Data Protection Policy

Introduction

Bradley Environmental is fully committed to compliance of the requirements of the General Data Protection Regulations (GDPR) that come into force on 25th May 2018.The main aim of the regulations is to strengthen and unify data protection for individuals.

This aim of this policy is to set out how the company shall comply with the key principles of the GDPR and to ensure that any information about people is collected lawfully and transparently, processed legally, used for legitimate purposes or processed via unambiguous consent mechanisms.

We are required to maintain certain personal data about individuals for the purposes of satisfying our operational and legal obligations. We recognise the importance of correct and lawful treatment of personal data as it helps to maintain confidence in our organisation and to ensure efficient and successful outcomes when using this data.

The types of personal data that we may process include information about current, past and prospective employees; clients and customers; suppliers and other organisations with whom we have dealings.

Personal data may consist of data kept on paper, computer or other electronic media; all of which is protected under the GDPR.

Principles

We endorse and adhere to the principles of the GDPR, which are summarised as follows:

Data must:

- Be collected lawfully and transparently and used for the intended purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and, where necessary, kept up to date.
- Only be kept for as long as is necessary for the purpose for which it was obtained.
- Be processed legally and in accordance with the data subject's rights.
- Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measure.

- Not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- Not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

These principles apply to obtaining, handling, processing, transportation and storage of personal data. Employees and agents of Bradley Environmental who obtain, handle, process, transport and store personal data for us must adhere to these principles at all times.

Types of Data

The GDPR outlines conditions for the processing of any personal data, and makes a distinction between personal data and "sensitive" personal data.

Personal data is defined as data relating to a living individual who can be identified from that data; or from that data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information regarding an individual's racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; or criminal proceedings or convictions.

Handling of Personal/ Sensitive Information

Bradley Environmental will, through appropriate management and the use of strict criteria and controls:

- Observe fully the conditions concerning the fair collection and use of personal information.

- Specify the purpose for which information is used and employees will be informed of this during the induction process.

- Collect and process information only to the extent that it is needed to fulfil operational needs or legal requirements.

- Endeavour always to ensure the quality of information used.

- Not keep information for longer than required, operationally or legally.

- Always endeavour to safeguard personal information by physical and technical means (i.e. keeping paper files and other records or documents containing personal/sensitive data in a secure environment; protecting personal data held on computers and computer systems by the use of secure passwords, which where possible, are changed periodically and ensuring that individual passwords are not easily compromised).

- Ensure that personal information is not transferred abroad without suitable safeguards.

- Ensure that the lawful rights of people about whom the information is held can be fully exercised.

In addition, Bradley Environmental will ensure that:

- There is someone with specific responsibility for data protection in the organisation (the designated Data Controller) – currently Teresa Page, Systems Manager.

- All staff managing and handling personal information understand that they are contractually responsible for following good data protection practice and sign a confidentiality statement as part of their company induction.

- All staff managing and handling personal information are appropriately trained to do so.

- All staff managing and handling personal information are appropriately supervised.

- A clear procedure is in place for anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, and that such enquiries are promptly and courteously dealt with.

- Methods of handling personal information are regularly assessed and evaluated.

- Any data sharing is carried out under a written agreement, setting out the scope and limits of the sharing.

- Any disclosure of personal data will be in compliance with approved procedures.

Note that, by law, Bradley Environmental has to provide employee liability information to any organisation that our employees are transferring to, in line with the Transfer of Undertakings Regulations.

IT Systems/Client data and Accounts data

IT Systems

Igaware Server:

The Igaware Linux Small Business Server is a standalone physical server that is held on site at each of our 4 offices Located in Halesowen, Ossett, St Asaph and Blackpool. Each server is secured within a locked cabinet/room. The main server is also protected by a burglar alarm which is maintained and service yearly.

The Igaware Server is professionally maintained by a reputable IT company (Igaware) and runs a security hardened operating system that is continuously updated automatically. In addition, the server has a built in UTM Firewall that includes firewall, SSL VPN, intrusion prevention, email filtering, web filtering and reporting.

Access to the server interface is restricted via 2-point security comprising of Username and Password entry, details of which are only available to members of the Company I.T Department and Server systems providers (Igaware). Remote access to the server is available to selected assigned members of Igaware support for the purpose of monitoring and maintaining the upkeep of its services and assisting Bradleys I.T Support department with any server related queries.

Server File Shares/folders, LAN and WAN access is restricted to users via I.T department. Users are assigned to only the files, folders and documents relevant to their role and do not have direct access to the server itself. User access can only be amended via a member of the I.T department upon written request from said users Manager or one of the Directors.

