Shard Capital Partners LLP
23rd Floor,
20 Fenchurch St,
London, EC3M 3BY

T +44 (0)207 186 9900
F +44 (0)207 186 9979
E info@shardcapital.com
W shardcapital.com

Data Protection Policy

1. Introduction

1.1 This Data Protection Policy ("Policy") applies to Shard Capital Partners LLP, which includes the following entities; Shard Capital Limited, SCSB Limited, Rubrics Asset Management Limited, Shard Merchant Capital Limited, Shard Capital AIFM LLP, Shard Credit Partners Limited, Alternative Resource Capital, Shard Capital Services Limited, Suir Valley Funds ICAV, Sure Ventures Plc (hereinafter referred to as the "Company", "we" or "us").

1.2 Throughout the business day the Company may need to collect personal information from our customers, employees and/or potential customers to ensure that we are providing the correct information in relation to the services we offer. Such data is collected from employees, customers, suppliers and clients and includes (but is not limited to), name, address, email address, data of birth, IP address, identification numbers, private and confidential information, sensitive information and bank details.

1.3 We may also be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to processing all personal information in accordance with the General Data Protection Regulation (EU) (2016/679) ("GDPR"), UK data protection laws and any other relevant data protection laws and codes of conduct (herein collectively referred to as "the data protection laws").

1.4 The protection of personal data requires that appropriate technical and organisational measures are taken to demonstrate a high level of data protection. The Company has adopted a number of internal and external data protection policies, which must be adhered to by employees of the Company.

1.5 Considering the above, The Company wants to ensure a high level of data protection as privacy is a cornerstone in gaining and maintaining the trust of our employees, customers and suppliers and thus, ensuring the Company's business in the future.

1.6 This Policy with guidelines for processing of personal data, constitutes the overall framework for processing of personal data within the Company.

2. Policy Statement

2.1 The Company has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, and ongoing monitoring and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities and we are proud to operate a 'Privacy by Design' approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

2.2 Additionally, the Company will monitor, audit and document internal compliance with the data protection policies and applicable statutory data protection requirements, including the GDPR.

2.3 The Company will also take the necessary steps to enhance data protection compliance within the organisation. These steps include the assignment of responsibilities, raising awareness and training of staff involved in processing operations. Please note that our Policy will be reviewed from time to time to consider any new obligations and that any personal data will hold will be governed by our most recent Policy

2.4 The Data Protection Officer (DPO) is Toby Raincock. The DPO will work in conjunction with the Compliance Officer and other relevant functions to ensure that all processes, systems and staff are operating compliantly and within the requirements of the data protection laws and its principles.

2.5 The Company is registered with The Information Commissioners Office (ICO) which is an independent regulatory office who reports directly to Parliament and whose role it is to uphold information rights in the public interest.

2.6 The Company appears on the Data Protection Register as a controller of personal information with ICO Registration number ZA014858.

3. Purpose

The purpose of this policy is to ensure that the Company meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and, in the individuals, best interest.

3.1 The data protection laws include provisions that promote accountability and governance and as such the Company has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data.

4. Definitions

4.1 **General Definitions**:

a. "**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.

b. "**Cross Border Processing**" means processing of personal data which:
   - takes place in more than one Member State; or
   - which substantially affects or is likely to affect data subjects in more than one Member State

c. "**Data controller**" means, the 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

d. "**Data processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

e. "**Data subject**" means an individual who is the subject of personal data

f. "**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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

g. "**Profiling**" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

h. "**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 data protection rules according to the purposes of the processing.

i. "**Third Party**" means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

4.2 **Personal Data**

4.2.1. Information protected under the GDPR is known as "personal data" and is defined as:
"*Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*"

4.2.2. Although, information regarding companies/businesses is not as such personal data, please note that information relating to your contacts within such companies/businesses, e.g. name, title, work email, work phone number, etc. is considered personal data.

