European Capital Partners (Luxembourg) S.A.
The « Company »
153-155b, rue du Kiem, L-8030 Strassen, Luxembourg
R.C.S. Luxembourg : B 134 746

DATA PROTECTION POLICY

Version: January 2025

1. DATA PROTECTION POLICY

Legal basis

1.1 EU Regulation 2016/679 known as the General Data Protection Regulation (**GDPR**) on data protection and privacy for all individuals within the European Union;

1.2 Replacing the EU Directive 95/46/EC;

1.3 Law of August 1st, 2018 on the protection of individuals with regards to the processing of personal data in criminal and national security measures;

2. DEFINITIONS

2.1 **Board** means the board of directors of the Company;

2.2 **Client** means an existing or potential client of the Company for Individual Portfolio Management Services and/or Non-Core Services –

2.3 **Consent** of the Data Subject 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;

2.4 **Company** means European Capital Partners (Luxembourg) S.A.

2.5 **Compliance Officer** means a person appointed by Management as the Company's compliance officer;

2.6 **Data Protection Officer** means a person acting as Company's Data Protection officer;

2.7 **Director** means any director of the Board;

2.8 **Data Controller** means any 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;

2.9 **Data Processing** means any operation or set of operations which is performed on Personal Data whether or not by automated means, as for instance data collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use and disclosure by transmission, dissemination or otherwise making available, restriction or destruction ;

2.10 **Data Processor** means any natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;

2.11 **Data Subject** means an identified or identifiable natural person;

2.12 **Members of Staff** means any person involved in the Company, including the Directors, the members of Senior Management and any Employee;

2.13 **Personal Data** means all information relating to a Data Subject;

2.13.1 Includes professional, trivial and/or public data;

2.13.2 Includes data that allow identification indirectly (e.g. an online identifier such as an IP address can be Personal Data if it can be linked to the individual);

2.13.3 Legal entities are not protected but **the individuals** working for these entities/representatives of the companies are protected;

2.13.4 Sensitive or special categories of Personal Data (health, racial or ethnic origin, religious / philosophical beliefs, political opinions, trade union memberships);

2.14 **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, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

2.15 **Recipient** means a natural or legal person, public authority, agency or another body, to which the Personal Data are disclosed, whether a third party or not. However, public authorities which may receive Personal Data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable GDPR rules according to the purposes of the processing;

2.16 **Regulation** means EU Regulation 2016/679 known as the General Data Protection Regulation;

2.17 **Senior Management** means the persons who effectively conduct the business of the Company within the meaning of article 102 (1) c) of the UCITS Act and article 7 (1) c) of the AIFM Act.

3. OBJECTIVE

3.1 This Data Protection Policy (the **Policy**) lays out strict requirements for processing Personal Data pertaining to customers, prospects, business partners and employees. It meets the requirements of the European Data Protection Directive and ensures compliance with the principles of national and international data protection laws. The policy sets an applicable data protection and security standard for the Company based on data protection principles.

3.2 This Policy ensures the adequate level of data protection prescribed by the GDPR.

4. CHANGES TO THIS DATA PROTECTION POLICY

This data protection policy will be updated on a regular basis, as well as when it is necessary in the event of changes in relevant legislation. This data protection policy and the personal data register will always contain information regarding the date at which the latest version comes into force. If the changes to this privacy policy are substantial or significant, data subjects will be explicitly informed, for example on the Company's website or via email.

5. SCOPE

Principles for the Processing of Personal Data

5.1 **Fairness and Lawfulness:** when processing Personal Data, the individual rights of the Data Subjects must be protected. Personal Data must be collected and processed in a legal and fair manner.

5.2 **Purpose limitation**: Personal Data are collected for specified, explicit and legitimate purposes and can be processed only for the purpose that was defined before the data collection. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.

5.3 **Transparency**: the Data Subject must be informed of how his/her data is being handled. In general, Personal Data must be collected directly from the individual concerned. When the data is collected, the Data Subject must either be aware of or informed of: the identity of the Data Controller, the purpose of data processing, third parties or categories of third parties to whom the data might be transmitted.

5.4 **Data Proportionality**: before processing Personal Data, it must be determined whether and to what extent the processing of Personal Data is necessary in order to achieve the purpose for which it is undertaken. Personal Data may not be collected in advance and stored for potential future purposes unless required or permitted by national law.

5.5 **Data Erasure**: Personal Data that is no longer needed after the expiration of legal or business process-related periods must be deleted (see §4.21). There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally that historical data must and/or can be retained.

5.6 **Factual accuracy; Rectification of data**: Personal Data on file must be correct, complete, and kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

5.7 **Confidentiality and data security**: Personal Data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

Reliability of Data Processing

5.8 Collecting, processing and using Personal Data is permitted only under the following legal bases, which can exist in parallel but at least one should always be present.

5.8.1 Customer and partner data

(a) **Data processing for a contractual relationship**: Personal Data of the relevant prospects, customers and partners can be processed to establish, execute and terminate a contract. This also includes advisory services for the partner under the contract if this is related to the contractual purpose. Prior to a contract – during the contract initiation phase – Personal Data can be processed to prepare bids or purchase orders or to fulfill other requests of the prospect that relate to contract conclusion. Prospects can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the prospects must be complied with.

(b) **Data processing for marketing purposes**: if the Data Subject contacts the Company to request information (e.g. request to receive information material about a product), Data Processing to meet this request is permitted.

