Data Protection Policy

Contents

1. Introduction

Singleton Event Services Ltd are dedicated to protecting all forms of data that may be collected or held by the company.

In addition the company will promote good data protection procedures through employee training and regular reviews of our policies and procedures.

In the event of a potential data protection breach, the company will immediately begin a thorough and transparent investigation of the circumstances of the breach.

2. Data Protection management

The nominated data protection controller within the company is Nigel Singleton.

3. Registration with ICO

The company is registered with the information commissioners office to hold personal data. This registration shall be renewed annually.

4. Identification of personal data

The company holds data that may be classed as personal data in the following forms:

- CCTV - computer
- Customer accounts records - computer
- Supplier accounts records - computer
- Contractor HR files – computer
- Patient Report forms - computer
- Customer marketing records – computer
- Phone conversations – recorded by 4com

5. Personal data security

Personal data is protected in the following way:

- CCTV – locked in the cupboard
- Customer accounts records – computers are password protected and accounts are password protected
- Supplier accounts records – computers are password protected and accounts are password protected
- Contractor HR files – computers are password protected
- Patient report forms - computers are password protected
- Customer marketing - computers are password protected

6. Information security

The companies IT system is protected by Microsoft defender and Malware Bytes software. The router for internet access also has a hardware firewall designed to protect from hacking and DOS type intrusion.

The Microsoft software is updated daily and automatically. The Malware Bytes software is updated weekly and manually when it is run.

All company computers are protected by password. Each employee has their own password. The company will ensure that all passwords are changed once every 6 months.

Computer screens are set to lock if the operator leaves the computer screen open.

7. Privacy statements

All the companies web sites that collect personal data have a privacy statement available for the general public to view.

8. Accuracy of personal data

The company will review and update marketing records annually.

9. Requests for access to personal data

Personal and sensitive data may only be released to a third party by formal application in writing or using the online data request form. In the event of such an application all attempts will be made to contact the person to whom the data belongs in order to request their permission. This does not apply in cases where the request may be made under the jurisdiction of UK law.
All requests for the release of personal data will be logged and retained by the company for a period of 6 years.

10. Marketing

The company holds databases of customer details for marketing purposes. These records have been obtained directly from online address directories such as Yell.com. The information we collect is freely available on the internet and therefore is not deemed to be personal data as defined under the Data Protection Act.

All company emails will contain a footer indicating the origin of the email.

11. Data protection breach procedure

In the event of a possible breach of the Data Protection Act, the company will contact the ICO and seek both clarification and advice on the correct course of action.
A full investigation will be conducted and an action plan drawn up to prevent any repeat of the data protection breach.

12. Disposal and deletion of personal data

The main records kept by the company are listed below and the deletion criterion is listed next to each category.

Type of data	Duration of record retention
Patient report forms	Indefinite
4com recorded phone calls	12 months
CCTV images	Approximately 2 weeks
Terminated contractor files	Deleted on termination
Requests for access to personal data	6 years
Accounts data - computer	6 years

Paper records shall be cross-cut shredded and/or incinerated to ensure they have been full destroyed.
Computer based records shall be deleted and overwritten.
In the event of replacement of a computer holding personal data, the hard drive shall be formatted and then destroyed to prevent access to any data.

13. Staff training

The company will provide basic training on Data protection on a regular basis. Data protection will also be discussed at team meetings to keep our procedures fresh in the mind.

14. Business continuity

The following tasks and frequencies have been designed to assist in a disaster recovery plan:

- Windows software –Manual check weekly.
- Company documents are held on the cloud.
- Accounts are held on Xero servers.
- Payroll is backed up each month.

This policy will be reviewed in light of changes in legislation and at least every 3 years and updated accordingly.