DATA PROTECTION POLICY

Introduction

Consort Limited is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

We hold personal data about our employees, customers, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Controller is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are followed.

Data Controller: Mr Steven Williams - Finance Director, Consort Limited
Address: Consort Limited, Units 1 - 4 Export Drive, Huthwaite, Sutton in Ashfield, Notts, NG17 6AF.
Tel No: 01623 440880 **Email**: swilliams@consortwindows.com.

1. BUSINESS PURPOSES

The purposes for which personal data may be used by the company:

Personnel, recruitment, administrative, financial, regulatory, payroll, legal and business development purposes.

Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice.

- Operational reasons, such as setting up of commercially sensitive customer and supplier information, maintaining accurate records of current and historical sales/purchase transactions, ensuring the confidentiality of security vetting and financial viability assessments, credit scoring, credit references and checking.

- Marketing the business.

- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or access requests.

- Investigating complaints, including security of information gathered from or passed to third parties.

- Ensuring business policies are adhered to such as company procedures, practices, policies covering email, fax and internet use.

- Requesting or giving of references, ensuring safe working practices, monitoring and managing staff, use of systems and facilities, monitoring staff absences, administration, reviews and performance assessments.

- Monitoring staff conduct, disciplinary matters.

- Initiatives to improve services and efficiency.

Personal Data

'Personal data' means any information relating to an identified or identifiable person - the 'data subject'.

An identifiable person is one who can be identified, directly or indirectly, by reference to information such as a name, identification number, location data, a system identifier or one or more factors specific to the person - physical, genetic, mental, economic, cultural or social identity.

Personal data we gather or hold may include: individuals' phone number, email address, educational background, financial and pay details, medical data, family contacts, details of certificates and diplomas, education and skills, marital status, nationality, job title and/or CV/application form.

Customer data we hold could include: personal and business names, directorships, addresses, contact details - landline, mobile and fax numbers, email addresses, sales data and purchase history, credit checking and referencing information.

Special Categories of Personal Data

Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences or related proceedings, and genetic and biometric information. Any use of special categories of personal data should be strictly controlled in accordance with this policy.

Data Controller

'Data Controller' means the person, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor

'Processor' means a person who processes personal data on behalf of the 'Data Controller'.

Processing

'Processing' means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation on, use, disclosure by transmission, making available to others if necessary, erasure or destruction.

Supervisory Authority

This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office.

Scope

This policy applies to all staff, who should be familiar with this policy and comply with its terms.

This policy supplements any other policies relating to data protection, including I.T related policies. We may add to or amend this policy by additional rules and guidelines from time to time. Any new or modified policy will be circulated to staff.

Who is Responsible for this Policy?

Our Data Controller, Mr Steven Williams, has overall responsibility for the day-to-day implementation of this policy. Employees should contact the Data Controller if they have any questions about this policy.

2. THE PRINCIPLES

Consort Limited shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. The Principles are:

1. Lawful, Fair and Transparent

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. Limited for its Purpose

Data can only be collected for a specific purpose.

3. Data Minimisation

Any data collected must be necessary and not excessive for its purpose.

4. Accurate

The data we hold must be accurate and kept up to date.

5. Retention

We will not store data longer than necessary.

6. Integrity and Confidentiality

The data we hold must be kept safe and secure.

3. ACCOUNTABILITY AND TRANSPARENCY

We will ensure accountability and transparency in all our use of personal data and Consort Limited will ensure all data processing activities comply with each of the Principles.

To comply with data protection laws and the accountability and transparency principles of GDPR, Consort Limited must demonstrate compliance. Each department is responsible for understanding their particular responsibilities to ensure we meet the following data protection obligations under GDPR:

- Fully implement appropriate measures to ensure we maintain up to date and relevant documentation on all processing activities
- Conduct Data Protection Impact Assessments
- Implement measures to ensure privacy, including:
- Data minimisation - only gather the information necessary for processing requirements
- Subject identification - anonymising information where possible
- Transparency
- Creating and reviewing security and privacy procedures on an ongoing basis

4. OUR PROCEDURES

Fair and Lawful Processing

We will process personal data fairly and lawfully in accordance with individuals' rights under the first principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this.

If we cannot apply a lawful basis (explained below) or our processing does not conform to the first principle, it may be unlawful. Data subjects have the right to have any data unlawfully processed erased.

Controlling and Processing Data

Consort Limited is classified as a Data Controller and Data Processor. We must maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully controlling and/or processing data.

