CIOTEK General Data Protection Regulations (GDPR) Policy

Context and Overview

Key Details

Policy prepared by: Shannon Stevens
Approved by board on: 03.03.2018
Policy became operational on: 02.04.2018
Next review date: 02.04.2019

Introduction

CIOTEK Limited need to gather and use certain information about individuals acting as sub contract consultants, clients, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data will 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 CIOTEK Limited:

- Complies with data protection law (including GDPR) 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 CIOTEK Limited 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 this 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 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:

- All staff and associates of CIOTEK Limited
- All contractors, suppliers and other people working on behalf of CIOTEK Limited

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 that can identify an individual

Data Protection Risks

This policy helps to protect CIOTEK Limited from some very real security risks, including:

- **Breaches of confidentiality;** for instance, information being given out inappropriately.
- **Failing to offer choice;** for instance, all individuals will 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 CIOTEK Limited has responsibility for ensuring data is collected, stored and handled appropriately. Each individual 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:

- The board of directors is ultimately responsible for ensuring that CIOTEK Limited meets it legal obligations.
- The Data Protection Officer, Shannon Stevens, is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all the 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 CIOTEK Limited 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.
    - Identifying and maintaining a professional relationship with a main IT subcontractor who is able to;

  - Ensure all systems, services and equipment used for storing data meet acceptable security standards.
  - Perform regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluate any third-party services the company is considering using to store or process data i.e. 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 outputs like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by this policy will be those who need it for their work.
- Data will not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- CIOTEK Limited will provide training to all employees to help them understand their responsibilities when handling data.
- Employees will keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used and they will never be shared.
- Personal data will not be disclosed to unauthorised people, either within the company or externally.
- 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.
- Employees will request help from their line manager or the data protection officer is they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data will be safely stored. Questions about storing data safely can be directed to the data controller.

When data is stored **on paper**, it will be kept in a secure place where unauthorised people cannot access 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 of filing cabinet.
- Employees will make sure paper and printouts are not left where unauthorised people could see them.
- Data printouts must 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 will be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable data (like a CD or DVD), these will be kept locked away securely when not being used.
- Data will only be stored on designated drivers and services, and will only be uploaded to approved cloud computing services.
- Servers containing personal data will be sited in a secure location, away from general office space.
- Data will be backed up frequently. Those backups will be tested regularly, in line with the company's standard backup procedures.
- Data will never be saved directly to laptops or mobile devices like tablets or smart phones.
- 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 CIOTEK Limited 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 will ensure the screens of their computers are always locked when left unattended.
- Personal data will not be shared informally. In particular, this will never sent via email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The Data Protection Officer can explain how to send data to authorised external contacts.
- Personal data will never be transferred outside of the EEA.
- Employees will 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 CIOTEK Limited to take reasonable steps to ensure data is kept accurate and up to date. 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 and possible.

- Data will be held in as few places as necessary. Staff will not create any unnecessary additional data sets.
- Staff will take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- CIOTEK Limited will make it easy for data subjects to update the information CIOTEK holds about them.

- Data will be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it will be removed from the database.
- It is the data protection officer's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Subject access requests

All individuals who are the subject of personal data held by CIOTEK Limited 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.

If individual contacts the company requesting this information, this is called a subject access request. These requests from individuals will be made by email, addressed to the data controller at support@CIOTEK.com. The data controller can supply a standard request form, although individuals do not have to use this.

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 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, CIOTEK Limited 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

CIOTEK Limited aims to ensure that individuals are aware that their data is being processed, and that they understand how the data is being used and 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 upon request.