Kelly Kadabra's Data Protection Policy

Context and Overview

Key details

- Policy prepared by: Mr R A Robinson
- Approved by Kelly Kadabra and on: 11/05/18
- Policy became operational on: 20/05/18
- Next review date: 01/11/18

Introduction

Kelly Kadabra needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet Kelly Kadabra's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 describes how organisations — including Kelly Kadabra — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

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

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

People, risks and responsibilities

Policy scope

This policy applies to:

- Kelly Kadabra
- All staff and volunteers of Kelly Kadabra
- All contractors, suppliers and other people working on behalf of Kelly Kadabra

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- plus, any other information relating to individuals

Data protection risks

This policy helps to protect Kelly Kadabra from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

- Everyone who works for or with Kelly Kadabra has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- Kelly Kadabra is ultimately responsible for ensuring that Kelly Kadabra meets its legal obligations.

The **Data Protection Officer** is responsible for:

- Keeping Kelly Kadabra 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 advice for Kelly Kadabra covered by this policy.
- Handling data protection questions from anyone else covered by this policy.
- Dealing with requests from individuals to see the data Kelly Kadabra holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle Kelly Kadabra's sensitive data.

Kelly Kadabra is responsible for:

- Ensuring all 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 that Kelly Kadabra is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.

General guidelines

- The only people able to access data covered by this policy will be Kelly Kadabra.
- Data **will not be shared informally**.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorized people.
- 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.

Data storage

- These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to Kelly Kadabra.

When data is **stored on paper,** it should be kept in a secure place where unauthorized people cannot see it.

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**.
- **Data printouts should be shredded** and disposed of securely when no longer required.

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

- Data should be **protected by strong passwords**.
- 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 **sited in a secure location**.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the Kelly Kadabra's standard backup procedures.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

- Personal data is of no value to Kelly Kadabra unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:
    - When working with personal data Kelly Kadabra will ensure **the screens of her computer is always locked** when left unattended.
    - Personal data **should not be shared informally**. In particular it should never be sent by
    - Personal data should **never be transferred outside of the European Economic Area**.

Data accuracy

- The law requires Kelly Kadabra to take reasonable steps to ensure data is kept accurate and up to date.
- The more important it is that the personal data is accurate, the greater the effort Kelly Kadabra should put into ensuring its accuracy.
- It is the responsibility of Kelly Kadabra when working 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**.
    - 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.
    - It is the Kelly Kadabra's responsibility to ensure **databases are checked against suppression files** every six months.

Subject access requests

All individuals who are the subject of personal data held by are entitled to:

- Ask **what information** Kelly Kadabra and 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 Kelly Kadabra requesting this information, this is called a subject access request.

- Subject access requests from individuals should be made by email, addressed to kelly@kellykadabra.com
- Individuals will be charged £10 per subject access request. Kelly Kadabra or will aim to provide the relevant data within 14 days.
- Kelly Kadabra will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

- Under these circumstances, Kelly Kadabra will disclose requested data. However, Kelly Kadabra will ensure the request is legitimate, seeking assistance from legal advisers where necessary.

Providing information

- Kelly Kadabra aims to ensure that individuals are aware that their data is being processed, and that they understand:
  - How the data is being used
  - How to exercise their rights

To these ends, Kelly Kadabra has a privacy statement, setting out how data relating to individuals is used by the company.