SOLUM FINANCIAL

Data Protection Policy

July 2024

Contents

1 Introduction

1.1 This Policy sets out Solum Financial Limited's ("**the Firm**") policies about Data Protection and the rights of customers, potential customers, and business contacts ("**Data Subjects**") in respect of their Personal Data under the General Data Protection Regulation ("**the Regulation**").

1.2 The Regulation defines "**Personal Data**" as any information relating to an identified or identifiable natural person (a Data Subject); 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.

1.3 The Regulation defines "**Process**" as 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, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.4 This Policy applies to all Personal Data processed by the Company.

1.5 This Policy outlines the procedures that are to be followed when dealing with Personal Data. The principles set out herein must be always followed by the Firm, its employees, and contractors.

1.6 The Firm places high importance on the correct, lawful, and fair handling of all Personal Data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

1.7 The Firm is considered a "**Data Processor**".

2 The Data Protection Principles

2.1 The Regulation sets out the following principles with which any party handling

Personal Data must comply. All Personal Data must be:

2.1.1 processed lawfully, fairly, and in a transparent manner in relation to the Data Subject.

2.1.2 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 not be considered to be incompatible with the initial purposes.

2.1.3 adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.1.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which they are processed, is erased, or rectified without delay.

2.1.5 kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed; and

2.1.6 processed in a manner that ensures appropriate security of the Personal Data.

3 Lawful, Fair, and Transparent Data Processing

3.1 The Regulation states that processing of Personal Data shall be lawful if at least one of the following applies:

3.1.1 the Data Subject has given consent to the processing of his or her Personal Data for one or more specific purposes.

3.1.2 processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract.

3.1.3 processing is necessary for compliance with a legal obligation to which the controller is subject.

3.1.4 processing is necessary to protect the vital interests of the Data Subject or of another natural person.

3.1.5 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.

3.1.6 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 fundamental rights and freedoms of the Data Subject which require protection of Personal Data.

3.2 The Firm does not deceive or mislead people when Personal Data is collected and the Firm only handle's Personal Data in ways that the Data Subject would reasonably expect.

4 Processed for Specified, Explicit and Legitimate Purposes

4.1 The Firm collects and processes the Personal Data set out in Clause 21 of this Policy.

4.2 The Firm only processes Personal Data for the specific purposes set out in Clause 22 of this Policy.

5 Adequate, Relevant and Limited Data Processing

5.1 The Firm will only collect and process Personal Data for and to the extent necessary for the specific purpose(s) informed to Data Subjects as under Clause 4, above.

6 Accuracy of Data and Keeping Data up to Date

6.1 The Firm shall ensure that all Personal Data collected and processed is kept accurate and up to date. The accuracy of data shall be checked when it is collected and or during further contact from the person or Firm thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7 Timely Processing

7.1 The Firm shall only keep Personal Data for as long as necessary to fulfil the purposes we collected it for. When the data is no longer required, all reasonable

steps will be taken to erase it without delay.

8 Secure Processing

8.1 The Firm shall ensure that all Personal Data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of data protection and organisational measures which shall be taken are provided in Clauses 23 and 24 of this Policy.

9 Accountability

9.1 The Firm's Data Protection Officer is Thu-Uyen Nguyen, tu@solum-financial.com.

9.2 The Firm shall maintain written internal records of Personal Data collection, holding, and processing, which shall incorporate the following information:

9.2.1 the name and details of the Firm, its Data Protection Officer.

9.2.2 the purposes for which the Firm processes Personal Data;

9.2.3 details of the categories of Personal Data collected, held, and processed by the Firm and the categories of Data Subject to which that Personal Data relates;

9.2.4 details, or categories, of any third parties that will receive Personal Data from the Firm.

9.2.5 details of how long Personal Data will be retained by the Firm; and

9.2.6 detailed descriptions of all technical and organisational measures taken by the Firm to ensure the security of Personal Data.

