Data Protection Policy

Context and Overview

Key details

- Policy prepared by: Miles Bradley
- Approved by board/management on: 02/01/2018
- Policy became operational on: 11/01/2018
- Next review date: 11/01/2019

Introduction

Kind Consultancy Ltd needs to gather and use certain information about individuals.

These can include candidates, 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 the company's data protection standards - and to comply with the law.

Why this policy exists

This data protection policy ensures Kind Consultancy Ltd:

- Complies with all relevant data protection law and follows 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 Kind Consultancy - must collect, handle and store personal information. In 2018 the General Data Protection Regulation will supersede and expand on these laws, and Kind Consultancy will be functioning in a GDPR compliant manner before GDPR comes into full effect on the 25th of May 2018.

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:

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 to be held for any longer than necessary
6. Processed in accordance with the rights of the 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.

In addition to these, GDPR introduces some more key tenets:

- Explicit permission is required to store and use any identifying personal data
- Subjects must be aware of exactly what their information will be used for, and must actively consent to that specific use

People, risks and responsibilities

Policy Scope

This policy applies to:

- The head office of Kind Consultancy Ltd
- All branches of Kind Consultancy Ltd
- All staff and volunteers of Kind Consultancy Ltd
- All contractors, suppliers and other people working on behalf of Kind Consultancy Ltd

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 or GDPR, this can include:

- Names of individuals
- Postal addresses
- E-mail addresses
- Telephone numbers
- Any other identifying information relating to individuals

Data Protection Risks

This policy helps to protect Kind Consultancy Ltd from some very real data security risks including:

- **Breaches of confidentiality**
- **Obtaining, holding or using data without proper consent (incurring fines)**

- **Failing to offer choice**
- **Reputational damage**

Responsibilities

Everyone who works for or with Kind Consultancy Ltd has some responsibility for ensuring data is collected stored and handled appropriately. Each team that handles 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:

- The **board of directors** is ultimately responsible for ensuring that Kind Consultancy Ltd meets its legal obligations
- The **data protection officer**, Matt Kind, 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 advice for 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 Kind Consultancy Ltd holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handles the company's sensitive data
- The **IT manager**, Kevin Redfern, 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 the company is considering using to store or process data. For instance, cloud computing services.
- The **marketing manager**, Miles Bradley, is responsible for:
    - Approving any data protection statements attached to communications such as e-mails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives by data protection principles.

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 shared informally**. When access to confidential information is required, employees can request it from their line managers.
- Kind Consultancy Ltd **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 the guidelines below.
- In particular, **strong passwords must 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 protection officer if they are unsure about any aspect of data protection.
- Employees will clearly recorded where all identifiable personal data has come from
- Large scale **'e-shot' e-mail marketing campaigns should be avoided** - explicit permission is needed from clients and potential clients confirming they want to receive marketing material from us

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 data is **stored on paper**, it should be kept in a secure place where unauthorised 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 of 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 or out on desks
- **Data printouts should be shredded** and disposed of securely when no longer required.
- **Data should not be transported off site** or transported in any form except for in those circumstances which subjects have given explicit permission for (ie. Submitting CVs to potential employers)

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 **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- 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 Kind Consultancy Ltd 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, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**.
- Personal data should **never be transferred outside of the European Economic Area** without the expressed permission of the data subject
- Employees **should not save copies of personal data to their own computers or removable devices or otherwise create copies of data**. Always access and update the central copy of any data.

Data accuracy

The law required Kind Consultancy Ltd 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 Kind Consultancy Ltd should put into ensuring its accuracy.

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 - for example, spreadsheets of contact details that are held on the central database
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.
- Kind Consultancy Ltd will make it **easy for data subjects to update the information** that Kind Consultancy Ltd 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.
- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files**

Subject access requests

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

- Ask **what information** the company holds about them and what that information is being used for
- 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, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at mat@kindconsultancy.com.

Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller 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 and General Data Protection Regulation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Kind Consultancy Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

Kind Consultancy Ltd 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, the company has a privacy statement, setting out how data relating to individuals is used by the company.

This is available on request. A version of this statement is also available on the company's website.

Incident and Breach Management

In the event of any member of Kind Consultancy committing or becoming aware of an information security or data protection breach, it must immediately be escalated to Mathew Kind. If Mathew is off site and out of contact, another member of senior management must be informed and Mathew must be made aware within 24 hours.