Head Office:
Lyndon House
58 - 62 Hagley Road
Birmingham B16 8PE
t: **0845 2626 260**
f: 0845 2626 269
e: **info@guardiansupport.co.uk**
w: guardiansupport.co.uk

DATA PROTECTION POLICY

Introduction

This Policy sets out the obligations of Bushell Investment Group Business Services Limited, TA Guardian Support, regarding data protection and the rights of data subjects in respect of their personal data and sensitive personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").
Guardian Support is classified as the Data Controller and or Data Processor for information that is supplied to us in the performance of a contract with us or due to an identified legitimate business interest.

What is personal Data?

The GDPR 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, 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.

What is Special Category Data

Sensitive personal data/special categories of data means 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, data concerning health, and individual's sexual orientation and criminal convictions.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data.

The Company is committed not only to the letter of the law, but also to the spirit of the law and 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.

The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- 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.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- 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 it is processed, is erased, or rectified without delay.

- 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.
- 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, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.
- 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.

The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects:

- The right to be informed (this notice)
- The right of access
- The right to rectification
- The right to erasure (also known as the 'right to be forgotten);
- The right to restrict processing
- The right to data portability
- The right to object and
- Rights with respect to automated decision-making and profiling

What Information do we hold and the legal basis for processing such Data?

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject.

Client Data/Authorised Contact Data

We collect the following personal information when contacted about our services as part of the sales process and/or in the performance of our contract with you, therefore we have assessed that there is a legitimate business reason for holding such data:

- Names,
- Address,
- telephone number,
- email address
- and partial date of birth (for security questioning, if required, and to receive a birthday card from Guardian Support). This information is not mandatory.
- Business Banking Information

Client Employee Data

As our core service is the provision of confidential HR, Employment Law and Health and Safety advice, documentation and legal services, as your legal advisors it is necessary for us to hold information regarding

client employees in the performance of our advisory obligations under contract with you and to assist clients in complying with their legal obligations as an employer/controller.
Information held will include:

- Name of employee
- Address of Employee
- Email Address of Employee
- Special Category Data (as outlined above)
- Employment Contractual Data

Supplier information
In order to become an approved supplier, we will hold business data on our approved supplier list.

Such data includes:

- Name
- Address
- Telephone Number
- Email Address
- Details of service

How we use information

Client Data/Authorised Contact Data

In order to enter into a contract with you or to fulfil our contractual obligations your information will be used as follows:

Sales	When contacting about our services details will be held on our sales proformas and within our Sales CRM system in order to obtain a quote for services
Authorised Contact	As a confidential advisory service your details are held on an authorised contacts form within your client account to ensure that only authorised contacts are able to access advice and services, and payments. We will also add you to our birthday list should partial date of birth be provided, although this is not mandatory.
Legal Updates & Marketing	Under your contract you will be provided with electronic legal updates, blogs, special offers via our mailer. As such you will be added to our data base for these purposes. Should you cease to be a client your name and email details will be retained on the mailer as it has been assessed that such information is business information and you will retain a legitimate business interest. However should you

wish to cease receiving such information there is the ability to unsubscribe, which will automatically remove you from any mailing lists.

Client Employee Data

As our core service is the provision of confidential HR, Employment Law and Health and Safety advice, documentation and legal services, as legal advisors it is necessary for us to hold information regarding client employees in the performance of our advisory obligations under contract and to assist clients in complying with their legal obligations as an employer/data controller.

Third Parties
Personal information will only be provided to third parties with explicit consent of our clients i.e booking training with 3rd Party suppliers (via booking forms), arranging Occupational Health Appointments (if applicable), or making business introductions.

Accuracy of Data and Keeping Data Up-to-Date
The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject. The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.
Should you believe such information is not accurate nor up to date you should contact:

Wendy Curlett – Operations Director
Guardian Support
8th Floor, Lyndon House
58-62 Hagley Road
Birmingham
B16 8PE

The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

Erasure of Personal Data
Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

- 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)
- The personal data has been processed unlawfully;
- The personal data needs to be erased in order for the Company to comply with a particular legal obligation**;**

Data Retention
The Company shall not keep personal data for any longer than is necessary, usually at least 6 years in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

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

In relation to electronic mailing, name and email address of authorised contacts will remain on our database indefinitely as it is deemed that there is a legitimate business interest. However, individuals will be able to unsubscribe from these electronic emails by pressing the unsubscribe button, which will automatically remove their data.

Secure Processing
The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

Accountability and Record-Keeping
The Company's Data Protection Officer is Wendy Curlett, Operations Director, Guardian Support, 8th Floor Lyndon House, 58 – 62 Hagley Road, Birmingham, B16 8PE, Telephone Number: 0845 26 26 260.