10 Privacy Impact Assessments

10.1. The Firm shall carry out Privacy Impact Assessments when and as required under the Regulation or required by the ICO. Data Privacy Impact Assessments shall be overseen by the Firm's Data Protection Officer and shall address the following areas of importance:

10.1.1 the purpose(s) for which Personal Data is being processed and the

processing operations to be carried out on that data.

10.1.2 Details of the legitimate interests being pursued by the Firm.

10.1.3 An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed.

10.1.4 An assessment of the risks posed to individual Data Subjects; and

10.1.5 Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of Personal Data, sufficient to demonstrate compliance with the Regulation.

11 The Rights of Data Subjects

11.1 The Regulation sets out the following rights applicable to Data Subjects:

11.1.1 the right to be informed.

11.1.2 the right of access.

11.1.3 the right to rectification.

11.1.4 the right to erasure (also known as the 'right to be forgotten')

11.1.5 the right to restrict processing.

11.1.6 the right to data portability.

11.1.7 the right to object

11.1.8 rights with respect to automated decision-making and profiling.

12 Keeping Data Subjects Informed

12.1 The Firm shall ensure that the following information is provided to Data Subjects when Personal Data is collected:

12.1.1 Details of the Firm including, but not limited to, the identity of Thu-Uyen Nguyen, the Data Protection Officer and contact details of the Firm.

12.1.2 The purpose(s) for which the Personal Data is being collected and will be processed (as detailed in Clauses 21 and 22 of this Policy) and the legal basis justifying that collection and processing.

12.1.3 Where the Personal Data is not obtained directly from the Data Subject,

the categories of Personal Data collected and processed.

12.1.4 The recipients or categories of recipients of the Personal Data.

12.1.5 Details of the length of time the Personal Data will be held by the Firm (or, where there is no predetermined period, details of how that length of time will be determined).

12.1.6 Details of the Data Subject's rights under the Regulation.

12.1.7 Details of the Data Subject's right to withdraw their consent to the Firm's processing of their Personal Data at any time.

12.1.8 Details of the Data Subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation).

12.1.9 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the Personal Data and details of any consequences of failing to provide it.

12.2 The Information set out above in Clause 12.1 shall be provided to the Data Subject at the following applicable time:

12.2.1 Where the Personal Data is obtained from the Data Subject directly, at the time of collection.

12.2.2 Where the Personal Data is not obtained from the Data Subject directly (i.e., from another party)

12.2.3 If the Personal Data is used to communicate with the Data Subject, at the time of the first communication; or

12.2.4 If the Personal Data is to be disclosed to another party before the Personal Data is disclosed.

13 Data Subject Access

13.1 A Data Subject may make a subject access request ("**SAR**") at any time to find out more about the Personal Data which the Firm holds about them. The Firm is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the Data Subject shall be informed of the need for the extension).

13.2 All subject access requests received must be forwarded to Thu-Uyen Nguyen,

the Firm's Data Protection Officer, tu@solum-financial.com.

13.3 13.3 The Firm does not charge a fee for the handling of normal SARs. The Firm reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a Data Subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14 Rectification of Personal Data

14.1 If a Data Subject informs the Firm that Personal Data held by the Firm is inaccurate or incomplete, requesting that it be rectified, the Personal Data in question shall be rectified, and the Data Subject informed of that rectification, within one month of receipt of the Data Subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the Data Subject shall be informed of the need for the extension).

14.2 In the event that any affected Personal Data has been disclosed to third parties, those parties shall be informed of any rectification of that Personal Data.

15 Erasure of Personal Data

15.1 Data subjects may request that the Firm erases the Personal Data it holds about them in the following circumstances:

15.1.1 It is no longer necessary for the Firm to hold that Personal Data with respect to the purpose for which it was originally collected or processed.