All users have access to individual work email account as well as access to any joint email accounts required for their role. All email access is assigned to users via the I.T department via request of the users, manager or a Director and restricted with username and password access. Both Usernames and passwords are created and assigned by a member of the I.T department and only made available to said individual, members of I.T support and (if requested) Bradley Environmental Consultants Directors.

Client/company data is encrypted and backed up on a daily basis for each office, with multiple copies being securely stored both on and off site.

More details of Igaware Server Security can be accessed via the following link: www.igaware.com/products/utm-firewall/

User (Local) Desktops/Laptops/Tablets:

Local machine user profiles are assigned via a member of the I.T Department and accessible with individual 2 - point security comprised of specific username and password combination. (Pre-determined and issued via I.T Department).

All Laptops/desktops run Kaspersky Endpoint Security10 anti-virus software, which is installed and updated by the I.T Department.

Maintenance on devices is undertaken as per our maintenance schedule ensuring that all systems are running to optimum efficiency and any security/software updates are installed in order to help neutralise security breaches and prevent instability.

Desktops/Laptops/Tablets can only access data via a secure connection to the corresponding offices server with file/share access being issued and restricted via a member of the I.T department at the request of the individual's manager or Director.

All user access to server data can be instantly revoked by a member of the I.T department via the Server interface thus preventing said user from accessing any shared data.

TEAMS (Server):

Internal use of the TEAMS Server is for recording and storing all information related to the completion of the following client requested services: Asbestos Consultancy, Safety and Environmental Consultancy and the provision of specific Training services.

The TEAMS Server is located within the Halesowen Office and operates on a Windows server 2008 r2 operating system with system/security updates being installed and managed remotely via the server supplier (Mark One Consultants)

The TEAMS server is located within our internal LAN, which is in turn managed and protected by our Igaware Server. (Details given above)

Data held on the TEAMS server is backed up nightly to the server itself and remotely to a mirrored TEAMS server located at Mark One Consultants data centre.

Mobile TEAMS:

Mobile TEAMS is a data collection package used for capturing and transferring survey/analytical data to various structures at the request of the client. Mobile TEAMS is installed onto Windows/Android tablets and held by surveyors and analysts for the purpose of recording data relevant to works requested by the client.

Upon completion data is remotely transferred back to the TEAMS Server so that it can be compiled, edited (if needed) and included within the final completed report before making available to the client.

Each tablet is given a unique PIN number so entry into the TEAMS software.

TEAMS Portal:

TEAMS allows the client unlimited secure access to our asbestos management web portal. Access to the portal is restricted via an individual username and password combination which will allow the user access to only information predetermined by the lead client contact for that particular business.

Furthermore, the system provides full traceability of all users for auditing purposes.

Usernames and passwords are created and added to the TEAMS server by a member of the I.T department upon written request from the lead client contact for a company.

Privileges can also be restricted for each user allowing them access to only certain types of information or specific projects; once again this is allocated by a member of our I.T department.

Once a user is added to the system login details are sent separately via email to the individual.

Website Portals (Asbestos and Environmental, Health and Safety Compliance):

Our Upload Portals are accessed through our Company website and allows clients access to reports carried out by Bradley Environmental Consultants at their request. Both portals contain SSL certificate Encryption to help better Secure any data being entered and uploaded to the server)

Client Access to the Upload Portal is comprised of individual Usernames and passwords which are created and added to the Upload Portal by a member of the I.T department upon written request from the lead client contact for a company. Upon creation login details are emailed to the user.

Client details stored on the Portal consist of first name, last name and email address of users along with client addresses.

The web portal is managed and maintained by the company Spiderscope.

Please see below for details of Spiderscope's Privacy Policy:
https://www.spiderscope.com/info/privacy-policy.asp

Sage 50 Accounts:

Sage 50 accounts is installed on accounts staff local desktops by a member of the I.T department and at the request of a Director or Accounts Manager.

Users connect to a Shared Sage datafile which is held on a secure Igaware Server share and only accessible by users specifically added to the computers user group. Sage User accounts are also restricted with individual usernames and passwords issued via the IT department. The addition of new users is restricted to members of the I.T Department.

Sage account login details are only available to the Accounts Manager, Directors and I.T Department.

As part of the Igaware server backup policies all sage data is backed up to encrypted external hard disks nightly in a 3 disk rotation. (1 disk locked in server room, 1 disk locked in safe, 1 disk secured remotely off site).

Pure360:

Pure360 is a web based email marketing and SMS software system used to access customers via mobile and web devices for the purpose of carrying out Marketing solutions. Access to the company profile is gained by way of specific username and password security verification created upon the initial activation of the account. Current access is restricted to members of the Marketing and I.T Department.

Details of Pure360 Privacy Policy can be accessed via the following link: https://www.pure360.com/privacy/

mypayroll.cloud (Online Payroll document access):

All staff have access to an online @mypayroll.cloud account which allows them to access any payroll related documentation held for them. Access is provided via individual username and password and restricted to members of the HR Department and the individual to whom the account is assigned.

Access to the mypayroll.cloud system is initially set up by our accountancy company Chartwells. Details of Chartwells Privacy policy can be found at the following link: http://www.chartwells.org.uk/images/Privacy_Statement.pdf

reallysimplesystems.com (CRM System)

Bradley Environmental utilises the CRM system Really Simple Systems for the purpose of tracking and recording Leads/Opportunities for our Sales and Marketing department. Access to the system is initially set up and Managed by the Business Development & Bid Manager who can assign, edit and

remove access and permissions to other members of the Sales and Marketing department if required.

Details of Really Simple Systems Privacy policy can be found at the following link: https://www.reallysimplesystems.com/privacy-policy/

Client Data

Any Client related data held within the TEAMS Server, Igaware servers and its related shares, folders etc is held for the purpose of undertaking services requested via our clients and in line with policy and procedures outlined by the company and other accredited bodies.

Data held on these systems includes:

Customer/Client (held on Igaware and TEAMS server):
Company Name, Address, email, telephone, Property Construction Type, Construction date, Property address, previous/current Survey data, sematic drawings, details of planned works i.e refurbishment/demolition, analytical data, any other additional documentation/comments provided by the client.

Suppliers (Held on Sage System/Igaware Server):

Name, address, telephone, email, sort code, bank account number (no credit card details held)

Company/Staff (Held on Igaware Server):
Name, address, telephone, email, DOB, National Insurance No, Contractual info, P45/46, Training records, Certificates, CV's, Job Application forms,

Client Data Requests (Reports)

Our preferred methods of delivery of reports to our clients is either via our secure upload portal located on our website or via our TEAMS portal which is located on our TEAMS server.

Website Upload system:

Individual clients have access via password to their own part of our website and we deposit files there for our clients to collect; an email alert is sent to the client that a report is there for collection.

To ensure client security, the system is "read only" to ensure reports cannot be altered. Clients can copy reports and files from the download system to their system and if required forward on to other interested parties who may be involved in particular projects.

TEAMS Portal:

TEAMS is hosted on a dedicated secure server located at our Head office and can be accessed securely from any location. The system allows unlimited users to be added with varying levels of access, ranging from read only to full administrator access.

Access to the portal is restricted via an individual username and password combination which will allow the user access to only information predetermined by the lead client contact for that particular business.

Physical PDF copies of reports are only supplied upon request and only to the client that ordered them; any third party request for a report is passed to the client for approval.

Original copies of reports remain stored within our TEAMS server.

Data Destruction

Hardware:

At the end of life computer hardware is professionally disposed of with guaranteed destruction of hard drives. Upon destruction accompanying certification (WEEE, inventory of hardware destruction etc) are stored securely on the network with access being restricted to members of the I.T Department.

Paperwork:

Any paper records we keep are scanned before shredding.

Sage 50 Accounts System:

Data can be deleted from Sage via Accounts Manager, HR Department or Finance Director. Corresponding Backup files can be deleted from the server by a member of the I.T department at the request of the Accounts Manager, HR Department or Director.

TEAMS System (Inc. TEAMS Portal):

Data can be deleted by Mark One Consultants or individuals with Administrative access to the TEAMS system. (Administrative access and other system access is assigned by member of IT Department).

Website Upload system:

Data can be removed from the Upload system by a member of the I.T Department at the request of the client or Director. Copies of reports are stored also within the Igaware server and can be re-uploaded if required.

Data is automatically removed from the system after a 3-month period unless a client has requested permanent storage.

Igaware Server:

Client data held on the Igaware Server can only be edited/deleted by a member of staff who has been given sufficient privileges to do so. Privileges are based on a user's job role and assigned by the I.T department upon request from the individual's manager or a Director of the Company.

Members of the I.T department and Server Maintenance providers (Igaware) are the only individuals who have access to assign user access privileges as well as adding, editing or removing users on the Igaware Server.

Marketing

For all of our "business to business" marketing activities we will ensure clients must have a legitimate interest in receiving our marketing contact or they must have given consent to receive our marketing. This information will be recorded for future reference.