(c) Marketing measures are subject to further legal requirements. Personal Data can be processed for marketing purposes or market and opinion research, provided that this is consistent with the purpose for which the data was originally collected. The Data Subject must be informed about the use of his/her data for marketing purposes. If data is collected only for marketing purposes, the disclosure from the data subject is voluntary. The Data Subject shall be informed that providing data for this purpose is voluntary. When communicating with the Data Subject, Consent shall be obtained from him/her to process the data for marketing purposes. When giving Consent, the Data Subject should be given a choice among available forms of contact such as regular mail, e-mail and phone.

(d) If the Data Subject refuses the use of his/her data for marketing purposes, it can no longer be used for these purposes and must be blocked from use for these purposes. Any other restrictions from specific countries regarding the use of data for marketing purposes must be observed.

(e) **Consent to Data Processing**: data can be processed following consent by the Data Subject. Before giving Consent, the Data Subject must be informed about the Transparency principle of this Data Protection Policy. The declaration of Consent must be obtained in writing or electronically for the purposes of

documentation. In some circumstances, such as telephone conversations, Consent can be given verbally. The granting of Consent must be documented.

(f) **Data Processing pursuant to legal authorization**: the Data Processing of Personal Data is also permitted if national legislation requests, requires or allows this. The type and extent of Data Processing must be necessary for the legally authorized Data Processing activity and must comply with the relevant statutory provisions.

(g) **Data Processing pursuant to legitimate interest**: Personal Data can also be processed if it is necessary for the legitimate interest of the Company. Legitimate interests are generally of a legal (e.g. collection of outstanding receivables) or commercial nature (e.g. avoiding breaches of contract). Personal Data may not be processed for the purposes of a legitimate interest if, in individual cases, there is evidence that the interests of the Data Subject merit protection, and that this takes precedence. Before data is processed, it is necessary to determine whether there are interests that merit protection.

(h) **Processing of highly sensitive data**: highly sensitive Personal Data can be processed only if the law requires this, or the data subject has given express Consent. This data can also be processed if it is mandatory for asserting, exercising, or defending legal claims regarding the Data Subject. If there are plans to process highly sensitive data, the Data Protection Officer must be informed in advance.

*5.8.2 **Employee data***

(a) **Data Processing for the employment relationship**: in employment relationships, Personal Data need to be processed to initiate, carry out and terminate the employment agreement. When initiating an employment relationship, the applicants' Personal Data are processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period (refer §4.21.5), unless the applicant has agreed to remain on file for a future selection process. Consent is also needed to use the data for further application processes or before sharing the application with related parties of the Company.

(b) In the existing employment relationship, Data Processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorized Data Processing apply.

(c) If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national laws have to be observed. In cases of doubt, Consent must be obtained from the Data Subject.

(d) There must be legal authorization to process Personal Data that is related to the employment relationship but was not originally part of the performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, Consent of the employee, or the legitimate interest of the company.

(e) **Data processing pursuant to legal obligation**: the processing of personal employee data is also permitted if national legislation requests, requires or authorizes this as part of the fulfillment of a legal obligation to which the controller is subject. The type and extent of Data Processing must be necessary for the legally obligatory Data Processing activity and must comply with the relevant statutory provisions. If there is room for legal flexibility, the interests of the employee that merit protection must be taken into consideration.

(f) **Consent to Data Processing**: employee data can be processed upon Consent of the person concerned. Declarations of Consent must be submitted voluntarily. Involuntary Consent is void. The declaration of Consent must be obtained in writing or electronically for the purposes of documentation. In certain circumstances, Consent may be given verbally, in which case it must be properly documented. In the event of informed, voluntary provision of data by the relevant party, Consent can be assumed if national laws do not require express Consent. Before giving Consent, the Data Subject must be informed in accordance with the Transparency principle.

(g) **Data Processing pursuant to legitimate interest**: Personal Data can also be processed if it is necessary to enforce a legitimate interest of the Company. Legitimate interests are generally of a legal (e.g. filing, enforcing or defending against legal claims) or financial (e.g. valuation of companies) nature.

(h) Personal Data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee outweigh the interests of the Data Controller. Before data is processed, it must be determined whether there are interests that merit protection and a Legitimate Interests Assessment (LIA) is performed by the DPO of the Company.

(i) Control measures that require processing of employee data can be put in place only if there is a legal obligation to do so or a legitimate reason can be proved to be present. Even if there is a legitimate reason, a proportionality test on the control measure must take place. The justified interests of the Company in performing the control measure (e.g. compliance with legal provisions and internal company rules) must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion and cannot be performed unless appropriate. The legitimate interest of the Company and any interests of the employee meriting protection must be identified and documented before any measures are taken. Moreover, any additional requirements under national law (e.g. rights of co-determination for the employee representatives and information rights of the Data Subjects) must be taken into account.

(j) **Processing of special categories of data**: special categories of Personal Data can be processed only under certain conditions. Personal data that reveal racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, and the health and sex life or sexual orientation of the Data Subject are considered to be part of special categories of data.

(k) The processing must be expressly permitted or prescribed under national law. Additionally, processing can be permitted if it is necessary for the responsible authority to fulfill its rights and duties in the area of employment law. The employee can also expressly consent to processing.

(l) **Telecommunications and internet**: telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by the Company primarily for work-related assignments. They are a tool and a Company resource. They can be used within the applicable legal regulations and internal company policies. In the event of authorized use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.

