General Data Protection Policy

Who are we:
EuroWindows Limited is incorporated in England and Wales and is a 'controller' under the General Data Protection Regulation.

The EU General Data Protection Regulation (GDPR) comes into force on 25 May 2018 and will supersede the current Data Protection Act 1998. GDPR will apply despite Brexit, and will impact all organisations that control or process personal data. It will grant data subjects a range of new rights, giving them more control over how their data is used. Organisations will be subject to new responsibilities and obligations, including the need to demonstrate compliance. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. This policy has been designed to comply with the General Data Protection Regulation 2018

The Data protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

What information will we collect from you:
We will only collect information that is relevant to the matter that we are dealing with, in particular we may collect the following information from you which is defined as 'personal data' This includes:

- Name, home address, contact details, date of birth, emergency contact details
- Financial details
- National insurance number
- Business activities of the person whose details we are processing
- Absence records
- Identification (passport details, birth certificate, proof of address)
- Driving licence
- Training records
- Performance information

We may also collect information that is referred to as being in a 'special category'. This could include:

- Physical or mental health details
- Racial or ethnic origin
- Religious beliefs or other beliefs of a similar nature
- Criminal convictions
- Sexual orientation
- Result of drug tests

This information is only collected during the recruitment process and used in such a way that it does not unfairly affect an applicant's chance of employment. Data on race, religion and sexual orientation is stored anonymously. Information on health and criminal convictions will be assessed in line with EuroWindows Ltd recruitment guidelines and stored for the duration of employment.

Who do we receive information from:

- The data subject themselves
- Employment and recruitment agencies
- Current, past and prospective employers
- Educators and examining bodies
- Central Government
- Supplier and service providers
- Financial organisations
- Business associates and professional advisors

How will we use your information:

We will use your information in our capacity as an employer, customer or supplier for the following purposes:

- Employment
- Administering contracts
- Processing your bank details in order to make a payment
- The prevention and detection of fraud
- Marketing
- Providing customer service
- Booking installation and service appointments with residents
- Health and Safety management
- Obtaining legal advice
- Providing Guarantees, warranties insurance, FENSA registrations
- Costco membership
- Life insurance
- Health insurance
- Pensions
- DBS checks
- CSC and training records
- Complying with statuary requirements
- Disaster recover planning
- Applying for certificates proving competency such as ConstructionLine, FORS, BSI

Who will we disclose your information to:

We will disclose your information to the following organisations and people:

- Government departments
- Insurance and Pensions companies
- Our legal advisers and external consultants, courts and tribunals
- Our business partners for the purpose of fulfilling contractual obligations
- Banks
- DBS checking services
- Training providers
- Employees involved in dealing with you as a customer, supplier, employee
- Partners, customers, and suppliers of EuroWindows Ltd

We will not share your information outside our organisation for any other purposes than those connected with our statutory obligations to disclose information or for the purpose of conducting our business. We will share name, contact phone number, email address and information relating to your employment. Within our organisation your information will only be made available to those people involved in dealing with you, as a customer, partner, supplier or employee. Only information deemed relevant will be shared.

Responsibilities:
Everyone who works for or with EuroWindows Limited, has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data, must ensure that it is handled and processed in line with this policy, and data protection principles.

The following have key areas of responsibility:

- The Board of Directors is ultimately responsible for ensuring that EuroWindows Limited meets its legal obligations
- The Data Controller, Jacob Prince is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advise or the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data EuroWindows Limited holds about them (also called 'subject access requests').
    - Checking and approving any contract or agreements with third parties that may handle the company's sensitive data.
    - Reviewing any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries.
    - Where necessary, working with other staff to ensuring marketing initiates abide by data protection principles.

- The **IT Manager, Chris Peak** is responsible for:

    - Ensuring all IT systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

General Staff Guidelines:

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be share informally. When access to confidential information is required, employees can request it from the Data Controller.
- EuroWindows Limited will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following guidelines below.
- In particular, strong passwords will be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.

- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the Data Controller, if they are unsure about any aspect of data protection.

Data Protection Procedure

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be contained in a locked cabinet.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Personal data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing personal data should be protected by approved security software and a firewall.
- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data likely to cause harm should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Personal data should never be transferred outside of the European Economic Area. We cannot guarantee that services used by EuroWindows Ltd transfer date via non EEA counties, but in as far as is practical, EuroWindows Ltd will only use services operating commercially within the EEA.
- Always access and update the central copy of any data.
- Employees should not save copies of personal data to their own computers, mobile phones, tablets or similar electronic devices.
- Employees who store personal data which is not connected to the company on computers, mobile phones, tablets or similar electronic devices, do so on the understanding that this data may be viewed, store and deleted by EuroWindows ltd. It is the employees' responsibility to insure they have the permission of the data subject to store data on devices owned by EuroWindows Ltd. No data likely to cause harm should be stored insecurely on mobile devices.

Data Storage:
These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Manager or Data Controller.

When personal data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. Data will be retained inline with EuroWindows'data retention policy.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.

- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded when no longer required.

Data Accuracy:
The law requires EuroWindows Limited to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- EuroWindows Limited will make it easy for data subjects to update the information EuroWindows Limited holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

How long will we keep your information for:
Data will be kept in accordance with our Data Retention Policy. A copy of which can be requested from the Data Controller.

What rights do you have:
You have a series of rights under the General Data Protection Regulation including:
The right to be informed
Right of access
Right of rectification
Right of erasure
Right to restrict processing
Right to data portability
Right to object to direct marketing
Right to review automated decision making
Right to compensation

Data subjects who wish to raise a concern over any of these rights should contact the data Controller

Data Breach:
EuroWindows Ltd. has a data breach procedure which will be followed on discovery of a failure in data protection.

Subject Access Requests:
All individuals who are the subject of personal data held by EuroWindows Limited, are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, it is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Data Controller at jacob.prince@euro-windows.co.uk

The Data Controller will provide the relevant data within 30 days.

The Data Controller will always verify the identity of anyone making a subject access request before handing over any information.

Who can you complain to if you are unhappy about what we have done with your information?:
If you are unhappy about how we are using your information, then initially you should contact the Data Controller and if your complaint remains unsolved then you can contact the Information Commissioners Office, details available at www.ico.org.uk

Policy dated 25/5/2018