As a Data Processor, we must comply with our contractual obligations and act only on the remit we need to use the data. We must:

- Not use a sub-processor without authorisation from the Data Controller. A sub-processor is an individual or organisation to which we may need to pass information.
- Co-operate fully with the ICO or other supervisory authority.
- Ensure security of the processing.
- Keep accurate records of processing activities.
- Notify the controller of any personal data breaches.
- Ensure all personal data is kept safe and secure and only viewed/shared for a specific, lawful reason.

If you are in any doubt about how we will handle data, contact the Data Controller for clarification.

Lawful Basis for Processing Data

We must establish a lawful basis for processing data which must be approved by the Data Controller. All actions taken on data must comply with the established, lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. **Consent**

We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose and we obtain updated consent where it is necessary to do so.

2. **Contract**

The processing is necessary to fulfil our obligations to the individual or business.

3. **Legal obligation**

We have a legal obligation to process the data (excluding a contract, which is mutually agreed).

4. **Vital interests**

Processing or passing on the data is necessary to protect a person's life or in a medical situation.

5. **Legitimate Interest**

The processing is necessary for the company's legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Deciding which Condition to Rely On

When making an assessment of the lawful basis, we will need to establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. We should not rely on a lawful basis if we can reasonable achieve the same purpose by some other means.

More than one basis may apply. We will apply what will best fit the purpose, not what is easiest.

Consort Limited will consider the following factors:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- Is the lawful basis relied on what the data subject would accept or expect?
- What is the impact of the processing on the individual?
- Are they likely to object to the processing?
- Are we able to stop the processing at any time on request?

Our commitment to the first Principle requires us to demonstrate that we have considered which lawful basis best applies to each processing purpose.

We must also ensure that individuals whose data is being processed by us are informed of the basis and intended purpose for processing their data. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

Whoever is responsible for implementing the privacy notice for the processing activity must be approved by the Data Controller.

5. SPECIAL CATEGORIES OF PERSONAL DATA

This means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Health
- Sexual orientation

In most cases where we process special categories of personal data, we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed, and to whom it will be disclosed.

The conditions for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data, that processing activity must cease.

6. RESPONSIBILITIES

Our Responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are followed
- Implement and review procedures to detect, report and investigate any data breaches
- Store data in a safe and secure way to ensure confidentiality
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

Data Processor Responsibilities

- Fully understand your data protection obligations
- Ensure that any data processing activities comply with company policy and are justified
- Data is not used in an unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause Consort Limited to breach data protection laws through the actions of others
- Raise any concerns, notify any breaches or errors and report anything suspicious or potentially illegal to the Data Controller

Responsibilities of the Data Controller

- Keeping everyone updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Ensure staff are aware of their data protection obligations
- Answering questions on data protection from staff, customers and other stake holders
- Responding to individuals such as customers and employees who wish to know what data is being held on them by the company
- Checking with third parties that handle the company's data that data protection procedures are in place and comply with Consort Limited's legal obligations

Responsibilities of the IT Department

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Ensuring third-party services, such as cloud services, legally comply with the principles for storage and processing of personal data

Responsibilities of the Sales/Marketing Department

- Working with the Data Controller to ensure content of data protection statements attached to any sales and marketing copy or website meet legal obligations
- Along with the Data Controller, addressing data protection queries from customers or other parties with which they may have contact
- Coordinating with the Data Controller to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

Accuracy and relevance

Consort Limited will ensure, as far as its extent that any personal data processed is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect the company to do this.

Individuals may ask that we correct inaccurate personal data relating to them. The Data Controller must be informed before any corrections have been made.

Data security

Personal data must be kept secure against loss, misuse, or inadvertent viewing. Where other organisations process personal data as a service on the company's behalf, the Data Controller will establish if any additional or specific data security arrangements need to be implemented with those third party organisations.

Storing Data Securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot view or access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be password protected
- Data stored on external devices should be password protected and locked away securely when not in use
- The Data Controller must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Personal data should never be saved directly to devices where such data is not protected or secured
- All servers containing sensitive data must be approved and protected by security software
- All possible measures must be put in place to keep data secure

Data Retention

The company will not retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons why the personal data was originally obtained.

Transferring Data Internationally

There are restrictions on international transfers of personal data. Personal data will not be transferred abroad, or anywhere else outside of normal rules and procedures, without express permission from the Data Controller.