(m) For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be logged for a temporary period. Evaluations of this data from a specific person can be made only in concrete, justified case of suspected violations of laws or policies of the Company.

Transmission of Personal Data

5.9 Transmission of Personal Data to Recipients outside or inside the Company is subject to the authorization requirements for processing Personal Data under the *Reliability of Data Processing* section. The data Recipient must be required to use the data only for the defined purposes.

5.10 If data is transmitted to a Recipient outside the Company and to a third country, this country must agree to maintain a data protection level equivalent to this Data Protection Policy. This does not apply if transmission is based on a legal obligation.

5.11 If data is transmitted by a third party to the Company, it must be ensured that the data can be used for the intended purpose.

Contract Data Processing

5.12 Data processing on behalf of the Company means that a provider is hired to process Personal Data, without being assigned responsibility for the related business process. In these cases, an agreement on Data Processing "on behalf" must be concluded with external providers. The Company retains full responsibility for the correct

performance of Data Processing. The provider can process Personal Data only as per the instructions from the Client.

5.13 The provider must be chosen based on its ability to cover the required technical and organizational protective measures. The order must be placed in writing. The instructions on Data Processing and the responsibilities of the Client and provider must be documented. The contractual standards for data protection provided by the Compliance Officer must be considered. Before Data Processing begins, the Client must be confident that the provider will comply with the obligations of the Regulation as well as the national law, as it has incorporated the Regulation. A provider can document its compliance with data security requirements in particular by presenting suitable certification, which the Company expects to be presented with.

5.14 In the event of cross-border Data processing, the relevant national requirements for disclosing Personal Data abroad must be met. Personal Data from the European Economic Area can be processed in a third country only if the provider can prove that it has a data protection standard equivalent to this Data Protection Policy. Suitable tools can be: (1) an agreement on EU standard contract clauses for contract Data Processing in third countries with the provider and any subcontractors; (2) participation of the provider in a certification system accredited by the EU for the provision of a sufficient data protection level; (3) acknowledgment of binding corporate rules of the provider to create a suitable level of data protection by the responsible supervisory authorities for data protection.

Rights of the Data Subject

5.15 Data Subjects have the following rights regarding their personal data and the way it is processed:

5.15.1 The right to be informed that processing is being undertaken, alongside the contact details of the Company;

5.15.2 The right to make subject access requests regarding the nature of information held and to whom it has been disclosed within the statutory 40 days;

5.15.3 The right to prevent processing likely to cause damage or distress, with making choices proportionate to the purpose;

5.15.4 The right to oppose to processing for purposes of direct marketing;

5.15.5 The right to be informed about mechanics of any automated decision-making process that will significantly affect them;

5.15.6 The right not to have significant decisions that will affect them taken solely by automated process;

5.15.7 The right to sue for compensation if they suffer damage by any contravention of the Regulation;

5.15.8 The right to obtain from the Company without undue delay the rectification of inaccurate data concerning him or her, or the erasure of personal data when the personal data are no longer necessary in relation to the purposes they were collected or otherwise processed by the Company;

5.15.9 The right to lodge a complaint with the supervisory authority, Commission Nationale pour la Protection des données personelles (CNPD)

Confidentiality of processing

5.16 Personal Data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees is prohibited. Any Data Processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is prohibited and will be considered a data breach. In order to ensure data minimization, ECP has integrated the “need-to-know” principle. Employees may have access to personal information only as far as the type and scope of the task in question allows them to. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities, which is performed by the DPO, Martin Rausch.

5.17 Employees are forbidden to use Personal Data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect privacy. This obligation shall remain in force even after employment has ended.

Data Storage, Retention and Disposal

5.18 It is the responsibility of the Senior Management to ensure that centralised records are maintained to meet the needs and reasonable expectations of customers, prospects, business partners and employees.

For employees, Human Resources has the responsibility of ensuring that centralised records are maintained. ECP has integrated an HR tool called Personio that is established in Munich, Germany and is subject to the Regulation. The tool is working on the basis of the data minimization principle and only process data with the purpose and legal basis assigned to it. It is also secured against intrusion and cyber-crime. The Company has performed an assessment on the sufficiency of the provider, according it is assured that the data being processed is being done so and is secure in accordance with the Luxembourg law of August 2018;

5.19 Where possible central databases (such as Microsoft Explorer, or VTiger) should be used to avoid duplication of information and to increase data security;

5.20 The Company is required to ensure that all data is accurate and up-to-date. Members of Staff have a responsibility to regularly update the records of customers, prospects, business partners and their own Personal Data;

5.21 The Company shall not retain any Personal Data for longer than is necessary or stipulated in the EU Regulation 2016/679 or Law of August 1st, 2018, on the protection of individuals with regards to the processing of personal data in criminal and national security measures. This means that all Personal Data should be destroyed or deleted when it is no longer required. Below are few examples of the most common cases applicable to the Company operations:

5.21.1 10 years for all evidence supporting a transaction or booking entry, including letters received or sent (art. 16 of Code of Commerce);

5.21.2 5 years for all documents in relation to AGM resolutions, Board resolutions, shareholders' register, bylaws (art. 157 of the law of 10 August 1915 as amended);

5.21.3 10 years for employment contracts, salary slips (art. 16 of Code of Commerce);

5.21.4 Employment duration for employee's evaluation (CNIL recommendation n°2005-002)

5.21.5 2 years for CVs collected during a recruitment process (CNIL recommendation n°02-017)

5.21.6 No legal or regulatory duration for data used for marketing purposes but the data processing must be subject to the Data Subject's consent.