4.2.3. In relation to the 'Special categories of Personal Data' the GDPR advises that:
"*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.*"

4.2.4. The Company ensures that a high level of care is afforded to personal data falling within the GDPR's 'special categories' (previously sensitive personal data), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

5. GDPR Principles

5.1 The Company collects and uses personal data for a variety of legitimate business purposes, including establishment and management of customer and supplier relationships, completion of purchase orders, recruitment and management of all aspects of terms and

conditions of employment, communication, fulfilment of legal obligations or requirements, performance of contracts, providing services to customers, etc

5.2 Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be incompatible with the initial purposes ('purpose limitation')
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

5.3 Article 5(2) requires that 'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles' ('accountability') and requires that firms show how they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

6. Legal basis for processing personal data

6.1 Processing of personal data requires a legal basis. The most predominant legal bases for processing personal data within the Company are:

a) Consent from the data subject for one or more specific purposes;
b) The performance of a contract to which the data subject is party
c) A legal obligation or requirement
d) Legitimate interests pursued by the Company

6.2 If the collection, registration and further processing of personal data on customers, suppliers, other business relations and employees are based on such a person's consent to the processing of personal data for one or more specific purposes, the Company shall be able to demonstrate that the data subject has consented to processing of such personal data.

6.3. Consent

6.3.1. Consent shall be:

a) Freely given
b) Specific
c) Informed
d) Unambiguous

The data subject must signify agreement to the processing of personal data by a statement or by a clear affirmative action, to him/her.

6.3.1. A request for consent shall be presented in a manner, which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.

6.3.1. To process special categories of personal data (sensitive personal data) the consent shall also be explicit

6.3.1. The data subject is entitled to withdraw his/her consent at any time and upon such withdrawal, we will stop collecting or processing personal data about that person unless we are obligated or entitled to do so based on another legal basis.

6.4 Necessary for the performance of a contract:

6.4.1 It will be legitimate to collect and process personal data relevant to 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. This applies to all sorts of contracts and agreements, including purchase orders, customer supply contracts, supplier contracts and employment agreements, etc. This also applies to the pre-contractual phase irrespective of the success of the contract negotiation or not.

6.5 Comply with a legal obligation

6.5.1 The Company has to comply with various legal obligations and requirements, which have basis in Union or Member State law. Such legal obligation, to which the Company is subject, may be sufficient as a legitimate basis for processing of personal data.

6.5.2 Such legal obligations include obligations to collect, register and/or make available certain types of information relating to employees, customers, etc. Such legal requirements will then form the legal basis for us to process the personal data, however, it is important to note whether the provisions allowing or requiring the Company to process certain personal data also set out requirements in relation to storage, disclosure and deletion.

6.6 Legitimate interests

6.6.1 Data will only be processed where it is necessary for the purposes of the legitimate interests pursued by the Company, and these interests or fundamental rights are not overridden by the interests of the data subject. The Company will, when deciding to process data ensure that the legitimate interests override the rights and freedoms of the individual and that the processing would not cause unwarranted harm. For instance, it is a legitimate interest of the Company to process personal data on potential customers in order to expand the business and develop new business relations. The data subject must be given information on the specific legitimate interest if processing is based on this provision.

7. Disclosure and transfer of personal data

7.1 Use of data processors

7.1.1 An external data processor is a company, which processes personal data on behalf of the Company and in accordance with the Company's instructions, e.g. in relation to HR systems, third party IT providers, etc. When the Company outsources the processing of personal data to data processors, the Company ensures that said company as a minimum applies the same degree of data protection as the Company. If this cannot be guaranteed, the Company will choose another data processor.

7.2 Data processing agreements

7.2.1 Prior to transfer of personal data to the data processor, the Company shall enter into a written data processing agreement with the data processor. The data processing agreement ensures that the Company controls the processing of personal data, which takes place outside the Company for which the Company is responsible.

7.2.2 With respect to the Company acting as data processor on behalf of other entities, the Company must ensure that any sub-data processor has executed a sub-data processing agreement with the Company, before transferring personal data to such sub-data processor.

