DATA PROTECTION POLICY

This document has been produced by To the core of things s.l.u, https://tothecoreofthings.consulting, a company offering consultancy services to INGOs, Foundations and multirateral organisations.

Data protection policy

Context and overview

Key details

- Policy prepared by: To the core of things
- Approved by board / management on: 01/06/2018
- Policy became operational on: 01/06/2018
- Next review date: 01/06/2020

Introduction

Our company 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 the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures our company:

- 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 new GDPR regulation from the European Union 2016/679 regulated in Spain through LOPD3/2018 describes how organisations 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
- All branches
- All staff and volunteers
- All contractors, suppliers and other people working on behalf of To the core of things

It applies to all data that the company holds relating to identifiable individuals. This can include:

- Any information relating to individuals (Names, Postal addresses, Email addresses, Telephone numbers, etc.)
- Any information related to the consultancy works (assessment studies, strategy policies, proposals, monitoring and evaluation reports, etc.)

Data protection risks

This policy helps to protect To the core of things from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately our without due consent.
- **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 To the core of things has the responsibility for ensuring data is collected, stored and handled appropriately.

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

In this regard, these people have key areas of responsibility:

- The **board** is ultimately responsible for ensuring that our company meets its legal obligations.
- The director will be the person in charge of data protection[1] in charge of:
    - 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 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. 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.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

[1] To the core of things does not currently fall under any of the cases for compulsory Data protection officer regulated under article 37.1 of the EU regulation further legislated under article 34.1 LOPD.

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.
- **Contract clauses with To the core of things will** include reference to confidentiality and data protection to regulate responsibilities of service providers and employees when handling data.
- Employees and service providers 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 and confidential 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 and service providers **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.
- Once contracts are terminated **all data from service contracts is to be completely deleted and removed** from any data storing devices (whether in digital or physical formats) from service contractors. Any later use of this data would constitute and infringement of this data protection policy and will hold service contractors liable.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the line manager or 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 out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees and service providers should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.

- **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:

- Employees and service contractors shall **follow security in a box digital security recommendations** with regards to data security, storage and management: https://securityinabox.org/en/. Specifically they should:
- Data should be **protected by strong passwords** that are changed regularly and never shared between employees or any other service providers.
- If data is **stored on removable media** (like a pen drive, external driver, 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 (approved could computing: google drive)**.
- 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 (following security in a box tools and advices: https://securityinabox.org/en/)**.
- All data

Data use

Personal data is of no value to To the core of things 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 and service providers 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, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The line manager can explain how to send data to authorised external

contacts.

- Personal data should **never be transferred outside of the European Economic Area unless expressely authorised**.

Data accuracy

The law requires To the core of things 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 To the core of things 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.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- To the core of things will make it **easy for data subjects to update the information our company** 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** every six months.

Subject access requests

All individuals who are the subject of personal data held by To the core of things 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 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 company at info@tothecoreofthings.com. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will not be charged per subject access request. The director will aim to provide the relevant data within 14 days.

The director 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, Law allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, To the core of things_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

To the core of things s.l.u_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.]