2 Wellington Place, Leeds, LS1 4AP
info@safeguardingmonitor.co.uk
www.safeguardingmonitor.co.uk
0330 400 4142

Data Protection Policy

1. INTRODUCTION

1.1. You have legal rights with regard to the way your personal data is handled. In the course of our business activities we collect, store and process personal data about our customers, suppliers and other third parties, and therefore in order to comply with the law and to maintain confidence in our business, we acknowledge the importance of correct and lawful treatment of this data. All people working in or with our business are obliged to comply with this policy when processing personal data.

1.2. This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from Data Subjects, for example, customers and business contacts, or that is provided to us by Data Subjects or other sources.

1.3. It also sets out our obligations in relation to data protection under the General Data Protection Regulation ("the Regulation").

1.4. This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data. The procedures and principles set out herein must be followed at all times by us and our employees, agents, contractors, or other parties working on behalf of the Company.

1.5. We aim to ensure the correct, lawful, and fair handling of your personal data and to respect your legal rights.

2. TERMINOLOGY

2.1. Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

2.2. Data Subjects for the purpose of this policy include all living individuals about whom we holds personal data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their personal information.

2.3. Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

2.4. Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

2 Wellington Place, Leeds, LS1 4AP
info@safeguardingmonitor.co.uk
www.safeguardingmonitor.co.uk
0330 400 4142

2.5. Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties. We are the data processor of all personal data provided by our customers.

3. THE COMPANY'S ROLE AS A DATA CONTROLLER

3.1. The Company shall ensure that the following information is provided to every Data Subject when personal data is collected:

a) Details of the Company including, but not limited to, the identity of its Data Protection Officer;

b) The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;

c) Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

d) Where the personal data is not obtained directly from the Data Subject, the categories of personal data collected and processed;

e) Where the personal data is to be transferred to one or more third parties, details of those parties;

f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place;

g) Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined);

h) Details of the Data Subject's rights under the Regulation;

i) Details of the Data Subject's right to withdraw their consent to the Company's processing of their personal data at any time;

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

k) 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;

l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

3.2. The information set out above shall be provided to the Data Subject at the following applicable time:

a) Where the personal data is obtained from the Data Subject directly, at the

2 Wellington Place, Leeds, LS1 4AP
info@safeguardingmonitor.co.uk
www.safeguardingmonitor.co.uk
0330 400 4142

time of collection;

b) Where the personal data is not obtained from the Data Subject directly (i.e. from another party):

c) If the personal data is used to communicate with the Data Subject, at the time of the first communication; or

d) If the personal data is to be disclosed to another party, before the personal data is disclosed; or

e) In any event, not more than one month after the time at which the Company obtains the personal data.

3.3. A Data Subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company 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).

3.4. All subject access requests received must be forwarded to James Inman, the Company's data protection officer. The Company does not charge a fee for the handling of normal SARs. The Company 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.

3.5. If a Data Subject informs the Company that personal data held by the Company 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 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). 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.

3.6. Data Subjects may request that the Company erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;

b) The Data Subject wishes to withdraw their consent to the Company holding and processing their personal data;

c) The Data Subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so);

d) The personal data has been processed unlawfully;

e) The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

2 Wellington Place, Leeds, LS1 4AP
info@safeguardingmonitor.co.uk
www.safeguardingmonitor.co.uk
0330 400 4142

3.7. Unless the Company 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). 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).

3.8. Data Subjects may request that the Company ceases processing the personal data it holds about them. If a Data Subject makes such a request, the Company 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. 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).

4. THE COMPANY'S ROLE AS A DATA PROCESSOR

4.1. The Company processes information on behalf of its customers, including personal detail and special personal data, under the following bases:

a) explicit consent from the Data Controller;

b) a contract between the Company and the Data Controller;

c) 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 Data Controller;

d) processing is necessary for the purposes of the 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, in particular where the Data Subject is a child.

4.2. The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to the Data Controller. It is the responsibility of the Data Controller to make the Data Subjects aware of this data processing.

4.3. The Company, to the fullest extent possible, shall provide the means to ensure that all personal data collected and processed is kept accurate and up-to-date, but this ultimate responsibility will lie with the Data Controller.

4.4. When requested by the Data Controller, the Company will erase any data belonging to the Data Controller held on its systems.

2 Wellington Place, Leeds, LS1 4AP
info@safeguardingmonitor.co.uk
www.safeguardingmonitor.co.uk
0330 400 4142

4.5. If the Company receives a SAR or data portability request from a Data Subject where data is controlled by the Data Controller, this will be forwarded to the Data Controller at the earliest available opportunity.

