Spring GDPR Policy

Effective as of 25th May 2018

Last Revised 26/10/2023

1 Introduction

Spring Operations Ltd is dedicated to respecting the legal rights, privacy and trust of all individuals whomit deals with. We place the highest importance on protecting the privacy rights of our clients and are committed to the continuous development and improvement of our services and internal procedures.

This policy has been introduced in line with EU Regulation 2016/679 General Data Protection Regulation. This policy shall set out the legal obligations of Spring Operations Ltd (registered company number 09610165) whose registered office Sunley House, Bedford Park, Croydon, CR0 2AP.

This policy shall set out the Company's obligations regarding the collection, processing, transfer, storage and disposal of personal data.

2 Definitions

2.1 "GDPR" mean the EU Regulation 2016/679 General Data Protection Regulation.

2.2 "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

2.3 "the Company" means Spring Operations Ltd and any of its trading names or subsidiaries.

2.4 "data controller" means the Company.

3 Key Principles of Data Protection

The GDPR sets out the following principles, with which any establishment handling personal data must comply with which states that all personal data must be;

3.1 Processed in a transparent manner which is lawful and fair to the data subject.

3.2 Collected for a specific, explicit, express and legitimate purpose. It must not be further processed in a manner that is not compatible with these purposes. For the avoidance of doubt, archiving, public interest, scientific or historical or statistical purposes are all deemed as compatible with the initial interest and shall not constitute a breach of this policy.

3.3 Limited to what is necessary for the purpose for which it was collected, relevant, adequate and accurate. Where necessary, this information must also be kept up to date and every reasonable step will be taken to ensure that any inaccurate data is erased or rectified immediately upon notification.

3.4 Kept in a form which permits the identification of a data subject for no longer than is necessary for the purpose for which it was initially or subsequently processed and stored.

3.5 Processed in a way which protects against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using sufficient technical or organisational measures.

3.6 All data will be processed in a manner that ensures the appropriate security or personal data. This includes protection against accidental loss, destruction, damage, unlawful and unauthorised processing.

4. Rights of the Data Subject

The following Parts of the GDPR set out the rights applicable to data subjects;

4.1 Part 12: The right to be informed

4.2 Part 13: The right to access

4.3 Part 14: The right to rectification

4.4 Part 15: The right to erasure

4.5 Part 16: The right to restrict processing

4.6 Part 17: The right to data portability

4.7 Part 18: The right to object

4.8 Part 19 & Part 20: Rights in relation to automated decision-making and profiling

We request that you refer to the aforementioned Parts of the GDPR for further information. However, should you require further clarification on any of the above points, please contact the Data Compliance Officer, whose details can be found in section 10 of this Policy.

5. Lawful, fair and transparent Data Processing.

5.1 The GDPR states that the processing of data shall be lawful if *at least one* of the following applies:

5.1.1 the data subject has given consent for their data to be processed for one or more specific reasons

5.1.2 the processing of data is necessary for the performance of a contract or to take steps at the request of the data subject prior to the commencement of a contract to which the data subject is party.

5.1.3 the processing is necessary in order for the data controller to comply with legal obligations.

5.1.4 processing is essential to protect the interests and rights of the data subject or any other natural persons

5.1.5 processing is necessary for the performance of duties under public interest or in exercise of official authority vested in the data controller.

5.1.6 processing is necessary for the purpose of legitimate interests pursued by the data 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, especially where the data subject in question is a child.

5.2 If the personal data in question is classified as special category data, then at least one of the following conditions must be met:

5.2.1 unless expressly prohibited by EU or EU Member State law, the data subject gives their explicit consent to the processing of such data for one or more specified purposes.

5.2.2 as so far as is authorised by EU or EU Member State law, the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security and social protection law.

5.2.3 the processing is necessary in order to protect the vital interests of the data subject or any other natural person where the data subject is physically or legally incapable of giving their consent.

5.2.4 the processing relates to personal data which is clearly made public by the data subject

5.2.5 the processing is necessary in the course of legal claims or where the courts are acting in their judicial capacity

5.2.6 the processing is necessary for substantial public interest reasons.

5.2.7 the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services pursuant to contract with a health professional, subject to the safeguards under Article 9(3) of the GDPR

5.2.8 the processing is necessary for public interest reasons.

5.2.9 the processing is necessary for archiving purposes in the public interest, scientific or historical or statistical purposes in accordance with Article 89 (1) of the GDPR.

5.2.10 the data controller is a foundation, association or other non-profit body with a philosophical, religious, political or trade-union aim and the processing is carried out in the course of a legitimate, authorised aim which relates solely to the members (former or present), of that body or to persons who have regular contact with it in relation to its purposes and the personal data is not disclosed outside the body without the consent of the data subjects.

6 Specified, explicit and legitimate purposes

6.1 The company collects and processes personal data which includes:

6.1.1 Personal data collected directly from data sources

6.1.2 Personal data obtained by third parties

6.2 The Company only collects, processes and holds personal data for the specific purposes set on in this policy or for other purposes expressly permitted by the GDPR.