5.21.7 The Company is applying specific retention period for different types of documents. Authorised to handle such documents, should regularly go through the documents and confidentially destroy the ones that are no longer being processed within the legal time limit (e.g. shredding, disposal as confidential waste, secure electronic deletion).

Security of Data

5.22 All staff are responsible for ensuring that any personal data (on others) which they hold is kept securely and that it is not disclosed to any unauthorized third party. The Company is demonstrating data minimization policy and all personal data are accessible only to those who need to use it. Based upon the sensitivity of the information in question, personal data information is kept:

5.22.1 In a lockable room with controlled access, or

5.22.2 In a locked drawer or filing cabinet, or

5.22.3 If computerised, password protected, or

5.22.4 If in external disks , the disks themselves kept securely.

5.22.5 Care should be taken to ensure that PCs and terminals are not visible except to authorized staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screensavers and manual records should not be left where they can be accessed by unauthorized personnel.

5.22.6 Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

Email Usage

5.23 The majority of e-mail communications that Members of Staff send or receive will be in relation to usual daily business. Staff should avoid using e-mail to send Personal Data of a sensitive nature or to express views about Data Subjects. This is because e-mail is an insecure medium and the sender has no control over the storage or use of the message after it has been sent.

Data Protection Control

5.24 Compliance with the Data Protection Policy and the applicable data protection laws is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of the Compliance Officer, the data protection coordinators, and other company units with audit rights or external auditors hired. The results of the data protection controls must be reported to the Compliance Officer. The Board must be informed of the primary results as part of the related reporting duties. On request, the results of data protection controls will be made available to the responsible data protection authority. The responsible data

protection authority can perform its own controls of compliance with the regulations of this Policy, as permitted under national law.

Data Protection Incidents

5.25 All employees must inform the Senior Management or the Compliance Officer immediately about cases of violations against this Data Protection Policy or other regulations on the protection of Personal Data.

5.26 In cases of improper transmission of Personal Data to third parties, improper access by third parties to Personal Data, or loss of Personal Data, a data breach report must be made immediately to the *Commission Nationale pour la Protection des Données* (**CNPD**) so that any reporting duties under national law can be complied with:

National Commission for Data Protection
15, Boulevard du JazzL-4370 Belvaux
Tél. : (+352) 26 10 60 -1

Responsabilities and Sanctions

5.27 The Board is responsible for all Data Processing of the Company. Therefore, they are required to ensure that the legal requirements, and those contained in the Data Protection Policy, for data protection are met (e.g. national reporting duties). The Senior Management is responsible for ensuring that organizational, HR, and technical measures are in place so that any Data Processing is carried out in accordance with data protection. Compliance with these requirements is the responsibility of the relevant employees. If official agencies perform data protection controls, the Compliance Officer must be informed immediately.

Compliance Officer – Data Protection Officer (DPO)

5.28 The Compliance Officer works towards compliance with national and international data protection regulations. He is responsible for the Data Protection Policy and supervises its compliance. The Compliance Officer is appointed by the Board of Directors of the Company and approved by the regulator. The Compliance Officer of the Company is carrying out the responsibilities of the Data Protection Officer.

5.29 Any Data Subject may approach the Compliance Officer at any time to raise concerns, ask questions, request information, or make complaints relating to data protection or data security issues. If requested, concerns and complaints will be handled confidentially.

5.30 If the Compliance Officer cannot resolve a complaint or remedy a breach of the Policy for data protection, the Senior Management must be consulted immediately to remedy data protection breaches.

5.31 Inquiries by supervisory authorities must always be reported to the Compliance Officer.

Tasks of the DPO

5.32 The DPO has to ensure that the data protection rules are respected in cooperation with the data protection authority.

5.33 The DPO must:

Ensure that controllers and data subjects are informed about their data protection rights, obligations and responsibilities and raise awareness about them;

Give advice and recommendations to Staff about the interpretation or application of the data protection rules.

Create and keep up to date a personal data register of processing operations within the Company. (Updates on the personal Data register will have to be followed up within).

Ensure data protection compliance within the Company and help the latter to be accountable in this respect.

Handle queries or complaints on request by Customers of the Company, the controller, other person(s), or on her own initiative;

Draw the Company Board's attention to any failure to comply with the applicable data protection rules.

5.34 The DPO has to ensure the below Compliance monitoring with Staff at the Company.

Accountability GDPR Article 24 Recitals 74, 75, 76, 77, 84	The Company has implemented organizational measures that ensure authorized management is informed, involved and accountable of personal data processing activities.	Specifically, the Company has implemented an appropriate data protection policy, it has formally allocated roles and responsibilities. Compliance is checking that regular reporting dashboards around data protection are transmitted to the authorized management (at least half yearly, if there are not any events of data breach or others that must be reported at exceptional time).

