Data protection policy

Context and overview

Introduction

Free to Be NLP and Coaching Ltd 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 is collected, handled and stored to comply with the law. This policy became operational on October 8th 2017 and will be reviewed bi-annually or should the company change the way it uses data.

Why this policy exists

This data protection policy ensures Free to Be NLP and Coaching Ltd:

- 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 Free to Be NLP and Coaching Ltd – 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:

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

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of Free to Be NLP and Coaching Ltd
- All staff and volunteers of Free to Be NLP and Coaching Ltd
- All contractors, suppliers and other people working on behalf of Free to Be NLP and Coaching 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 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 Free to Be NLP and Coaching Ltd 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 Free to Be NLP and Coaching Ltd has some responsibility for ensuring data is collected, stored and handled in line with this policy and data protection principles.

These people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that Free to Be NLP and Coaching Ltd_meets its legal obligations.

- The data protection officer, Caroline Tyrwhitt, is responsible for:

- Ensuring the company is up-to-date about data protection responsibilities, risks and issues.
- Reviewing data protection procedures and policies
- Arranging data protection training for staff.
- Handling data protection questions from staff.
- Dealing with requests from individuals to see the data Free to Be NLP and Coaching Ltd holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- 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.
- Working with other directors, staff and sub-contractors to ensure IT systems that use data abide by data protection principles.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets.
- Working with other directors, staff and sub-contractors to ensure marketing initiatives abide by data protection principles.

General guidelines

- The only people able to access data covered by this policy are those who need it for their work.
- Data is not be shared informally.
- The company will keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords will be used and they will never be shared.
- Personal data will not be disclosed to unauthorised people.
- Data will be regularly reviewed and updated if it is found to be out of date. If no longer required, it will be deleted and disposed of.

Data storage

These rules describe how and where data is safely stored.

When data is stored on paper, it is 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 or files will be kept in a locked drawer or filing cabinet and not left where unauthorised people could see them.
- Data printouts will be shredded and disposed of securely when no longer required.

Data that is stored electronically, will be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data will be protected by strong passwords that are changed regularly and never shared.
- If data is stored on removable media, these will be kept locked away securely when not being used.
- Data will only be stored on designated drives and servers, and only uploaded to approved cloud computing services.
- Servers containing personal data will be sited in a secure location.
- Data will be backed up frequently. Those backups will be tested regularly.
- Data saved directly to laptops while at courses or to take to courses will be encrypted.
- All servers and computers containing data will be protected by approved security software and a firewall.

Data use

Personal data is of no value to Free to Be NLP and Coaching 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, screens of computers are always locked when left unattended.
- Personal data will not be shared informally or shared unnecessarily.
- Data will be encrypted before being transferred electronically.
- Personal data will not be transferred outside of the European Economic Area.

Data accuracy

The law requires Free to Be NLP and Coaching 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 Free to Be NLP and Coaching Ltd should put into ensuring its accuracy.

- Data will be held in as few places as necessary..
- The company will take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Free to Be NLP and Coaching Ltd will make it easy for data subjects to update the information the company holds about them. For instance, via the company website.
- Data will be updated as inaccuracies are discovered. For instance, if a client can no longer be reached on their stored telephone number, it will be removed from the database.
- The company will check marketing databases against industry suppression files every six months.

Subject access requests

All individuals who are the subject of personal data held by Free to Be NLP and Coaching Ltd 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.

Subject access requests from individuals should be made by email at welcome@freetobenlpandcoaching.co.uk. The company can supply a standard request form, although individuals do not have to use this.

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

The company 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, Free to Be NLP and Coaching Ltd will disclose requested data. However, the company will ensure the request is legitimate, seeking legal advice where necessary.

Providing information

Free to Be NLP and Coaching 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 policy, setting out how data relating to individuals is used by the company. Please refer to the policy on the company website.