6.3 Data subjects are kept informed of the purpose or purposes for which the Company uses their personal data.

7 Adequate, Relevant and Limited Data Processing

The Company will only collect and process personal data to the extent necessary for the specific purpose/s of which the data subject has been, or will be, informed as stated in Part 12 of this policy.

8 Data Accuracy

8.1 The Company will ensure that all personal data which is collected or processed and subsequently held, will be accurate and up-to-date. This also applies to the rectification of personal data at the request of the data subject.

8.2 The accuracy of personal data shall be checked when it is collected and at reasonably practicable intervals thereafter. Upon notification of inaccurate data, the Company will take all necessary steps to amend or erase the data without delay.

9 Data Retention

9.1 The Company will not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

9.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of the data without delay.

9.3 For specific details on retention times, please contact the Data Protection Officer.

10 Secure Processing

The Company shall ensure that all personal data is kept secure and protected against unlawful or unauthorised use and accidental loss, destruction or damage.

11. Accountability

The Data Protection Officer is:

Samar Shaheryar
hello@springmove.com

11.1 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and formonitoring internal compliance with this Policy and with the GDPR and other relevant legislation.

11.2 The Company shall keep internal records of all personal data collection, holding and processing.

12. Data Protection Impact Assessments

The Company shall carry out Data Protection Impact Assessments for all new projects and/or new uses of personal data and which may result in a high risk to the rights and freedoms of a data subject under the GDPR.

12.1 Data Protection Impact Assessments will be overseen by the Data Protection Officer.

12.2 Data Protection Impact Assessments will address the following:

12.2.1 The type of personal data to be collected, held and processed.

12.2.2 The purpose/s for which the personal data is to be used

12.2.3 The objectives of the Company

12.2.4 How the personal data is to be used

12.2.5 The parties who are to be consulted (internal and/or external)

12.2.6 The necessity and proportionality of the data processing with respect to the purpose/s for which it is being processed.

12.2.7 Risk posed to data subjects.

12.2.8 Risks posed both within and to the Company

12.2.9 Proposed measure to minimise and manage identified risks.

13 Keeping Data Subjects Informed

13.1 Where personal data is collected directly from a data subject, those data subjects will be informed of its purpose at the time of collection

13.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose either when first contact is made with the data subject or before the transfer of data is made *or* as soon as is reasonably practicable to do so but not in any event, more than one month after the personal data is obtained.

13.3 Upon communication with the data subject, as detailed in the above 12.1 and 12.2 occurrences, the following information will be provided:

13.3.1 Details of the Company, including but not limited to, the identity of the Data Protection Officer, who manages and oversees all data protection activity.

13.3.2 The purposes for which this information is being collected and the legal basis for justifying that collection and processing.

13.3.3 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed.

13.3.4 Where data is to be transferred to one or more third parties, details of those parties.

13.3.5 Details of the data subjects right to complain to the Information Commissioner's Office

13.3.6 Details of any automated decision-making or profiling that will take place using the personal data

13.3.6 For the avoidance of doubt, we do not transfer any data outside of the European Economic area but should this change in the future, all data subjects will be informed of the

details of this transfer, including the safeguards in place for the protection of the data subjects information.

14 Subject Access Requests

14.1 Data subjects may make a Subject Access Request (SAR) at any time to enquire about personal data which the Company holds on them, what it is doing with that personal data and why.

14.2 Data subjects must make any SAR's in writing using the Company's SAR Form or by other written communication. All SAR's should be addressed to the Data Protection Officer, Samar Shaheryar at hello@springmove.com

14.3 All SAR's will be handed by the Company's Data Protection Officer.

14.4 Data subjects can expect a response to their SAR within one month of receipt, however, in the unlikely event of numerous requests or of the request being especially complex, this response time may be extended to two months, however, all data subjects will be informed in writing if a delay is likely to occur.

14.5 The Company does not charge a fee for the normal handling of SAR requests however, we reserve the right to do so in instances of unusually complex cases or for the repeat request of previously provided information.

15 Restriction of Personal Data Processing

Data subjects may request that the Company ceases processing the personal data it holds about them. In the event of such a request the Company shall retain only the amount of personal data concerning that subject that is necessary to ensure that the personal data in question is not processed any further. In the event that personal data has been disclosed to third parties, they shall too be informed of the applicable restrictions on processing the data in question, unless it is impossible to do so or would require a disproportionate and unreasonable effort.

16 Objections to Personal Data Processing

16.1 Where the data subject objects to the Company processing their data for marketing purposes, the Company shall cease to do so immediately.

16.2 Where a data subject objects to the Company processing their data based on their legitimate interests, the Company will cease to do so unless the processing is necessary for the conduct of legal claims.

17 Amendment of Incorrect Data

17.1 Data subjects have the right to have any incorrect data held on them, corrected.

17.2 The Company shall make any amendments to data within one month of being notified.

17.3 In the event that any of this data has been transferred to a third party, the Company will notify the third party of the necessary amendments within one month of being notified by the data subject.

