Data protection policy

Context and Overview

Key details

- Policy prepared by: Paul Noble
- Approved by Managing Director on: 03rd January 2018
- Policy became operational on 03rd January 2018
- Next review date 02nd January 2019

Introduction

Telecoms Advisor Ltd needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people that the company 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 comply with the law.

Why this policy exists

This policy ensures Telecoms Advisor Ltd

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

Data protection law

The Data Protection Act 1998 controls how your personal information is used by organisations, businesses or the government.

Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the EEC without adequate protection

There is stronger legal protection for more sensitive information, such as:

- ethnic background
- political opinions
- religious beliefs
- health
- sexual health
- criminal records

People, risks and responsibilities

Policy scope

This policy applies to:

- All staff of Telecoms Advisor Ltd
- All contractors, suppliers and other people working on behalf of Telecoms Advisors 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
- Any other information relating to individuals

Data Protection risks

This policy helps to protect Telecoms Advisor Ltd from some very real data security risks, including:

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

Responsibilities

Everyone who works for or with Telecoms Advisor Ltd has some responsibility for ensuring data is collected, stored and handled appropriately. Each entity that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The Managing Director is responsible for:

- Reviewing all data protection responsibilities, risks and issues.
- Arranging data protection training and advice for the people covered by this policy.
- Responding to data protection questions from staff and others covered by this policy.
- Dealing with requests from individuals to see data the company holds about them (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.
- Evaluating any third party services the company is considering using to store or process data. For instance, cloud computing services.

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 manager.
- **Telecoms Advisor 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.
- **Strong passwords should be used** and the company password policy should be adhered to.
- 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 if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Managing Director.

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 for some reason:

- When not required, the paper or files should be kept in a **locked drawer or filing cabinet**.
- Employees should ensure paper and printouts **are not left where unauthorised people could see them**.
- **Data printouts should be shredded** and disposed of securely when no longer required.

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, these should be kept locked away securely when not in use.
- Data should only be stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing service**.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be **backed up frequently**. These backups should be tested regularly.
- Data should **never be saved directly** to laptops or other mobile devices.
- All servers and computers containing data should be protected **by approved security software and a firewall**.

Data use

Personal data is of no use to Telecoms Advisor 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**. In particular, it should never be sent by email (other than secure email), as this form of communication is not secure.
- Data **must be encrypted before being transferred electronically**.
- Personal data should **never be transferred outside of the European Economic Area.**
- Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

Data accuracy

The law requires Telecoms Advisor Ltd to take reasonable steps to ensure data is kept secure and up to date.

The more important it is that the personal data is accurate, the greater the effort should be put into ensuring 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.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.
- The company will make it easy for data subjects to update the information it holds about them.
- 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.

Subject access requests

All individuals who are the subject of personal data held by Telecoms Advisor 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 obligation**s.

If an individual contacts the company requesting this information, this is called a **subject access request**.

Such requests from individuals should be made by email to support@pcitelecom.co.uk. A standard request form is available, although individuals do not have to use this.

A charge of £10 per request will be levied. The request will aim to be fulfilled providing the relevant data within 14 days once verification of the person making the request is ascertained.

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, Telecoms Advisor Ltd will disclose requested data. However, the company will ensure the request is legitimate, seeking assistance from the company's legal advisors where necessary.

Providing information

Telecoms Advisor 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.

This is available on request.