		The data protection policies (or updates thereof) are approved by the authorized management at least annually. The formal reporting lines are described in the policy. The documentation on decisions impacting data protection can be retrieved (for example, in the content of minutes of the Senior Management meetings).
Review of policies and procedures GDPR Article 24 Recitals 74, 75, 76, 77, 84	The Company reviews, on a regular basis and at least annually, the operational effectiveness of its data protection governance policies and procedures and adapts them accordingly.	Compliance is checking that policies and procedures that involve handling of personal data are constantly updated, if there is a need, and at least annually. The Company is also training the personnel to follow the procedures.
Quality of purpose definition GDPR Article 5 Recitals 29, 116, 123	For each processing activity in scope, the Company has implemented measures to ensure that: • it has formally **assessed that the purpose(s)** for which it collects the data are specific, explicit and legitimate;• it does **not further process** the data in a manner that is incompatible with those	Compliance Officer is ensuring that the register of processing activities is obtained and that there is an assessment whether the purpose of the data processing activities are well described and defined to ensure that data collected are specific, explicit and legitimate.

	purposes;• purposes have been described in a way that allows data subjects to understand and assess the impact in regard to their privacy.	Furthermore, the Company ensures that the privacy notice is obtained and that there is an assessment whether the processing activities are in the scope of the notice.
Accuracy of the data source and updates of the data GDPR Article 5 Recitals 29,116,123	For each processing activity in scope, the Company has implemented measures that ensure that data sources used to collect personal data are relevant and the collected and processed data is accurate. Furthermore, it is ensured that the personal data is kept up to date and the accuracy of the personal data is reviewed on a regular basis and at least annually.	This is achieved by compliance monitoring and the regular updating of the policies and procedures as mentioned above.
Data protection by design/ by default GDPR Article 25 Recital 78	The Company has implemented measures that ensure that data protection principles are integrated at the earliest possible stage when a new data processing activity is developed.	Compliance monitoring checks that data protection by design/ be default are considered in the existing and future organizational and technology processes and procedures. In particular, there are measures in place that ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Assessment of sufficiency GDPR Article 28 Recital 81	For each processing activity in scope, here the Company uses a processor, it has assessed that the processor is providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements and ensure the protection of the rights of the data subject.	ECP has ensured that all its providers are either subject to the GDPR as members of the EAA or if not, they have implemented sufficient safeguards that provide the same level of protection. Due Diligence is being performed in all cases an activity is being outsourced, which includes a review on the controls in place by the proposed data processor to ensure that any data being processed by it is secured and processed in accordance with the Luxembourg law of August 2018.
Data Protection Impact Assessment GDPR Article 35 Recital 72, 84, 89-95	For each processing activity in scope, the entity has assessed and documented the decision to perform DPIA. In case the Company decides either to not perform a DPIA or to perform one.	The DPO decides whether the assessment should be carried out. Furthermore, the relevant staff receives adequate training to understand the need to consider a DPIA at the early stages of any plan involving personal data.

When is the appointment of a DPO mandatory?

According to art. 37(1) GDPR, three specific cases require the appointment of a DPO. As regards to the Company the DPO could only be appointed through Article 37 (1) b, which states that if the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale. Luxembourg law of August 2018 does not put in place other or different requirements. The Company has appointed

a Data Protection Officer, since according to Recital 97 of the Regulation, the core activities of the Company, which is part of the private sector, relate its primary activities which indeed include processing of personal data in a large scale.

Digital Operational Resilience Act (DORA) – Regulation (EU) 2022/2554

DORA establishes uniform requirements concerning the security of network and information systems supporting the business processes of financial entities needed to achieve a high common level of digital operational resilience. Even though DORA does not introduce sector-specific rules on personal data protection, indirectly substantial part of its requirements, being targeted at the security of network and information systems and ensuring digital operational resilience, reflects the ways in which financial entities equally comply with GDPR requirements. In this respect, it is important to look at the interplay between the GDPR and DORA, specifically in the key areas where their requirements intertwine, and what would be necessary to effectively comply with them. At this point, it is noteworthy that the GDPR remains fully applicable to the financial sector, and none of the DORA requirements will derogate the general rules of GDPR. The Company in its capacity as an Alternative Investment Fund Manager is under the scope of the DORA Regulation and specifically it must abide with the requirements which concern any undertaking providing digital or data services, including providers of cloud computing services, software, data analytics services, data centers, but excluding providers of hardware components and undertakings authorised under Union law which provide electronic communication services, which provide their services to the financial entities. These are so-called ICT third-party service providers. As mentioned before, a sufficiency assessment is always performed before a new relationship is created within the company and a third-party service provider, following Article 28 and Recital 81 of the GDPR Regulation. With the DORA Regulation, this assessment is also required. That being said, compliance with the GDPR and the existence of properly maintained data inventories, including registers under Article 30 of the GDPR, facilitate the Company in its efforts to comply with DORA. Another requirement under DORA is to perform a risk assessment upon each major change in the network and information system infrastructure, in the processes, or procedures, affecting its functions, supporting processes, or information assets. This requirement intertwines in certain cases with the requirements to carry out Data Protection Impact Assessments ('DPIAs') under Article 35 of the GDPR. Although not every major change in the network and information system infrastructure, the

processes, or procedures, affecting the Company's functions, supporting processes, or information assets would result in the necessity to carry out a DPIA, the risk assessment under DORA could serve as an initial assessment on whether a DPIA under the GDPR is necessary, since such a risk assessment includes an assessment of the risks related to the protection and security of personal data as far as the latter is processed in the respective networks, systems, processes, or information assets. However, these assessments will have a different scope and content. Under GDPR adopts a risk-approach without specifying the required technical and organizational measures as minimal standards to ensure level of security of the processed personal data, DORA Regulation introduces specific requirements regarding the security measure that financial entities should implement. Meaning that the Company should consider these requirements as an indication of what should be considered as adequate technical and organisational measures to ensure the security of the personal data in the financial sector.