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;
- The purposes for which the Company collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the Company and
- Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

Data Protection Impact Assessments

The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

- The type(s) of personal data that will be collected, held, and processed;
- The purpose(s) for which personal data is to be used;
- The Company's objectives;
- How personal data is to be used;
- The parties (internal and/or external) who are to be consulted;
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- Risks posed to data subjects;
- Risks posed both within and to the Company; and
- Proposed measures to minimise and handle identified risks.

Data Subject Access

- Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.
- Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection Officer at Guardian Support, Floor 8, Lyndon House, 58 – 62 Hagley Road, Birmingham, B16 8PE.
- Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
- All SARs received shall be handled by 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.

Restriction of Personal Data Processing

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 concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
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).

Data Portability
The Company processes personal data using automated means. For example all authorised contacts registered for our services will have their nominated emails addresses added to our automated mailing list to receive legislative updates via a newsletter, company blogs in addition to any product offers or company updates as deemed appropriate. This is in performance of the contract.

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 right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in electronic format.

Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

Objections to Personal Data Processing
Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling).

Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

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 GDPR, "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.

Automated Decision-Making
The Company does not use personal data in automated decision-making processes.

Profiling
Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning

that person's performance at work, economic situation, health, personal preferences, interest's relatability, behaviour, location or movements.

The Company does not use personal data for profiling purposes

Cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners, who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Our website uses Google Analytics and Google Retargeting in order to compile reports on activity on our website. Google stores this information on servers in the USA and the transfer of such data is governed by the EU-US privacy shield framework. Google may also transfer this information to third parties where required to do so by law. Google will not associate your IP address with any other information held by Google.

By continuing to use our website you consent to our cookies. This privacy policy only applies to this website. Should any blogs and legal updates contain links to other sites or news stories you should read their own specific privacy policy.

Should you wish to reject or block the use of cookies, you can do so at any time, usually by clicking the "help" on your browser. Cookies are specific to individual browser so if you use more than one browser you will need to delete cookies on each. Please be aware that by rejecting cookies it may reduce the functionality of website features.

Data Security - Transferring Personal Data and Communications
The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- All emails containing personal data attachments must have document password protected.
- All emails containing personal data must be marked "confidential";
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
  Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted.
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using recorded delivery or courier (dependant on size) and the envelope or container marked strictly "private and confidential".

Data Security - Storage
The Company shall ensure that the following measures are taken with respect to the storage of personal data.

- All data is stored on our cloud based server via office 365 and some secure third party websites including but not limited to Active Campaigner, Monkey Tree, Worldpay, EKM, One Page and Sales radar.
- All electronic copies of personal data should be stored securely using passwords with system access restricted to relevant people. I.E client employee data is held in their client file, with access only to the consultants. Additionally, internal Guardian Support employee data is held in a secure cabinet and within a secure electronic folder with access restricted to senior management only.
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- No personal data is kept onsite. All data is saved on the cloud and replicated throughout Microsoft 8 data centres around the world which use Azure disk encryption
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of Directors and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
- 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 agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

Data Security - Disposal
When 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 through shredding and or deletion of electronic formats (ensuring that information is still not contained within a deleted box and is permanently wiped).

Data Security - Use of Personal Data
The Company shall ensure that the following measures are taken with respect to the use of personal data:

- No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from a Director of the company as the registered office.
- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the data subject, the client or a Director of Guardian Support.
- Personal data must be handled with care at all times and should not be left unattended or on

view to unauthorised employees, agents, sub-contractors, or other parties at any time;

- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
- Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Individual processor or Marketing Manager to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates not more than 30 days after the updates are made available by the publisher or manufacturer, unless there are valid technical reasons not to do so; and
- No software may be installed on any Company-owned computer or device without the prior approval of the IT Department and or Director.

Organisational Measures

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

- 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 GDPR and under this Policy, and shall be provided with a copy of this Policy;
- 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;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- All personal data held by the Company shall be reviewed periodically, and disposed of or archived in accordance with retention periods;
- 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;
- 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 GDPR and this Policy by contract;
- 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 GDPR; and
- 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.

Transferring Personal Data to a Country Outside the EEA

The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA, should it be deemed necessary in the performance of the contract i.e if the client has an international office.

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

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
- The transfer is made with the informed consent of the relevant data subject(s);
- The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
- The transfer is necessary for important public interest reasons;
- The transfer is necessary for the conduct of legal claims;
- 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; or

- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

Data Breach Notification

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

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.

In the event that a personal data breach is likely to result in a high risk 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.

Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
- The likely consequences of the breach;
- 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.

Implementation of Policy

This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	Brendan Wincott
Position:	Managing Director
Date:	25th May 2018
Due for Review by:	25th May 2019
Signature: