What this Policy covers

Everyone has rights with regard to how their personal information is handled. During the course of our business activities, it is necessary for us to collect, store and process personal information about our staff, customers, suppliers and other third parties. The correct and lawful treatment of this data is an essential part of maintaining trustworthy business relationships and be an attractive employer, and, ultimately, provide for successful business operations.

This policy details individual rights and obligations in relation to information about current, past and prospective suppliers, clients and employees as well as other third parties we hold relationships with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Legislation.

This policy does not form part of any employee's contract of employment and may be amended at any time.

Definition of the terms

- **"Data"** is information which is held electronically, or in certain paper-based filing systems.
- **"Data subject"** is any person whose personal data is being collected, held or processed.
- "**Data controllers"** are the people or organisations that determine the purpose(s) for which, and the manner in which, any personal data is processed.
- **"Data processors"** include any person or organisation that processes personal data on the instruction of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.
- **"Data users"** are all individuals, including employees, whose work involves processing personal data.
- **"Personal data"** is any information that relates to a living individual who can be identified from that information.
- **"Processing"** is any use that is made of personal data, including collecting, storing, amending, disclosing or destroying it.
- **"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or political beliefs, trade union membership, health, sex life or sexual orientation and biometric data.
- **"Criminal records data"** means information about an individual's criminal convictions and offences and information relating to criminal allegations and proceedings.

Anybody with access to the personal, special categories or criminal records data of employees or of third parties must comply with this Policy.

Data protection principles

The Company processes personal data in accordance with the following data protection principles:

- the Company processes personal data lawfully, fairly and in a transparent manner;
- the Company collects personal data only for specified, explicit and legitimate purposes;
- the Company processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of the processing;
- the Company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;
- the Company retains personal data only for the period necessary for the processing;

- the Company adopts appropriate measures to make sure that personal data is secure and is protected against unauthorised or unlawful processing and from accidental loss, destruction or damage.

Data processing

Where we collect personal data directly from data subjects, we will inform them about the purpose(s) for which we intend to process the personal data.

If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter, but always within one month of having collected the personal data.

Data processing basis

The company process data only on the grounds permitted in data protection legislation;

- we have the data subject's consent, or
- that the processing is necessary for:
    - the performance of a contract with the data subject;
    - for the compliance with a legal obligation; or
    - for the legitimate interest of the data controller or another party to whom the data is disclosed (in those instances the data subject will be advised both of the interest and the details of data shared). In cases, the type of data disclosed under this reason may seriously impact on the interests or fundamental rights of data subjects, it will not be shared.
- any other lawful basis for processing, as defined in GDPR.

Sensitive personal data

The Company will process special categories and criminal records data primarily where it is necessary to enable the Company to meet its legal obligations and in particular to ensure adherence to health and safety legislation or for equal opportunities monitoring purposes.

If the company intends to process sensitive personal data, further details will be issued.

Transfers to third parties

If at any time during delivery of contract, the company chooses to appoint a sub-contractor, it ensures that they are able to fulfil their data protection responsibilities to the same or higher standard than the terms outlined in this policy.

The sub-contractor's right to process personal data terminates automatically, for whatever reason, on expiry or termination of this Agreement or the sub-contract, whichever is earlier.

We do not disclose personal data to a third party (including a sub-contractor) in any circumstances unless:

- it is necessary to provide the service or
- we have the Client's prior written consent.

For third party requests, the Company shall use reasonable endeavours to advise the Client in advance of such disclosure, unless it is prohibited by law or regulation from notifying the Client of that disclosure, in which case it shall do so as soon as practicable thereafter (where permitted by law or regulation).

Transfer of Personal Data to a Restricted Country

We shall not make (nor instruct or permit a third party to make) a data transfer unless European Commission recognised that the legal framework in place in that country, territory, sector or international organisation provides adequate protection for individuals' rights and freedoms for their personal data.