7. RIGHTS OF INDIVIDUALS

Individuals have rights to their data which we must respect and comply with to the best of our ability. We will ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- Providing privacy notices which are concise, transparent and easily accessible, written in clear and plain language.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Enabling individuals to access their personal data and any additional information held.
- Allowing individuals to be aware of the reason for processing data.

3. Right to rectification

- We must rectify or amend the personal data of an individual if requested because it is believed to be inaccurate or incomplete.
- This must be done without delay, and no later than one month. This can be extended to two months with permission from the Data Controller.

4. Right to erasure

- We must delete or remove an individual's data if requested and there is no legitimate reason for its continued processing.

5. Right to restrict processing

- We must comply with any request to restrict the processing of personal data if not done for a legal or legitimate reason.
- We can legally store personal data if it has been restricted, but not processed further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We must provide individuals with their data if requested so that they can reuse it for their own purposes.
- We must provide data in a commonly used format and send it directly to another data controller if the person on whom we hold data requests us to do so in writing.

7. Right to object

- We must respect the right of an individual to object to data processing if that objection has a legal basis.
- We must respect the right of an individual to object to being subjected to direct marketing.
- We must respect the right of an individual to object to us processing their data for statistical reasons unless doing so is a statutory obligation.

8. PRIVACY NOTICES

When to supply a Privacy Notice

- A privacy notice will be supplied at the time the data is obtained if it has been obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within one month of obtaining the data.
- If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.
- If disclosure to another recipient is necessary, the privacy notice must be supplied prior to the data being disclosed.

What to include in a Privacy Notice

Privacy notices must be concise, transparent, easily accessible and written in clear and plain language.

The following information will be included in a privacy notice to all data subjects:

- Identification and contact information for the Data Controller
- The purpose of processing the data and the lawful basis for doing so
- Any legitimate recipient of the personal data, including third parties

- The legitimate interests of a third party, if applicable
- The right to object or withdraw consent at any time, if applicable
- Details of data not obtained directly from the data subject
- The retention period of the data and details on the data disposal after the retention period
- The right to lodge a complaint with the ICO and internal complaint procedures (details of the complaint should be forwarded to the Data Controller)
- The source of the personal data, and whether it came from publicly available sources such as websites, outside agencies, recruitment websites etc. (only for data not obtained directly from the data subject)
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

9. SUBJECT ACCESS REQUESTS

What is a Subject Access Request?

An individual has the right to receive confirmation that their data is being processed and why, and have access to their personal data.

How we will deal with Subject Access Requests

We will provide an individual with a copy of the information they request, free of charge. This must be provided within one month of the request. We will endeavour to supply data in a commonly used format where possible, but may only be able to provide a paper copy.

If complying with the request is complex, the deadline can be extended by two months, but the individual must be informed of the extension within one month. The Data Controller must have approved the deadline extension.

We can refuse to respond to certain requests, and can, if the reasons for the request are unfounded or if the information requested is excessive, charge a fee. If the request is for a large quantity of data, we can ask the individual to specify the information they are requesting. This can only be done with prior consent from the Data Controller.

Once a subject access request has been made, no amendments to any of the data requested are permitted. Doing so is a criminal offence.

Data Portability Requests

We will provide the data requested in a structured, commonly used and easily understood format. This would normally be a spreadsheet, word document or the format available from the system holding the information. Failing that, a paper copy will be provided. This data will be provided to the individual who has requested it, or to the data controller they have requested it be sent to. This will be done free of charge and no later than one month. This can be extended to two months for complex or numerous requests with consent from the Data Controller, but the individual must be informed of the extension within one month.

10. RIGHT TO ERASURE

What is the Right to Erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed.
- Where consent is withdrawn.
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed or otherwise breached data protection laws.

How we Deal with the Right to Erasure

We can only refuse to comply with a right to erasure in the following circumstances:

- We need the information to continue the employment relationship
- To ensure the company can comply with a statutory / legal obligation or to provide information requested by an official authority.
- For public health purposes in the public interest.
- For historical research or statistical purposes.
- To commence or defend legal claims.

If personal data that needs to be erased has been passed onto other parties or recipients, they will be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

The Right to Object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We should inform the individual of their right to object at the first point of communication, i.e. in the privacy notice and offer a way for individuals to object that suits their personal circumstances e.g. by letter or email etc.