18 Data Erasure

In the event that:

18.1 It is no longer necessary for the Company to hold the personal data with respects to the original purpose/s for which it was collected or

18.2 The data subject wishes to withdraw their consent to the Company holding and processing their data or

18.3 The data subject objects to the Company holding and processing their personal data (except under the instances previously stated under section 15.2 of this Policy) or

18.4 The personal data has been processed unlawfully or

18.5 A legal obligation of the Company requires that the personal data is erased, then the data subject has the right to request the Company erases the personal data it holds aboutthem.

18.6 If the data has been transferred to a third party, then they too shall be informed if the data subjects request to have this data erased, within one month of the request being received by the Company

18.7 Unless the Company has reasonable and legitimate grounds to refuse an erasure request, then this shall be done within one month of receipt of the request. This may be extended to two months under special circumstances and in the event of this, the data subject will be informed in writing.

19 Data Portability

19.1 Data subjects have the right to request copies of their personal data via an SAR and use it for other purposes.

19.1 To facilitate the right to data portability, the Company shall make the applicable personal data available in both written format and electronically.

19.2 The Company shall favour electronic communication in the first instance, and will only provide written copies upon specific request.

20 Communications and Transferring Personal Data

The Company shall take the following measures with respect to all communications and transfers of data;

20.1 All emails containing personal data will be encrypted.

20.2 All emails containing personal data will be marked “Confidential” in the subject line

20.3 All transfers of personal data will only be made over secure networks

20.4 Personal data transferred internally via hardcopy will be passed directly to the intended recipient

20.5 Personal data transferred externally via hardcopy shall be transferred in a suitable container marked “Confidential” and addressed for the attention of the intended recipient

20.6 Where personal data is to be transferred via facsimile, the intended recipient will be notified beforehand by telephone and requested that they await the specific documents arrival to prevent any interception or loss of the transfer.

21 Data Storage

The Company shall ensure that the following steps are taken with respect to the safe storage of personal data:

21.1 All hardcopies of personal data should be stored securely in locked cabinets or drawers

21.2 All employees are to observe and comply with a "clear desk" policy

21.3 No personal data is to be stored on any mobile device (including but not limited to, mobile phones and laptops) irrespective of whether the device belongs to the Company or not.

21.4 Any transfer of data to a mobile device personally belonging to a contractor, agent or other parties working on behalf of the Company (excluding employees) shall only be done if where the party concerned has agreed to comply fully with this policy and the GDPR. This may require the provision of evidence that they have suitable policies and safeguards in place to be able to do so, upon request.

21.5 Employees are not permitted, under any circumstances, to store personal data on any mobile device, personal or otherwise.

22 Retention Timescales

All data shall be retained for no longer than is legally or reasonably required for the purpose/s of which it was originally collected. For specific details of time scale, please contact the Data Protection Officer.

23 Disposal of Hardcopy Personal Data

All hardcopy data shall be shredded in-house and disposed of securely by an independent, specialised recycling company. The details of whom are available upon written request to the Data Protection Officer.

24 IT Security

24.1 All software will be kept up to date and the Company's Managing Director will be responsible for ensuring that any and all security related updates are installed as soon as is reasonably practicable to do so.

24.2 No software may be installed on any Company device without the prior approval of the IT Department

24.3 All electronic devices owned by the Company will be protected by a high-strength password. All passwords must contain upper case letters, upper case letters and numbers.

25 Internal Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

25.1 Any employees, agents, contractors or other parties working for or on behalf of the Company shall be made fully aware of their individual responsibility to comply with this policy and the GDPR and will be provided with a copy of this Policy.

25.2 Unnecessary access to personal data will not be permitted under any circumstances to employees, agents, contractors or other parties. Access will only be permitted for the purpose of an aforementioned party being able to carry out their lawful and permitted duties as required by the Company.

25.3 All employees, agents, contractors or other parties will be suitably trained in the handling of personal data and will be supervised in doing so by the Data Protection Officer and their Senior Management.

25.4 Personal data shall be reviewed periodically and methods for collecting and processing personal data will be reviewed at regular intervals to ensure compliance and best practice.

25.5 The performance of employees, agents, contractors and other parties shall be regularly reviewed and evaluated.

25.6 All employees, agents, contractors and other parties working on behalf of the Company handling personal data are bound to do so in accordance with this Policy and the principles of the GDPR. For the avoidance of doubt, all agents, contractors and other parties will ensure that all of their employees who are involved in the processing of personal data are held to the same conditions.

25.7 Where any agent, contractor or parties working on behalf of the Company handling personal data fails in their duties to comply with this Policy and the GDPR, they indemnify and hold the Company harmless against any costs, damages, liability, loss, claims or proceedings which may arise out of that failure.

26 Data Breach Notification

All personal data breaches must be reported to the Data Protection Officer immediately.

26.1 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of the data subject, the Data Protection Officer will ensure that the Information Commissioners Office is informed of the breach within 72 hours of becoming aware of it.

26.2 In the unlikely event that a personal data breach is likely to result in high risk to the rights and freedoms of the data subject, the Data Protection Officer will inform all those affected directly and without undue delay.