The Company is implementing DORA requirements through various policies and specifically the ICT Risk Management Policy, the IT Policy and the Outsourcing, Delegation & Counterparty Policy.

European Capital Partners (Luxembourg) S.A.
The « Company »
153-155b, rue du Kiem, L-8030 Strassen, Luxembourg
R.C.S. Luxembourg : B 134 746

APPENDIX I – DATA SUBJECT ACCESS REQUEST FORM

1. Details of the person requesting the information
Full name:
Address:
Telephone number:
Email:

2. Are you the Data Subject?
☐ YES
If you are the Data Subject please supply evidence of your identity i.e. ID card, passport, driving license, birth certificate or any certified true copy of the afore-mentioned documents (please go to question 5)

☐ NO
If you are acting on behalf of the Data Subject with their written authority, that authority must be enclosed (please complete questions 3 and 4)

3. Details of the Data Subject (if different to 1.)
Full name:
Address:
Telephone number:

Email:

4. Please describe your relationship with the Data Subject that leads you to make this request for information on their behalf.

European Capital Partners (Luxembourg) S.A.
The « Company »
153-155b, rue du Kiem, L-8030 Strassen, Luxembourg
R.C.S. Luxembourg : B 134 746

5. Please state below specific information or document(s) you wish to see (e.g. subscription document, employment contract, etc.), please describe these below:

Declaration

I, _____, certify that the information given on this application form to European Capital Partners (Luxembourg) S.A. is true. I understand that it is necessary for European Capital Partners (Luxembourg) S.A. to confirm my Data Subject's identity and it may be necessary to obtain more detailed information in order to locate the correct information.

Signed _____ Date _____

Please return the completed form to European Capital Partners (Luxembourg) S.A., 153-155b, rue du Kiem , L-8030 Strassen, Grand-Duchy of Luxembourg.

Documents which must accompany this application are: (1) evidence of your identity, (2) evidence of the Data Subject's identity (if different from above), (3) evidence of Data Subject's consent to disclose to a third party (if required as indicated above).

European Capital Partners' use only Request received:

Date completed:
Received by:
Additional notes:

European Capital Partners (Luxembourg) S.A.
The « Company »
153-155b, rue du Kiem, L-8030 Strassen, Luxembourg
R.C.S. Luxembourg : B 134 746

-

APPENDIX II – EMPLOYEE STATEMENT

[**MM DD, YYYY**]

To the Compliance Officer/Date Protection Officer

I _____ hereby declare having read and understand the terms of Data Protection Policy.

I collect and use personal data from, and about, current and former customers, prospects, business partners and fellow employees.

I understand and ensure that all afore-mentioned personal data have been:

- obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the person concerned;
- processed within the strict terms of the Company's internal Data Privacy Policy;
- Relevant for the purposes for which it is used or to be used;
- Accurate, complete and up to date;
- Kept for no longer than is necessary for its declared purpose;
- Held in the full knowledge of the person concerned;
- Protected from unauthorised cross border transmission to any other state which does not meet those standards laid down by the Council of Europe Convention (1981), the EC Data Protection Directive (95/46/EC) and the EU Regulation 2016/79.

The principal purposes for holding Personal Data may include:

- Consent from the person concerned;
- The provision of services as stipulated in an applicable contract;
- The compliance with a legal obligation;
- Legitimate interest e.g., market research and marketing;

Date:

Signature:

APPENDIX III – PRIVACY STATEMENT

1. INTRODUCTION

1.1 The European Commission has adopted a renewed data protection framework in May 2016 named the General Data Protection Regulation (**GDPR**). The GDPR will replace the current Directive[1] and will be directly applicable in all Member States without the need for implementing national legislation. It has come into force since May 25, 2018. The objective of this regulation is to enhance EU citizens' rights and protection over their Personal Data.

1.2 The Company has therefore put in place this Statement to set forth the principles and requirements governing the collection, use and disclosure of customer information, including their Personal Data, in compliance with laws and regulations applicable in Luxembourg, in particular the General Data Protection Regulation and the Luxembourg Law of 2018.

[1] EU Directive 95/46/EC

1.3 This Statement is to be read jointly with the Company's Data Protection Policy available on www.ecp.lu.

2. COLLECTING PERSONAL DATA

2.1 The type of Personal Data the Company collects, uses and discloses for legal and business purposes are listed below:

2.1.1 Identification documents incl. passport copies, ID cards, driving licenses;

2.1.2 Contact details e.g. name, address, telephone number, email address;

2.1.3 Curriculum vitea e.g. education, training, qualifications, profession;

2.1.4 Personal characteristics e.g. age, gender, nationality, marital status, date and place of birth;

2.1.5 Evidence of tax residency;

2.1.6 Extract of the criminal record;

2.1.7 Bank references incl. financial information;

2.1.8 Name screening (comparison with lists of sanctions).

3. PURPOSE FOR COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

3.1 The purposes for which Personal Data relating to a natural person may be collected, used and disclosed may include:

3.1.1 For contractual purpose:

(a) Complying with or enforcing the terms and conditions of any contract or agreement entered into by or on behalf of the Company;

(b) The provision of the Company services including portfolio management, risk management, compliance, reporting, etc.;

(c) The procurement of transaction and data processing;

(d) Processing, confirming and fulfilling customers' or other natural persons' requests regarding the Company's services and/or transactions;