The Right to Restrict Automated Profiling or Decision Making

We, or third party agents acting on behalf of the company, may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated profiling e.g. recruitment via an employment agency, process followed for acceptance, refusal or limitation of customer business.
- Offer simple ways for them to challenge any decision about them.
- Carry out regular checks to ensure systems are working as intended.

11. THIRD PARTIES

Using Third Party Controllers and Processors

As a Data Controller and Data Processor, Consort Limited will use third party data controllers and/or data processors who will be required to set out how they will meet their liabilities, obligations and responsibilities for processing personal data.

As a Data Controller, we will only work with processors who can provide sufficient guarantees under GDPR that the rights of data subjects will be respected and protected.

Contracts and Agreements

These must comply with the standards set out by the Information Commissioner's Office. Our agreement with data controllers and/or data processors will identify the subject matter and duration of the processing, the nature and purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the data recipient.

At a minimum, our contracts should include terms that specify:

- They are acting on written instructions.
- Confirmation that those involved in processing the data are subject to a duty of confidence.
- Appropriate measures will be taken to ensure the security of the processing.
- Sub-processors will only be engaged with the prior consent of Consort Limited and under specific agreements and circumstances confirmed in writing.
- The company would assist the processor in dealing with Subject Access Requests, where requested, and allowing data subjects to exercise their rights under GDPR.
- Deletion or return of all personal data at the end of the agreement as per the requirements of Consort Limited.
- Allowing audits and inspections, and the provision of whatever information necessary for organisations to meet their legal obligations.
- Nothing will be done by either party to infringe the requirements of GDPR.

12. CRIMINAL OFFENCE DATA

Criminal Record Checks

Any criminal record checks are justified by law, should not be undertaken based solely on the consent of the subject. They must be justifiable and proportionate. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. The Data Controller must authorise a criminal records check, if necessary.

13. CCTV MONITORING

CCTV monitoring takes place to ensure security of the premises.
Consort Limited has considered the potential impact on individual's privacy and has taken this into account when adopting this method to secure the site.

Use of the CCTV System

- The Operation's Director is responsible for the operation of the CCTV system.
- The CCTV monitoring station is located within the Operations Director's office.

- The Operations Director is solely responsible for the recordings and no other person has access to recorded footage without his specific consent.
- Location of cameras are determined by the Operation's Director in collaboration with the CCTV monitoring company to provide the widest view of the site.
- No cameras are placed in sensitive areas such as washroom facilities.
- Employees are aware of the surveillance and location of security cameras on site by way of notices.

- The CCTV information may be used for the following purposes:

  - Any issue involving security of the site; break in's, intruders, thefts, vehicle tampering, misdemeanours or other sufficiently serious matters by outsiders.
  - To provide corroborative evidence on serious employee matters during working hours such as those that may lead to disciplinary action.
  - To assist with identifying persons responsible for damage to vehicles whilst on site belonging to employees or the company.
  - Identifying employees or suppliers speeding whilst on site.
  - To assist the police or other statutory bodies in the execution of their duties.
  - Monitor supplier or contractor activities whilst on site.

Time Limit for Recordings

- The system records activity on site for 24 hours per day.
- The system is set to overwrite recordings every 3 weeks.
- Historical recordings that go back further than 3 weeks are not recoverable.

Copies of Recordings

Copies of recordings are not routinely kept and will only be made for specific purposes. A record of any copies made will be kept with reasons why a copy has been made, and no copies will be passed on without the express consent of the Operations Director or in the case of a statutory body (such as the police), an official written request.

14. AUDITS, MONITORING AND TRAINING

Data Audits

Regular data audits to manage risk will look at information on what data is held, where it is stored, how it is used, who is responsible, and any further regulations or retention timescales that may be relevant.

Monitoring

Consort Limited will keep this policy under review and amend or change it as required. The Data Controller must be notified of any breaches of this policy. Everyone is expected to comply with the full remit of this policy at all times.

Training

Please ask if you are unsure of the data protection requirements specific for your role.

Reporting Breaches

All members of staff have an obligation to report actual or potential data protection compliance failures to the Data Controller as soon as they become aware of the breach or potential breach.

This allows us to:

- Investigate the failure and for the Data Controller to take remedial action if necessary.
- Maintain a register of compliance failures.

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Failure to Comply

We take compliance with this policy very seriously. Failure to comply puts the organisation at risk and may lead to disciplinary action under our procedures or dependent upon circumstances, dismissal.

If you have any questions or concerns about anything in this policy, please contact the Data Controller.