INTRODUCTION

As a business we have to collect and use information about people, be they customers, potential customers, suppliers or members of staff. This personal information must therefore be handled properly and stored securely whether it be on paper, in computer records or recorded by any other means.

With the introduction of GDPR into European Law, it is now not just important in maintaining confidence and professionalism, it's a legal requirement.

This policy applies to the processing and maintenance of personal data kept by us in connection with:

- Human Resources
- Finance
- Marketing

It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

DEFINITIONS

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, email address, location or online identifier.

We do not gather any personal data that is specified within the definition of "Special categories of personal data" - an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. Nor do we gather any genetic and biometric data or criminal offence records.

"Data processing" is any operation or set of operations which 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, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing will be fair, lawful and transparent
b) data be collected for specific, explicit, and legitimate purposes
c) data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
d) data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) data is not kept for longer than is necessary for its given purpose
f) data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g) we will comply with the relevant GDPR procedures for international transferring of personal data

TYPES OF DATA HELD

We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data:

Human Resources

a) personal details such as name, address, phone numbers
b) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on your education and employment history etc
c) details relating to pay administration such as National Insurance numbers, bank account details and tax codes
d) medical or health information
e) information relating to your employment with us, including:
   i) job title and job descriptions
   ii) your salary
   iii) your wider terms and conditions of employment
   iv) details involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
   v) internal and external training modules undertaken

All of the above information is required to effectively manage our staff. More information is available from your manager.

Finance

a) Company or personal details such as name, address, phone numbers
b) details of your order, products and services purchased
c) details relating your products - supplied documents including architectural drawings, photographs and sketches
d) details of other contracted individuals or companies such as your architects, interior designers or electrical contractors

Marketing

a) an individuals name and email address

Once you make direct contact with us, we will ask for further details including:

a) If you are a trade or direct customer
b) your direct contact details
c) you location and shipping address

into a CV or included in a CV cover letter, references from former employers, details on your education and employment history etc
c) details relating to pay administration such as National Insurance numbers, bank account details and tax codes

YOUR RIGHTS

As an employee, you have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it;
b) the right of access to the data we hold on you.
c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
e) the right to restrict the processing of the data;
f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
g) the right to object to the inclusion of any information;
h) the right to regulate any automated decision-making and profiling of personal data.

As a customer, you have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it;
b) the right of access to the data we hold on you.
c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
d) the right to have data deleted in certain circumstances where the data is not required for company financial records, which must be maintained for 6 years in accordance with UK Law.
e) the right to restrict the processing of the data;
f) the right to object to the inclusion of any information;
g) the right to regulate any automated decision-making and profiling of personal data.

As a recipient of any of our marketing channels, you have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it;
b) the right of access to the data we hold on you.
c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
d) the right to have data deleted in certain circumstances. This is also known as 'erasure';
e) the right to restrict the processing of the data;
f) the right to transfer the data we hold on you to another party. This is also known as 'portability';
g) the right to object to the inclusion of any information;
h) the right to regulate any automated decision-making and profiling of personal data.

RESPONSIBILITIES

In order to protect personal data all our staff who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed a Data Protection Officer who holds responsibility for reviewing and auditing our data protection systems and handling requests and complaints.

SECURITY

Human Resources
Hard copy personal information is to be kept in a secured location. Digital copy personal information is to be held on a secure hard drive using password protection.

Finances
Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Marketing

Employees are aware of their roles and responsibilities when their role involves marketing to members of the general public. All employees are instructed to only store details for which we have been given documented consent and to only use the agreed method and frequency of marketing.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

THIRD PARTY SUPPLY

We never engage third parties to process data on our behalf, nor do we ever use supplied third party in conjunction with the data we hold.

ACTION ON BREACHES OF DATA

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

TRAINING

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the Company are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

DATA PROTECTION COMPLIANCE

Our Data Protection Officer is:

Paul Carr
General Manager, Curiousa Ltd
paul@curiousa.co.uk
01629 826284
0776 4800488