safeguards by contacting the Company.

1. **How long are Personal Data kept**

The Company keeps Personal Data for only as long as it needs to. This will depend on the purpose for which the Personal Data is used, as set out in this Policy. If the Personal Data can no longer be used, it will be deleted or made anonymous by removing all details that identify a person.

If permission was asked and obtained to process Personal Data and no other lawful grounds exist to continue with that processing, and the permission is withdrawn, the Personal Data will also be deleted.

1. **For what reasons is contact allowed**

The Company may contact any Data Subject in respect of whom Personal Data is collected for the following reasons:

* [Service communications]
* [Marketing communications and editorial newsletters]
* [*please complete with other reasons*]

1. **Rights of the Data Subjects regarding Personal Data kept by the Company**

The Company respects the rights of its Data Subjects according to Chapter III of the GDPR. As such, Data Subjects must be offered and be made aware of the following rights:

* a right to request a copy of the Personal Data held on the Data Subject and information on the origin of those data
* a right to rectify inaccurate Personal Data;
* a right to withdraw consent previously given for the use of Personal Data at any time, without affecting the lawfulness of processing based on consent before its withdrawal
* a right to receive a machine-readable copy of a Data Subject’s Personal Data, so that they can manage and transmit it to another data controller
* a right to ask to delete Personal Data or restrict how they are used. There may be exceptions to the right to erasure for specific legal reasons which, if applicable, must be set out in response to a Data Subject’s request.
* where applicable, a right to object to processing of their Personal Data for certain purposes.
* a right to lodge a complaint with a data protection supervisory authority concerning the processing of Personal Data by the Company.

1. **Changes to this Policy**

If the Company decides to change its this Policy, it will post the changes [*describe location*]. If the changes are significant, the Company may also choose to email all registered users with the new details. If required by law, the Company will get permission or give Data Subjects the opportunity to opt out of any new uses of data.

1. **Approval, amendments and entry into force**

This Policy has been issued and approved by [the Board of Directors/Management/other governing or supervisory body] who is responsible for the adequacy and appropriate overall implementation of the Policy.

Additions, revisions, amendments and abolishment of this Policy are to be approved by [the Board of Directors/Management/other governing or supervisory body]. This Policy will enter into force upon its adoption by [the Board of Directors/Management/other governing or supervisory body].