15.1.2 The Data Subject wishes to withdraw their consent to the Firm holding and processing their Personal Data.

15.1.3 The Data Subject objects to the Firm holding and processing their Personal Data (and there is no overriding legitimate interest to allow the Firm to continue doing so) (see Clause 18 of this Policy for further details concerning Data Subjects' rights to object);

15.1.4 The Personal Data has been processed unlawfully.

15.1.5 The Personal Data needs to be erased for the Firm to comply with a particular legal obligation.

15.2 Unless the Firm has reasonable grounds to refuse to erase Personal Data, all requests for erasure shall be complied with, and the Data Subject informed of the erasure, within one month of receipt of the Data Subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the Data Subject shall be informed of the need for the extension).

15.3 In the event that any Personal Data that is to be erased in response to a Data Subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16 Restriction of Personal Data Processing

16.1 Data subjects may request that the Firm ceases processing the Personal Data it holds about them. If a Data Subject makes such a request, the Firm shall retain only the amount of Personal Data pertaining to that Data Subject that is necessary to ensure that no further processing of their Personal Data takes place.

16.2 In the event that any affected Personal Data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17 Data Portability

17.1 The Firm processes Personal Data using automated means. Webforms from the Firm websites, i.e., "Contact Us" section on the Firm's website.

17.2 Where Data Subjects have given their consent to the Firm to process their Personal Data in such a manner or the processing is otherwise required for the performance of a contract between the Firm and the Data Subject, Data Subjects have the legal right under the Regulation to receive a copy of their Personal Data and to use it for other purposes (namely transmitting it to other data controllers, e.g., other organisations).

17.3 To facilitate the right of data portability, the Firm shall make available all applicable Personal Data to Data Subjects in the following format[s]:

17.3.1 HTML, CSV, or Excel, PDF

17.4 All requests for copies of Personal Data shall be complied with within one month of the Data Subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the Data Subject shall be informed of the need for the extension).

18 Objections to Personal Data Processing

18.1 Data subjects have the right to object to the Firm processing their Personal Data based on legitimate interests (including profiling), direct marketing (including profiling).

18.2 Where a Data Subject objects to the Firm processing their Personal Data based on its legitimate interests, the Firm shall cease such processing forthwith, unless it can be demonstrated that the Firm's legitimate grounds for such processing override the Data Subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

18.3 Where a Data Subject objects to the Firm processing their Personal Data for direct marketing purposes, the Firm shall cease such processing forthwith.

19 Automated Decision Making

19.1 The Firm does not conduct any Automated Decision Making.

20 Profiling

20.1 The Firm does not conduct any Profiling.

21 Personal Data

21.1 The following Personal Data may be collected, held, and processed by the Firm:

21.1.1 Personal contact details such as name, title, addresses, telephone numbers, and email addresses

21.1.2 Business Email address

21.1.3 Job Title(s)

21.1.4 Past and Current Employers

21.2 The Firm may collect information in the following ways:

21.2.1 Information received whilst completing a mandate with a client

21.2.2 Firm Website via WebForms

21.2.3 Social Media, including Twitter and LinkedIn

21.2.4 Bloomberg

21.2.5 Recommendations and referrals

21.2.6 CVs

21.2.7 Google or other search engines

22 Lawful Basis for Processing

22.1 All data Processed by the Firm must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information)

22.2 The Firm will never share or sell your data without your consent; unless required to do so by law or to pursue a legitimate interest.

22.3 The Firm will only retain Personal Data for as long as is necessary and for the purpose(s) specified in this notice.

22.4 The purposes and reasons for the Firm processing Personal Data are detailed below:

22.4.1 Required for the completion of a Contract during an engagement.

22.4.2 Direct Marketing where the Firm has a Legitimate Interest.

22.4.3 Engaging in the Firm's Surveys where the Firm has a Legitimate Interest.

23 Data Protection Measures

23.1 The Firm shall ensure that all its employees, contractors, or other parties working on its behalf comply with the following when working with Personal Data:

23.1.1 All emails containing Personal Data must be sent using the Firm email address. The Firm utilises Office 365 which sends emails via TLS/ SSL IPEC and AES.