4.6. Upon receiving a data portability request or SAR from a Data Controller, the Company will respond to this as soon as practicable and in any event within ten working days.

5. DATA PORTABILITY

5.1. Where Data Subjects have given their consent to the Company to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Company 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).

5.2. To facilitate the right of data portability, the Company shall make available all applicable personal data to Data Subjects or Data Controllers in the following format:

a) For scanned information or information which the company does not hold in an editable format, PDF or image file;

b) For written information in which the company holds it in an editable format, as a docx, rtf or pages file;

c) For tabular information in which the company holds it in an editable format, as a xlsx, csv or numbers file;

d) For information retrieved from a database, as a csv or sql file.

5.3. Where technically feasible, if requested by a Data Subject, personal data shall be sent directly to another Data Controller.

5.4. 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).

6. DATA SECURITY

6.1. The Company 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.

6.2. The Company has 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. Further details of these can be provided to Data Subjects and Data Controllers on request.

2 Wellington Place, Leeds, LS1 4AP
info@safeguardingmonitor.co.uk
www.safeguardingmonitor.co.uk
0330 400 4142

7. OBJECTIONS

7.1. Data Subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

7.2. Where a Data Subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company'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.

7.3. Where a Data Subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith.

7.4. Where a Data Subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the Data Subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

8. PRIVACY IMPACT ASSESSMENTS

8.1. The Company shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Company's data protection officer and shall address the following areas of importance:

a) The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;

b) Details of the legitimate interests being pursued by the Company;

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

9. ACCOUNTABILITY

9.1. The Company's data protection officer is James Inman, Managing Director.

10. ORGANISATIONAL MEASURES

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

2 Wellington Place, Leeds, LS1 4AP
info@safeguardingmonitor.co.uk
www.safeguardingmonitor.co.uk
0330 400 4142

10.2. Only employees, agents, sub-contractors, or other parties working on behalf of the Company 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 Company;
10.3. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.
10.4. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised.
10.5. Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
10.6. The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.
10.7. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract.
10.8. All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation.
10.9. Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

11. DATA BREACH NOTIFICATION

11.1. All personal data breaches must be reported immediately to the Company's data protection officer.
11.2. 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.
11.3. 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 Part 27.2) 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.
11.4. Data breach notifications shall include the following information:
a) The categories and approximate number of Data Subjects concerned;

2 Wellington Place, Leeds, LS1 4AP
info@safeguardingmonitor.co.uk
www.safeguardingmonitor.co.uk
0330 400 4142

b) The categories and approximate number of personal data records concerned;
c) The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
d) The likely consequences of the breach;
e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

12. INTERNATIONAL TRANSFERS

12.1. The Company shall only store and transfer personal data in the United Kingdom except where set out in Schedule 1.

13. IMPLEMENTATION

13.1. This Policy shall be deemed effective as of 1st May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

2 Wellington Place, Leeds, LS1 4AP
info@safeguardingmonitor.co.uk
www.safeguardingmonitor.co.uk
0330 400 4142

SCHEDULE 1: INTERNATIONAL TRANSFERS OF DATA

The Company makes every attempt to store and transfer data only in the United Kingdom, and the Company's own servers which store sensitive personal data are all hosted in the United Kingdom.

For operational reasons, the Company uses the following products as data processors, which are hosted in the United States:

Help Scout

Help Scout is our system used to handle support tickets. Help Scout "complies with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries." For more information, see https://www.helpscout.net/company/legal/gdpr/

Box

We use Box as our file storage system, to store contracts, invoices and other files we have been sent by customers. Box "effectuates EU personal data transfers pursuant to our Processor Global Binding Corporate Rules and Controller Global Binding Corporate Rules (BCRs) approved in August 2016 by the European Data Protection Authorities." For more information, see https://cloud.app.box.com/v/BoxBCRsFAQ

G Suite

G Suite is used to handle our calendars and email accounts. Google's states their "certification under the EU-US and Swiss-U.S. Privacy Shield Frameworks includes G Suite and Google Cloud Platform. We have also gained confirmation of compliance from European Data Protection Authorities for our model contract clauses, affirming that our current contractual commitments for G Suite and Google Cloud Platform fully meet the requirements under the Data Protection Directive to legally frame transfers of personal data from the EU to the rest of the world." For more information, see https://cloud.google.com/security/gdpr/