The company may make live calls to any business number that is not registered on the TPS or the CTPS, but will only do so if the business hasn't objected to calls in the past. The company will ensure the number is displayed and will create a do not call list.

The company will also:

- Ensure there is a clear way to unsubscribe from emails for clients.
- Will ensure that "business to consumers" marketing activities are to consumers who have specifically opted in to receive email marketing (this includes sole traders).
- Clients can ask to remove all information that we hold for them under the 'right to be ignored'. If this is requested all information on the client will be deleted from all platforms.
- Keep records of consent from those that have opted in or showed legitimate interest and information on date of call or sign up and whether clients are interested in our services and specific interest.
- When sending electronic marketing messages, the company shall tell the recipient who they are and provide a valid contact address.

The company displays a privacy policy on the website so that customers know how their information is being used:

Data

- All data held by the marketing department on clients to be kept in secure folders with restricted access.
- Marketing lists will be updated every 6 months.

Access to Personal Data

All individuals who are the subject of personal data held by us are entitled to:

- Ask what information we hold about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Have inaccurate personal data corrected or removed.
- Prevent us from processing information or request that it is stopped if the processing of such data is likely to cause substantial, unwarranted damage or distress to the individual or anyone else.
- Require us to ensure that no decision which significantly affects an individual is solely based on an automated process for the purposes of evaluating matters relating to him/her, such as conduct or performance.
- Be informed what we are doing to comply with our obligations under the Data Protection Act.

This right is subject to certain exemptions which are set out in the GDPR. Any person who wishes to exercise this right should make a request in writing to Kim Racey, HR Manager.

We reserve the right to charge the maximum fee payable for each subject access request. If personal details are inaccurate, they will be amended upon request. If by providing this information we would have to disclose information relating to or identifying a third party, we will only do so provided the third party gives consent, otherwise we may edit the data to remove the identity of the third party.

Personal information will only be released to the individual to whom it relates. The disclosure of such information to anyone else without their consent may be a criminal offence. Any employee who is in doubt regarding a subject access request should check with Kim Racey, HR Manager.

We aim to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month of receipt of a written request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

Employee Responsibilities

All employees must ensure that, in carrying out their duties, Bradley Environmental is able to comply with its obligations under the act. In addition, each employee is responsible for:

- Checking that any personal data that he/she provides to us is accurate and up to date.

- Informing us of any changes to information previously provided, eg change of address.

- Checking any information that we may send out from time to time, giving details of information that is being kept and processed.

- If, as part of their responsibilities, employees collect information about other people or about other employees they must comply with this policy. This includes ensuring the information is processed in accordance with the GDPR, is only processed for the purposes for which it is held, is kept secure, and is not kept any longer than is necessary.

- Employees are reminded that the GDPR does not just apply to records held relating to our employees, but also to any client files/records. Information stored on clients should be reviewed regularly to ensure it is accurate and up to date. All documents, whether hand written or stored in emails (current or deleted) are potentially disclosable in the event of a request from an employee or client.

Data Security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

All staff are responsible for ensuring that any personal data which they hold is kept securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

HR Information

We collect, store and process your personal information both to set up and manage the employment contract with you (article 6 (1)(b) of the GDPR) and to ensure that we carry out or obligations under employment law.

Bradley Environmental shall be entitled to retain and process all relevant information and any necessary personal data relating to employees and transmit such data to appropriate third parties in accordance with provisions and principles of the GDPR for the purposes of administering employment terms and conditions and benefits.

All HR information will be stored securely with restricted access. Where the company has a legitimate reason to share information with a third party their GDPR compliance will be checked before information is shared. Employees will be informed of records held at induction.

Retention and Disposal of Data

Information will be kept in line with our document retention guidelines. All employees are responsible for ensuring that information is not kept for longer than necessary. Documents containing any personal information will be disposed of securely, and paper copies will be shredded.

Registration

Bradley Environmental is registered in the Information Commissioner's public register of data controllers.

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

Teresa Page, Systems Manager is our Data Controller and is responsible for ensuring compliance with the Data Protection Act, for notifying and updating the Information Commissioner of our processing of personal data, and for the monitoring and implementation of this policy on behalf of Bradley Environmental.

Kim Racey, HR Manager has overall responsibility for implementing and monitoring this policy, which will be reviewed on a regular basis following its implementation (at least annually) and additionally whenever there are relevant changes in legislation or to our working practices.

This policy is not contractual but indicates how Bradley Environmental intends to meet its legal responsibilities for data protection. Any breach will be taken seriously and may result in formal disciplinary action. Any employee who considers that the policy has been breached in any way should raise the matter with his/her manager or Kim Racey, HR Manager.