23.1.2 Where any Personal Data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely using Database removal.

23.1.3 Personal Data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.

23.1.4 Where Personal Data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail, registered to sign for, or another secure, signed for postal service.

23.1.5 All hardcopies of Personal Data, along with electronic copies stored on physical, removable media should be stored in a secure location. The Firm locks the premises overnight to safely secure this information.

23.1.6 No Personal Data may be transferred to any employees, contractors, or other parties, whether such parties are working on behalf of the Firm or not, without the authorisation of Thu-Uyen Nguyen via tu@solum-financial.com;

23.1.7 No Personal Data should be permanently stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Firm or otherwise.

23.1.8 No Personal Data should be transferred to any device personally belonging to an employee and Personal Data may only be transferred to devices belonging to contractors, or other parties working on behalf of the Firm where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation.

23.1.9 All Personal Data stored electronically should be backed up daily with backups stored onsite and offsite.

23.1.10 All electronic copies of Personal Data should be stored securely using passwords.

23.1.11 All passwords used to protect Personal Data should be changed regularly. All passwords must contain a combination of uppercase and lowercase letters and numbers.

24 Organisational Measures

24.1 The Firm shall ensure that the following measures are taken with respect to the collection, holding, and processing of Personal Data:

24.1.1 All employees, contractors, or other parties working on behalf of the Firm shall be made fully aware of both their individual responsibilities and the Firm's responsibilities under the Regulation and under this Policy and shall be provided with a copy of this Policy.

24.1.2 Only employees, contractors, or other parties working on behalf of the Firm that need access to, and use of, Personal Data in order to carry out their assigned duties correctly shall have access to Personal Data held by the Firm;

24.1.3 All employees, contractors, or other parties working on behalf of the Firm handling Personal Data will be appropriately supervised.

24.1.4 Methods of collecting, holding and processing Personal Data shall be regularly evaluated and reviewed, on an annual basis.

24.1.5 All employees, contractors, or other parties working on behalf of the Firm handling Personal Data will be bound to do so in accordance with the principles of the Regulation and this Policy.

25 Transferring Personal Data to a Country Outside the EEA

25.1 The Firm may from time-to-time transfer ('transfer' includes making available remotely) Personal Data to countries outside the EEA.

25.2 The transfer of Personal Data to a country outside of the EEA shall take place only if one or more of the following applies:

25.2.1 The transfer is to a country (or international organisation) which provides appropriate safeguards.

25.2.2 The transfer is made with the informed consent of the relevant Data Subject(s).

25.2.3 The transfer is necessary for the performance of a contract between the Data Subject and the Firm (or for pre-contractual steps taken at the request of the Data Subject).

25.2.4 The transfer is necessary for important public interest reasons.

25.2.5 The transfer is necessary for the conduct of legal claims.

25.2.6 The transfer is necessary to protect the vital interests of the Data Subject or other individuals where the Data Subject is physically or legally unable to give their consent.

26 Data Breach Notification

26.1 All Personal Data breaches must be reported immediately to the Firm's Data Protection Officer.

26.2 If a Personal Data breach occurs and that breach is likely to result in a risk to the rights and freedoms of Data Subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

26.3 In the event that a Personal Data breach is likely to result in a high risk (that is a higher risk than that described under Clause 26.2) to the rights and freedoms of Data Subjects, the Data Protection Officer must ensure that all affected Data Subjects are informed of the breach directly and without undue delay.

26.4 Data breach notifications shall include the following information:

26.4.1 The categories and approximate number of Data Subjects concerned.

26.4.2 The categories and approximate number of Personal Data records concerned.

26.4.3 The name and contact details of the Firm's Data Protection Officer (or other contact point where more information can be obtained).

26.4.4 The likely consequences of the breach.

26.4.5 Details of measures taken, or proposed to be taken, by the Firm to address the breach including, where appropriate, measures to mitigate its possible adverse effects.