7.2.3 If the data processor/sub-data processor is located outside the EU/EEA, please refer to clause 7.3.4 below.

7.3 Disclosure of personal data

7.3.1 Before disclosing personal data to others, please consider whether the recipient is employed by the Company or not. You can share personal data with other employees of the Company, if the Company has a legitimate business purpose in the disclosure.

7.3.2 It is your responsibility to ensure that the recipient has a legitimate purpose for receiving the personal data and to ensure that sharing of personal data is restricted and kept to a minimum.

7.3.3 You must show even more caution before sharing personal data with persons or entities outside of the Company. Personal data shall only be disclosed to third parties acting as individual data controllers if a legitimate purpose for such transfer exists. If the recipient is acting as a data processor, please refer to clause 7.1 above.

7.3.4 If the third-party recipient is located outside the EU/EEA in a country not ensuring an adequate level of data protection, the transfer can only be completed if a transfer agreement has been entered into between the Company and the third party. The transfer agreement shall be based on the EU Standard Contractual Clauses.

8. Rights of the data subjects

Shard Capital Partners LLP
23rd Floor,
20 Fenchurch St,
London, EC3M 3BY

T +44 (0)207 186 9900
F +44 (0)207 186 9979
E info@shardcapital.com
W shardcapital.com

8.1 Duty of information

8.1.1 When the Company collects and registers personal data on data subjects, e.g. employees, job applicants, customers, suppliers, other business partners, etc., the Company is obligated to inform such persons about:

a) The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
b) the categories of personal data concerned;
c) the legitimate interests pursued by the Company, if the processing is based on a balancing of interests;
d) the recipients or categories of recipients of the personal data, if any;
e) where applicable, the fact that the Company intends to transfer personal data to a third country and the legal basis for such transfer;
f) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
g) the existence of the right to request from the Company access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
h) where the processing is based on the data subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
i) the right to lodge a complaint with the Company via the correct procedure or with a supervisory authority;
j) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
k) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

This information will in most cases be provided via a privacy notice on the Company's home page.

8.2 Right to access

8.2.1 Any person whose personal data the Company is being processed, including the Company employees, job applicants, external suppliers, customers, business partners, etc. has the right to request access to the personal data which the Company processes or stores about him/her.

8.2.2 If the Company processes or stores personal data about the data subject, the data subject shall have the right to access the personal data and the reasons for the data to being processed.

8.2.3 The data subject shall have the right to obtain from the Company without undue delay the rectification of inaccurate personal data concerning him or her.

8.2.4 The data subject shall have the right to obtain from the Company the erasure of personal data concerning him or her without undue delay and the Company shall have the obligation to erase personal data without undue delay, unless required by law to retain any information for a prescribed period of time, for example, by tax authorities.

8.2.5 The data subject shall have the right to obtain from the Company restriction of processing, if applicable.

8.2.6 The data subject shall have the right to receive the personal data registered in a structured and commonly used and machine-readable format, if applicable.

8.2.7 The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on a balancing of interests, including profiling.

8.2.8 Any request received from a data subject to exercise the rights in this clause is answered as soon as reasonably possible, and no later than 30 days from receipt. Requests shall be forwarded without delay to the DPO and will be supported by relevant stakeholders to process the request to meet the reply deadline

9. Data Protection by Design and Data Protection by Default

9.1 New products, services, technical solutions, etc. must be developed so that they meet the principles of data protection by design and data protection by default.

9.1.1 Data protection by design means that when designing new products or services due consideration to data protection is taken.

a) the Company will take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

b) the Company shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet data protection requirements and protect the rights of data subjects.

9.1.2 Data protection by default requires that relevant data minimisation techniques are implemented.

a) The Company shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

b) This minimisation requirement applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

c) Such measures shall ensure that by default personal data is not made accessible without careful consideration.

10. Records of processing activities

10.1 The Company shall as data controller maintain records of processing activities under the Company's responsibility. The records shall contain the following information:

a) The name and contact details of the Company;
b) the purposes of the processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;
e) where applicable, transfers of personal data to a third country, including the identification of that third country and, if relevant, the documentation of suitable safeguards;
f) where possible, the envisaged time limits for erasure of the different categories of data;
g) where possible, a general description of the applied technical and organisational security measures.

10.1.1 The Company registers the processing activities in a privacy management tool.

10.1.2 The Company shall make the records available to relevant data protection authorities upon request.

10.2 The Company as data processor

10.2.1 As a data processor, the Company shall maintain records of all categories of processing activities carried out on behalf of a data controller, containing:

a) The name and contact details of the Company and of each controller on behalf of which the Company processes data;
b) the categories of processing carried out on behalf of each controller;
c) if applicable, transfers of personal data to a third country, including the identification of that country and, if relevant, the documentation of suitable safeguard;
d) where possible, a general description of the applied technical and organisational security measures.

the Company registers the processing activities in relation to internal data processing in a data management tool.

11. Deletion of personal data

11.1 Personal data shall be deleted when the Company no longer has a legitimate purpose for the continuous processing or storage of the personal data, or when it is no longer required to store the personal data in accordance with applicable legal requirements.

11.2 Detailed retention periods with respect to various categories of personal data are specified in the Company's retention policy, which can be seen at Appendix 1.

12. Assessment of risk

12.1 If the Company processes personal data that is likely to result in a high risk for the persons whose personal data is being processed, a Data Protection Impact Assessment (DPIA) shall be carried out.

12.1.1 A DPIA imply that the Company will, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with data protection requirements.

12.2 The technical and organisational measures shall be reviewed and updated where necessary and no later than every 6 months.

12.2.1 Adherence to approved codes of conduct or approved certification mechanisms may be used as an element by which to demonstrate compliance with the appropriate technical and organisational measures pursuant to this clause.

12.2.2 The measures referred to in paragraph 1 shall include the implementation of an IT security policy, which shall be complied with at all times.

13. National requirements

13.1 The Company shall comply with both the GDPR and national data protection legislation.

13.2 National legislation may include provisions regarding the processing of personal data which contradict the policies and guidelines on data protection established in the United Kingdom.

13.3 If applicable national legislation requires a higher level of protection for personal data than such policies/guidelines, such stricter requirements are to be complied with. If the Company's policies/guidelines are stricter than the local legislation, our policies/guidelines must be complied with.

14. Contact

14.1 If you have any questions regarding the content of this Policy, please contact the Data Protection Officer at the Company.

Shard Capital Partners LLP
23rd Floor,
20 Fenchurch St,
London, EC3M 3BY

T +44 (0)207 186 9900
F +44 (0)207 186 9979
E info@shardcapital.com
W shardcapital.com

Appendix 1- GDPR Record Retention Schedule

Please refer to individual policy and procedure documents in addition to this schedule. This schedule is applicable to records involving personal information only.

Item	Retention Duration	Detail
Records of Regulated Business		
New client on-boarding records	5 years after termination of the client relationship.	Money Laundering Regulations 2017 & FCA rules
New client account	5 years after termination of the client relationship.	FCA Rules
Client Treasury records	5 years after termination of the client relationship.	FCA Rules
Client & trade reporting	5 years after termination of the client relationship.	FCA Rules
Email campaigns (new, existing and historic clients)	5 years after the campaign	FCA Rules
PA Dealing Records	5 years after approval	FCA Rules
Insider Lists and external (market sounding) insider lists	5 years after termination of the client relationship.	FCA Rules
Bloomberg and internal chat data, e-mails	5 years after termination of the client relationship	FCA Rules
STOR/Near Misses/RO	5 years after submission/investigation closes	FCA Rules
SAR records	5 years after submission/investigation closes	FCA Rules
Recruitment and HR	Please refer to Human Resources Record Retention Policy	