(e) For security, business continuity, emergency contact and travel purposes;

3.1.2 For legal obligation:

(a) Conducting customer checks, in particular anti-money laundering ("AML") checks pursuant to the law of 12 November 2004 on anti-money laundering and counter-terrorism financing (the **2004 Law**);

(b) Complying with the obligations, requirements or arrangements for disclosing and using personal data that apply to the Company, as follows:

(i) Regulatory and/or legal provisions, in particular anti-money laundering and counter-terrorism financing legislation, which require the compliance with Know-Your-Customer (KYC) obligations and therefore the identification, verification and background screening purposes of any natural person the Company is directly or indirectly in business relationship with;

(ii) Any notifications, directives or guidelines issued by any legal, regulatory, governmental, tax, law enforcement or other authorities, or self-regulatory or industry bodies or associations of financial services providers;

(iii) Any contractual commitment with local or foreign legal, regulatory, supervisory, governmental, tax, law enforcement or other authorities, or self-regulatory or industry bodies or associations of financial services providers;

(b) For security, business continuity, emergency contact and travel purposes;

3.1.3 For marketing purposes:

(a) Developing business relationships with prospects;

(b) Providing information and updates, e.g. newsletters, mailing and investor updates, about the Company services and performance;

(c) Organizing events or conferences;

3.1.4 For legitimate interests:

(a) All other incidental purposes relating thereto and other purposes to which the individuals or organizations may from time to time agree.

4. DISCLOSURE OF PERSONAL DATA & CUSTOMER INFORMATION

4.1 Customer information including their Personal Data will be kept confidential and securely stored in the Company's premises. A limited number of persons have access to these Personal Data.

4.2 However, the Company may provide and/or disclose such data and information to the following parties for the above purposes, where applicable:

4.2.1 Any agent, contractor or third-party service provider who provides administrative, telecommunications, information technology, transaction and data processing, payment or securities clearing debt collection, business

processing, mailing, call center, operational or other services to the Company in connection with the operation of its business;

4.2.2 Any other person under a duty of confidentiality to the Company e.g. its auditors, independent director, etc.;

4.2.3 Any person, body or authority to whom the Company is under an obligation or otherwise required, advised, recommended or expected to make disclosure under the requirements of any laws, rules or regulations binding on or applying to the Company, or any disclosure under and for the purposes of any notifications, directives, guidelines or guidance given or issued by or agreement with any legal, regulatory, governmental, tax, law enforcement or other authorities, or self-regulatory or industry bodies or associations of financial services providers with which the Company is obliged, required, advised, recommended or expected to comply, or any disclosure pursuant to any contractual or other commitment of the Company with local or foreign legal, regulatory, supervisory, governmental, tax, law enforcement or other authorities, or self-regulatory or industry bodies or associations of financial services providers, all of which may be within or outside Luxembourg and may be existing currently and in the future;

4.2.4 Any actual or proposed assignee of the Company or participant or sub-participant or transferee of the Company's rights in respect of a natural person or an organization;

4.2.5 Third-party financial institutions, custodians, clearing houses, insurers, credit card companies, securities and investment services providers;

4.2.6 The Company’s professional service providers and advisers including lawyers, notaries, tax advisers, auditors and accountants;

4.2.7 Any party in respect of which such disclosure is requested and/or consented to by the customer and/or natural person;

4.2.8 The list of third parties to which your personal data may be transferred is available upon request to be addressed to the contact person (see §12.2).

4.2.9 In the event of a merger, acquisition, restructuring, or sale of all or part of our business or assets, your personal data may be transferred to the acquiring or successor entity as part of the transaction. Such transfer will comply with Luxembourg's data protection laws, including the GDPR, and will be subject to the following safeguards:

- purpose limitation: the acquiring or successor entity will process your personal data only for the purposes outlined in this Privacy Policy or for closely related purposes that are compatible with the original purposes of processing
- legal basis: The transfer of personal data will be based on one of the lawful grounds under GDPR, such as compliance with a legal obligation, legitimate interest, or, where applicable, your consent.
- security measures: We will ensure that the transfer is conducted securely, using encryption and other appropriate technical and organizational measures.

Notification: You will be informed in a timely manner about the transaction, the identity of the new data controller, and any significant changes to how your personal data is processed.

Commented [OT1]: New clause, as discussed after the Eurinvest Project. Let me know if you agree.

5. TRANSFER OF PERSONAL DATA AND CUSTOMER INFORMATION OUTSIDE OF LUXEMBOURG AND OUTSIDE OF THE EU

5.1 The Company may in certain circumstances transfer customer information including their Personal Data outside Luxembourg and the EU for the above purposes, where applicable.

5.2 Such information may be disclosed, processed, stored or maintained in accordance with the local data protection laws, rules and regulations applicable in the relevant jurisdictions.

5.3 The Company shall ask the Data Subject for his/her explicit consent before transferring any personal data to a third country having an insufficient level of protection.

5.4 The Company may also adopt the Commission's contractual clauses with any third party listed in section 4. located in a third country having an insufficient level of protection in order to guarantee EU level of protection by this third party.

6. DISCLOSURE OF PERSONAL DATA OF THIRD PARTIES TO THE COMPANY

6.1 Before disclosing any Personal Data relating to its employees, contractors and other individuals to the Company shall (1) ensure that those natural persons are duly notified and made aware of this Statement, (2) shall undertake and represent those natural persons have procured their consent to the collection, use and disclosure of their Personal Data as described in this Statement.

