CRUATECH
Integrating people and technology

# Data Protection Policy

## Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of Cruatech Ltd includes obligations in dealing with personal data, to ensure that the organisation complies with the requirements of the relevant Irish legislation, namely the Irish Data Protection Act (1988), and the Irish Data Protection (Amendment) Act (2003).

## Why the Policy Exists

Cruatech Ltd must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed, and stored by Cruatech Ltd in relation to its staff, volunteers, service providers and clients during its activities. Cruatech Ltd makes no distinction between the rights of Data Subjects who are employees, volunteers, or clients, and those who are not. All are treated equally under this Policy.

## Scope

During its daily organisational activities, Cruatech Ltd acquires, processes, and stores personal data in relation to:

- The office of Cruatech Ltd
- All staff and volunteers of Cruatech Ltd
- All contractors, suppliers and other people working on behalf of Cruatech Ltd
-

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR AND IRISH DATA PROTECTION ACT 2018. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Bank details
- any other information relating to individuals.

Cruatech Ltd acts as both a Data Controller & Data Processor

Everyone who works for Cruatech Ltd has some 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.

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that Cruatech Ltd meets its legal obligations.
- Risk and issues are the responsibilities of the company directors
- 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 request from individuals to see the data Cruatech Ltd holds about them.
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- Cruatech is responsible for:

1. Ensuring all systems, service and equipment used for storing data meet acceptable security standards.
2. Performing regular checks and scans to ensure security hardware and software is functioning properly.
3. Evaluating any third-party service, the company is considering using to store or process data. For instance, cloud computer services emails and letters.

Not all staff members and volunteers will be expected to be experts in Data Protection legislation. However, Cruatech Ltd is committed to ensuring that its staff and volunteers have sufficient awareness of the legislation to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff/volunteers must ensure that the person responsible for the management of Data Protection is informed, and in order that appropriate corrective action is taken.

## The Data Protection Principles

The following key principles are enshrined in the Irish legislation and are fundamental to the Cruatech Ltd Data Protection policy.

## 1. Obtained and processed fairly and lawfully.

For data to be obtained fairly, the data subject will, at the time the data are being collected, be made aware of:

- The identity of the Data Controller-
- The purpose(s) for which the data is being collected
- The person(s) to whom the data may be disclosed by the Data Controller
- Any other information that is necessary so that the processing may be fair. Cruatech Ltd will meet this obligation in the following way.
- Where possible, the informed consent of the Data Subject will be sought before their data is processed.
- Where it is not possible to seek consent, Cruatech Ltd will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.
- Where Cruatech Ltd intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view. Please see the CCTV policy that covers the limited area we cover in this area.
- Processing of the personal data will be carried out only as part of Cruatech Ltd lawful activities, and Cruatech Ltd will safeguard the rights and freedoms of the Data Subject.
- The Data Subject's data will not be disclosed to a third party other than to a party contracted to Cruatech Ltd and operating on its behalf.
- 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, Cruatech Ltd will disclose requested data. However, the office manager will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

## 2. Obtained only for one or more specified, legitimate purposes.

- Cruatech Ltd will obtain data for purposes which are specific, lawful, and clearly stated. A Data Subject will have the right to question the purpose(s) for which Cruatech Ltd holds their data, and Cruatech Ltd will be able to clearly state that purpose or purposes.

## 3. Not be further processed in a manner incompatible with the specified purpose(s).

- Any use of the data by Cruatech Ltd will be compatible with the purposes for which the data was acquired.

## 4. Kept safe and secure.

- Cruatech Ltd will employ high standards of security in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by Cruatech Ltd in its capacity as Data Controller.
- Data must be encrypted before being transferred electronically.
- Access to and management of staff and customer records is limited to those staff members who have appropriate authorisation and password access.
- When not required, the paper or 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.
- Data printout should be shredded and disposed of securely when no longer required.
- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets except for the obligatory 3 backups necessary to avoid data breach

## 5. Kept accurate, complete, and up to date where necessary.

Cruatech Ltd will:

- ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy.
- conduct periodic reviews and audits to ensure that relevant data is kept accurate and up to date. Cruatech Ltd conducts a review of sample data every six months to ensure accuracy; staff and volunteer contact details and details on next-of-kin are reviewed and updated every two years.
- conduct regular assessments to establish the need to keep certain Personal Data.
- Staff should take every opportunity to ensure date is updated. For instance, by confirming a customer's details when they call.

## 6. Adequate, relevant, and not excessive in relation to the purpose(s) for which the data were collected and processed.

Cruatech Ltd will ensure that the data it processes in relation to Data Subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

## 7. Not be kept for longer than is necessary to satisfy the specified purpose(s).

- Cruatech Ltd has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format.
- Once the designated retention period has elapsed, Cruatech Ltd undertakes to destroy, erase, or otherwise put this data beyond use.

## 8. Be managed and stored in such a manner that, in the event a data subject submits a valid subject access request seeking a copy of their personal data, this data can be readily retrieved and provided to them.

- This process is covered under Subject Access Requests

## Lodging, Processing & Storing Data Subject Access Requests

Cruatech Ltd has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

As part of the day-to-day operation of the organisation, Cruatech Ltd in active and regular exchanges of information with Data Subjects. Where a formal request is submitted by a Data Subject in relation to the data held by Cruatech Ltd, such a request gives rise to access rights in favour of the Data Subject.

Cruatech Ltd must acknowledge the Data Subject Access Request within 30 days and depending on the nature and extent of the request they can provide the information that is requested.

If you would like to lodge a Subject Access Request, please email info@cruatech.com and you request will be acknowledged within 7 days. The office manager will always verify the identity of anyone making a subject access request before handing over any information.

## Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

## Data

- This includes both automated and manual data.
- Automated data means data held on computer or stored with the intention that it is processed on computer.
- Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.

## Personal Data

- Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller. (If in doubt, Cruatech Ltd refers to the definition issued by the Article 29 Working Party and updated from time to time.)

## Sensitive Personal Data

- A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.

## Data Controller

- A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.

## Data Subject

- A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.

## Data Processor

- A person or entity who processes Personal Data on behalf of a Data Controller based on a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.

## Data Protection Officer

- A person appointed by Cruatech Ltd to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients

## Relevant Filing System

- Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

## Key details

- Policy prepared by:
- Approved by board / management on:(if applicable)
- Policy became operational on:
- Next review date:
- Policy Updated