Data Retention Policy

We shall not retain Personal Data for longer than is necessary to perform the contract, fulfil a legal obligation, or protect other legitimate companies' interests;

Data subject rights

Data protection legislation prescribes the way in which the Company may collect, retain and handle personal data. It outlines that each data subject has the following rights:

- The right to access and be informed about data held by a data controller
- The right to have inaccurate data amended
- In some instances, the right to erasure, restrict processing and to object the processing of their personal data
- Rights in relation to automated decision making and profiling

The Company will comply with the requirements of data protection legislation and all employees, contractors and other third parties who handle personal data in the course of their work must also comply with it.

Subject access requests

Data subjects have the right to make a subject access request. It has to be done formally, including what information is being requested and addressed to the Company's nominated data officer.

Any requests sent to an employee will be immediately forwarded to the nominated data officer.

There is no fee for the information request, however, in cases where a request is unfounded or excessive (including repetitive requests), then a reasonable fee (based on the administrative cost) may be charged.

The company will respond to a request within one month from the date we receive it. In some cases, such as where the Company processes large amounts of the individual's data, response time may be extended to three months of the date the request is received. In that instance, the individual will be informed about the extension within one month of receiving the original request.

The company may refuse to provide certain personal data in response to a request from an individual where the relevant legislation provides an exemption. There are very few exemptions for non-disclosure and the application of these exemptions require careful consideration.

Data security

We will process the personal data we hold in accordance with the objectives of the Information Security Policy.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures or policies, or if they put in place adequate measures which are the same or higher standard.

The company employs the following security procedures:

- Entry controls. Any stranger seen on Walter Lilly premises should be challenged.
- Secure storage. All physical documents containing personal data are kept in lockable storage.
- Methods of disposal. Paper documents are disposed of in the confidential waste bins. Digital storage devices should be appropriately wiped when they are no longer required.
- Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock their computer when it is left unattended

Data processor responsibilities

Each employee is responsible for helping the Company keep your personal data accurate and up to date. This includes their own personal data provided to the Company as well as the information processed on behalf of the business.

An employee who has access to the personal data of other individuals, our clients in the course of their employment, contract, internship or apprenticeship is classed as a data processor and is relied on to help the company to meet its data protection obligations.

Any data processor is required to maintain data security by protecting the confidentiality, integrity and access of personal data, defined as follows:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access including password protection, and secure file storage and destruction);
- not to remove personal data or devices containing or that can be used to access personal data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failure to observe these requirements may amount to a disciplinary offence which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee, customer or client data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to your dismissal or contract termination without notice.

Accuracy of personal data

The Company will review personal data regularly to ensure that it is accurate, relevant and up to date.

To ensure the Company's files are accurate and up to date, and so that the Company is able to contact you or, in the case of an emergency, another designated person, you must notify the Company as soon as possible of any change in your personal details (e.g., change of name, address, telephone number, loss of driving licence where relevant, next of kin details, etc).

Security of personal data

The Company will ensure that personal data is not processed unlawfully, lost or damaged. If you have access to personal data during the course of your employment, you must also comply with this obligation. If you believe you have lost any personal data in the course of your work, you must report it to your manager immediately. Failure to do so may result in disciplinary action up to and including dismissal without notice.

Data breaches

The Company will record all data breaches regardless of its effect.

A breach of personal data that poses a risk to the rights and freedoms of individuals, will be reported it to the Information Commissioner within 72 hours of discovery.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, affected individuals will be informed about a breach, its likely consequences and the mitigation measures which have been taken.

Complaints

If you have concerns about an organisation's information rights practices, contact Commercial Director Duncan Beach who is acting as a Data Protection Officer:

By email: duncan.beach@walterlilly.co.uk
By telephone: 020 8730 6238

If you feel that your concerns are not recognised or dealt in an inappropriate manner, the Information Commissioner's Office website is there for further support and advice.

FURTHER INFORMATION:

- IT Security Policy
- Retention Policy
- Employee Handbook

C. Butler

Chris Butler | Managing Director