7. UPDATE OF PERSONAL DATA AND CUSTOMER INFORMATION

7.1 Customers, and other organizations or natural persons who provide (or authorize the provision of) information to the Company undertake that such information is true, accurate and complete.

7.2 In order to ensure the accuracy and validity of Personal Data collected, used and disclosed, natural persons have the right to notify the Company in writing promptly upon any changes in their Personal Data.

8. ACCESS AND CORRECTION OF PERSONAL DATA

8.1 Pursuant to the Regulation and the Luxembourg Law of 2018, natural persons may request access to or make corrections to their Personal Data. Such request may be sent to Compliance Officer/Data Protection Officer (refer to §12.2).

9. WITHDRAWAL OF CONSENT

9.1 Pursuant to the Regulation and the Luxembourg Law of 2018, customers may withdraw their consent to the collection, use or disclosure of their Personal Data.

9.2 However, if a customer or individual does not provide or withdraw such consent or fails to provide requisite Personal Data, the Company may be unable to initiate or continue a relationship with the natural persons or organization concerned.

10. ANTI-MONEY LAUNDERING AND CTF LEGISLATION

10.1 AML-CTF legislation in this context encompasses the AML Directives, Luxembourg laws, CSSF circulars, FATF recommendations and guidance documents, and any other source of regulation related to anti-money laundering and combatting the financing of terrorism. The Company is obliged to act in accordance with the 2004 Law. Customers are asked to actively support the Company in obtaining certain types of information, including those required under anti-money laundering laws and regulations in Luxembourg.

10.2 The Company is required to ask customers questions regarding their identity, the company or association they belong to, their legal representatives, authorized signatories, source of funds and, if necessary, also regarding individual transactions.

10.3 The Company also has a duty to verify the identity of the respective ultimate beneficial owner of the customer or of the assets brought in.

How can consent affect data protection under AML-CTF legislation?
Can AML-CTF information only be processed if one individual has explicitly given her/his consent to do so?

The following aspects are important in this regard:

- Consent is one of the six legal bases for data processing, (see answer to the question 'What is a lawful basis for processing' within the general aspects section of this Q&A document). Consent will not always be the easiest or most appropriate basis.
- In the case of AML-CTF legislation, the adequate lawful basis for processing will be compliance with a legal obligation of the Company: Consent is not required.

As a result of the fact that AML legislation provides for specific derogations (see art. 6(10) of the Law of 13 February 2018), such AML legislation will prevail, but it should work hand in hand with the GDPR. This means that one should consider the changes related to the 4AMLD and 5AMLD in parallel to the GDPR. This will force companies/data controllers/processors to embed privacy requirements in AML policies and procedures. The same way one trains its staff on AML, the same way one should train its staff regarding data protection. The Company has implemented this in its practices and is carrying out mandatory annual training of all its personnel on both of these subjects, among other things.

11. AUTOMATIC EXCHANGE OF INFORMATION

11.1 By application of the US Foreign Account Tax Compliance Act (**FATCA**) and the Common Reporting Standards (**CRS**) regulations concerning automatic exchange of information, as well as the 2002 Law on the protection of natural persons in relation to the processing of their personal data, natural persons declare being informed, acknowledge and agree, that their Personal Data and financial information provided by the Company to financial institutions for the purposes mentioned in section 2. of this Statement may be thereafter potentially used by the financial institutions in the execution of their FATCA and CRS duty to provide information to the Luxembourg tax authorities. That information can in turn be forwarded to the relevant foreign tax authorities, including the relevant US tax authorities.

11.2 The Customer must provide any additional information that might be required from time to time by the Company for the purpose of the FATCA and CRS laws and failure to do so within the prescribed timeframe may trigger a reporting to the Luxembourg tax authorities.

12. CONTACT PERSON WITHIN THE COMPANY

The person to whom requests for access to, or correction of personal data or withdrawal of consent for the processing of personal data or for information regarding the Company's policies and practices and kinds of Personal Data held by the Company is to be addressed as follows:

- By post: European Capital Partners, 153-155b, rue du Kiem, L-8030, Strassen, Luxembourg, under the attention of Mr. Martin Rausch
- By mail: compliance@ecp.lu, under the attention of Mr. Martin Rausch.

13. DATA PROTECTION REGULATOR

In cases of non-compliance with the law and/or regulatory provisions, a data breach report must be filed with the *Commission Nationale pour la Protection des Données* (**CNPD**):

Commission Nationale pour la Protection des Données

15, Boulevard du Jazz

L-4370 Belvaux, Luxembourg

14. MISCELLANEOUS

14.1 This Statement shall be deemed an integral part of all contracts, agreements, facility offer letters, account mandates and other binding arrangements which customers or other individuals or organizations have entered into or intend to enter into with the Company.

14.2 This Statement may be updated from time to time to reflect changes and/or developments in data protection and banking secrecy laws, regulations, guidelines, codes and industry practices in Luxembourg.

14.3 The Company periodically updates the features of the Website to better serve its customers. The Company reserves the right to change this Privacy Statement without advance notice and any modifications are effective when they are posted here. The date of the newest version will be posted below. Please check back frequently, especially before you submit any personally identifiable information at this Website, to see if the Privacy Statement has changed. By using this Website, you indicate your understanding and acceptance of the terms of

the Privacy Statement posted at the time of your use. If you have any questions, please contact the Company, using the ways of communication stated above. *(see 12.1)*